Технологии аутентификации (тезисы)

По материалам Шаньгин В.Ф. «Защита компьютерной информации. Эффективные методы и средства»

Идентификация

- Процедура распознавания пользователя по его идентификатору.

Аутентификация

- Процедура проверки подлинности заявленного пользователя, процесса либо устройства

Авторизация

- Процедура наделения полномочиями пользователя в пределах системы на основе правил и ограничений, установленных в ней.

Администрирование

- Регистрация действий пользователя в сети по правилам заданным в системе (доступ к ресурсам, действия с приложениями, история изменений и т. д.)

Группы методов аутентификации

- Методы, использующие пароли и коды
- Строгая аутентификация на основе криптоалгоритмов
- Биометрическая аутентификация
- Аппаратно-программные системы аутентификации

Методы, использующие пароли и коды

- Аутентификация на основе многоразовых паролей
- Аутентификация на основе одноразовых паролей
- Аутентификация на основе PIN-кода

Строгая аутентификация

- Строгая аутентификация на основе асимметричных криптоалгоритмов
  - Аутентификация на основе асимметричных алгоритмов
  - Аутентификация на основе электронной цифровой подписи
- Строгая аутентификация на основе симметричных криптоалгоритмов
  - Протоколы с симметричными алгоритмами шифрования
  - Протоколы на основе однонаправленных ключевых и хэш-функций

Биометрическая аутенитификация

- Дактилоскопические методы
- Методы на основе формы ладони
- Аутентификация по лицу
- Аутентификация по голосу
- Аутентификация по радужной оболочке глаза
  - По рисунку радужной оболочки
  - По кровеносным сосудам глаза
- Смешанные типы
  - Статические методы
  - Динамические методы

Аппаратно-программные системы аутентификации

- iButton («таблетка»)
- Контактные смарт-карты ISO7816(части 1-10)
- Радиочастотные идентификаторы
- Бесконтактные смарт-карты ISO/IEC 14443 и ISO/IEC 15693
- USB – ключи («токены»)

Основные атаки на протоколы аутентификации

- «Маскарад» - нарушитель выдает себя за легального пользователя системы
- Подмена стороны аутентификационного обмена (interleaving attack) – нарушитель участвует третьей стороной для подмены информации в сеансе обмена
- Повторная передача (replay attack) – повторная передача аутентификационных данных пользователем
- Принудительная задержка (forced delay) – перехват и передача информации спусты некоторое время
- Атака с выборкой текста (chosen text attack) – перехват траффика с целью получения информации о долговременных криптоключах

Методы защиты от атак на протоколы аутентификации

- Использование механизмов «запрос-ответ», меток времени, случайных чисел и идентификаторов, цифровых подписей
- Привязка результата аутентификации к дальнейшим действиям пользователя (использование секретных сеансовых ключей при дальнейшев взаимодействии)
- Дополнительная эвристическая аутентификация в рамках уже установленного сеанса