УДК 681.5.08

А.И. Гладышев[1]

ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИИ СЕГОДНЯ

В статье приводятся показатели развития инфокоммуникационных технологий, формулируются задачи оптимизации криптографической защиты информации в условиях сверхпроводящей и агрессивной информационной среды.

Ключевые слова: *безопасность информации, проблемы обеспечения безопасности информации, защита данных.*

A.I. Gladyshev

PROBLEMS OF ENSURING INFORMATION SECURITY TODAY

The article presents the indicators of ICT development and formulates the optimization problem of cryptographic protection of information in terms of superconducting and aggressive information environment.

Keywords: *information security, problems of ensuring information security, data protection.*

Причина неожиданных и неприятных явлений, как обычно, в том, что количество медленно и подло переходит в качество. Мегацель компьютерной индустрии – «информационная сверхпроводимость» в той самой цифровой вселенной: бесконечная память, бесконечная производительность, бесконечная скорость передачи информации.

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

До середины 1990-х годов совершенно отдельной отраслью были суперкомпьютеры и процессоры для них. Но массовость производства (с неизбежной дешевизной) «обычных» микропроцессоров привели к их проникновению в область суперкомпьютеров. С переходом на многоядерную архитектуру микропроцессоры превратились в «суперкомпьютеры на чипе». Если 1 Гфлопс в 1997 году стоил 96,4 тыс. долл. (суперкомпьютер IBM ASCI Red), то в 2008 году этот показатель составляет всего 15 долл. (суперкомпьютер Cray CX-1). Желающие получить представление о том, что такое современные суперкомпьютеры, могут обратиться к рейтингу Top500, который составляется два раза в год (www.top500.org, российский аналог – www.top50.ru).

Память и коммуникативность. Аналогично закон Мура действует и на снижение стоимости памяти как оперативной, так и энергонезависимой. Собственно Гордон Мур говорил вообще о микросхемах: их миниатюризация одинаково влияет и на память, и на производительность, и даже на коммуникативность – ведь везде мы имеем дело с одной и той же микроэлектронной базой. «Информационная сверхпроводимость» наблюдается и в коммуникативности, причем в глобальном диапазоне – от системных шин и локальных сетей до Интернета [3; 5].

Наиболее частая угроза информационной безопасности – кража информации. И здесь злоумышленников прежде всего интересует развитие сверхпроводимости в аспекте «память», в меньшей степени – коммуникативность. 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.

На каждую 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).

[1] Кандидат технических наук, доцент, доцент кафедры ИТиЕНД НОУ ВПО «Российский новый университет».

Воспрепятствовать этому технически очень трудно. На 4-гигабайтную флэшку можно записать абсолютно все, если речь идет не о голливудском фильме, а о «настоящей» информации [1; 2]. 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 угроз: это и распространение вирусов, и рассылка спама, и хакерские атаки. Причем за последние 5 лет, как отмечают аналитики, эти направления прочно слились и коммерциализовались. 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 самоутверждения, 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? [2]. Некоторые задачи взлома систем защиты (подбор ключа или прообраза для хэш-функции) обладают свойством практически абсолютной распараллеливаемости, то есть разбиении 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 производительности отдельных микропроцессоров или компьютеров. Пока мы не говорили о роли аспекта коммуникативности в информационной безопасности. Самое время сказать и о нем, и о синергетическом эффекте одновременного роста производительности, памяти и коммуникативности.

В сверхпроводящей и агрессивной информационной среде оказываются методы криптографической защиты информации, которые попрежнему считаются самым надежным звеном в сложных цепях систем защиты информации [1].

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 потребуется времени. В современных шифрах длина ключа составляет 128–256 бит (американский стандарт DES и отечественный ГОСТ 28147-89), и принято считать, что запас прочности здесь огромный [2].

Но те методы защиты информации, которые сегодня считаются 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 1,5 года, то есть каждые полтора года прочность криптографического ключа «съедается» на 3-4 двоичных разряда ежегодно. Это наглядно демонстрируют конкурсы, которые проводит среди добровольцев фирма RSA Data Security (США) по взлому распространенных криптосистем (в качестве стимула выступает денежная премия). Так, в 1977 г. авторы криптосистемы RSA опубликовали 129-значное десятичное число, предположив, что на факторизацию (открывающую путь к взлому системы) уйдет несколько миллионов лет, однако решение было найдено уже в 1994 г. В 1999 г. на интернет-кластерах из компьютеров добровольцев были разложены числа в 140 и 155 десятичных разрядов, в 2006 г. – 220. Характерны и итоги конкурса по взлому шифра DES (поиск 56-разрядного ключа): в 1997 г. шифр был взломан за 96 суток (DESCHALL Project: распределенная сеть из компьютеров добровольцев, число узлов до 78 тыс.), в 1999 г. – меньше чем за сутки (специализированный компьютер EFF Deep Crack стоимостью 250 тыс. долл.), в 2006 г. практически тот же результат был показан на специализированном компьютере COPACOBANA, который стоил всего 10 тыс. долл. Создатели стандарта DES (1977 г.) рассчитывали, что запаса прочности хватит на 25 лет, однако уже в 1998 г. была в срочном порядке развернута работа по выработке нового стандарта AES (принят в 2001 г.) [8].

Это все иллюстрирует взаимодополнение в аспекте «производительность – коммуникативность». О балансе «память – производительность» слышал каждый, кто хоть немного инте-

ресовался криптографией. Скромный вычислительный ресурс в ряде задач можно компенсировать огромной памятью. Существуют, например, несколько сайтов, которые предлагают быстрый взлом хэш-образов паролей на основе так называемых радужных таблиц. Если кратко – то, рассчитав и правильно разместив в памяти хэш-образы для большого количества паролей (в первую очередь часто используемых), можно практически мгновенно находить искомый пароль, хотя на «честный» даже на мощном компьютере на это ушло бы несколько часов или дней. Наиболее известный из таких проектов – RainbowCrack.com, который наработал уже более 1 Тб таблиц [7].

Стоит ли сгущать краски и отказаться 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 всё же больше играет на руку злоумышленникам [5].

Например, использование сверхъемких устройств хранения информации трудно предотвратить технологически, хотя в корпоративных системах защиты информации можно использовать «теневое копирование» – то есть запись всего, что записывается на внешние носители или передается через Интернет. А вот в задачах криптографии прогресс играет скорее на руку тем, кто зашифровывает информацию, чем тем, кто пытается прочитать ее без знания ключа [3]. Увеличение длины ключа всего на 1 бит, увеличивает объем работы по перебору ключей в два раза. 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 в несколько мегабит в режиме сложения по модулю 2 (гаммирования) с защищаемыми данными, при котором достигается одновременно и высокая стойкость шифрования, и предельная скорость шифрования. 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 [6].

Одним словом, восхищаясь технологическим прогрессом, не стоит забывать о том, что им так же восхищаются и те, кто стоит по другую сторону информационных баррикад [4].

Все вышесказанное относится только к развитию вычислительной техники в рамках существующих технологий (микро-), однако переход к нанокомпьютерам, квантовым устройствам может означать скачкообразное увеличение информационной сверхпроводимости. Нанокомпьютеры обещают сразу на несколько порядков увеличить емкость памяти и производительность микропроцессоров (за счет создания большого числа ядер). Впрочем, в долгосрочной перспективе возможно это уложится в закон Мура. В отличие от нанокомпьютеров, где изменения хотя и серьезные, но все-таки чисто количественные, квантовые компьютеры обещают, например, быстрое решение задачи факторизации больших чисел (разложение на множители больших чисел), что сделает тривиальной задачу взлома 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 – «облако вычислений», создание единой среды из разрозненных компьютеров, часть из которых обычно простаивает, в то время как другая работает с перенапряжением. В 2008 г. 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 долларов

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 всю ту же стоимость 1 гигафлопса.

Литература

1. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. – М. : Радио и связь, 1999.

2. ГОСТ Р 34.10-94. Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма. – М., 1995.

3. ГОСТ Р 34.11-94. Информационная технология. Криптографическая защита информации. Функция хэширования. – М., 1995.

4. ГОСТ Р 34.10-2001 Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи. – М., 2001.

5. Гладышев А.И. Разработка имитационной модели вирусной эпидемии на основе модели биологических вирусов: принципы, основные параметры, описание и зависимости // Вестник Российского нового университета. – 2012. – Выпуск 4. Управление, вычислительная техника и информатика. – С. 17–21.

6. Гладышев А.И., Жуков А.О. Использование в автоматизированной системе контроля полномочий биометрической идентификации // Вестник Российского нового университета. – 2013. – Выпуск 4. Управление, вычислительная техника и информатика. – С. 95–99.

7. Гладышев А.И. Удобство и безопасность компьютерных систем. В чем противоречие? // Вестник Российского нового университета. – 2012. – Выпуск 4. Управление, вычислительная техника и информатика. – С. 89–93.

8. Гладышев А.И., Жуков А.О. Достоинства и недостатки имитационного моделирования с использованием нейронных сетей // Вестник Российского нового университета. – 2013. – Выпуск 4. Управление, вычислительная техника и информатика. – С. 53–56.