



Простой мысленный эксперимент: кладем в карман любимую 4-гигабайтную «флешку», садимся в машину времени и переносимся всего лишь на 20 лет назад. Выходим из машины и демонстрируем землянам (а за это время едва сменилось одно человеческое поколение) сие чудо-устройство по цене ужина в ресторане. Нас примут или за мошенника, или за инопланетянина.

Сергей Баричев/
bar@computerra.ru/
Евгений Крысанов/
ekrysanov@yandex.ru/

Защита информации в эпоху «информационной сверхпроводимости»

Мы давно не замечаем, насколько быстро развиваются инфокоммуникационные технологии*. Мегабайты, гигагерцы, терафлопсы, далее везде. Компании бодро рапортуют об очередном преодолении рубежа, СМИ дорисовывают для обывателей радужные картины «цифровой вселенной», компьютерный же криминал в предвкушении потирает руки. Да и обывателям нравятся обе вселенные. Одна официальная — с теми удовольствиями, что рекламируют фирмы. Другая неофициальная — например, безымянная домовая сеть типа «Липкино онлайн», где накануне премьеры блокбастера уже лежит качественная цифровая копия. Там же (как и на пиратских лотках) — развалы краденого софта и базы данных для начинающих частных сыщиков.

Причина неожиданных и неприятных явлений, как обычно, в том, что количество медленно и

подло переходит в качество. Сверхцель компьютерной индустрии — «информационная сверхпроводимость» в той самой цифровой вселенной: бесконечная память, бесконечная производительность, бесконечная скорость передачи информации. И все при минимальной цене. Незаметный на первый взгляд рост возможностей компьютерной техники приводит на определенном этапе к тому, что у злоумышленника в руках по доступной цене оказываются средства, от которых у Джеймса Бонда (образца 70-х годов, конечно) потекли бы слюнки. Полсотни долларов — и миниатюрный проходной разъем для клавиатуры аккуратно запишет в свою гигабайтную память все, что набирается на клавиатуре в течение месяца.

Защищать информацию в таких условиях — все равно что создавать резервуары для сверхтекучих жидкостей. Давайте честно посмотрим на то, как меняются показатели этой сверхпроводимости.

Закон Мура в действии

Возможности любой информационной системы определяются в трех измерениях: производительность вычислений, память, коммуникативность.

С производительности и начнем. В 1971 году на рынке появился первый микропроцессор 4004 (Intel, США). С того момента развитие вычислительных способностей определялось так называемым законом Мура**: «Каждые полтора года количество транзисторов в микропроцессоре удваивается» (другими словами, удваивается производительность за те же деньги), что приводит к экспоненциальному удешевлению вычислений. В процессоре 4004 было 2 тыс. транзисторов, в 286-м (1982) — уже 134 тыс., в 486-м (1989) — 1,2 млн, в Pentium III (1999) — почти 10 млн, в Intel Dual Core (2005) — более 1 млрд. Но это все процессоры для массовых ПК, где практически весь прирост производительности проедается оконно-кнопочными излишествами и «небывальными удобствами» для пользователей.

* Термин «инфокоммуникационные», а не просто «информационные» — замечательное изобретение отечественных чиновников; ниже мы увидим, что именно неотделимость технологий обработки информации от технологий передачи усугубляет проблему защиты информации.

** Гордон Мур — один из основателей Intel, подметивший чрезвычайно устойчивую тенденцию, названную затем в его честь.

■ Профессиональное мнение

■ **Михаил Калинин**,
генеральный директор
компании **StarForce
Technologies**



Сегодня проблема защиты информации особенно актуальна. И все указывает на то, что эта проблема будет существовать и через многие годы. Однако необходимо помнить, что в несколько раз увеличиваются не только возможности криптоанализа, но и возможности разработчиков технологических систем защиты информации. Конечно, всё, что создается с помощью человеческого или компьютерного ума, в итоге можно сломать, другое дело — сколько это займет времени. И хотя на флешке в 4 Гбайт можно вынести с работы любую информацию, все же некоторое

программное обеспечение защищается от копирования с помощью, например, того же продукта StarForce Corporative для серверных приложений или решения для защиты электронных документов StarForce Content. В этом случае, даже если человек скопирует ка-

ким-то способом информацию из защищенной системы документооборота или отдельный документ, то не сможет их открыть ни на каком другом компьютере, кроме рабочего. На взлом информации, «утекшей» за пределы компании, может понадобиться очень много времени, от нескольких дней до нескольких месяцев. Данная информация может оказаться уже не настолько востребованной и даже устаревшей. Кроме того, нельзя рассматривать криптографию в отрыве от проблемы хранения паролей и ключей. Если можно перехватить пароль во время ввода или чтения из файла, то надежность криптоалгоритма уже неважна. В

случае с криптографией нужно помнить также о защите программного обеспечения от изучения (реверс-инжиниринга). Из российских разработок известно решение StarForce Crypto, которое защищает исполняемый код приложения от отладчиков и дизассемблеров. Злоумышленник не сможет разобрать защищенную таким решением программу на кусочки и вычленив из них нужные ему сведения. Соответственно, интеллектуальная собственность останется у ее владельца. Естественно, что криптографические и иные способы защиты информации будут совершенствоваться, так же как и системы их взлома. Единственное, что мы можем — это быть всегда начеку и разрабатывать новые решения. Только практика покажет, насколько правильным путем мы идем. <

В сверхпроводящей и агрессивной информационной среде оказываются методы криптографической защиты информации.

Однако есть еще одна ниша (тоже, кстати, массовая), где ставка за победу в вычислительной гонке — без преувеличения «больше, чем жизнь»: проигравший уходит с рынка. Это видеоускорители и игровые приставки. И потому успехи здесь еще больше впечатляют. Так, если сегодня средний ПК «предлагает» за \$300 (в расчет идет только системный блок) производительность в 1 Гфлопс (1 млрд операций с плавающей точкой в секунду), то приставка SonyPlayStation 3 уже в 2006 году обеспечивала 2 Гфлопса***. В настольных ПК видеоускорители превратились в самую настоящую опухоль: по вычислительной мощности они опережают центральный процессор в разы, что заметно даже по размерам вентиляторов****.

До середины 90-х годов совершенно отдельной отраслью были суперкомпьютеры и процессоры для них. Но массовость производства и неизбежная дешевизна «обычных» микропроцессоров привели к их проникновению в область суперкомпьютеров. Символичен хотя бы тот факт, что знаменитая фирма Cray (штучные суперкомпьютеры) в 1996 году была куплена Silicon Graphics (почти штучные графические суперкомпьютеры), которая в свою очередь спустя пару лет объявила о переходе на... архитектуру Intel и отказе от собственных микропроцессоров MIPS. Такой тренд буквально за 5–10 лет привел к обвальному удешевлению самих суперкомпьютеров в пересчете на производительность. Да и с переходом на многоядерную архитектуру микропроцессоры превратились в «суперкомпьютеры на чипе». Если 1 Гфлопс в 1997 году стоил \$96,4 тыс. (суперкомпьютер IBM ASCI Red), то в 2008 году этот показатель составляет всего \$15 (суперкомпьютер Cray CX-1). Желющие получить представление о том, что такое современные суперкомпьютеры, могут обратиться

к рейтингу ТОП-500, который составляется два раза в год (www.top500.org, российский аналог — www.top50.ru).

Аналогично закон Мура действует и на снижение стоимости памяти — как оперативной, так и энергонезависимой. Гордон Мур говорил вообще о микросхемах; их миниатюризация одинаково влияет и на память, и на производительность, и даже на коммуникативность: везде мы имеем дело с одной и той же микроэлектронной базой. Что касается памяти — если в 1995 году 1 Мбайт оперативной памяти стоил \$40, то к концу 1996-го — уже \$4, а в 2008-м — 1 цент. Аналогично дешевеют и энергонезависимые запоминающие устройства (жесткие диски, записываемые компакт-диски, флеш-память и т. д.). «Информационная сверхпроводимость» наблюдается и в коммуникативности, причем в глобальном диапазоне — от системных шин и локальных сетей до Интернета.

Проблемы в одном измерении

Наиболее частая угроза информационной безопасности — кража информации. И здесь злоумышленников прежде всего интересует развитие сверхпроводимости в аспекте памяти, в меньшей степени — коммуникативности. Все же переписать информацию на носитель и унести — намного быстрее и безопаснее, чем «прокачать». Тут достаточно привести только российскую статистику крупных краж информации с последующим распространением на пиратском рынке. Одной из первых краде-

*** В 2008 году астрофизик Гуарав Ханна из MIT построил суперкомпьютер из 16 приставок PlayStation 3 для изучения черных дыр, причем основным стимулом было как раз получение дешевых гигафлопсов.

**** В 2007 году российская фирма Elcomsoft объявила о том, что ее ПО позволяет использовать графическую плату GeForce 8xxx (имеющую, по сути, суперкомпьютерную параллельную архитектуру) для ускорения поиска хеш-образов паролей примерно в 25 раз, то есть час вместо суток, сутки вместо месяца!

■ Валерий Ледовской, аналитик компании «Доктор Веб»



Действительно, сегодня становится сложнее защитить информацию. Вычислительные мощности современных компьютеров растут на глазах. И они используются не только в благих целях.

Авторы вредоносных программ, наряду с прочими методами, применяют и шифрование для блокирования доступа пользователя к его документам. В других случаях используется полиморфизм — как вредоносного кода, так и используемых упаковщиков исполняемых файлов. Алгоритмы упаковщиков и распаковщиков исполняемых вредоносных файлов усложняются с каждым днем, и вручную их проанализировать

просто невозможно. Часто используется обфускация (запутывание) вредоносных скриптов на веб-сайтах. И тем не менее неразрешимых проблем в области защиты информации нет. В частности, довольно просто с помощью увеличения длины ключа или незначительного усложнения алгоритмов шифрования отодвинуть решение проблемы доступа к зашифрованной информа-

ции на неопределенное время. Если мы говорим о шифровании постоянных потоков данных, то для их защиты от доступа неавторизованных для этого лиц достаточно приучить себя часто менять ключи шифрования. Скажем, один или несколько раз в сутки. Возможны и другие простые в практической реализации решения, позволяющие многократно усилить степень защиты. В частности, различные антивирусные и антиспам-разработки Dr.Web, которые на протяжении долгих лет показывают прекрасные результаты по детектированию и нейтрализации разнообразных интернет-угроз. При этом, конечно, не следует забывать следить за текущими возможностями суперкомпьютеров и распределенных вычислительных сетей. ◀

мерциализовались. Например, создаются вирусы, которые впоследствии выстраивают так называемые зомби-сети для удаленных атак и рассылки спама, и все это ради банальной прибыли — only business. Эпоха романтиков-студентов вроде Роберта Морриса, создающих вирусы из любопытства и желания самоутвердиться, канула в Лету.

Второй, менее очевидный побочный эффект: дешевые коммуникации открыли возможности создания высокопроизводительных систем из любых устройств, разве что не из микрокалькуляторов. При чем здесь суперкомпьютеры и информационная безопасность? Некоторые задачи взлома систем защиты (подбор ключа или прообраза для хеш-функции) обладают свойством практически абсолютной «распараллеливаемости», то есть разбиения задачи на независимые подзадачи, которые могут решаться одновременно на разных вычислительных устройствах. При высокой скорости соединений между вычислительными модулями (будь то системная шина, локальная сеть или

Интернет) возникает возможность создания дешевых метакомпьютеров — кластеров, линейно объединяющих производительность отдельных микропроцессоров или компьютеров. Теперь самое время сказать о роли аспекта коммуникативности в информационной безопасности и о синергетическом эффекте одновременного роста производительности, памяти и коммуникативности.

ных баз данных стала база МГТС в середине 90-х: характерно, что во времени это совпало с появлением первого емкого съемного носителя — записываемого CD. Затем утекла информация об абонентах «Билайна» (1996, 2004), МТС (2002), в 2003 году на пиратских дисках появились базы всех (!) абонентов питерских операторов («Мегафон», «Дельта Телеком», «Телеком XXI»), FORA, «Северо-Западный Телеком» и «Петерстар» — всего около 5 млн записей). Тогда компания после внутреннего расследования не разгласила источник утечки, но уверила, что виновные наказаны. Не оставались в стороне базы данных государственных служб: результаты переписи населения (2002), РКЦ Центробанка (2005), Пенсионного фонда (включая информацию о месте жительства, доходах, телефонах) — сначала Московского региона (2005), затем Красноярского края (2006), базы данных ВЭД и ГИБДД (2005). Можно с уверенностью сказать, что абсолютно все они украдены с использованием самых обычных носителей информации сотрудниками соответствующих организаций и компаний, причем далеко не нижнего уровня.

На каждую такую крупную базу — сотни и тысячи баз данных клиентов, операций и т. д., которые уносятся сотрудниками фирм при уходе с работы — или просто на всякий случай (по данным Ponemon Institute, 59% сотрудников хотя бы раз уносили с работы конфиденциальные данные). Воспрепятствовать этому технически очень трудно. На 4-гигабайтную флешку можно записать абсолютно все, если речь идет не о голливудском фильме, а о «настоящей» информации. И такие случаи остаются либо неизвестными, либо по понятным причинам не выносятся за пределы компаний. О том, что становится известным, можно прочитать, например, на сайте отечественной компании InfoWatch.

Об отрицательном влиянии на информационную безопасность другого аспекта — коммуникативности — можно говорить много. Наиболее очевидные угрозы видны на примере Интернета, который стал благодатной средой сразу для целого «букета»: это и распространение вирусов, и рассылка спама, и хакерские атаки. Причем за последние 5 лет, как отмечают аналитики, эти направления прочно соединились и ком-

муницировались. Например, создаются вирусы, которые впоследствии выстраивают так называемые зомби-сети для удаленных атак и рассылки спама, и все это ради банальной прибыли — only business. Эпоха романтиков-студентов вроде Роберта Морриса, создающих вирусы из любопытства и желания самоутвердиться, канула в Лету.

Криптография: проблема в трех измерениях

В сверхпроводящей и агрессивной информационной среде оказываются методы криптографической защиты информации, которые по-прежнему считаются самым надежным звеном в сложных цепях систем защиты информации.

Для большинства криптографических систем математически строго доказывается стойкость. Например, если алгоритм шифрования не имеет врожденных изъянов, то нетрудно подсчитать, сколько ключей потребуется злоумышленнику перебрать, чтобы найти правильный, и сколько на это понадобится времени. В современных шифрах длина ключа составляет 128–256 бит (американский стандарт DES и отечественный ГОСТ 28147-89); принято считать, что запас прочности здесь огромный.

Но те методы защиты информации, которые сегодня представляются надежными, завтра могут оказаться прозрачными для злоумышленников. По мнению авторов статьи, ситуация усугубляется тем, что из-за возможности взаимного дополнения производительности, памяти и коммуникативности возникает эффект «закона Мура в кубе». Имея увеличение характеристик по трем направлениям, в соответствии с законом Мура можно говорить о том, что возможности криптоанализа увеличиваются в 8–10 раз каждые полтора года, то есть прочность криптографического ключа «съедается» на 3–4 двоичных разряда ежегодно. Это наглядно демонстрируют проводимые среди добровольцев фирмой RSA Data Security (США) конкурсы по взлому распространенных криптосистем (в качестве стимула выступает денежная премия). Так, в 1977-м авторы криптосистемы RSA опубликовали 129-значное де-

■ Дальше — хуже

Все вышесказанное относится только к развитию вычислительной техники в рамках существующих технологий (микро-), однако переход к нанокomпьютерам, квантовым устройствам может означать скачкообразное увеличение информационной сверхпроводимости. Нанокomпьютеры обещают сразу на несколько порядков увеличить емкость памяти и производительность микропроцессоров (за счет создания большого числа ядер). Впрочем, в долгосрочной перспективе это, возможно, уложится в закон Мура. В отличие от нанокomпьютеров (где изменения хотя и серьезные, но все-таки чисто количественные), квантовые компьютеры обещают, например, быстрое решение задачи фактори-

зации больших чисел (разложения их на множители), что сделает тривиальным взлом асимметричных шифров, на которых держатся, например, все защищенные интернет-технологии. Кстати, один из создателей асимметричного шифра RSA Леонард Адельман еще 15 лет назад увлекся идеей биокомпьютеров (построенных на ДНК) и показал, что они намного быстрее могут решать некоторые задачи, чем обычные компьютеры. Наконец, стоит сказать и об одной технологии уже сегодняшнего дня — виртуализации вычислений. О виртуализации говорят сейчас много; один из модных терминов — «вычислительное облако», создание единой среды из разрозненных компьютеров, часть из которых обычно простаивает, в то время как другая —

работает с перенапряжением. В 2008 году появилась новость, которая, на первый взгляд, никакого отношения к защите информации не имеет. Открылся web-сервис Amazon Elastic Computing Cloud (EC2), в рамках которого есть возможность приобретать машинное время такого виртуального компьютера. Ориентировочная стоимость сервиса — 10 центов за один час аренды среднестатистического ПК. Расчеты показывают, что для подбора 56-разрядного ключа потребуется около \$2 млн и 200 часов. Конечно, это пока дорого, но ведь речь идет только о зарождении такого мощного направления, как виртуализация вычислений, способная на несколько порядков удешевить все ту же стоимость 1 гигафлопса. ◀

Итоги

Стоит ли сгущать краски и отказываться от прогресса ради безопасности? Конечно, нет. Тем более что сам прогресс неизбежен. Правильным представляется использование современных информационных технологий не только для работы с информацией, но и для ее защиты. Правда, здесь угрозы информационной безопасности можно разделить на те, в которых прогресс создает равные шансы для защиты и нападения, и те, в которых прогресс все же больше играет на руку злоумышленникам.

Например, использование сверхемких устройств хранения информации трудно предотвратить технологически, хотя в корпоративных системах защиты информации можно использовать «теневое копирование» — то есть сохранение всего, что записывается на внешние носители или передается через Интернет. А вот в задачах криптографии прогресс играет на руку скорее тем, кто ши-

сяточное число, предположив, что на факторизацию (открывающую путь к взлому системы) уйдет несколько миллионов лет, однако решение было найдено уже в 1994 году. Еще пять лет спустя на интернет-кластерах из компьютеров добровольцев были разложены числа в 140 и 155 десятичных разрядов, в 2006-м — в 220. Характерны и итоги конкурса по взлому шифра DES (поиск 56-разрядного ключа): в 1997 году шифр был взломан за 96 суток (DESCHALL Project: распределенная сеть из компьютеров добровольцев, число узлов до 78 тысяч); в 1999-м — меньше чем за сутки (специализированный компьютер EFF Deer Crack стоимостью \$250 тыс.); в 2006 году практически тот же результат был показан на специализированном компьютере COPACOBANA, который стоил всего \$10 тыс. Создатели стандарта DES (1977) рассчитывали, что запаса прочности хватит на 25 лет, однако уже в 1998-м была в срочном порядке развернута работа по выработке нового стандарта — AES (принят в 2001 году).

Это все иллюстрирует взаимодополняемость в аспекте «производительность — коммуникативность». О балансе «память — производительность» слышал каждый, кто хоть немного интересовался криптографией. Скромный вычислительный ресурс в ряде задач можно компенсировать огромной памятью. Существует, например, несколько сайтов, которые предлагают быстрый взлом хеш-образов паролей***** на основе так называемых «радужных таблиц». Рассчитав и правильно разместив в памяти хеш-образы для большого количества паролей (в первую очередь часто используемых), можно практически мгновенно находить искомым пароль, тогда как на «честный» способ даже на мощном компьютере ушло бы несколько часов или дней. Наиболее известный из таких проектов — RainbowCrack.com, который наработал уже более 1 Тбайта таблиц.

***** В защищенных системах (например в ОС Windows NT/2000/XP) пароли хранятся в преобразованном с помощью так называемых хеш-функций виде — для исключения дискредитации при непосредственном доступе злоумышленника.

Эффект «закона Мура в кубе» означает необходимость перехода к существенно большей длине ключа в криптографических системах.

фрует информацию, чем тем, кто пытается прочитать ее без знания ключа. Удлинение ключа всего на 1 бит удваивает объем работы по перебору ключей. Другое дело, что если речь идет о принятии каких-то стандартов, то их трудно менять слишком часто: вспомним, что стандарт DES поменяли на AES практически «на последней минуте матча».

Эффект «закона Мура в кубе» означает необходимость перехода к существенно большей длине ключа в криптографических системах. Речь может идти даже о возвращении в соответствии с законом диалектики к истокам научной криптографии, когда К. Шенноном было доказано, что идеальную криптостойкость дает система одноразового шифрования. На практике это означает, например, использование ключей длиной несколько мегабит в режиме сложения по модулю 2 (гаммирования) с защищаемыми данными, при котором достигаются одновременно и высокая стойкость шифрования, и предельная его скорость. Это лишь одно решение, которое лежит на поверхности. Проблема защиты информации в условиях «информационной сверхпроводимости», безусловно, приведет в практическую плоскость и более сложные решения — например, квантовые каналы, по крайней мере теоретически обещающие идеальную криптостойкость.

Одним словом, восхищаясь технологическим прогрессом, не стоит забывать, что им восхищаются и стоящие по другую сторону информационных баррикад. ◀