Сертификация в телекоммуникационных сетях.

В.В. Сырин,
vitaliy@rmg.ru

Введение.

Реализация защищённых транзакций в телекоммуникационной среде требует решения таких задач как обеспечение конфиденциальности, целостности транспортируемого сообщения, идентификация и аутентификация второй стороны, и проверка её авторизованности. Конфиденциальность сообщения достигается применением средств шифрования. Наиболее распространёнными из них являются системы с использованием симметричного и асимметричного ключа шифрования. Целостность транспортируемого сообщения достигается применением средств электронной подписи.

Идентификация и аутентификация довольно важные и сложные в своём решении задачи. Телекоммуникационная среда не позволяет иметь визуального контакта для подтверждения, что вторая сторона именно та за которую она себя выдаёт. Без однозначного решения задач идентификации и аутентификации не возможно так же проверить авторизованность второй стороны.

Обмен шифрованными сообщениями требует распространение ключей шифрования. Системы с симметричной системой шифрования нуждаются в обеспечении высокого уровня безопасности при распространении ключа, так как его компрометация повлечёт за собой полное раскрытие информации двухстороннего обмена. Поэтому в настоящее время наиболее используемыми стали системы с асимметричным ключом шифрования. В такой системе открытый ключ может распространяться свободно, так как не существует зависимости между открытым ключом для шифрования сообщения и закрытым для его дешифрования, который хранится только у получателя сообщения. Получив открытый ключ по телекоммуникационной среде можно установить шифрованный двусторонний обмен сообщениями, но сам по себе открытый ключ не гарантирует, что он принадлежит именно тому, именем которого вторая сторона себя могла идентифицировать.

Системы электронной подписи основаны на алгоритмах с открытым ключом шифрования. Здесь так же возникает проблема с идентификацией второй стороны, от которой получен открытый ключ для проверки электронной подписи.

Одним из решений перечисленных выше проблем, идентификация сторон и распространение открытых ключей, является применение цифровых сертификатов. Система цифровых сертификатов основана на том, что существует третья сторона, которая выпускает сертификаты,

проводит идентификацию стороны запросившей сертификат и тем самым является гарантом достоверности информации о владельце сертификата.

Задачей данной статьи является обзорный анализ существующих алгоритмов, принципов реализации, построения систем сертификации, рассмотрение эффективности и безопасности работы этих систем в телекоммуникационных сетях. А так же поиск уязвимых мест в алгоритмах и системах сертификации, поиск тех областей в данной тематике, которые требуют дополнительных исследований и доработки.

Регистрация сертификата и его использование.

В узком смысле слова сертификаты предназначены для удостоверения асимметричного открытого ключа.

Процесс создания сертификата и его использования можно представить несколькими этапами:

- Безопасно создаются асимметричные открытые и секретные ключи.
- Секретный асимметричный ключ передается его владельцу.
- Открытый асимметричный ключ помещается в базу данных и администрируется центром выдачи сертификатов (Certification Authority или CA).
- На основе открытого асимметричного ключа создаётся сертификат пользователя.
- Для сертификата ставится цифровая подпись центра выдачи сертификатов с помощью вычисления его хэш-функции. Полученное значение шифруется с использованием асимметричного секретного ключа цифровой подписи CA, а затем полученная строка символов добавляется к сертификату. Цифровая подпись CA необходима, так как процесс распространения сертификатов уязвим к атаке, в ходе которой атакующий вмешивается во взаимодействие между отправителем и получателем и может модифицировать трафик, передаваемый между ними. Поэтому открытый асимметричный ключ получателя "подписывается" CA. Это означает, что CA использовал свой асимметричный секретный ключ для шифрования асимметричного открытого ключа получателя. Только CA знает асимметричный секретный ключ CA, поэтому есть гарантии того, что открытый асимметричный ключ получателя получен именно от CA.
- Сформированный сертификат передаётся его владельцу.
- Создается электронная подпись для сообщения транзакции с помощью вычисления его хэш-функции. Полученное значение шифруется с использованием асимметричного секретного ключа цифровой подписи отправителя, а затем полученная строка символов добавляется к передаваемому сообщению.

- Отправитель запрашивает у CA сертификат асимметричного открытого ключа шифрования получателя и при получении, проводит идентификацию CA и проверку целостности сертификата. Расшифровывается хэш-функция сертификата с использованием открытого ключа CA. Повторно вычисляется хэш-функция содержимого сертификата и две эти хэш-функции сравниваются для проверки того, что сертификат не был изменен.
- С помощью асимметричного открытого ключа шифрования получателя сообщение шифруется и передаётся ему.
- Получатель сообщения расшифровывает сообщение с помощью своего асимметричного секретного ключа шифрования.
- Получатель запрашивает у CA сертификат асимметричный открытый ключ цифровой подписи отправителя.
- Проводит идентификацию CA и проверку целостность сертификата способом описанным выше.
- С помощью асимметричный открытый ключ цифровой подписи отправителя проводит идентификацию отправителя и целостность полученного сообщения. [5]

Обслуживание цифровых сертификатов и протоколы.

Основным компонентом центра выдачи сертификатов CA является сервер цифровых сертификатов. Серверы цифровых сертификатов реализуются по-разному, но все они преследуют одну цель - подпись и распространение цифровых сертификатов защищенным образом. Поэтому, как правило, сервер цифровых сертификатов представляет собой защищенную систему каталогов, организованную, например, по протоколу X.500 или LDAP (Lightweight Directory Access Protocol).

Подавляющее большинство существующих серверов сертификатов совместимо со стандартом X.509 CCITT (теперь ITU). Такие сервера имеют иерархическую структуру. Другая ветвь основана на PGP серверах. Они также могут иметь иерархическую структуру и применяют шифрование PGP, но их также можно использовать в одноранговой среде - такой метод более гибок, чем строгий иерархический подход.

Серверы X.509 могут генерировать сертификаты для клиентов и серверов. Клиентские сертификаты, как правило, применяются в электронной почте, а серверные - в SSL-соединениях. При обнаружении нового сертификата пользователю выдается запрос, и при удовлетворительном ответе сертификат сохраняется для последующих соединений.

Аналогичным образом работают и серверы PGP, но они используют сертификаты одного типа и не поддерживают сертификатов X.509. Сертификат PGP обычно хранится в "связке"

сертификатов (keyring). Клиент PGP работает с двумя "связками" - одной общей (public), другой частной (private). Частная "связка", как правило, содержит секретные ключи, используемые для шифрования и цифровых подписей. Сертификаты общей связки применяются для шифрования/проверки отправляемой или получаемой информации. Сервер PGP выполняет для клиента роль хранителя общей "связки". В отличие от системы X.509, клиент PGP может создавать свои пары ключей и сертификаты. Это позволяет двум пользователям с клиентами PGP генерировать собственные ключи друг для друга и обмениваться их открытой частью, а затем посылать снабженную подписью или зашифрованную электронную почту без участия сервера сертификатов. [2]

К одной из задач CA относится ответственность за ведение и публикацию списка недействительных сертификатов (Certificate Revocation List, CRL). Сертификат может быть объявлен недействительным, например, в результате компрометации асимметричного секретного ключа или смены работы его владельца. В списки CRL не включают просроченные сертификаты, поскольку дата срока действия указана в каждом сертификате. [4]

Структура сертификата.

Цифровой сертификат может содержать различную информацию; как правило, это открытый ключ и сведения о владельце (например, адрес электронной почты). Еще более важно, что цифровой сертификат включает в себя цифровую подпись на основе личного ключа уполномоченного по выдаче сертификатов CA. Подлинность сертификата можно проверить с помощью открытого ключа CA. Кроме того, цифровые сертификаты содержат серийный номер и дату окончания их действия.

На рисунке 1 приведена упрощённая структура сертификата, соответствующему стандарту X.509.

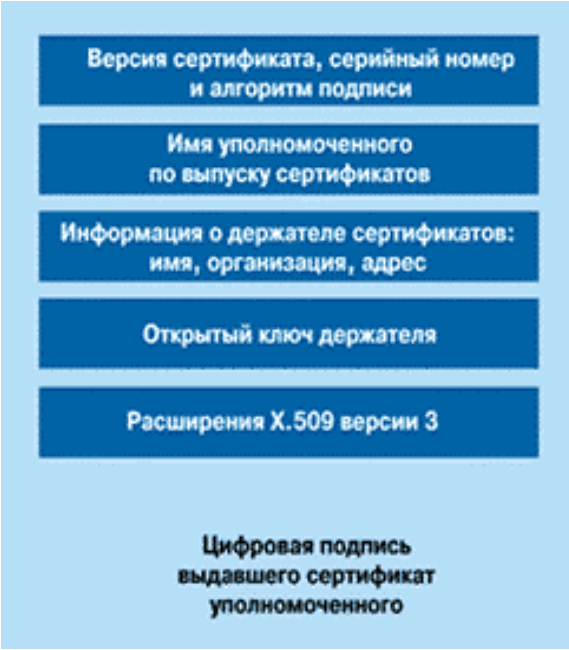

Рис. 1

Кроме того цифровой сертификат может принадлежать к одному из четырёх классов, указывающих на тип приложений, для которых он предназначен, и на уровень надежности.

Класс 1. Использование, например, при нерегулярных путешествиях по Web, отправке и получении шифрованной электронной почты. На этом уровне требуется уникальное имя или адрес электронной почты для выдачи Digital ID.

Класс 2. Использование при обмене электронной почтой внутри компании и в подписных интерактивных службах. На этом уровне идентичность частного лица должна быть подтверждена независимо.

Класс 3. Использование при обмене электронной почтой внутри компании, электронных банковских операциях, покупке дорогостоящих предметов и в членских интерактивных службах. На этом уровне частное лицо должно явиться лично или предоставить подтверждающие документы.

Класс 4. Использование при крупных финансовых операциях. На этом уровне CA наводит справки о частном лице или компании, запрашивающем ID. [4]

Заключение.

В настоящее время не существует единой глобальной системы сертификации. Создано множество разработок реализации работы с сертификатами для различных протоколов и сервисов в телекоммуникационных сетях.

Наиболее распространённой и давно использующей инфраструктуру цифровых сертификатов является электронная почта. Вложения электронной почты формата MIME (Multipurpose Internet

Mail Extension) шифруются средствами Secure/MIME (S/MIME) по технологии X.509 или средствами Pretty Good Privacy (PGP)/MIME по технологии PGP.

Широкое распространение также получили системы корпоративной сертификации. Организациям это позволяет, соблюдая конфиденциальность, работать внутри корпоративной intranet или extranet.

Использование систем сертификации распространено в столь популярной сегодня электронной коммерции, электронного банкинга и проведения иных финансовых операций в телекоммуникационных сетях.

Протокол SET, реализующий платёжную схему с использованием кредитных карт, также применяет для идентификации сторон и распространении открытых ключей систему сертификации на основе X.509. Элементом сертификата, служащий для идентификации заказчика является хеш-функция номера его кредитной карты. Так как сертификаты распространяются без шифрования, то использование хеш-функция вместо номера кредитной карты позволяет избежать компрометации и несанкционированного использования кредитной. [6]

Выводы.

Система сертификации решает одну из важных задач – идентификация второй стороны, что является неотъемлемой частью осуществления безопасных транзакций в телекоммуникационных сетях.

Как упоминалось ранее, не существует единой глобальной системы сертификации, что усложняет использование систем безопасности в глобальных телекоммуникационных сетях.

Остаётся ряд и других не решённых проблем с распространением сертификатов:

- X.509 подразумевает, что ключи безопасно раздаются, и не описывает способ решения этой проблемы - а только указывает на существование этой проблемы. Не существует стандартов для решения этого.

- Нет надежного способа проверить, между какими компьютерами осуществляется взаимодействие. Есть вид атаки, при котором атакующий маскируется под CA и получает данные, передаваемые в ходе взаимодействия. Для этого атакующему достаточно перехватить запрос к центру сертификации ключей и подменить его ключи своими. Эта атака может успешно продолжаться в течение длительного времени.

- Электронная подпись сертификата центром сертификации не всегда гарантирует их аутентичность, так как ключ самого CA может оказаться скомпрометированным. X.509 описывает способ электронной подписи ключей CA центрами сертификации ключей более высокого уровня и называет его "путь сертификации". X.509 рассматривает проблемы,

связанные с проверкой корректности открытого ключа, предполагая, что эта проблема может быть решена только при отсутствии разрыва в цепочке доверенных мест в распределенном справочнике открытых ключей пользователей. Нет способа обойти это.

- X.509 предполагает, что пользователь уже имеет доступ к открытому ключу CA. Как это осуществляется, в нем не определяется.

- Компрометация центра сертификации ключей весьма реальная угроза. Компрометация CA означает. Что все пользователи этой системы будут скомпрометированы. И никто не будет знать об этом. X.509 предполагает, что все ключи, включая ключи самого CA, хранятся в безопасном месте. Внедрение системы справочников X.509 (где хранятся ключи) довольно сложно, и уязвимо к ошибкам в конфигурации.

- CA могут оказаться узким местом. Для обеспечения устойчивости к сбоям X.509 предлагает, чтобы база данных CA была реплицирована с помощью стандартных средств X.500; это значительно увеличит стоимость криптосистемы. А при маскараде под CA будет трудно определить, какая система была атакована.

- Система справочников X.500 сложна в установке, конфигурировании и администрировании. Доступ к этому справочнику должен предоставляться, например, с помощью дополнительной службы подписки. Сертификат X.509 предполагает, что каждый человек имеет уникальное имя. Выделение имен людям - задача еще одной доверенной службы - службы именования.

Все перечисленные, не решённые проблемы можно отнести к двум классам:

- Проблемы целостности и безопасности сертификатов при распространении их по телекоммуникационным сетям. Существование этой проблемы связано с тем, что сертификаты распространяются порой по незащищённым телекоммуникационным сетям.
- Сложность организации и безопасности CA.

Решение этих проблем будет заключаться в разработка алгоритмов сертификации с учётом всех фаз генерации, распространения серификатов и стандартизации этих алгоритмов.

Литература.

1. Т. Купи Серверы сертификатов, или общение без страха. // Сети. – 1998, №9.
2. У. Вонг Обслуживание цифровых сертификатов. // LAN. – 1998, №7-8.
3. А. Карве Кто ты такой? // LAN, 1997, №3.
4. Д. Кузье Электронная коммерция.-М.: Русская Редакция, 1999.
5. Дж. Чандлер Введение в криптографию. - http://www.citforum.ru/internet/securities/crypto_1.shtml
6. Book 1: SET Secure Electronic Transaction Specification. Business Description. Version 1.0, 31 мая 1997.
7. Book 2: SET Secure Electronic Transaction Specification. Programmer’s Guide. Version 1.0, 31 мая 1997.
8. Book 3: SET Secure Electronic Transaction Specification. Formal Protocol Definition. Version 1.0, 31 мая 1997.