Криптографические протоколы

Лекция 7

Протоколы распределения ключей (Часть 1)

Деркач Максим Юрьевич

October 11, 2018

Ссылки

1. ISO/IEC 11770-1:2010 – Information technology – Security techniques – Key management – Part 1: Framework
2. ISO/IEC 11770-2:2008 – Information technology – Security techniques – Key management – Part 2: Mechanisms using symmetric techniques
3. ISO/IEC 11770-3:2008 – Information technology – Security techniques – Key management – Part 3: Mechanisms using asymmetric techniques
4. ISO/IEC 11770-4:2006 – Information technology – Security techniques – Key management – Part 4: Mechanisms based on weak secrets
5. СТБ 34.101.45-2013 "Информационные технологии и безопасность. Алгоритмы электронной цифровой подписи и транспорта ключа на основе эллиптических кривых". http://apmi.bsu.by/assets/files/std/bign-spec19.pdf
6. СТБ 34.101.60-2014 "Информационные технологии и безопасность. Алгоритмы разделения секрета". http://apmi.bsu.by/assets/files/std/bels-spec12.pdf

Протоколы распределения ключей

Определения и понятия

Определение 1

Протокол распределения ключей (key establishment protocol)- это криптографический протокол, в процессе выполнения которого общий секрет доступен двум или более сторонам для последующего использования в криптографических целях.

Протоколы распределения ключей подразделяются на два класса:

- протоколы транспортировки ключей,
- протоколы обмена ключами.

Определение 2

Протокол транспортировки ключей (key transport)- это протокол, распределения ключей, в котрых один участник создает или другим образом приобретает секрет и безопасным образом передает его другим участникам.

Определение 3
Протокол обмена ключами (key exchange) - это протокол, распределения ключей, в котрых общий секрет вырабатывается двумя или более участниками как функция от информации.

Классификация протоколов распределения ключей

- По типу выработки ключей:
  1. обновление ключей (key update) - выработка совершенно нового ключа, не зависищего от ключей выработанных в прошлых сеансах выполнения ппротокола;
  2. выработка производных ключей (key derivation) - выработка нового ключа на основе уже существующих у участников криптосистемы.

Протоколы распределения ключей

Определения и понятия

Классификация протоколов распределения ключей

- По типу :
  1. протоколы с предраспределенными ключами (key pre-distribution) - протоколы распределения, в которых результирующие ключи полностью определены априори начальным ключевым материалом (схемы разделения секрета);
  2. протоколы динамического распределения ключей (dynamic key establishment) - протоколы распределения, в которых ключи, вырабатываемые участниками, различны в различных сеансах протокола.
- По типу используемых криптосистем:
  1. симметричные;
  2. асимметричные.
- По количеству сторон:
  1. с участием "третьей стороны" (сервер аутентификации, центр распределения ключей, удостоверяющий центр и др.);
  2. без участия "третьей стороны".

Протоколы распределения ключей

ISO/IEC 11770-2

Mech. #2 (Однораундовый протокол)

1. $A -> B : E_{K_{AB}}(KS)$

A генерирует KS.

Mech. #1 (Однораундовый протокол)

TVP - переменная

1. $A -> B : TVP$
   $KS = f(K_{AB}, TVP)$, где f - одностороняя функция.

Mech. #3 (Однораундовый протокол)

1. $A -> B : E_{K_{AB}}(KS||T_A/N_A||ID_B)$

T_A/N_A - проверяет корректность момента времени или номера сессии.

ID_B - против атаки отражения.

Протоколы распределения ключей

ISO/IEC 11770-2

Mech. #4 (Двухраундовый протокол)

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

Mech. #4 (Модификация для двустороней аунтетификации)

1. $B -> A : R_B$
2. $A -> B : E_{K_{AB}}(KS||R_A||R_B||ID_B)$
3. $B -> A : E_{KS}(R_A)$

Mech. #6

K_A - часть ключа KS, которая принадлежит A.
K_B - часть ключа KS, которая принадлежит B.
$KS = f(K_A, K_B)$

1. $B -> A : R_B$
2. $A -> B : E_{K_{AB}}(K_A||R_A||R_B||ID_B)$
3. $B -> A : E_{K_{AB}}(K_B||R_A||R_B)$

Протоколы распределения ключей

ISO/IEC 11770-2

Mech. #5

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

Протоколы распределения ключей

Бесключевой протокол Шамира (Трёхпроходный протокол Шамира)

Коммутирующее шифрующее преобразование

$\forall M,\ K_1,\ K_2\ :\ E_{K_1}(E_{K_2}(M)) = E_{K_2}(E_{K_1}(M))$

$E_K(M) = M \oplus K$ - слабое преобразование.

$E_{K_A}(M) = M^a mod p$, где a - зависит от K_A, p - простое.

1. $A -> B : E_{K_A}(KS)$
2. $B -> A : E_{K_B}(E_{K_A}(KS))$
3. $A -> B : D_{K_A}(E_{K_B}(E_{K_A}(KS))) = E_{K_B}(KS)$

Отсутствует аутентификация, вместо B злоумышленник может вступить в протокол со своим ключом.

Протоколы распределения ключей

Трёхсторонние протоколы

Wide-Mouth-Frag

1. $A->S : ID_A||E_{K_{AS}}(T_A||ID_B||KS)$
2. $S->B : E_{K_{BS}}(T_S||ID_A||KS)$

Интервалы времени должны быть достаточно короткими.

Yahalom

1. $A->B : ID_A||R_A$
2. $B->S : ID_B||E_{K_{BS}}(ID_A||R_A||R_B)$
3. $S->A :$
$$m_a = E_{K_{AS}}(ID_B||KS||R_A||R_B)||$$
$$m_b = E_{K_{BS}}(ID_A||KS)$$
4. $A->B : m_b||E_{KS}(R_B)$

$E_{KS}(R_B)$ - нет проверки новизны.

Протоколы распределения ключей

Трёхсторонние протоколы

BAN-Yahalom

1. $A->B : ID_A||R_A$
2. $B->S : ID_B||R_B||E_{K_{BS}}(ID_A||R_A)$
3. $S->A : R_B||$
   $m_a = E_{K_{AS}}(ID_B||KS||R_A)||$
   $m_b = E_{K_{BS}}(ID_A||KS||R_B)$
4. $A->B : m_b||E_{KS}(R_B)$

Атака чередования сеансов и подмены типов

1. $I(A)->B : ID_A||R_A$
2. $B->I(S) : ID_B||R_B||E_{K_{BS}}(ID_A||R_A)$

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

2' $B->I(S) : ID_B||R'_B||E_{K_{BS}}(ID_A||(R_A||R_B))$

3. $-----------$
4. $I(A)->B : E_{K_{BS}}(ID_A||R_A||R_B)||E_{R_A}(R_B)$

Протоколы распределения ключей

Needham-Schroeder (NSSK)

1. $A -> S : ID_A || ID_B || R_A$
2. $S -> A : E_{K_{AS}}(R_A || ID_B || KS || E_{K_{BS}}(KS || ID_A))$
3. $A -> B : E_{K_{BS}}(KS || ID_A)$
4. $B -> A : E_{KS}(R_B)$
5. $A -> B : E_{KS}(R_B - 1)$

Протоколы распределения ключей

Протокол Деннинг - Сакко

1. $A -> S : ID_A || ID_B$
2. $S -> A : E_{K_{AS}}(ID_B || KS || T_S || E_{K_{BS}}(ID_A || KS || T_S))$
3. $A -> B : E_{K_{BS}}(ID_A || KS || T_S)$
4. $B -> A : E_{KS}(R_B)$
5. $A -> B : E_{KS}(R_B - 1)$

1. $A -> B : ID_A$
2. $B -> A : E_{K_{BS}}(ID_A || R_B)$
3. $A -> S : ID_A || ID_B || R_A || E_{K_{BS}}(ID_A || R_B)$
4. $S -> A : E_{K_{AS}}(R_A || ID_B || KS || E_{K_{BS}}(KS || R_B || ID_A))$
5. $A -> B : E_{K_{BS}}(KS || R_B || ID_A)$
6. $B -> A : E_{KS}(R'_B)$
7. $A -> B : E_{KS}(R'_B - 1)$

Протоколы распределения ключей

Rellare $K_{AS} = (K_{AS}^{C} || K_{AS}^{M})$

1. $A -> B : ID_A || R_A$
2. $B -> S : ID_A || ID_B || R_A || R_B$
3. $S -> A : E_{K_{AS}^{C}}(KS) || M_{K_{AS}^{M}}(ID_A || ID_B || R_A || E_{K_{AS}^{C}}(KS))$
4. $S -> B : E_{K_{BS}^{C}}(KS) || M_{K_{BS}^{M}}(ID_B || ID_A || R_B || E_{K_{BS}^{C}}(KS))$

Протокол Неймана - Стабалабайки

Этап 1

1. $A -> B : ID_A || R_A$
2. $B -> S : ID_B || E_{K_{BS}}(ID_A || R_A || T_B) || R_B$
3. $S -> A : E_{K_{AS}}(ID_B || R_A || KS || T_B) || E_{K_{BS}}(ID_A || KS || T_B) || R_B$
4. $A -> B : E_{K_{BS}}(ID_A || KS || T_B) || E_{KS}(R_B)$

Этап 2

1. $A -> B : R_A^{'} || E_{K_{BS}}(ID_A || KS || T_B)$
2. $B -> A : R_B^{'} || E_{KS}(R_A^{'})$
3. $A -> B : E_{KS}(R_B^{'})$

Протоколы распределения ключей

Атака 1 Этап 1

1. $I(A) -> B : ID_A || R_A$
2. $B -> I(S) : ID_B || E_{K_{BS}}(ID_A || R_A || T_B) || R_B$
3. $- - - - - - - - - - - - - - - -$
4. $I(A) -> B : E_{K_{BS}}(ID_A || R_A || T_B) || E_{R_A}(R_B)$

Этап 2

1. $I(A) -> B : R'_A || E_{K_{BS}}(ID_A || R_A || T_B)$
2. $B -> I(A) : R'_B || E_{R_A}(R'_A)$
3. $I(A) -> B : E_{R_A}(R'_B)$

Протоколы распределения ключей

Атака 2 Этап 1

1. $A->B : ID_A||R_A$
2. $B->S : ID_B||E_{K_{BS}}(ID_A||R_A||T_B)||R_B$
3. $S->A : E_{K_{AS}}(ID_B||R_A||KS||T_B)||E_{K_{BS}}(ID_A||KS||T_B)||R_B$
4. $A->B : E_{K_{BS}}(ID_A||KS||T_B)||E_{KS}(R_B)||E_{KS}(R_B)$

Этап 2

1. $I(A)->B : R'_A||E_{K_{BS}}(ID_A||KS||T_B)$
2. $B->I(A) : R'_B||E_{KS}(R'_A)$

1' $I(A)->B : R'_B||E_{K_{BS}}(ID_A||KS||T_B)$

2' $B->I(A) : R''_B||E_{KS}(R'_B)$

3. $I(A)->B : E_{KS}(R'_B)$

Протоколы распределения ключей

Протокол Отвея - Рисса

M - ID сеанса.

v - бит направленности.

1. $A->B : M||ID_A||ID_B||E_{K_{AS}}(vR_A||M||ID_A||ID_B)$
2. $B->S :$
   $M||ID_A||ID_B||E_{K_{AS}}(vR_A||M||ID_A||ID_B)||E_{K_{BS}}(R_B||M||ID_A||ID_B)$
3. $S->B : M||E_{K_{AS}}(R_A||KS)||E_{K_{BS}}(R_B||KS)$
4. $B->A : M||E_{K_{AS}}(R_A||KS)$

Протоколы распределения ключей

Атака 1

KS - 64 бита, M - 32 бита, ID_A, ID_B - 16 бит.

$len(KS) = len(M + ID_A + ID_A)$

1' $A->I(B) : M||ID_A||ID_B||E_{K_{AS}}(vR_A||M||ID_A||ID_B)$

4' $I(B)->A : M||E_{K_{AS}}(R_A||M||ID_A||ID_B)$

Атака 2

1. $A->B : M||ID_A||ID_B||E_{K_{AS}}(vR_A||M||ID_A||ID_B)$
2. $B->I(S) :$
   $M||ID_A||ID_B||E_{K_{AS}}(vR_A||M||ID_A||ID_B)||E_{K_{BS}}(R_B||M||ID_A||ID_B)$
3. $I(S)->B :$
   $M||E_{K_{AS}}(vR_A||M||ID_A||ID_B)||E_{K_{BS}}(R_B||M||ID_A||ID_B)$
4. $B->A : M||E_{K_{AS}}(vR_A||M||ID_A||ID_B)$

Протоколы распределения ключей

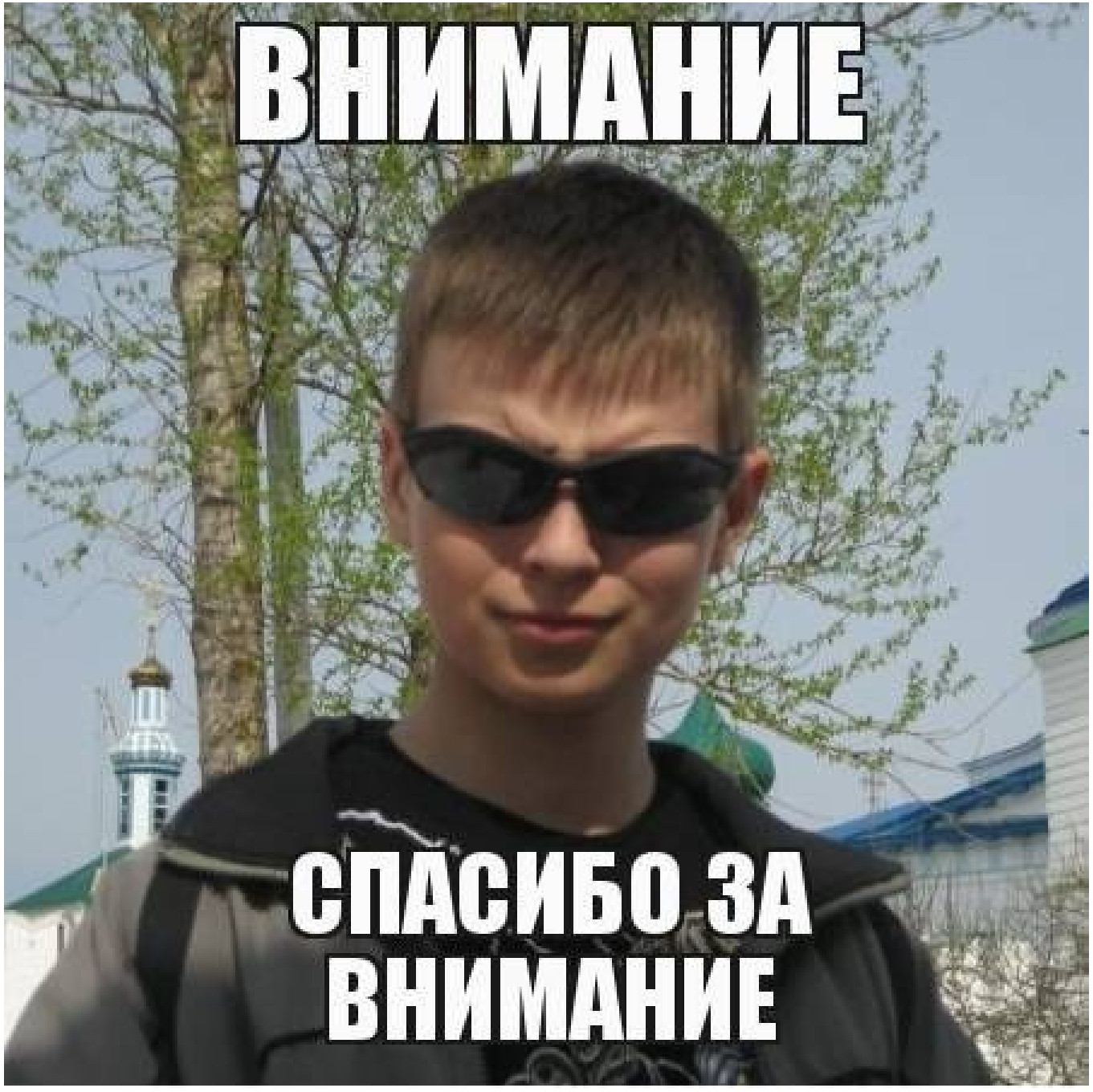
1. $A->S : TVP_A||ID_B||text$
2. $S->A :$
   $text_4||E_{K_{AS}}(TVP_A|KS||ID_B||text_3)||E_{K_{BS}}(T_S/N_S||KS||ID_A||text_2)$
3. $A->B :$
   $text_6||E_{K_{BS}}(T_S/N_S||KS||ID_A||text_2)||E_{KS}(T_A/N_A||ID_B||text_5)$
4. $B->A : text_5||E_{KS}(T_B/N_B||ID_A||text_2)$

1. $B->A : R_B||text_1$
2. $A->S : R'_A||R_B ID_B||tetx_2$
3. $S->A :$
   $text_5||E_{K_{AS}}(R'_A|KS||ID_B||text_4)||E_{K_{BS}}(R_B||KS||ID_A||text_3)$
4. $A->B :$
   $text_7||E_{K_{BS}}(R_B||KS||ID_A||text_3)||E_{KS}(R_A||R_B||text_6)$
5. $B->A : text_9||E_{KS}(R_B||R_A||tetx_8)$

Протоколы распределения ключей

Mech. #10

1. $A->S : TVP_A||ID_B$
2. $S->A :$
   $E_{K_{AS}}(TVP_A||KS||ID_B||text_1)||E_{K_{BS}}(T_S/N_S||KS||ID_A||text_2)||$
3. $A->B :$
   $E_{K_{BS}}(T_S/N_S||KS||ID_A||text_2)||E_{KS}(T_A/N_A||ID_B||text_3)$
4. $B->A : E_{KS}(T_B/N_B||ID_A||text_4)$


ВНИМАНИЕ
СПАСИБО ЗА ВНИМАНИЕ