МОДЕЛИ АТАК ЭЛЕКТРОННО-ЦИФРОВОЙ ПОДПИСИ И ИХ ВОЗМОЖНЫЕ РЕЗУЛЬТАТЫ

Анасович Ю.В., Анасович В.Д.
УО Белорусский государственный университет транспорта
bsut@bsut.by

Электронная цифровая подпись – это реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющей распознать владельца сертификата ключа подписи, а также установить отсутствие искажений информации в электронном документе. [2] Электронная цифровая подпись в электронном документе равнозначна собственноручной подписи в документе на бумажном носителе при одновременном соблюдении следующих условий:

• сертификат ключа подписи, относящийся к этой электронной цифровой подписи, не утратил силу (то есть действует) на момент проверки или на момент подписания электронного документа при наличии доказательств, определяющих момент подписания;

• электронная цифровая подпись используется в соответствии со сведениями, указанными в сертификате ключа подписи.

При этом электронной документ с электронной цифровой подписью имеет юридическое значение при осуществлении отношений, указанных в сертификате ключа подписи.

Поскольку электронная цифровая подпись (далее – ЭЦП) – это средство защиты информации, то ЭЦП должна обеспечивать выполнение следующих основных функций:

• подтверждать, что подписывающее лицо сознательно подписало электронный документ;

• подтверждать, что документ подписало именно подписывающее лицо и только оно;

• ЭЦП должна существенно зависеть от подписываемого документа, в том числе от имеющихся в нем отметок времени;

• подписывающее лицо не должно иметь возможности отказаться впоследствии от факта подписи электронного документа.

Однако, возможны ситуации, когда электронно-цифровая подпись находится в опасности. Анализ возможностей подделки подписей – задача криптоанализа. Попытку сфальсифицировать подпись или подписанный документ криптоаналитики называют «атака».

В своей работе в 1984 году американские ученые Шафи Гольдвассер, Сильвио Микали и Рональд Ривест описывают следующие модели атак, которые актуальны и в настоящее время [3]:

• атака с использованием открытого ключа. Криптоаналитик обладает только открытым ключом;

- атака на основе известных сообщений. Противник обладает допустимыми подписями набора электронных документов, известных ему, но не выбираемых им;
- адаптивная атака на основе выбранных сообщений. Криптоаналитик может получить подписи электронных документов, которые он выбирает сам.

Также в работе описана классификация возможных результатов атак:

- 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.

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

При безошибочной реализации современных алгоритмов электронной подписи получение закрытого ключа алгоритма является практически невозможной задачей из-за вычислительной сложности задач, на которых построена электронная подпись. Гораздо более вероятен поиск криптоаналитиком коллизий первого и второго родов. Коллизия первого рода эквивалентна экзистенциальной подделке, а коллизия второго рода — выборочной. С учётом применения хеш-функций, нахождение коллизий для алгоритма подписи эквивалентно нахождению коллизий для самих хеш-функций. [1]

Коллизия хеш-функции — это равенство значений хеш-функции на двух различных блоках данных.

Итак, рассмотрим подделку электронного ключа подробнее (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 txt-файла, чаще всего в формате DOC или HTML.

Если у фальшивого набора байт и произойдет коллизия с хешем исходного документа, то должны выполниться три 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. Некоторые форматы подписи даже защищают целостность текста, но не служебных полей.

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

Далее рассмотрим получение двух документов с одинаковой подписью или коллизию второго рода.

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

Существуют такой вид атак как социальные атаки. Они 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.

Важной проблемой всей криптографии с открытым ключом, в том числе и систем электронной подписи, 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 ведёт базы (списки) выданных и отозванных сертификатов. Обратившись в сертификационный центр, можно получить собственный сертификат открытого ключа, сертификат другого пользователя и узнать, какие ключи отозваны.

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, защищённость ключа полностью зависит от защищённости компьютера, и пользователь может подписывать документы только на этом компьютере.

Наиболее защищённый способ хранения закрытого ключа – хранение на смарт-карте. Для того, чтобы применять смарт-карту, пользователю необходимо не только её иметь, но и ввести PIN-код, то есть, получается двухфакторная аутентификация. После этого подписываемый документ или его хеш передаётся в карту, её процессор осуществляет подписывание хеша, и передаёт 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 немного сложнее, чем с других устройств хранения.

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

Список использованных источников:

1. Рябко, Б. Я. Основы современной криптографии для специалистов в информационных технологиях / Б. Я. Рябко, А. Н. Фионов— Б.м.: Научный мир, 2004. — 173 с.
2. Электронная цифровая подпись [Электронный ресурс]. – Режим поступа: http://www.russika.ru/t.php?t=3897. – Дата обращения: 25.02.2019.
3. Goldwasser, Shafi. «A digital signature scheme secure against adaptive chosen-message attacks.» / Shafi Goldwasser, Silvio Micali, and Ronald Rivest. SIAM Journal on Computing, 17(2):281—308, Apr. 1988.