Тема 7 Практика и проблемы внедрения электронного документооборота

7.1. Подделка подписей.

Анализ возможностей подделки подписей — задача криптоанализа. Попытку сфальсифицировать подпись или подписанный документ криптоаналитики называют «атака».

Модели атак и их возможные результаты:

Полный взлом цифровой подписи. Получение закрытого ключа, что означает полный взлом алгоритма.

Универсальная подделка цифровой подписи. Нахождение алгоритма, аналогичного алгоритму подписи, что позволяет подделывать подписи для любого электронного документа.

Выборочная подделка цифровой подписи. Возможность подделывать подписи для документов, выбранных криптоаналитиком.

Экзистенциальная подделка цифровой подписи. Возможность получения допустимой подписи для какого-то документа, не выбираемого криптоаналитиком.

Ясно, что самой «опасной» атакой является адаптивная атака на основе выбранных сообщений, и при анализе алгоритмов ЭП на криптостойкость нужно рассматривать именно её (если нет каких-либо особых условий).

При безошибочной реализации современных алгоритмов ЭП получение закрытого ключа алгоритма является практически невозможной задачей из-за вычислительной сложности задач, на которых ЭП построена. Гораздо более вероятен поиск криптоаналитиком коллизий первого и второго рода. Коллизия первого рода эквивалентна экзистенциальной подделке, а коллизия второго рода — выборочной. С учетом применения хэш-функций, нахождение коллизий для алгоритма подписи эквивалентно нахождению коллизий для самих хэш-функций.

7.2. Подделка документа (коллизия первого рода)

Злоумышленник может попытаться подобрать документ к данной подписи, чтобы подпись к нему подходила. Однако в подавляющем большинстве случаев такой документ может быть только один. Причина в следующем:

Документ представляет из себя осмысленный текст.

Текст документа оформлен по установленной форме.

Документы редко оформляют в виде Plain Text-файла, чаще всего в формате DOC или HTML.

Если у фальшивого набора байт и произойдет коллизия с хэшем исходного документа, то должны выполниться 3 следующих условия:

Случайный набор байт должен подойти под сложно структурированный формат файла.

То, что текстовый редактор прочитает в случайном наборе байт, должно образовывать текст, оформленный по установленной форме.

Текст должен быть осмысленным, грамотным и соответствующим теме документа.

Впрочем, во многих структурированных наборах данных можно вставить произвольные данные в некоторые служебные поля, не изменив вид документа для пользователя. Именно этим пользуются злоумышленники, подделывая документы.

Вероятность подобного происшествия также ничтожно мала. Можно считать, что на практике такого случиться не может даже с ненадёжными хэш-функциями, так как документы обычно большого объёма — килобайты.

7.3. Получение двух документов с одинаковой подписью (коллизия второго рода).

Куда более вероятна атака второго рода. В этом случае злоумышленник фабрикует два документа с одинаковой подписью, и в нужный момент подменяет один другим. При использовании надёжной хэш-функции такая атака должна быть также вычислительно сложной. Однако эти угрозы могут реализоваться из-за слабостей конкретных алгоритмов хэширования, подписи, или ошибок в их реализациях. В частности, таким образом можно провести атаку на SSL-сертификаты и алгоритм хэширования MD5.

7.4. Социальные атаки

Социальные атаки направлены не на взлом алгоритмов цифровой подписи, а на манипуляции с открытым и закрытым ключами.

Злоумышленник, укравший закрытый ключ, может подписать любой документ от имени владельца ключа.

Злоумышленник может обманом заставить владельца подписать какой-либо документ, например, используя протокол слепой подписи.

Злоумышленник может подменить открытый ключ владельца на свой собственный, выдавая себя за него.

Использование протоколов обмена ключами и защита закрытого ключа от несанкционированного доступа позволяет снизить опасность социальных атак.

7.5. Управление открытыми ключами.

Важной проблемой всей криптографии с открытым ключом, в том числе и систем ЭП, является управление открытыми ключами. Так как открытый ключ доступен любому пользователю, то необходим механизм проверки того, что этот ключ принадлежит именно своему владельцу. Необходимо обеспечить доступ любого пользователя к подлинному открытому ключу любого другого пользователя, защитить эти ключи от подмены злоумышленником, а также организовать отзыв ключа в случае его компрометации.

Задача защиты ключей от подмены решается с помощью сертификатов. Сертификат позволяет удостоверить заключённые в нём данные о владельце и его открытый ключ подписью какого-либо доверенного лица. Существуют системы сертификатов двух типов: централизованные и децентрализованные. В децентрализованных системах путём перекрёстного подписывания сертификатов знакомых и доверенных людей каждым пользователем строится сеть доверия. В централизованных системах сертификатов используются центры сертификации, поддерживаемые доверенными организациями.

Центр сертификации формирует закрытый ключ и собственный сертификат, формирует сертификаты конечных пользователей и удостоверяет их аутентичность своей цифровой подписью. Также центр проводит отзыв истекших и компрометированных сертификатов и ведет базы выданных и отозванных сертификатов. Обратившись в сертификационный центр, можно получить собственный сертификат открытого ключа, сертификат другого пользователя и узнать, какие ключи отозваны.

7.6. Хранение закрытого ключа.

Смарт-карта и USB-брелоки eToken

Закрытый ключ является наиболее уязвимым компонентом всей криптосистемы цифровой подписи. Злоумышленник, укравший закрытый ключ пользователя, может создать действительную цифровую подпись любого электронного документа от лица этого пользователя. Поэтому особое внимание нужно уделять способу хранения закрытого ключа. Пользователь может хранить закрытый ключ на своем персональном компьютере, защитив

его с помощью пароля. Однако такой способ хранения имеет ряд недостатков, в частности, защищенность ключа полностью зависит от защищенности компьютера, и пользователь может подписывать документы только на этом компьютере.

В настоящее время существуют следующие устройства хранения закрытого ключа:

- Дискеты
- Смарт-карты
- USB-брелоки
- Таблетки Touch-Memory

Кража или потеря одного из таких устройств хранения может быть легко замечена пользователем, после чего соответствующий сертификат может быть немедленно отозван.

Наиболее защищенный способ хранения закрытого ключа — хранение на смарт-карте. Для того, чтобы использовать смарт-карту, пользователю необходимо не только её иметь, но и ввести PIN-код, то есть, получается двухфакторная аутентификация. После этого подписываемый документ или его хэш передается в карту, её процессор осуществляет подписывание хэша и передает подпись обратно. В процессе формирования подписи таким способом не происходит копирования закрытого ключа, поэтому все время существует только единственная копия ключа. Кроме того, произвести копирование информации со смарт-карты сложнее, чем с других устройств хранения.

В соответствии с законом «Об электронной подписи», ответственность за хранение закрытого ключа владелец несет сам.

7.7. Социальные проблемы внедрения ЭП и электронного документооборота.

Предприятию, которое решило перейти на электронный документооборот, не нужно выполнять сложных преобразований и затратных операций. В первую очередь необходимо перевести все бумажное делопроизводство в электронный вид. Это предлагается сделать при помощи таких простых средств, как Microsoft Office или его бесплатный аналог OpenOffice.org., то есть привычные карточки, бланки и типовые формы необходимо создать в электронном виде на компьютере. Сотрудники предприятий и должностные лица должны работать с ними, как с бумажными документами, но заполнять на компьютерной технике и подписывать ЭЦП. Существуют и такие

бумажные документы, которые не требуют подписи, например пояснительные записки или открытые письма.

Для них предлагается использовать ЭП в качестве идентификатора для определения принадлежности документа. Для осуществления электронного документооборота важно, чтобы все участники электронного взаимодействия имели идентичные средства работы с ЭП, то есть чтобы можно было подписывать и проверять подпись на любом компьютере в информационной системе, иначе электронный документооборот теряет свой смысл.

В странах с развитой экономикой ЭП используется уже более 10 лет, причем не только на крупных, но и на средних и небольших предприятиях. Исследование законодательства и принципов работы зарубежных ЭП показало, что их прямой перенос на российские предприятия оказывается не релевантным. Это можно доказать на примере американской системы DSS (Digital Signature Standard) или DSA. Шифрование в таких системах идеально подходит для американских предприятий, но может оказаться неработающим в России, поскольку документы должны содержать кириллические, а не только латинские символы, а зашита должна осуществляться в соответствии со степенью секретности – это касается не только военной государственной тайны, но и коммерческой тайны. Очевидным является тот факт, что зарубежная техническая поддержка и работа через американские серверы делает невозможным прямой перенос этой системы в Россию, поскольку информация может подвергаться взлому.