Доклад по теме: Атаки цифровой подписи

Выполнила: Лебедева Ольга Андреевна, НПМмд-02-25, 1032219337

Содержание

Список иллюстраций

Введение

Современные цифровые подписи [1] стали основой доверия в электронной среде — от банковских операций до государственных систем. Однако, как и любые криптографические механизмы, они уязвимы перед различными видами атак.

Цель работы

Провести анализ основных видов атак на системы электронной цифровой подписи, классифицировать их по методам реализации и возможным последствиям.

Задачи

1. Дать определение ЭЦП и раскрыть ее ключевые функции.
2. Изучить и систематизировать основные модели атак на ЭЦП, включая адаптивные атаки, атаки на основе коллизий хеш-функций и социальные атаки.
3. Привести реальные примеры успешных атак на криптографические алгоритмы, лежащие в основе ЭЦП.
4. Сформулировать выводы о наиболее актуальных угрозах и основных мерах по противодействию им.

Актуальность темы

В условиях повсеместной цифровизации электронный документооборот становится неотъемлемой частью бизнеса, государственных услуг и повседневной жизни. Ключе-

вым элементом, обеспечивающим юридическую значимость и безопасность электронных документов, является электронная цифровая подпись (ЭЦП). Она гарантирует целостность документа, идентифицирует его автора и обеспечивает неотрекаемость. Однако, как и любая технология, ЭЦП не является абсолютно неуязвимой. Растущая зависимость от цифровых взаимодействий делает системы на основе ЭЦП привлекательной мишенью для злоумышленников. Понимание существующих моделей атак на ЭЦП является критически важным для разработки надежных систем защиты, оценки рисков и формирования цифровой грамотности пользователей.

Гипотеза

Можно предположить, что наибольшую практическую опасность представляют не теоретические атаки на математическую основу ЭЦП, а атаки, эксплуатирующие слабые места в реализации алгоритмов, уязвимости вспомогательных компонентов (таких как хеш-функции) и ошибки пользователей на организационном и индивидуальном уровнях.

Проблематика

Несмотря на криптографическую стойкость современных алгоритмов ЭЦП, существует разрыв между теоретической безопасностью и реальными угрозами. Многие пользователи и организации ошибочно полагаются на абсолютную надежность ЭЦП, не уделяя достаточного внимания уязвимостям, связанным с реализацией алгоритмов, использованием устаревших хеш-функций, а главное – рискам, возникающим из-за человеческого фактора и ошибок в процедурах использования и хранения ключей. Недостаточная информированность о спектре возможных атак создает ложное чувство безопасности.

Методы исследования

Теоретический анализ научной литературы и публикаций в области криптографии, систематизация и классификация информации, сравнительный анализ.

Структура работы

Доклад состоит из введения, двух основных разделов (определение и функции ЭЦП, анализ видов атак), заключения и списка использованных источников.

ЭЦП: определение, функции и принцип работы

Сущность и юридический статус ЭЦП

Электронная цифровая подпись (ЭЦП) — это специальный реквизит электронного документа, созданный путем криптографического преобразования информации. Проще говоря, это уникальная цифровая метка (набор байтов), которая однозначно связывает документ с лицом, его подписавшим, и защищает этот документ от подделки.

С юридической точки зрения, в соответствии с законодательством многих стран, квалифицированная ЭЦП равнозначна собственноручной подписи на бумажном носителе при одновременном соблюдении двух условий:

1. Сертификат ключа проверки подписи действует на момент подписания документа или на момент его проверки.
2. Подпись используется в соответствии со сведениями, указанными в сертификате.

Это придает электронному документу, подписанному ЭЦП, полную юридическую силу.

Ключевые функции ЭЦП

ЭЦП как средство защиты информации призвана обеспечивать выполнение следующих фундаментальных функций:

1. Аутентификация. Подпись подтверждает, что документ подписан именно заявленным лицом (владельцем закрытого ключа) и никем иным. Это отвечает на вопрос: “Кто подписал?”.
2. Целостность. ЭЦП позволяет обнаружить любые, даже малейшие, изменения в документе, сделанные после его подписания. Если документ был изменен, проверка подписи не пройдет. Это отвечает на вопрос: “Был ли документ изменен?”.
3. Неотрекаемость (Non-repudiation). Подписавшее лицо не может впоследствии отказаться от факта подписания документа, так как только оно должно обладать уникальным закрытым ключом. Эта функция обеспечивает доказательную силу подписи.

Принцип работы ЭЦП на простом примере

Основой ЭЦП является асимметричная криптография, которая использует связанную пару ключей: закрытый и открытый.

• Закрытый ключ — это секретный, известный только владельцу код, который хранится в строгой тайне и используется для создания подписи. Аналогия: уникальный оттиск вашей личной печати или ручка, которой только вы можете подписаться.

• Открытый ключ — это доступный всем желающим код, который используется для проверки подписи. Аналогия: специальная лупа, позволяющая любому убедиться в подлинности оттиска вашей печати.

Упрощенная схема работы:

1. Формирование подписи (на стороне отправителя). Исходный электронный документ пропускается через специальную математическую функцию (хеш-функцию), которая преобразует его в короткую уникальную строку фиксированной длины — хеш (или “слепок” документа). Этот хеш шифруется с помощью закрытого ключа отправителя. Результат этого шифрования и является электронной цифровой подписью. Подпись присоединяется к документу, и эта связка отправляется получателю.

2. Проверка подписи (на стороне получателя). Получатель получает документ и подпись. С помощью открытого ключа отправителя (который должен быть достоверным) получатель расшифровывает полученную подпись. В результате он получает исходный хеш, который отправитель вычислил на своем этапе. Далее получатель самостоятельно вычисляет хеш от полученного документа по тому же алгоритму. Если хеш, полученный после расшифровки подписи, идентичен хешу, вычисленному получателем, значит: Подпись подлинная (ее создал владелец закрытого ключа). Документ не был изменен (целостность сохранена).

ЭЦП обеспечивает надежную и юридически значимую защиту электронных документов, основанную на строгих математических принципах. Однако, как и любая система, она имеет уязвимости, анализ которых рассматривается в следующем разделе.

Классификация и механизмы атак на системы ЭЦП

Атаки на системы электронной цифровой подписи принято разделять на два фундаментальных класса [2]: криптографические, нацеленные на взлом математических алгоритмов, и социальные (или нефункциональные), эксплуатирующие человеческий фактор и уязвимости в процессах использования системы.

Адаптивная атака на основе выбранных сообщений

Аналогия: Представьте, что злоумышленник получил возможность приносить вам на подпись любые документы по своему выбору. Вы подписываете их, не видя подвоха. Изучая коллекцию ваших подлинных подписей на этих документах, злоумышленник анализирует манеру вашего почерка и уникальные элементы росчерка. Его цель — понять принцип создания подписи, чтобы впоследствии самостоятельно подделывать ваш автограф на любых других документах.

Техническая реализация: В данном сценарии злоумышленник взаимодействует с системой подписи, передавая ей для подписания произвольные электронные документы и получая корректные цифровые подписи. Ключевой особенностью является адаптивность: выбор каждого следующего документа зависит от анализа ранее полученных подписей. Таким образом, атакующий активно исследует алгоритм, пытаясь выявить скрытые зависимости или статистические закономерности. Конечной целью является обнаружение уязвимости, позволяющей либо вычислить закрытый ключ, либо разработать

метод подделки подписей для произвольных сообщений. Устойчивость современного алгоритма ЭЦП считается доказанной, если он успешно противостоит этой модели атаки.

Атаки, основанные на коллизиях хеш-функций

Данный тип атак направлен не на алгоритм подписи напрямую, а на его неотъемлемый компонент — хеш-функцию.

Коллизия 1-го рода (Экзистенциальная подделка)

Аналогия: Допустим, у вас есть официально заверенная копия паспорта. Злоумышленник методом бессистемного перебора пытается создать другой документ, который чисто случайно даст идентичный паспорту набор контрольных цифр. Если ему это удастся, то юридическая сила вашего паспорта условно распространится и на этот бессмысленный документ.

Техническая реализация: Атакующий, имея валидную подпись для одного документа, пытается найти любой другой документ, который даст идентичный хеш. Если такая коллизия будет найдена, подпись окажется корректной и для второго документа. Практическая ценность этой атаки невелика, так как найденный документ с высокой вероятностью будет представлять собой семантически бессмысленную последовательность данных.

Коллизия 2-го рода (Выборочная подделка)

Аналогия: Мошенник заранее изготавливает два разных, но осмысленных документа, которые сконструированы так, что их контрольные цифры идентичны. Он предоставляет вам на подпись только один из них. Подписав его, вы автоматически придаете юридическую силу и второму документу.

Техническая реализация: Это целенаправленный поиск коллизии, при котором атакующий находит два заранее выбранных осмысленных сообщения с идентичным

хешем. Для криптографически слабых хеш-функций существуют эффективные методы нахождения таких пар. Классическим примером является атака на алгоритм MD5, когда исследователи продемонстрировали возможность создания двух различных SSL-сертификатов с одинаковой цифровой подписью, что позволяло генерировать фальшивые, но верифицируемые как подлинные, сертификаты. Это наглядный урок о том, что криптографические стандарты не вечны. Они должны постоянно тестироваться и обновляться по мере роста вычислительных мощностей и развития методов криптоанализа. После демонстрации атак MD5 был повсеместно признан устаревшим и небезопасным для использования в критически важных приложениях. Его место заняли более стойкие алгоритмы, такие как SHA-256 и SHA-3.

Социальные и инфраструктурные атаки

Несмотря на криптографическую стойкость современных алгоритмов, значительная доля успешных атак реализуется через эксплуатацию уязвимостей в сопутствующей инфраструктуре и процедурах использования. Данный класс угроз обходит математические механизмы защиты, нацеливаясь на организационные недостатки и человеческий фактор.

Компрометация закрытого ключа

Суть атаки: Наиболее прямолинейный способ обхода защиты, заключающийся в получении несанкционированного доступа к секретному криптографическому материалу.

Механизм реализации: Закрытый ключ, будучи основой безопасности, часто хранится в виде файла на рабочей станции пользователя, защищенного программным паролем. Атакующий может извлечь этот ключ следующими способами:

1. Внедрение вредоносного программного обеспечения (клавиатурные шпионы, трояны);
2. Получение физического доступа к носителю информации;
3. Использование уязвимостей в операционной системе или криптографическом ПО.

Подмена открытого ключа

Суть атаки: Нарушение корректности процесса верификации подписи путем фальсификации открытого ключа, используемого для проверки.

Механизм реализации: Атака нацелена на инфраструктуру открытых ключей (Public Key Infrastructure, PKI). Злоумышленник может:

1. Скомпрометировать сервер репозитория открытых ключей или службы каталогов;
2. Сгенерировать поддельный сертификат, имитирующий легитимного владельца;
3. Внести изменения в хранилище доверенных корневых сертификатов на компьютере жертвы.

В результате, документ, подписанный атакующим своим собственным закрытым ключом, будет успешно проходить процедуру проверки с использованием подмененного открытого ключа, что приведет к ошибочному признанию его подлинности.

Злоупотребление протоколами слепой подписи

Суть атаки: Использование легитимных криптографических протоколов, предназначенных для обеспечения анонимности, для мошеннического получения подписи без информирования подписывающей стороны о содержании документа.

Механизм реализации: В рамках протокола слепой подписи (например, протокол Чаума) атакующий выполняет следующую последовательность действий:

1. Исходное сообщение маскируется с помощью специального коэффициента (фактора ослепления), преобразуясь в неразличимую последовательность данных.
2. Ослепленное сообщение передается подписывающей стороне, которая, не зная его содержания, применяет к нему свою электронную подпись.
3. Получив подписанное ослепленное сообщение, злоумышленник применяет обратную процедуру (снятие ослепления), получая в итоге валидную цифровую подпись для исходного, скрытого от жертвы документа.

Данная атака опасна тем, что позволяет получить легальную подпись для документа, который подписывающая сторона никогда не одобрила бы при явном ознакомлении с его содержимым.

Заключение

Анализ современных атак на системы ЭЦП наглядно демонстрирует фундаментальный принцип криптографии - не существует вечных алгоритмов. Каждая криптографическая система имеет ограниченный срок жизненного цикла, определяемый как развитием вычислительных мощностей, так и прогрессом в методах криптоанализа. История уязвимостей алгоритмов MD5 и SHA-1 служит убедительным доказательством того, что даже широко распространенные и проверенные временем стандарты со временем теряют свою надежность.

Это обусловливает необходимость постоянного совершенствования систем электронной подписи по нескольким направлениям: переход на более стойкие алгоритмы хеширования, развитие защищенных методов хранения ключей, усиление инфраструктуры PKI и разработка новых криптографических протоколов. Только при условии непрерывного развития и адаптации к новым угрозам системы ЭЦП могут сохранять свою надежность и соответствовать требованиям цифровой эпохи.

Библиографическая справка

[1] Статья «Электронная подпись»

[2] https://www.tsutmb.ru/nauka/internet-konferencii/2019/aktualnye_problemy/5/Anosovich.pdf