– ***корпоративное управление ключами:*** управление ключами шифрования предприятия путем их интеграции в различные технологии шифрования данных при их хранении (дисковые массивы, магнитная лента и т.д.).

Облегчение бремени нормативно-правового соответствия и уменьшение сложности системы защиты данных

RSA Data Protection Manager объединяет токенизацию RSA с шифрованием на уровне приложений, комбинируя в одном продукте две наиболее часто используемые технологии. Шифрование традиционно считается предпочтительным способом обеспечения защиты данных в приложениях, а токенизация (подмена либо маскирование данных, как ее еще называют) – один из лучших методов сокращения расходов, связанных с достижением нормативно-правового соответствия.

RSA Data Protection Manager призван расширить возможности организаций по использованию токенизации. Чтобы защитить данные платежных карт, RSA объединила свою технологию токенизации с услугами таких партнеров, как First Data Corporation и VeriFone. Однако токенизация может обеспечить защиту не только платежных систем, ее можно применять и в других отраслях: при предоставлении финансовых услуг (защита информации, идентифицирующей личность, номеров социального страхования) и в здравоохранении (защита конфиденциальной информация медицинских карт).

Токенизированные данные сохраняют оригинальный формат, что ограничивает влияние этой технологии на приложение при сохранении высокого уровня защиты. Кроме того, метки способны сохранять некоторую часть исходных данных (например, последние четыре цифры номера социального страхования), так что другие приложения потенциально могут использовать метки, даже не получая доступа к реальной информации.

Riverbed: новые решения для облачных сред

Ноябрь 2010 г. – Компания Riverbed анонсировала 2 решения – Riverbed Cloud Steelhead™ и Riverbed Whitewater™ для использования в облачных средах. Оба решения позволяют ускорять миграцию данных в публичных облаках и одновременно улучшать производительность приложений, хостируемых в публичных облаках.

В частности, Cloud Steelhead v1.0 будет интегрирован с Amazon EC2 и Virtual Private Cloud (Amazon VPC). Чтобы гарантировать бесшовную интеграцию, образы Cloud Steelhead будут разворачиваться на базе Steelhead® Discovery Agent. Riverbed Cloud Portal даст возможность простого управления и легкого клонирования, позволяющего администраторам использовать существующие установки и конфигурации Cloud Steelhead.

Криптография в России: настоящее и возможные перспективы

Александр Ширманов – генеральный директор компании “Код Безопасности”.

SN. Информационная безопасность (ИБ) – одно из немногих направлений ИТ-отрасли, где Россия пытается поддерживать собственные стандарты. Основная особенность современных ИТ-инфраструктур – возможность шифрования данных "на лету" со скоростью 8–10 Гбит/с (например, с помощью серверной карты размером с ладонь). Уже в 2011 г. 10 Гбит/с конвергентные (LAN+SAN) сети станут стандартом использования. По оценкам некоторых экспертов, чтобы поддержать подобную скорость для гостовских алгоритмов, необходимы около 20 современных блейд-серверов. Каковы Ваши оценки?

А.Ш. По мнению специалистов “Кода Безопасности”, на алгоритмах по ГОСТу вполне достижима скорость в 5 Гбит/с на 1U блейде. Скорость в 10Гбит/с не потребует более 3 1U блейдов при условии, что под этой скоростью имеется в виду скорость шифрования множества соединений от разных, параллельно работающих сетевых абонентов. На мой взгляд, это даже более реальная ситуация, чем необходимость шифрования трафика отдельно взятого абонента со скоростью 10 Гбит/с. Например, при создании электронного правительства, где каждый гражданин должен иметь возможность получать услуги государства в электронной форме, действительно понадобятся высокие скорости шифрования совокупности десятков тысяч одновременных соединений, однако каждое из них будет требовать невысокой скорости шифрования (ведь скорости в 10Мбит/с гарантированно хватает для работы с любым сайтом).

SN. Современный ИТ-мир стремительно становится распределенным. В этой связи, по Вашему мнению, при существующих скоростях шифрования трафика Россия не окажется ли "в хвосте" с точки зрения информационной защищенности при магистральной передаче данных?

А.Ш. Я думаю, этого не случится. Магистральные каналы сейчас шифруют с помощью западной аппаратуры, использующей западные алгоритмы (и это разрешено, насколько я помню, постановлением правительства). Я не знаю, есть ли сейчас проблемы с ввозом такого оборудования, однако до сих пор законодательно было разрешено использование западной криптографии в банкоматах, в операционных системах и в каналообразующем оборудовании.

SN. В чем, по Вашему мнению, основные проблемы, связанные с повышением производительности гостовской криптографии?

А.Ш. Основная проблема российской криптографии, которая сдерживает повышение производительности потокового шифрования данных в сети до уровня западной криптографии, в том, что применяемый для таких случаев режим шифрования по ГОСТу не допускает распараллеливания операций. В соответствии с методикой ФСБ, каждый сетевой пакет разбивается на блоки и обрабатывается строго последовательно – от первого до последнего блока. Параллельная обработка отдельных блоков пакетов не допускается, так как в алгоритме используется результат обработки (шифрования) предыдущего блока, за счет чего достигаются высокая надежность шифрования и устойчивость к подмене данных, не уступающие самым современным зарубежным криптоалгоритмам, например AES256, и превосходящие западные алгоритмы с меньшей длиной ключа (такие как AES128, AES192, 3DES).

Однако в зависимости от ценности информации, требование надежности может уступать требованию скорости. Для таких случаев в алгоритме AES предусмотрена возможность применения ключей разной длины (от 128, 192 или 256 бит), а в алгоритме ГОСТ такой возможности нет.

Следует отметить, что AES, в отличие от ГОСТ, позволяет применять параллельную обработку данных внутри каждого блока шифрования, что по мнению экспертов, создает преимущество в скорости при аппаратной реализации алгоритма. Именно это “врожденное” свойство алгоритма используется западными производителями для создания высокопроизводительных аппаратных криптоускорителей.

SN. На Западе в настоящее время идет активный перевод средств ИБ на аппаратный уровень. В первую очередь это коснулось функций шифрования данных. На текущий момент такие микропроцессоры устанавливаются на жестких дисках, ленточных приводах, серверных адаптерах, SAN-директорах, материнских платах.

Недавно Intel купила McAfee. В ближайшей перспективе следует ожидать погружения на уровень массово выпускаемых микропроцессоров не только самой технологии AES, но и многих функций управления, связанных с шифрованием. Появляются анонсы о соглашениях и других вендоров в этом направлении.

Сейчас технологии ИБ активно интегрируются в состав базового ПО (ядра). Понятие ОС может относиться абсолютно ко всем уровням ИТ-инфраструктур.

В настоящее время в России имеются существенные трудности с ввозом импортного оборудования и ПО со встроенной стойкой криптографии, не относящегося только к банкоматам. С учетом сказанного, как отделить, что можно ввозить, а что нельзя, не совсем ясно. Уже в ближайшей перспективе, например, производители могут отказаться от производства HDD без функции шифрования. В связи с тем, что российский ИТ-рынок составляет доли процента мирового никто специально не будет "вычищать" ИТ-решения под законодательные требования России. В этом случае уже в ближайшие 2–3 года не окажется ли Россия в ситуации, когда фактически ничего нельзя будет ввозить, включая например, стандартные компьютеры и серверы?

А.Ш. Действительно, такая перспектива существует. В качестве примера могу сослаться на одну из публикаций на тему реализации AES в новых процессорах Intel – *http://www.thg.ru/cpu/aes_clarkdale/index.html*. И, в связи с тем, что, насколько мне известно, в ближайшей перспективе внесение изменений в методику или алгоритм шифрования ГОСТ в аспекте повышения скорости шифрования в приложениях не планируется, могут быть сложности в удовлетворении потребностей современных корпоративных датацентров. Т.е без должной аппаратной поддержки (серийно выпускаемых плат/чипов) современные требования к безопасности данных по показателю стоимость/производительность обеспечить будет невозможно. Здесь нужно отметить и то, что в России аппаратные ИБ-решения корпоративного класса не производятся.

Я полагаю, что правильным подходом было бы установление разных уровней требований к криптозащите информации различных уровней конфиденциальности. Например, для коммерческих структур было бы правильно разрешить им самостоятельно определять применяемые алгоритмы шифрования (в т.ч. западные). Для информации ограниченного доступа (включая коммерческую тайну) разумно оставить требования, продиктованные государством или согласованные с государством отраслевой саморегулирующейся организацией, так как эта информация охраняется именно государством (например, коммерческая тайна частных компаний обеспечивается государственной защитой от кражи третьими лицами. Отсюда логично, что государство имеет право продиктовать или согласовать требования к ее защите).

В настоящее время разработчики “Кода Безопасности” проводят исследовательские работы по созданию высокопроизводительных средств потового шифрования трафика, использующего алгоритм ГОСТ, например, с помощью использования мощных многопроцессорных серверов Intel последних моделей и серверных материнских плат и чипсетов с увеличенным размером кэша. И нам в значительной степени удалось продвинуться. Например, мы уже можем заявить, что сможем поддержать потоковую обработку 5Gbps трафика на 1U-серверах.

Гораздо больших результатов можно достичь при одновременной обработке потоков информации от нескольких сетевых источников – когда параллельно обрабатываются пакеты разных параллельных соединений. Например, такая обработка информации характерна для ЦОДов. Но данный проект находится в самой начальной фазе. Поэтому пока не могу сообщить конкретных цифр по нему.

Безусловно, разработка аппаратных ускорителей для шифрования по алгоритму ГОСТ в России могла бы еще в большей степени сдвинуть решение этой проблемы и повысить скорость как минимум в несколько раз по сравнению с программными решениями. Но для этого требуется обеспечить гарантированное качество безотказной работы таких чипов в условиях высокой круглосуточной нагрузки, а также обеспечить стабильность качества отдельных чипов в серийном производстве. В общем, здесь мы ждем инициативу от российских производителей аппаратных устройств.

SN. Помимо криптооборудования и ПО, в современных корпоративных ИТ-инфраструктурах для поддержания ИБ большое значение играют системы управления ключами. Причем наиболее используемых в мире всего несколько штук, что говорит об определенном уровне сложности их разработки. В настоящее время они также запрещены в России. Какова ситуация с отечественными разработками в этой области, и в какой мере они способны интегрироваться с западными аналогами?

А.Ш. Если речь идет о Token Management Systems (TMS), которые, например, предлагаются компаниями Aladdin и RSA, то мне не известны какие-либо проблемы с ввозом и применением в России таких программных средств.

SN. Подытоживая, что Вы хотели бы выделить как резюме?

А.Ш. В качестве выводов хотелось бы отметить следующие:

1. По статистике, до 90% Интернет-трафика – это спам. На мой взгляд, нет необходимости шифровать все подряд с использованием именно алгоритма ГОСТ. Если шифровать ГОСТОм только охраняемую государством информацию, то действующий алгоритм ГОСТ позволит решить эту задачу, так как такой информации много не бывает. И скорости выше 10 Гбит/с в части информации ограниченного доступа вряд ли появятся в обозримом будущем.

2. Если ставить задачу о поддержке российских производителей криптографии (аппаратуры и программного обеспечения), тогда однозначно нужно решать вопрос с алгоритмом шифрования в части возможности распараллеливания его работы. Кроме того, помогла бы поддержка государства, например, ввиде грантов при условии, что изделия, сочетающие в себе западные и российские алгоритмы, созданные российскими производителями, будут иметь экспортный потенциал (например, аналогично опыту Израиля http://www.unova.ru/article/5513).

3. Также помогло бы озвучивание долгосрочной позиции государства в области применения западной и российской криптографии в России, в зависимости от категории обрабатываемой информации. Дело в том, что инвестиции в производство аппаратных средств шифрования начинают окупаться не менее чем через 3 года, и неопределенность в отношении вопроса, что будет через 3-5 лет в России с шифрованием, сдерживает инвестиции в этой области.

IBM: новая архитектура хранения удваивает скорость аналитики

Ноябрь 2010 г. – На конференции Supercomputing 2010, корпорация IBM сообщила подробности о новой архитектурной модели хранения данных, разработанной учеными IBM, которая позволит преобразовывать терабайты "чистой" информации в применимые на практике знания в 2 раза быстрее, чем это было возможно ранее*). Новая архитектура, идеально подходящая для приложений облачных вычислений и рабочих нагрузок с интенсивной обработкой данных – подобно цифровым медиа, финансовой аналитике и извлечению из данных ценной информации – сэкономит клиентам часы сложных вычислительных процессов без необходимости осуществления значительных инвестиций в инфраструктуру. Создав наиболее инновационную и эффективную архитектурную модель для задач высокопроизводительных вычислений, с лучшими показателями производительности, масштабируемости и использования ресурсов подсистемы хранения данных, IBM одержала заслуженную победу в конкурсе Storage Challenge (“Проблема хранения данных”).

Выполнение аналитических задач с огромными массивами данных приобретает сегодня все большую важность, однако организации могут пока лишь продолжать соответствующим образом наращивать мощности своих корпоративных систем хранения. Компании стремятся найти возможности решения проблем громадных объемов сохраняемых данных и достижения новых уровней информированности и знания своего бизнеса, и, поэтому, им необходимы альтернативные технологии, такие как облачные вычисления, чтобы идти в ногу с растущими требованиями к хранению данных, а также эффективно управлять гибкостью рабочих нагрузок через быстрое развертывание системных ресурсов для различных видов рабочих нагрузок.

"Компании буквально наталкиваются на непреодолимое препятствие, будучи не

*) Согласно результатам эталонных тестов MapReduce Benchmarks, проведенных на 16-узловом кластере с 4 SATA-дисками в каждом узле для сравнения файловых систем GPFS-SNC и HDFS.