почему оси ненадежны — тенденции развития хакерских атак

крис касперски, но-email

эта статья возникла в результате бесед с Самуелем Джебамаи (Samuel Jebamani) — ведущим разработчиком антивирусной компании K7 Computing (малоизвестной в России, но захватившей четверть японского рынка). обсуждая тенденции развития операционных систем и анализируя источники возможных угроз, мы пришли к любопытным, хотя и противоречивым выводам, которые наверняка будут интересны широкой аудитории читателей, бизнес которых так или иначе связан с компьютерной безопасностью.

введение

Листая компьютерные журналы и просматривая периодику, складывается устойчивое впечатление, что ситуацию с безопасностью иначе как критической не назовешь. Сеть буквально кишит злобными хакерами, вездесущими вирусами (которых не берут антивирусы), мутирующими червями, проходящими сквозь межсетевые экраны словно нож через масло. Критические дыры в программном обеспечении обнаруживаются каждый день, а заплатки отсутствуют месяцами… Без оборонительных комплексов (приобретаемых за отдельные деньги) и высококвалифицированных специалистов, лучше сразу сворачивать свой бизнес и ложиться на рельсы, в ожидании поезда, которые все равно не придет, т. к. хакеры подломали центральный компьютер управления железнодорожными сообщениями и не сегодня завтра захватят спутники, атомные электростанции и мир (как виртуальный, так и физический) рухнет в один момент.

Рисунок 1 балансируя на грани пропасти

Ну, пресса вообще склонна все преувеличивать. Типичная ситуация: по TV передают о жутком землетрясении, разрушившим чуть ли не половину Таиланда вместе с примыкающими к нему странами. Взволнованный, звоню своим приятелям. — О да! — смеются они — землетрясение было столь крупным, что совсем незаметным и если бы не ваше (в смысле российское) TV, они бы (Тайцы) о нем так бы и не узнали.

Прогнозы, предвещающие "конец Интернета", появляются все чаще и чаще, причем их распространяют не только журналисты, падкие на сенсации, но и вполне респектабельные руководители антивирусных компаний. Это просто маркетинговая политика у них такая. Надо же как-то продавать свой товар…

С другой стороны, найти пользователя, никогда не сталкивающего с вирусами, довольно проблематично, особенно если мы говорим о Windows-подобных системах, количество вирусов под которые возросло настолько, что уже не поддается никакому учету и контролю. Новые штаммы появляются с такой скоростью, что сотрудники антивирусных компаний просто физически не успевают их анализировать, что неизбежно влечет за собой лавинообразный рост ложных срабатываний — антивирусы пропускают вирусы или ругаются на честные программы, нервируя пользователей и ломая бизнес ее разработчикам.

"Вопреки усилиям врачей пациент жив и умирать не собирается" — примерно тоже самое можно сказать и о безопасности операционных систем. Глобальные эпидемии действительно случаются, но носят единичный характер и хотя аналитические центры рапортуют о миллиардных убытках, особого доверия эти цифры не внушают. Бизнес вообще основан на рисках и стабильное процветание - недостижимый идеал.

Очень трудно говорить о безопасности, оставаясь полностью беспристрастным. Тут у каждого эксперта свое мнение, подкрепленное мощной доказательной базой с кучей цифр и графиков. Вот только никакой корреляции тут не наблюдается и если одни фирмы утверждают, что потрясения, случившиеся на стыке XX и XXI веков больше не повторятся — основные дыры уже заткнуты и хакерские атаки теперь носят лишь потенциальный характер (косвенно подтверждаемый отсутствием масштабных эпидемий за последние несколько лет), другие же — демонстрируют примеры боевого кода, с легкостью пробивающего новомодные защитные механизмы и от очередной эпидемии нас удерживает лишь отсутствие злобных хакеров, сочетающих агрессивность с профессионализмом в нужных пропорциях.

То есть, глобальные эпидемии более не вспыхивают отнюдь не потому, что в "Багдаде все спокойно", а просто никто из хакеров не заинтересовался очередной обнаруженной дырой настолько, чтобы бросить все текущие дела и засесть за написания вируса, рискуя своей свободой, карьерой… Спецслужбы всех стран активно борются с компьютерными вандалами и прецеденты тюремных заключений (не говоря уже об астрономических штрафов) уже имеются, что служит своеобразным сдерживающим фактором, намного сильнее отпугивающих хакеров от вирусов, чем широко разрекламированные, но в действительности легко вскрываемые защитные механизмы. Или все-таки нет?!

Словом, тут есть о чем поговорить. Статья носит ярко выраженный спорно-провокационный характер, но она и задумывалась такой!

XXI век — расцвет средневековья?

Прежде, чем рассуждать куда катится мир и что нас ждет, необходимо ответить на один простой вопрос: действительно ли операционные системы небезопасны или все мы стали жертвой массированной пропаганды? В средние века верили в ведьм и не просто верили, но и писали многочисленные трактаты (подтвержденные, естественно, богатым фактическим материалом). В конце XX века все верили в НЛО и барабашек. Правда, как только фотоаппараты с автоматической фокусировкой получили массовое распространение и стало очень трудно получить смазанный кадр, охотники на НЛО свернули свои "исследования" и постепенно страсти улеглись.

Рисунок 2 мир средневековья

Теперь мы можем с уверенностью сказать, что оборотней не существует, а если бы внеземные цивилизации существовали, то их космические корабли давно бы бороздили наше космическое пространство (см. поиск по Гуглу "Парадокс молчания Шкловского"). Поразительно, что даже теперь, после серии убийственных разоблачений, находятся люди, верующие во всю эту чушь.

С (не)безопасностью наблюдается приблизительно та же самая картина. Что-то вроде массового помрачения сознания на почве страха перед неизвестным. Мало кто из пользователей (и даже администраторов) отчетливо представляет себе как _реально_ функционируют черви и вирусы, и еще меньше количество народу дизассемблировало их код, досконально разобравшись в алгоритмах вторжения и многочисленных ограничениях, налагаемых "окружающей средой". Написать жизнеспособного вируса очень трудно и потому большинство вирусов представляют собой всего лишь запись в антивирусной базе.

Интернет это не среда обитания малвари — это _кладбище_ червей, вирусов и прочей заразы, зачастую гибнущей еще на начальной фазе размножения. Это кладбище идей и алгоритмов, не работающих в новом окружении (новые версии операционных систем, новые схемы распространения программного обеспечения).

Рисунок 3 кладбище малвари

Наконец, мир не ограничивается одной лишь продукцией компании Microsoft. На главной странице официального сервера разработчиков операционной системы OpenBSD красуется надпись "две критические удаленные дыры более чем за десять лет промышленной эксплуатации". Сравните это с _сотнями_ критических дыр NT-подобных систем и сделайте соответствующие оргвыводы. И хотя считается, что xBSD пригодна только для серверного рынка, а на рабочих станциях без Microsoft не обойтись, это откровенная вражеская пропаганда.

Рисунок 4 OpenBSD – одна из самых безопасных операционных систем

Apple Mac OS X основана на BSD, поверх которой "натянут" красивый, удобный, хорошо продуманный и интуитивно-понятный пользовательский интерфейс, намного более дружелюбный к пользователю, чем Windows. К тому же все крупные программные пакеты (такие как Microsoft Office, Adobe Photoshop) портированы под Mac, успешно работающий в бизнес сфере, пускай и удерживающий существенно меньший процент рынка, чем Microsoft, агрессивность маркетинговой политики которой всем хорошо известна и которая прилагает все усилия, чтобы показать, что не безопасность компьютерных систем — явление повсеместное и что у конкурентов дела обстоят ничуть не лучше, а даже хуже.

Рисунок 5 мир Apple

Очередная ложь!!! Как известно, подавляющее большинство червей распространяются через вложения электронной почты – прилепляя к письму исполняемый файл. В 9x и NT-подобных системах право на чтение файла равносильно праву на его запуск и потому даже пользователь с максимально ограниченными правами может запускать вновь создаваемые файлы, что, очевидно, является _гигантской_ дырой в подсистеме безопасности.

В UNIX-подобных системах исповедуются другой подход. Тип файла определяется не по расширению (которое может быть любым), а по атрибуту, причем, рядовые пользователи могут только запускать файлы, но присвоить вновь созданному файлу атрибут исполняемого — таких прав у них просто нет!!! И хотя эта система содержит ряд дефектов (например, можно передать файл ассоциированному с ним языку программирования), атаки почтовых клиентов под UNIX носят чисто лабораторный характер, не находящий широкого практического применения.

свобода в обмен на безопасность

"Те, кто готов поступиться свободой во имя безопасности, не заслуживают ни свободы, ни безопасности" — сказал Бенджамин Франклин (американский политический деятель 18-века, один из отцов основателей США). Microsoft, похоже, придерживается диаметрально противоположного мнения, явно и неявно давая нам понять, что свобода и безопасность — вещи взаимоисключающие.

По какому пути идет развитие Windows? Пользователям предоставляется все меньше и меньше свободы, даже администратор уже не бог, а мальчик на побегушках. В x86-64 редакциях NT-подобных систем он даже не может загрузить драйвер, без соответствующий цифровой подписи!!! Microsoft планомерно лишает его рычагов управления системой, грубо говоря, превращая Windows в реактивный истребитель с автопилотом, с минимальными функциями ручного управления, что вплотную приближает администратора к простым пользователям.

Рисунок 6 мир Microsoft

Возникает резонный вопрос: а зачем же тогда нужен администратор, если система считает, что может позаботиться о себе и сама. Ответ: а он и не нужен. Ну разве, что тонер в принтере поменять. Microsoft упорно пытается построить мир, в котором человеческий разум заменен машинным и должность администратора упразднена до фиктивной. С точки зрения бизнес-пользователей это действительно очень завлекательная схема. Сколько бы ни стоила лицензия на Windows, зарплата квалифицированного администратора — это намного более существенная статья расходов, особенно если в организации больше сотни компьютеров и, соответственно, один администратор с ними ни за что не справится.

Никто не спорит, что компьютер как раз и создавался для того, чтобы заменить человека в некоторых областях, но область искусственного интеллекта в этот список не входит в силу технической невозможности реализации "думающей" машины. К тому же, любая автоматическая система намного сложнее ручной, а чем система сложнее, тем выше вероятность, что она откажет.

Задумаемся, почему американцы смогли успешно слетать на Луну еще в до компьютерную эпоху и запустили кучу автоматических межпланетных станций, а в последние годы космическую отрасль постигла череда сплошных неудач. Космические роботы в лучшем случае выполняют 10%-15% от поставленной задачи, а чаще отказывают еще до передачи первых снимков.

Парадокс? Плохая карма или цепь досадных случайностей? Вовсе нет. Разработчики забыли о главном принципе всех машин и механизмов: simplicity, в узких кругах известный как KISS-принцип (Keep It Simple Stupid/Silly – Делай Это Проще, Дурачок). Космические аппараты первых поколений были простыми до безобразия, они держались буквально на честном слове, но… успешно летали! Что же касается покорения Луны, то в ходе операции "Аполлон" постоянно возникало огромное количество проблем, большинство из которых космонавты решали, не задумываясь и даже не считая это проблемой. А вот если марсианский зонд не может съехать с посадочного модуля или "забыл" развернуть солнечную батарею в нужном направлении для подзарядки батарей — это конец.

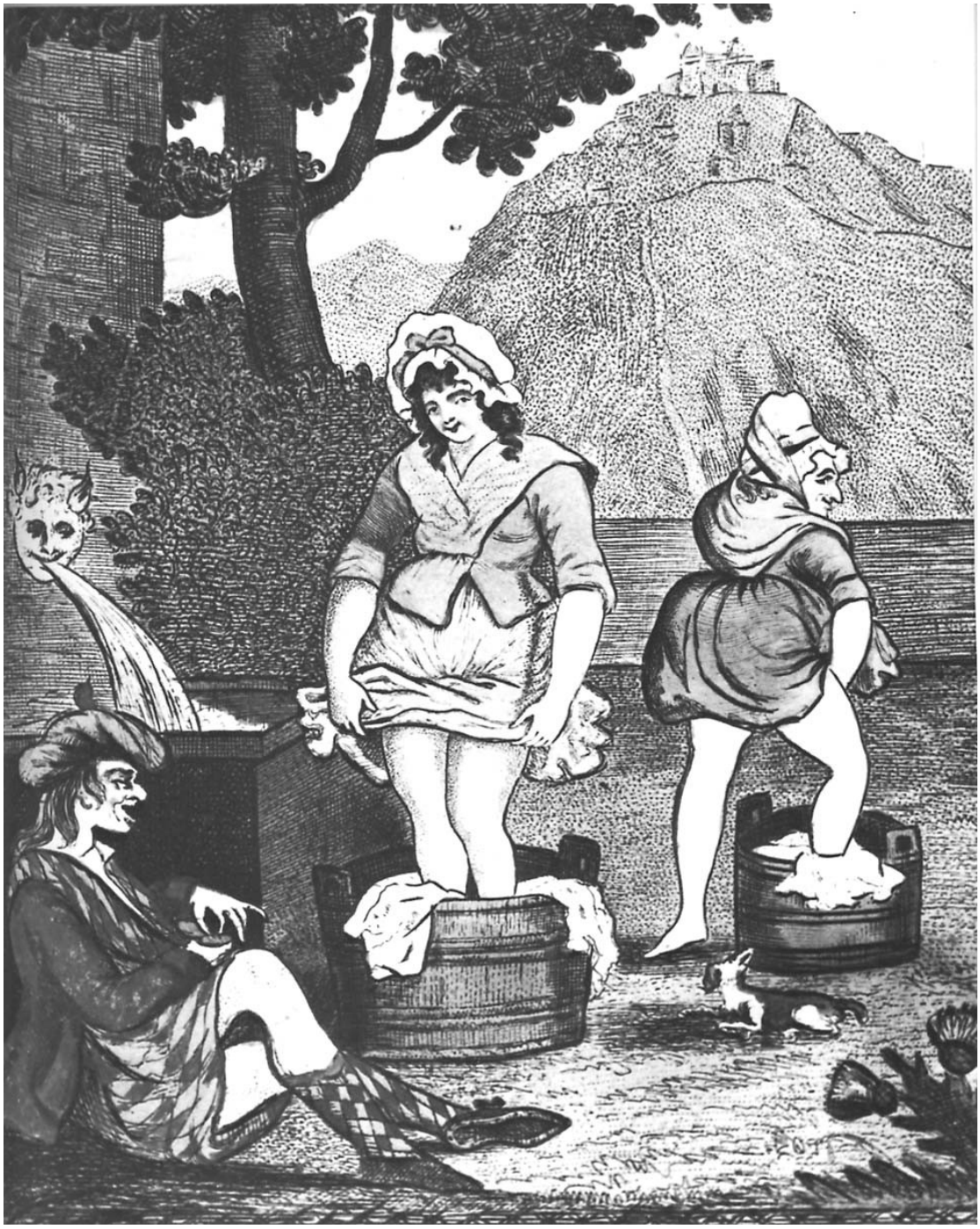

Рисунок 7 положительная карма ручной работы

Но оставим космос и вернемся к операционным системам. UNIX содержит совсем немного (чуть больше сотни) системных вызовов (из которых активно используется лишь пара десятков) и эти вызовы принимают считанное количество параметров, а потому UNIX-программисты могут удержать все необходимые им знания в голове. Windows – насчитывает десятки тысяч (!) API-функций, принимающих десятки параметров, вынуждая программистов постоянно держать справочник под рукой. Никто не в состоянии удержать в голове все (или хотя бы основные) API-функции Windows, не говоря уже об особенностях их поведения. Отсюда — ошибки проектирования, дефекты систем безопасности и прочие неприятные вещи.

К сожалению, Linux/BSD перенимает худшие черты Windows, двигаясь тем же порочным путем. Программисты работают над созданием всевозможных "мастеров", систем автоматического распознания и подключения новых устройств и т.д., короче говоря пытаются научить систему то, что с легкостью делает любой администратор, превращая компьютер в подобие тостера с парой кнопок. Все остальное хозяйство скрыто под капотом. Никаких

рычагов управления. Никто, даже администратор не может толком сказать, что сейчас происходит в системе, потому что система заботится о себе сама.

Настоящий рай для вирусов и червей. Доверие это прекрасно, но только не тогда, когда речь идет о доверии к автоматике. Машинный "интеллект" (ну или его имитация) мыслит шаблонно, он не способен к "подозрительности", лишен "интуиции", а потому обмануть его проще просто. Взять хотя бы эвристические механизмы, в создание которых вкладываются огромные усилия и деньги. Проводятся серьезные научные исследования… вот только вся эта эвристика элементарно обходится даже начинающими хакерами и реально она вылавливает только "пионерские" вирусы. Какой огромное достижение!!!

Или вот персональные брандмауэры. Вещь вроде бы хорошая, но… в попытке "подружить" их с пользователями разработчики превзошли все границы здравого смысла. Сообщения в стиле: "угроза! уровень опасности — низкий. событие: изменение контрольной суммы исполняемого файла. рекомендации: рекомендуется разрешить данное действие". Вы что-нибудь поняли?! Лично я (квалифицированный программист) — только ушами повел. А как должна поступать, например, моя пассия? Неудивительно, что рядовые пользователи на _все_ запросы антивируса/брандмауэра автоматически отвечают "yes", даже не читая, что там написано — все равно это не поможет разобраться в ситуации.

Интересно — какого ответа ожидает брандмауэр на такой вопрос? Быть может, программа изменилась потому, что скачала из сети обновление или в нее внедрился вирус? Для принятия решения, необходимо дополнительная информация, а если ее нет, остается отвечать наугад независимо от своей квалификации. Разработчики защитных систем считают, что выхода нет, но они заблуждаются и не хотят смотреть по сторонам.

Лучше бы они брали пример с производителей фотокамер, традиционно имеющих три режима: полный автомат, при котором камера принимает все решения самостоятельно, не обращаясь за помощью к фотографу, поскольку те, кто пользуются таким режимом навряд ли смогут ответить что-то вразумительное. Так зачем их отвлекать раздражающими вопросами? Методом тыка автоматика может решить все проблемы и сама. В результате мы получаем кошмарные снимки, на которые без содрогания смотреть невозможно, но… каков фотограф, таков и снимок.

Полуавтоматический режим предполагает, что владелец камеры уже прочитал несколько книжек и способен помочь автоматике избежать грубых просчетов и ошибок, а потому ему предоставляется определенная творческая свобода и рычаги для управления. Камера работает так же как в полностью автоматическом режиме, но теперь конечное решение остается не за автоматикой, а за фотографом.

Ручной режим предназначен для тех, кто в совершенстве овладел аппаратом и четко знает чего он хочет. Все решения принимает фотограф. Автоматика может лишь неназойливо указывать ему, что экспозиция (например) нереально завышена, но откуда же автоматике знать _почему_ она завышена? Может это творческий замысел такой, чтобы получить портрет в стиле голливудского high key, а вовсе не пьяный фотограф. В автоматическом режиме такого эффекта добиться практически нереально, в полуавтоматическом приходится не по детски извращаться, а вот в ручном — пожалуйста, делай, что хочешь.

Вот было здорово, если бы защитные механизмы имели аналогичные уровни автоматизма. "Зеленый квадрат" (на жаргоне фотографов — полный автомат) возлагает ответственность за принятие всех решений на брандмауэр/антивирус, что дает весьма посредственный эффект, но если за штурвалом сидит пользователь типа "секретарша", то по другому все равно не получится.

Полуавтомат — предоставляет пользователю максимум информации о ситуации, предлагает оптимальное (с точки зрения автомата) решение, но при этом позволяет вмешиваться в процесс, корректируя решения автомата. Большинство современных защитных систем как раз и работают в режиме полуавтомата, смысла в котором нет. Если пользователь недостаточно квалифицирован, чтобы вмешиваться в работу автомата, пускай включает "зеленый квадрат", а если же он продвинутый гуру — то советы автоматики его будут ужасно раздражать.

Ручной режим (на данный момент не реализованный ни в одном защитном комплексе) предполагает, что ситуацией рулит пользователь, а защита просто предоставляет ему необходимые рычаги управления. Фактически, отладчики уровня ядра (Soft-Ice, Syser) и есть защитные комплексы ручного типа, но, к сожалению, они не предназначены для непосредственного распознавания атак и потому их приходится использовать в паре с полуавтоматическими защитами.

Самое главное, что необходимо понять — автоматика это всего лишь красивая игрушка. Компьютер — это не тостер. И даже не фотоаппарат. А потому, пользователи

должны обучаться работать с ним не только посредством мыши и не впадать в ступор от слов типа "порт", "протокол", etc.

Даже если превратить компьютер в приставку типа "Денди" с заранее предустановленными программами и заблокировать возможность установки новых программ на уровне операционной системы или даже (о боже!) процессора, то от дыр в сетевых приложениях (браузерах, почтовых клиентах) все равно никуда не деться и атаки по-прежнему останутся возможными.

матрешка в матрешке

Мысленно перенесемся в средневековое царство MS-DOS и процессоров типа 8086. Разделение команд на "обычные" и "привилегированные" отсутствует и машинный код, получивший управление, может делать абсолютно все, что ему вздумается, например, удалять файлы с атрибутом "только на чтение", блокировать работу антивирусов (и чтобы удалить такие вирусы приходилось загружаться со специальной "стерильной" дискеты).

В 80286 появляются первые защитные механизмы, доведенные до логического конца в 80386 и Windows 95, наконец-то, разделяет адресные пространства процессов так, чтобы одна программа не могла обращаться к памяти другой программы, если та этого не хочет. А в Windows NT появляется и разделение привилегий на уровне пользователей, что открывает ошеломляющие перспективы, позволяя создавать безопасные многопользовательские системы, где непривилегированные пользователи уже не могут навредить ни системе, ни другим пользователям. Тоже самое относится и к программам, запущенным от их имени. Фантастика да и только!

Все мы прекрасно знаем, что как ни крути рычаги управления XP, и как ни ограничивай пользователя в правах, навредить он все равно сможет. Было бы желание… а за его реализацией дело не станет. А вот куча программ с урезанными правами просто не запускаются. И не потому, что они спроектированы неправильно (как укоряет их Microsoft), по другому просто никак не получается. Допустим, у нас есть программы прожига лазерных дисков. Запись на лазерный диск вполне рядовая операция, и требовать наличия прав администратора для ее осуществления — глупо. Но… все штатные механизмы, встроенные в NT-подобные системы, предназначенные для работы с оптическими накопителями, только под администратором и работают. А драйвера сторонних производителей, во-первых, требуют администраторских прав для совей установки (которая, впрочем, может осуществляться всего один раз, что не есть проблема), но… чем больше у нас "левых" драйверов, тем выше риск, что один из них пробьет тоннель сквозь барьер системы безопасности. Конкретный пример: ASPI32-драйвера от компании Adaptec (использующиеся многим пишущим ПО) страдают хронической мигренью и при определенных обстоятельствах предоставляют непривилегированным пользователям низкоуровневый доступ к жесткому диску, позволяя делать с ним все, что угодно: читать данные других пользователей, обнулять все сектора от A до Z и даже заливать "мусорный" микрокод, приводящий к выходу жесткого диска из строя.

Теоретически (подчеркивают, теоретически) в правильно спроектированной операционной системе, работающей под управлением x86-процессоров 80386 или выше, можно безбоязненно запускать программы из-под ограниченного пользователя. И они _ничего_ плохого не смогут сделать. А если программе не хватает ограниченных прав, то это наводит на серьезные размышления — может быть, ну ее, такую программу?! В UNIX-системах все обстоит именно так, ну или практически так, а вот в Windows…

Пользователи Windows вынуждены постоянно держать под рукой виртуальную машину (типа VM Ware), проверяя программы на вшивость. Дело ведь не только в вирусах. "Честно", но некорректно написанная программа может "уронить" систему так, что потребуется ее полная переустановка.

Поразительно, но именно такое решение и предлагается в качестве основной защиты! Производители процессоров даже встроили поддержку аппаратной виртуализации, чтобы сократить накладные расходы на эмуляцию и это при том, что практически все виртуальные машины содержат дыры, позволяющие вирусам вырваться за их пределы… и с ростом популярности виртуальных машин вероятность появления таких вирусов все больше и больше. Это на данный момент их нет, но что будет завтра? Еще один уровень виртуализации? Еще одна матрешка внутри другой?

Помилуйте, господа!!! Все, что нужно для защиты, содержится в 80386 процессоре. Остается только спроектировать правильную операционную систему и ведь для этого даже думать головой особо не надо — достаточно воспользоваться готовыми решениями,

разработанными много лет назад еще в эпоху майнфреймов. Если бы каждый пользователь майнфрейма мог завалить всю систему… Ох, не будем о плохом. Тогда умели считать стоимость машинного времени и проектировали реально надежные системы.

если бы Microsoft строила автомобили…

Говорят (врут, конечно), что на выставке компьютерной техники COMEX Билл Гейтс сравнил компьютерную индустрию с автомобильной и заявил: "*Если бы General Motors развивали технологии так, как компьютерная индустрия, мы бы ездили на автомобилях за $25, расходуя галлон бензина на 1000 миль*".

"*Да, но вас устроило бы, чтобы ваш автомобиль портился дважды в день?" — ответил представитель GM. Помимо этого: при любом изменении дорожной разметки вам пришлось бы покупать новый автомобиль; при выполнении обычного маневра ваш автомобиль мог бы заглохнуть, и вам приходилось бы перезапустить двигатель; чтобы перевозить несколько человек одновременно, вам потребовался бы "Автомобиль 95" или "Автомобиль NT"; Macintosh выпускал бы автомобили на солнечных батареях, которые были бы проще в управлении, но могли бы ездить лишь по 5% дорог; владельцам Macintosh пришлось бы покупать дорогостоящий Microsoft Upgrade, после чего их машины ездили бы медленнее; сигнальные датчики топлива, масла и охлаждения были бы заменены единым датчиком "general car fault";. новые сиденья вынудили бы всех подогнать задницы под один размер; воздушная предохранительная подушка перед срабатыванием спрашивала бы: "Are you sure?*".

Рисунок 8 ослы, конечно, животные упрямые, зато они не ломаются как машины

Конечно, это анекдот, но аналогия между автомобилем и операционной системой вполне уместна, однако, если автомобильная индустрия насчитывает без малого две сотни лет, то операционные системы появились сравнительно недавно. С другой стороны, стадию взрывного роста они уже давно миновали. Концептуально новые идеи закончились уже во восьмидесятых и теперь наблюдаются лишь вариации на старые темы.

Фундаментальным отличаем автомобилей от операционных систем является "reuse"-концепция, заключающая в повторном использовании уже готовых и апробированных решений. Новый автомобиль всегда строится на базе старого, но не в буквальном, а переносном смысле. Все узлы и агрегаты проектируются и отливаются заново, даже такая мелочь как болты М12.

А вот операционные системы представляют собой сплошное нагромождение кода. Некоторые файлы исходных текстов, входящих в состав Server 2008 датированы… 1988 годом. Операционная система представляет собой довольно шаткое сооружение, состоящее из многочисленных наслоений, очень похожее на автомобиль, построенный на базе парового дилижанса и сохранивший значительную часть узлов последнего.

Программисты только в исключительных случаях переписывают код с нуля. Обычная практика — добавление новых слоев абстракции поверх старых. Сложность сооружения при этом неуклонно увеличивается, количество связей между узлами экспоненциально возрастает, а

самое неприятное в том, что узлы, спроектированные десятилетия назад, теперь оказываются совершенно в иных условиях, к которым они чисто физически не готовы.

Если кто-то верит, что Linux (в противовес Windows) была написана с нуля, то он жестоко ошибается. Linux основана на учебной операционной системе Minix, и в процессе своего развития не брезговала передирать куски кода из BSD-систем, которые сами по себе представляют нехилое скопление осадочных слоев… По исходным текстам Linux'a можно проследить не только историю развития языка Си (на котором написано его ядро), но и всей компьютерной индустрии в целом.

Рисунок 9 хронология осадочных слоев машинного кода

В этом и состоит фундаментальная проблема программирования, отличающего его от прочих инженерных дисциплин и путей выхода из ситуации не нашел еще никто. Только постоянное "вылизывание" старого кода способно остановить растущую лавину наслоений. Взять хотя бы две близкие по духу операционные системы: Free- и OpenBSD. Первая развивая намного активнее второй, но и дефектов в ней… скажем там, намного больше, чем в OpenBSD. А Microsoft, ставящая телегу впереди лошадей, вообще представляет собой скопление ошибок проектирование, количество которых от версии к версии только увеличивается.

заключение

Никто не знает какое будущее нас ждет и как измениться мир даже через несколько лет. Windows взрывообразно увеличивается в размерах (достаточно сравнить размер дистрибутивов), код теряет управляемость и начинает жить своей собственной жизнью. Microsoft, похоже, осознает проблему, но все предпринятые ею шаги (например, .NET) только усугубляют ситуацию. Почему? Давайте отбросим всю рекламную шелуху и посмотрим правде в глаза. Платформа .NET получила статус международного стандарта в 2001 году (см. ECMA-335) и сейчас готовится отпраздновать свой юбилей — для компьютерной индустрии это огромный срок! Нам обещали управляемый (managed) код, безопасное программирование, интеграцию различных языков… Microsoft вложила в продвижение .NET огромные деньги, но… так не смогла их окупить. Низкое быстродействие, сложность сопряжения .NET программ с внешней средой и друг с другом (чтобы из C# программы вызывать код, написанный на Си++, скомпилированный в .NET сборку "родным" MS-компилятором, приходится устраивать "танцы" с бубном, получая смесь управляемого и неуправляемого кода, сводящую на нет все заявленные преимущества .NET).

Известно, что первую версию Vista компания Microsoft пыталась реализовать на .NET (пре-альфа дистрибутивы которой рассылались бета-тестерами), однако, затем осознала, что добиться приемлемой производительности и надежности не получится. Похоронив миллионы строк уже написанного кода, Microsoft взяла за основу ядро от Server 2003, впоследствии доработанное до Server 2008 и — что самое поразительное — в минимальном комплекте поставки (режим Core) Server 2008 вообще не устанавливает .NET, при этом обеспечивая базовый функционал.

Возникает резонный вопрос — если сама Microsoft не может соорудить на базе .NET нормальное программное обеспечение, чего же она ожидает от всех нас? Конечно, обладая практически безграничными финансовыми возможностями, она сможет продлить агонию .NET еще на несколько лет, но революция в области программирования, увы, не свершилась. Программы не стали более надежными и безопасными.

Тем не менее, эксперименты, проводимые компаний Microsoft в области программного обеспечения можно только приветствовать. Это же замечательно, что кто-то в состоянии вложить пару миллиардов долларов в новую технологию, чтобы посмотреть пойдет она или не пойдет (рынок все равно всех расставит по своим местам и никакой маркетинг не позволит продвинуть мертворожденное дитя, что пример с .NET и подтверждает).

Если сравнить Windows с горной рекой, то BSD течет по равнине. Медленно, спокойно и величаво. Никаких революционных инноваций в ней не появится, вместо того, чтобы искусственно создавать у пользователей новые потребности, разработчики BSD-систем предпочитают "оттачивать" уже написанный код, исправлять обнаруженные ошибки проектирования, устанавливать новые распорки.

Linux… ну Linux это всегда неожиданность. Стремясь потеснить Microsoft и завоевать симпатии простых пользователей, некоторые составители дистрибутивов перешли на полностью графический интерфейс, нашпигованный кучей мастеров — уродливое сооружение. Продвинутые пользователи от этой графики только плюются им подавай привычную командную строку, а еще лучше сразу BSD, которая специально для профессионалов и предназначена без всяких скидок на "ламеризм". А вот до "нормальных" пользователей Linux еще недостаточно "отупел" и в Windows они чувствуют себя гораздо комфортнее, да и привычнее.

В общем, Linux либо вернется к истокам, либо превратится в монстра еще похуже, чем Windows. А, быть может и нет…

Рисунок 10 мрак близкого и далекого будущего: чем дальше — тем мрачнее

интервью с экспертом
Samuel Jebamani
core team leader фирмы K7 Computing

Рисунок 11 Samuel Jebamani

Рисунок 12 Samuel Jebamani

KK: представитесь пожалуйста.

SJ: меня зовут Samuel Jebamani, я руковожу сплоченной командой программистов, работающих над интегрированным защитным комплексом, включающим себя антивирус, брандмауэр, спам-фильтр и некоторые другие компоненты. Главным образом наша продукция ориентирована на японский рынок, однако, имеется и англоязычная версия нашего продукта, демонстрационную версию которого можно скачать с http://k7computing.com/k7_av.asp;

KK: считаете ли Вы, что антивирусный рынок это большой мыльный пузырь, держащийся на страхе пользователь и готовый лопнуть в любой момент;

SJ: наша многолетня история, ведущая еще с 1992 года, позволяет оценить ситуацию, что называется в ретроспективе. В эпоху MS-DOS вирусные эпидемии бушевали по трем основным причинам: а) децентрализованной модели распространения программного обеспечения (попросту говоря, пользователи копировали программы друг у друга); б) беззащитностью операционной системы и невозможностью создать защиту на базе процессоров тех времен; в) невозможности оперативной рассылки обновленных

антивирусных баз, в результате чего, выражаясь образным языком, брошенный окурок, вызывал пожар планетарных масштабов — вирусы пересекали континенты и океаны…

KK: а сейчас?!

SJ: а вот сейчас ситуация радикальным образом изменилась и прежние каналы распространения вирусов перестали работать. да, люди по прежнему качают варез из файлообменных сетей, но наличие антивирусов позволяет пресечь болезнь еще _до_ заражения (этим, главным образом, занимаются проактивные технологии). с другой стороны, вирусы получили новые каналы распространения —Интернет. И если раньше было можно жить и без антивируса, не устанавливая никакого программного обеспечения, кроме того, что куплено легальным путем, то теперь любой узел, подключенный к Сети является потенциальной жертвой;

KK: согласен, операционные системы и программное обеспечение содержат многочисленные дыры и потому заразиться можно даже не выполняя никаких действий вообще. но! разработчики операционных систем активно борются с дырами, многие почтовые службы отказываются пересылать исполняемые файлы (даже если они и не являются вирусами). что будете делать вы, когда все дыры в осях будут заткнуты и вирусы потеряют свой основной канал распространения?

SJ: при всем моем нежелании выступать в роли пророка, раз уж мне задан такой прямой (и, кстати говоря, несколько бестактный вопрос) все-таки скажу, что дыры в операционных системах — это навсегда. я не люблю аналогий, но давайте возьмем механический сейфы, совершенствующиеся в течении многих тысячелетий (!). что нам мешает создать сейф, который нельзя взломать? банк, который нельзя ограбить?

KK: неизбежные дефекты проектирования, пресловутый человеческий фактор…

SJ: именно!!! технологии нападения совершенствуются параллельно с технологиями защиты, иногда, на какое-то время, одна сторона обгоняет другую вперед и тогда наступает либо смутное время, либо хрупкое состояние, именуемое "миром";

KK: многие считают, что антивирус должен стать неотъемлемой частью операционной системы, Вы не боитесь, что Microsoft реализует нечто подобное и тогда всем остальным компаниям придет конец?

SJ: Bill always win, да? Но Microsoft уже имеет свой антивирус и имеет она его еще со времен MS-DOS. Ну и что? Это кого-то беспокоит? Слухи о могуществе Microsoft и о том, что она может с легкостью расправиться с любым из конкурентов чудовищно преувеличены, все ссылаются на пример IE vs Netscape, почему-то забывая, что Netscape, возродившийся в виде Fire-Fox, не только не был раздавлен и растоптан, но еще и наступает IE на пятки. Другие примеры расправы с конкурентами у Вас есть?

KK: гм, примеров у меня, пожалуй нет (хотя это не значит, что их нет вообще — ключевое слово у меня). Словом, Вы не видите никакой угрозы со стороны Microsoft?

SJ: нет, не вижу. Во-первых, мы ориентированы на тот рынок, на котором позиция Microsoft никогда не была сильна, а, во-вторых, почитав блоги их сотрудников, вы обнаружите, что они считают за достижение ручную распаковку файла, упакованного каким-нибудь простеньким протектором. конечно, это не самые сильные разработчики. в Microsoft очень много умных людей, но… все они уже задействованы на других участках "фронта". видите ли, разработка антивирусов не самый доходный бизнес и даже если Microsoft захочет прибрать его к рукам, при ее организации труда он станет вообще убыточным.

KK: но все-таки антивирус (под называние Microsoft Bit Defender) появился, так?

SJ: а вы смотрели кого он ловит? вирусов? так ведь нет. на самом деле Bit Defender понадобился Microsoft для возможности блокирования драйверов, подписанных украденными сертификатами или выданных фирмам, занимающимся разработкой вредоносных программ. получение цифрового сертификата для подписи драйверов — чисто формальная процедура, ни от чего не спасающая. Microsoft осознала тактическую ошибку и тут же вставила в операционную систему "костыль", чтобы выиграть время на разработку нового защитного механизма, впрочем, это только мое личное мнение, которое может не совпадать с официальной позицией Microsoft, но низкое качество Bit Defender'a это факт, не требующий доказательств;

KK: последний вопрос. ваш прогноз относительно (не)безопасности Висты и Server 2008?

SJ: судя по всему нас ждут очень интересные времена. наша исследовательская лаборатория обнаружила огромное количество дыр в обоих, причем, исправить эти дыры одним движением руки у Microsoft не получится, поскольку они зарыты очень

глубоко. Тут требуется серьезный редизайн ядра. Так что несколько последующих версий Windows обещают быть весьма плодотворным компостом для хакеров и вирусописателей и количество дыр по моим прогнозам никак не снизится, а только возрастет и этот рост мы можем наблюдать уже сегодня, но лучше не пытаться заглянуть в будущее (которое всегда переменчиво), а решать текущие проблемы. У Microsoft слишком много операционных систем, особенно в 64-битной линейке и все они требуют индивидуального подхода, поскольку не обеспечивают даже номинального уровня совместимости, особенно на ядерном уровне, без доступа к которому разработка качественных защитных механизмов немыслима и где, кстати говоря, гнездиться очень много критических дыр.

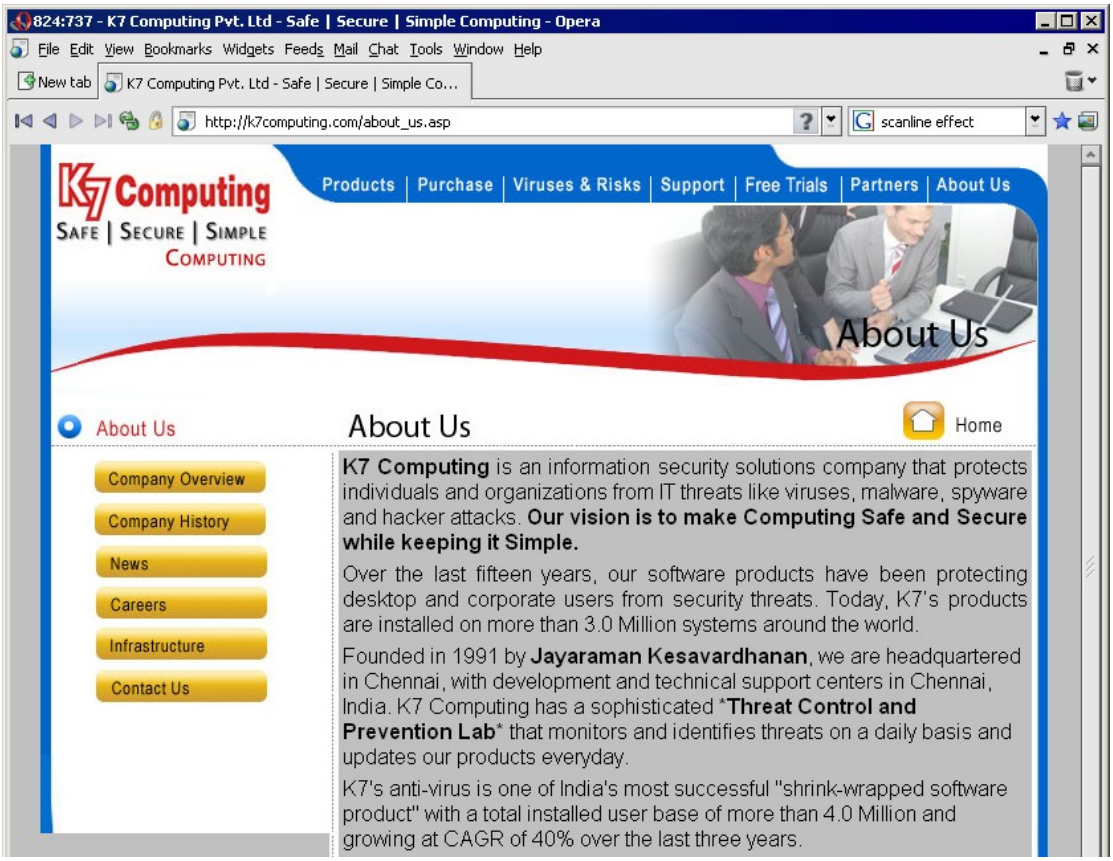

Рисунок 13 K7 Computing – фирма, специализирующаяся на безопасности