Криптографические протоколы

Лекция 5

Протоколы сильной аутентификации

Деркач Максим Юрьевич

October 16, 2019

Ссылки

https://habr.com/post/154229/
https://habr.com/en/company/dataart/blog/262817/

Классификация протоколов сильной аутентификации

* на основе симметричных алгоритмов шифрования;
* на основе асимметричных алгоритмов шифрования;
* на основе ЭЦП.

Протоколы сильной аутентификации

На основе симметричных алгоритмов шифрования

ISO/ IEC 9798 - 2

1. $A -> B : text_2 || E_{K_{AB}}(T_A / N_A || ID_B || text_1)$
2. $B -> A : text_4 || E_{K_{AB}}(T_B / N_B || ID_A || text_3)$

1. $B -> A : R_B || text_1$
2. $A -> B : text_3 || E_{K_{AB}}(R_B || ID_B || text_2)$

1. $B -> A : R_B || text_1$
2. $A -> B : text_3 || E_{K_{AB}}(R_A || R_B || ID_B || text_2)$
3. $B -> A : text_5 || E_{K_{AB}}(R_B || R_A || text_4)$

Замечание Длина $ID_B || text_2$ не должна равняться длине $text_4$

Протоколы сильной аутентификации

На основе симметричных алгоритмов шифрования

Протокол Ву-Лама (Woo-Lam)

1. $A -> B : ID_A$
2. $B -> A : R_B$
3. $A -> B : E_{K_{AT}}(R_B)$
4. $B -> T : E_{K_{BT}}(ID_A || E_{K_{AT}}(R_B))$
5. $T -> B : E_{K_{BT}}(R_B)$

Протоколы сильной аутентификации

На основе симметричных алгоритмов шифрования

Атака параллельного сеанса

1 $I(A) -> B : ID_A$

1' $I -> B : ID_I$

2 $B -> I(A) : R_B$

2' $B -> I : R_B^*$

3 $I(A) -> B : E_{K_{IT}}(R_B)$

3' $I -> B : E_{K_{IT}}(R_B)$

4 $B -> T : E_{K_{BT}}(ID_A || E_{K_{IT}}(R_B))$

4' $B -> T : E_{K_{BT}}(ID_I || E_{K_{IT}}(R_B))$

5 $T -> B : E_{K_{BT}}(MYCOP)$

5' $T -> B : E_{K_{BT}}(R_B)$

Протоколы сильной аутентификации

На основе симметричных алгоритмов шифрования

Протокол Отвея-Риса

1. $A -> B : ID_A||ID_B||K_{AT}(ID_A||ID_B||N_A||R_A)||N_A$
2. $B -> T : ID_A||ID_B||K_{AT}(ID_A||ID_B||N_A||R_A)||$
   $K_{BT}(ID_A||ID_B||N_A||R_B)||N_A$
3. $T -> B : E_{K_{AT}}(K||R_A)||E_{K_{BT}}(K||R_B)||N_A$
4. $B -> A : E_{K_{AT}}(K||R_A)||E_K(R_A||R_B)||N_A$
5. $A -> B : E_K(R_B)$

Протокол с использованием хэш-функции

1. $B -> A : R_B||text_1$
2. $A -> B : text_3||H_{K_{AB}}(R_A||R_B||ID_B||text_2)$
3. $B -> A : text_5||H_{K_{AB}}(R_B||R_A||ID_A||text_4)$

Протоколы сильной аутентификации

На основе асимметричных алгоритмов шифрования

С использованием хэш-функции

1. $B -> A : h(R_B)||ID_B||E^{pub}_{K_A}(R_B||ID_B)$
2. $A -> B : R_B$

NSPK

1. $A -> B : E_{K^{pub}_B}(R_A||ID_A)$
2. $B -> A : E_{K^{pub}_A}(R_A||R_B)$
3. $A -> B : E_{K^{pub}_B}(R_B)$

Протоколы сильной аутентификации

На основе асимметричных алгоритмов шифрования

Атака параллельного сеанса NSPK

1 $A->I : E_{K_I^{pub}}(R_A||ID_A)$

1' $I(A)->B : E_{K_B^{pub}}(R_A||ID_A)$

2 $B->I(A) : E_{K_A^{pub}}(R_A||R_B)$

2' $I->A : E_{K_A^{pub}}(R_A||R_B)$

3 $A->I : E_{K_I^{pub}}(R_B)$

3' $I(A)->B : E_{K_B^{pub}}(R_B)$

Протоколы сильной аутентификации

На основе асимметричных алгоритмов шифрования

Защита

- 2 $B->A : E_{K_{\boldsymbol{A}}^{\boldsymbol{pub}}}(R_A||R_B||ID_B)$
- 3 $A->B : E_{K_{\boldsymbol{h(R_B)}}}(ID_B)$

Протоколы сильной аутентификации

С использованием ЭЦП

1. $A -> B$:
   $cert_A || T_A/N_A || ID_B || text_2 || sign_A(T_A/N_A || ID_B || text1)$
2. $B -> A$:
   $cert_B || T_B/N_B || ID_A || text_4 || sign_B(T_B/N_B || ID_A || text3)$

1. $B -> A : R_B || text_1$
2. $A -> B$:
   $cert_A || R_A || R_B || ID_B || text_3 || sign_A(R_A || R_B || ID_B || text_2)$
3. $B -> A$:
   $cert_B || R_B || R_A || ID_A || text_5 || sign_B(R_B || R_A || ID_A || text_4)$

Протоколы сильной аутентификации

С использованием ЭЦП

Атака

1. $I(B) -> A : R_B$
2. $A -> I(B) : cert_A||R_A||R_B||ID_B||sign_A(R_A||R_B||ID_B)$

1' $I(A) -> B : R_A$

2' $B -> I(A) : cert_B||R'_B||R_A||ID_A||sign_B(R'_B||R_A||ID_A)$

3. $I(B) -> A : cert_B||R'_B||R_A||ID_A||sign_B(R'_B||R_A||ID_A)$

Протоколы сильной аутентификации

Примеры[Аутентификация по сертификатам]

Сертификат представляет собой набор атрибутов, идентифицирующих владельца, подписанный certificate authority (CA).

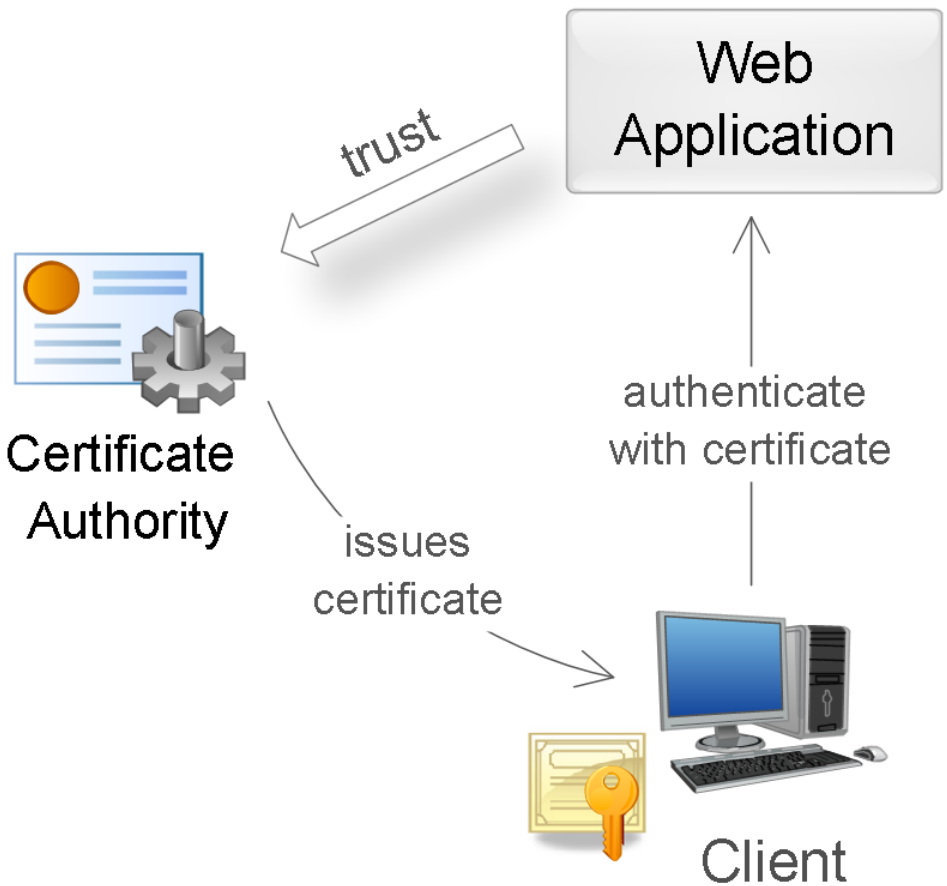
CA выступает в роли посредника, который гарантирует подлинность сертификатов.

Также сертификат криптографически связан с закрытым ключом, который хранится у владельца сертификата и позволяет однозначно подтвердить факт владения сертификатом.

Протоколы сильной аутентификации

Примеры[Аутентификация по сертификатам]

В веб-приложениях традиционно используют сертификаты стандарта X.509. Аутентификация с помощью X.509-сертификата происходит в момент соединения с сервером и является частью протокола SSL/TLS.



Протоколы сильной аутентификации

Примеры[Аутентификация по сертификатам]

Во время аутентификации сервер выполняет проверку сертификата на основании следующих правил:

1. Сертификат должен быть подписан доверенным certification authority (проверка цепочки сертификатов).
2. Сертификат должен быть действительным на текущую дату (проверка срока действия).
3. Сертификат не должен быть отозван соответствующим CA (проверка списков исключения).

Протоколы сильной аутентификации

Примеры[JWT]

JSON Web Token (JWT) — содержит три блока, разделенных точками: заголовок, набор полей (claims) и подпись.

Первые два блока представлены в JSON-формате и дополнительно закодированы в формат base64.

Набор полей содержит произвольные пары имя/значения, притом стандарт JWT определяет несколько зарезервированных имен (iss, aud, exp и другие).

Подпись может генерироваться при помощи и симметричных алгоритмов шифрования, и асимметричных.

{ «alg»: «HS256», «typ»: «JWT» }.
{ «iss»: «auth.myservice.com», «aud»: «myservice.com», «exp»: «1435937883», «userName»: «John Smith», «userRole»: «Admin» }.
S9Zs/8/uEGGTVVtLggFTizCsMtwOJnRhjaQ2BMUQhcY


SOMEONE FIGURED OUT MY PASSWORD,
NOW I HAVE TO RENAME MY DOG.