Криптографические протоколы

Лекция 3

Управление ключами

Жизненый цикл ключей

Деркач Максим Юрьевич

October 5, 2020

Ссылки

https://habr.com/post/154229/
https://habr.com/en/company/dataart/blog/262817/
https://en.wikipedia.org/wiki/Pass_the_hash

Управление ключами

Цель управления ключами

Цель управления ключами - нейтрализация следующих угроз:

1. компрометация конфиденциальности секретных ключей (СК).
2. компрометация аутентичности секретных ключей (СК) и открытых ключей (ОК).
3. несанкционированное использование секретных ключей (СК) и открытых ключей (ОК).

Управление ключами

Политика безопасности

Политика безопасности определяет:

1. угрозы, которым должна противостоять система;
2. правила и процедуры, которым необходимо руководствоваться в процессе управления ключами.
3. ответственность и подотчетность всех субъектов, участвующих в управлении ключами.
4. все виды записей, которые должны сохраняться.

Классификация ключей

Классификация ключей по значимости

1. **Главный ключ** - не защищается криптографическими средствами, а для защиты применяются физические или организационные средства/методы;
2. **Ключи шифрования ключей**;
3. **Ключи шифрования данных**.

Классификация ключей

Классификация ключей по сроку действия

1. **Ключи с длительным сроком действия**: главный ключ и ключи для шифрования ключей;
2. **Ключи с коротким сроком действия**: ключи для шифрования данных.

Жизненный цикл ключей

1. Регистрация пользователей системы;
2. Генерация ключей:
   - Генерация ключей пользователями.
   - Генерация ключей центром.
3. Установка ключей;
4. Регистрация ключей (связь ключа с пользователем с помощью сертификата);
5. Использование ключей.
6. Хранение ключа защиты;
7. Замена/обновление ключа: при истечении срока использования;
8. Архивирование ключа: ключ в дальнейшем не используется для шифрования данных или подписи, однако может быть использован для расшифрования старой информации;
9. Уничтожение ключа, в том числе информации по которой можно восстановить его;
10. Восстановление ключа, если ключ был удален, но не

Особенности управления ключами

Особенности управления ключами в симметричных к/с

- Большое количество ключей: хранить неудобно и небезопасно.
- Для сокращения объема информации у обычного пользователя можно применить дополнительное распределение ключей.
- Представление сертификата секретных ключей: $cert_A = E_{K_S}(K_{AS}, ID_A, t)$, где t - срок действия сертификата.
- Сертификат может храниться только у самого пользователя.

1. $A -> S : cert_A || E_{K_{AS}}(ID_B || M) || cert_B$
2. $S -> A : E_{K_{BS}}(M || ID_A)$
3. $A -> B : E_{K_{BS}}(M || ID_A)$

Особенности управления ключами

Особенности управления ключами в асимметричных к/с

- Получение участниками сертификата:
  - Пользователь сам генерирует пару ключей и запорашивает сертификат. ТДС проверяет уникальность ключа!!!. Сам пользователь несет ответственность за генерацию.
  - ТДС генерирует и создает сертификаты.
- Отзыв сертификата (добавить).
- Большое число сертификатов у конечного пользователя.