Управление ключами

Лекция по дисциплине
«Основы защиты информации»
доцента кафедры СПКБ
Гродненского государственного университета
имени Янки Купалы
к.т.н. Ливак Е.Н

Системы управления ключами

Проблема:

- для обмена зашифрованными сообщениями между двумя участниками криптосистемы необходимо, чтобы обоим участникам обмена были заранее доставлены тщательно сохраняемые в секрете ключи для шифрования и расшифрования сообщений.

✔ Обмениваться между собою зашифрованными сообщениями желают УДАЛЕННЫЕ пользователи.

Системы управления ключами

Проблема:

- для сети из N пользователей необходимо иметь одновременно в действии
  N * (N-1)/ 2 различных ключей
  (при N=1000 количество необходимых ключей близко к 50.000)

✔ Из соображений безопасности <u>секретные ключи должны меняться как можно чаще</u>

⇒ изготовление, упаковка и рассылка их с надежными курьерами из некоего абсолютно надежного центра становится задачей совершенно нереальной

Решение проблемы

Технология открытого распределения ключей

Public Key Infrastructure

Суть:

- ✔ пользователи самостоятельно с помощью датчиков случайных чисел генерируют свои индивидуальные ключи, которые хранят в секрете на своем носителе: дискете, специальной магнитной или процессорной карточке, таблетке энергонезависимой памяти

- ✔ затем каждый пользователь из своего индивидуального ключа вычисляет с помощью известной процедуры свой «открытый ключ», который он делает общедоступным для обмена конфиденциальными сообщениями.

Решение проблемы

1. Открытыми ключами пользователи могут обмениваться между собой непосредственно перед передачей зашифрованных сообщений

2. Поручить третьей стороне сбор всех открытых ключей пользователей в единый каталог

   - Администратор каталога должен заверить открытые ключи пользователей своей подписью и разослать этот каталог всем остальным участникам обмена.

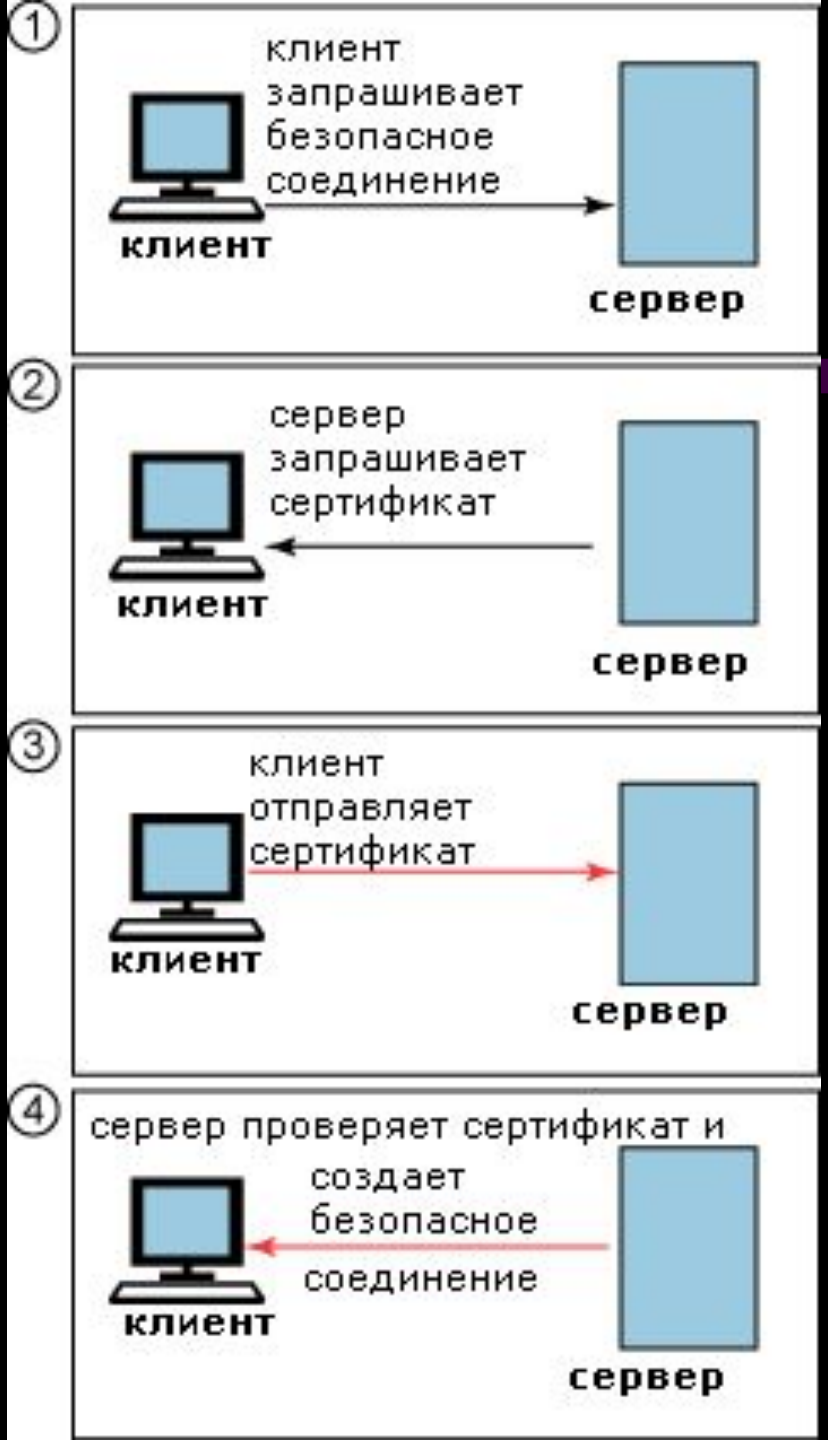
Службы администрирования открытых ключей называются

центрами сертификации Certificate authority (CA).

Примерами центров сертификации являются американские компании VeriSign, GTE.

Открытые ключи, заверенные ЦС, называют сертификатами

- ✔ X.509 — стандарт, описывающий формат и синтаксис сертификатов


1
клиент запрашивает безопасное соединение
клиент
сервер
2
сервер запрашивает сертификат
клиент
сервер
3
клиент отправляет сертификат
клиент
сервер
4
сервер проверяет сертификат и создает безопасное соединение
клиент
сервер

Обычно сертификаты хранятся

- как объекты службы каталогов
- или на специально выделенных для этого серверах

✔ В случае компрометации ключа или изменения данных самого сертификата сертификаты должны отзываться

✔ Главная задача сертификата — установить соответствие между пользователем и его открытым ключом

В состав полей сертификата стандарта X.509 входят:

- номер версии стандарта X.509;
- номер сертификата;
- идентификатор алгоритма ЭЦП;
- идентификатор сертификационной службы, выдавшей сертификат;
- идентификатор владельца сертификата;
- срок действия сертификата;
- сертифицируемый открытый ключ.

Цифровые сертификаты в основном применяются для двух целей:

- установить личность владельца;
- сделать доступным первичный ключ владельца

- Цифровой сертификат выпускается проверенной CA и выдается только на ограниченное время.
- После истечения срока действия сертификата его необходимо заменить

- В стандартном веб-браузере, который поддерживает SSL, в разделе security можно увидеть список известных организаций, которые "подписывают" сертификаты.

- Технически создать свою собственную CA достаточно просто, но также необходимо уладить юридическую сторону дела, и с этим могут возникнуть серьезные проблемы.

Public Key Infrastructure (PKI) - Инфраструктура Открытых Ключей

Этим термином описывается полный комплекс

- программно-аппаратных средств,
- а также организационно-технических мероприятий,

необходимых для использования технологии с открытыми ключами.

- Основным компонентом инфраструктуры является система управления цифровыми ключами и сертификатами.

Системы управления ключами

- Пакет PGP (компания PGP Филиппа Циммермана)

1) возможности шифрования сообщений симметричными блочными алгоритмами,
2) распределение симметричных ключей с помощью асимметричного алгоритма шифрования RSA,
3) создание электронных подписей сообщений.

Системы управления ключами

- Протокол Kerberos

(Массачусетский технологический институт)

1) Хранение личных ключей в защищенной БД. (Ключ известен только Kerberos и его владельцу)
2) Доверенный посредник между двумя абонентами, желающими обменяться секретными ключами.

Kerberos также предоставляет услуги аутентификации и рассылки ключей.

Системы управления ключами

Алгоритмы

- Diffie-Hellman
- KEA (Key Exchange Algorithm)