Криптографические протоколы

Лекция 4
Протоколы аутентификации: классификация, атаки
Протоколы "слабой" аутентификации

Деркач Максим Юрьевич

September 20, 2018

Ссылки

https://habr.com/post/154229/

Протоколы аутентификации

Определения

Определение 1
Аутентификация - подтверждение подлинности.

Определение 2
Идентификация - однозначное именование (присвоение уникальных имён или признаков) компонентов автоматизированной системы и всех лиц (пользователей), взаимодействующих с системой.

Определение 3
Протокол аутентификации - криптографический протокол, в ходе которого одна сторона удостоверяется в идентичности другой стороны, вовлеченной в протокол, а также убеждается в том, что вторая сторона активна во время или непосредственно перед моментом выполнения протокола.

Классификация аутентификации

+ По количеству доказывающих сторон:
  * одностороняя - доказывающая сторона A и проверяющая сторона B;
  * двустороняя - обе стороны A и B доказывают свою подлинность друг другу.

+ По устойчивости:
  * протоколы "слабой" аутентификации (на основе фиксированных или одноразовых паролей);
  * протоколы "сильной" аутентификации (на основе запроса типа "вопрос-ответ");
  * протоколы основанные на техники доказательства знания.

Цель протокола - установление того факта, что проверяемая сторона является той, за кого она себя выдаёт.

Возможны два исхода: подтверждение подлинности, не подтверждение.

Протоколы слабой аутентификации

Фиксированные пароли

$A -> S : ID_A || P$

Угрозы:

1. раскрытие пароля (разглашение, восстановление из системной информации);
2. перехват пароля (внутри системы);
3. угадывание пароля.

Атаки на фиксированные пароли:

1. повторное использование пароля;
2. тотальный перебор;
3. атака со словарём.

Фиксированные пароли

Приёмы повышения стойкости

1. Хранение в компьютерной системе файлов паролей в защищенном режиме (с защитой от чтения/записи).
2. Хранение в системе не самих паролей, а их образов.
3. Задание правил выбора паролей.
4. Ограничение попыток ввода пароля.
5. Добавление "соли" к паролю (добавление случайной величины к паролю перед обработкой его однонаправленной функцией).
6. Многофакторная аутентификация.

Фиксированные пароли

Многофакторная аутентификация

1. Смарт-карта
2. Электронный идентификатор
3. Биометрические аутентификаторы
4. SMS-аутентификация

Фиксированные пароли

Использование криптографических методов для повышения стойкости

На сервере обычно хранятся пароли в зашифрованном виде либо хэш от пароля.

1. $A -> S : ID_A$
2. $S -> A : R_S || text_A$
3. $A -> S : ID_A || h_1(R_S || h_2(p_A || text_A))$

где $ID_A, text_A, h_2(p_A||text_A)$ хранятся на проверяющей стороне(сервере).

Однако такой протокол неустойчив к атаке MITM и атаке параллельного сеанса.

Одноразовые пароли

1. Разделяемые списки одноразовых паролей: пользователь и система имеют заранее определенный список паролей, который каждый из них хранит самостоятельно. При выполнении очередного сеанса протокола аутентификации выбирается пользователем и проверяется системой очередной пароль из этого списка .
2. Последовательно обновляемые одноразовые пароли: Первоначально пользователь и система имеют только один пароль , условно с номером i. Затем пользователь создает и передает системе пароль под номером i-1, зашифрованный на ключе, вычисленном из i-го пароля. Такой метод затруднительно реализовать при ненадежном канале связи (при возможности обрыва связи).
3. Последовательности одноразовых паролей, основанные на однонаправленных функциях.

Одноразовые пароли

Схема Лэмпорта с одноразовыми паролями (RFC 1760 - The S/Key One-Time Password System)

На проверяющей стороне(сервере) хранятся $ID_A, h^n(p_A)$, где n - достаточно большое.

1. $A -> S : ID_A || h^{n-1}(p_A)$
2. Сервер вычисляет $h(h^{n-1}(p_A))$ и сравнивает с хранящимися данными, если совпало, то аутентификация пройдена успешна, и запись обоновляется на $ID_A || h^{n-1}(p_A)$.

S/Key

1. $A -> S : ID_A$
2. $S -> A : m$
3. $A -> S : h^{m-1}(p_A)$

Одноразовые пароли

Схема Лэмпорта с одноразовыми паролями (RFC 1760 - The S/Key One-Time Password System)

Существует атака

1. $A -> I(S) : ID_A$
2. $I(A) -> S : ID_A$
3. $S -> I(A) : m$
4. $I(S) -> A : m - 1$
5. $A -> I(S) : h^{m-2}(p_A)$
6. $I(A) -> S : h(h^{m-2}(p_A))$

Следующий раз

1. $I(A) -> S : ID_A$
2. $S -> I(A) : m - 1$
3. $I(A) -> S : h^{m-2}(p_A)$