Создание защищенных информационных систем на базе средств криптографической защиты информации

Костевич Андрей Леонидович, заведующий НИЛ компьютерной безопасности, НИИ прикладных проблем математики и информатики БГУ, кандидат физико-математических наук. Стаж работы в области компьютерной безопасности: 15 лет.

Каково место криптографических методов защиты информации при построении систем защиты информации?

Под защитой информации традиционно понимают обеспечение конфиденциальности, целостности и доступности информации. Понятно, что этого можно добиться различными способами: организационными, техническими, реализацией политики управления доступом и т.д. Однако, криптографические методы занимают особое место в системах защиты информации в любой информационной системе: только криптографические методы гарантированно могут защитить информацию при передаче по общедоступным каналам связи (а такими являются все современные каналы связи), а также при угрозе физического доступа или кражи носителей информации. Ни одни другие методы не смогут обеспечить защиту информации в таких условиях.

Насколько легко реализовывать данные угрозы: получать доступ к информации, передаваемой по общедоступным каналам связи, например к сети единого национального процессингового центра РБ на основе ВОЛС?

Современные информационные системы являются распределенными, связь между их частями осуществляется через общедоступные сети передачи информации, в частности, через Интернет, через беспроводные сети передачи данных.

Приведем достаточно обыденный пример: пользователь в системе интернет–банкинга оплачивает счета с домашнего компьютера. Связь в квартире зачастую обеспечивается по беспроводной технологии Wi-Fi, злоумышленнику для доступа к данной информации достаточно находиться на некотором расстоянии от точки доступа Wi-Fi, использовать обычный ноутбук с поддержкой Wi-Fi и бесплатное программное обеспечение–перехватчик данных. За пределами квартиры информация передается по общедоступным кабельным сетям, к которым, при особом желании, злоумышленник также может получить физический доступ. Соответственно, он может получить доступ и к передаваемой информации: номеру счета и паролю доступа. Необходимость защиты такой информации понятна даже неспециалисту. И таких примеров можно привести очень много, особенно в банковской сфере.

Не надо думать, что существуют какие-то специальные каналы передачи информации, которые могут защитить от угрозы перехвата, например оптоволоконные каналы. В 2009 году австралийскими специалистами с использованием общедоступного оборудования стоимостью порядка $500 продемонстрирован показательный пример перехвата данных, передаваемых по городским оптоволоконным каналам связи. Причем среди перехваченной информации оказалась банковская информация биржи в Мельбурне.

Таким образом, все определяется мотивацией и возможностями злоумышленника: следует исходить из того, что существует техническая возможность перехвата информации, передаваемой по любым каналам.

Поэтому владельцам информационных систем важны 100% гарантии невозможности доступа злоумышленников к их информации. Однако **гарантировать** невозможность доступа злоумышленника к каналам передачи информации невозможно, даже в сети единого национального процессингового центра РБ. Поэтому единственной возможностью защиты информации в этом случае является применение криптографических методов.

Можно ли говорить о 100% гарантии защиты информации при использовании криптографических методов?

Существует строгая математическая формулировка стойкости, обеспечиваемой применением криптографических методов. Но если говорить просто, то действительно можно утверждать о 100% гарантии защиты информации. Взглянем на Закон Республики Беларусь «Об электронном документе и электронной цифровой подписи»: применения такого криптографического алгоритма как электронная цифровая подпись достаточно, чтобы электронный документ имел такую же юридическую силу, как и традиционный бумажный документ. Если возникнут сомнения в подлинности электронного документа и дело дойдет до суда, то суд будет безоговорочно доверять выводам о подлинности электронного документа, сделанным сертифицированным средством криптографической защиты информации.

Представьте, какие в связи с этим открываются перспективы: внедрив электронную цифровую подпись можно отказываться от бумажных документов, число административного персонала сокращается, скорость обработки документов возрастает… Весь мир идет по пути широкого внедрения электронной цифровой подписи и других криптографических методов защиты информации.

Как же выбрать средство криптографической защиты информации? Что можно сказать о надежности имеющихся продуктов?

Можно рекомендовать использовать сертифицированные средства защиты информации, в том числе средства криптографической защиты информации. Это позволяет соблюдать требования национального законодательства в области защиты

информации. Это также обеспечивает отсутствие существенных недостатков в средствах: по опубликованной статистике США в порядка 50% средств криптографической защиты информации, представленных на сертификацию, независимыми аудиторами выявляются существенные уязвимости. Проведение сертификации приводит к устранению выявленных уязвимостей в средствах криптографической защиты информации. Что можно после этого сказать о надежности средств, не проходивших сертификацию или другую независимую оценку? Наверное, ничего хорошего... А ведь надо обеспечить надлежащий уровень защищенности информационной системы в целом.

Как же обеспечить надлежащий уровень защищенности информационных систем?

На белорусском рынке имеется достаточно много сертифицированных средств, однако их перечень не такой большой, как хотелось бы. Поэтому понятно стремление организаций использовать существующие иностранные продукты для защиты информации в своих информационных системах. Однако, повторюсь, это стремление наталкивается на требования национального законодательства в области защиты информации: требуется проведения сертификации или государственной экспертизы таких продуктов для независимого подтверждения их характеристик. Отметим, что сертификация или государственная экспертиза является обязательной для государственных информационных систем и систем, обрабатывающих так называемые персональные данные. Остальные владельцы информационных систем должны сами определять достаточность мер по защите информации. Например, в банковской сфере действуют международные стандарты по защите банковской информации: Payment Card Industry Data Security Standard (PCI DSS).

Получить подтверждение надлежащего уровня защиты достаточно сложно: мало просто разработать и внедрить систему защиты информации,требуется убедить в ее надежности независимого аудитора. Это является одной из главных проблем для разработчиков: разработка становится не единственной главной задачей, а выбор технологии разработки может существенно затруднить вторую главную задачу — подтвердить достаточность уровня защиты.

С этой точки зрения использование криптографических методов защиты информации существенно облегчает жизнь: для средств криптографической защиты информации существует достаточно простая система сертификации, их можно использовать для гарантированного предотвращения большого перечня угроз. Поэтому использование сертифицированных средств криптографической защиты информации зачастую является единственной возможностью подтверждения надлежащего уровня защиты информации в информационной системе.

Кто проводит экспертизу? Проведение экспертизы систем защиты информации — независимого аудита — требует достаточно высокой квалификации проверяющего. Поэтому экспертиза является лицензируемым видом деятельности: проведение экспертиз на соответствие национальным требованиям по защите информации регулируется Оперативно аналитическим центром при Президенте Республики Беларусь; право на проведение экспертиз на соответствие корпоративным требованиям определяется соответствующим регулятором. Поэтому, например, проведение аудита белорусских банков на соответствие PCI DSS проводят иностранные аудиторы, имеющие лицензию в данной корпоративной системе безопасности платежных систем.

Возникают ли проблемы при создании систем защиты информации на базе средств криптографической защиты информации?

Если говорить о создании системы защиты информации для одной отдельно взятой информационной системы, то здесь отечественные разработчики накопили достаточно большой опыт и особых проблем не возникает. Особенно если процесс создания сопровождается независимой экспертизой.

Проблемы возникают при организации взаимодействия информационных систем, разработанных различными разработчиками. Особенно остро вопрос стоит при взаимодействии систем защищенного электронного документооборота: отсутствие единых форматов данных существенно затрудняет их объединение. Плохо, если различные государственные структуры не могут обмениваться электронными документами. Отметим, что в настоящее время Национальным банком ведутся работы по разработке стандартов, призванных обеспечить совместимость. Однако разработчикам средств криптографической защиты информации потребуется еще какое-то время, чтобы выполнить все разрабатываемые требования.

Обычным пользователям не слишком много известно о криптографических методах защиты информации, как же им защищать свою информацию?

К сожалению, да. Зато необходимость применения криптографических методов все более очевидной становится для разработчиков информационных систем и продуктов.

Поэтому обычный пользователь автоматически становится обладателем целой линейки надежных средств криптографической защиты информации: в операционные системы семейств Windows и Linux встроена поддержка протокола IPSec для защиты информации на сетевом уровне, протокола TLS для защиты на уровне приложений, для разных операционных систем предлагаются средства шифрования дисков (например, TrueCrypt, Bitlocker) и т.п. Хотя даже самые надежные средства криптографической защиты информации могут быть бездумно настроены и эксплуатироваться таким образом, что не смогут обеспечить гарантированный уровень защиты.

Показательным примером является пример компрометации Skype спецслужбами Египта с помощью специального вредоносного программного обеспечения: согласно опубликованным сведениям, спецслужбы Египта устанавливали на компьютеры местных революционеров специальное программное обеспечение, которое перехватывало видео на этапе его передачи от видеокамеры до шифрования перед его передачей. Другим показательным примером является поток атак на российские системы интернет–банкинга: как со стороны внутренних нарушителей, так и со стороны хакеров.

Как же потенциальным пользователям получить необходимые сведения о криптографических методах защиты информации и правильном их применении?

Белорусский государственный университет осуществляет подготовку специалистов по специальности «Компьютерная безопасность». Также в БГУ действуют курсы повышения квалификации в области информационной безопасности, на которых также рассказывают и о криптографических методах защиты информации. ■