Ежегодная международная научно-практическая конференция
«РусКрипто’2019»

Об одном способе противодействия MITM-атакам на основе протоколов, использующих общую память Отправителя и Получателя в модели секретной связи

Сорокин Илья Игоревич, спикер,
Магистрант кафедры «Информатика и защита информации»

Александров Алексей Викторович, науч. руководитель,
Доцент кафедры «Информатика и защита информации», к.ф.-м.н.

Владимирский государственный университет им. А.Г. и Н.Г. Столетовых

Постановка задачи

$F_k^{\pm 1}$ — функция шифрования / дешифрования

m = |k| — размер симметричного ключа шифрования

H_k — хэш-функция сильно сопротивляющаяся поиску коллизий

Общая память, стартовые значения

$D_A = \{d_1 \ldots, d_n\}$ $D_B = \{d_1 \ldots, d_n\}$

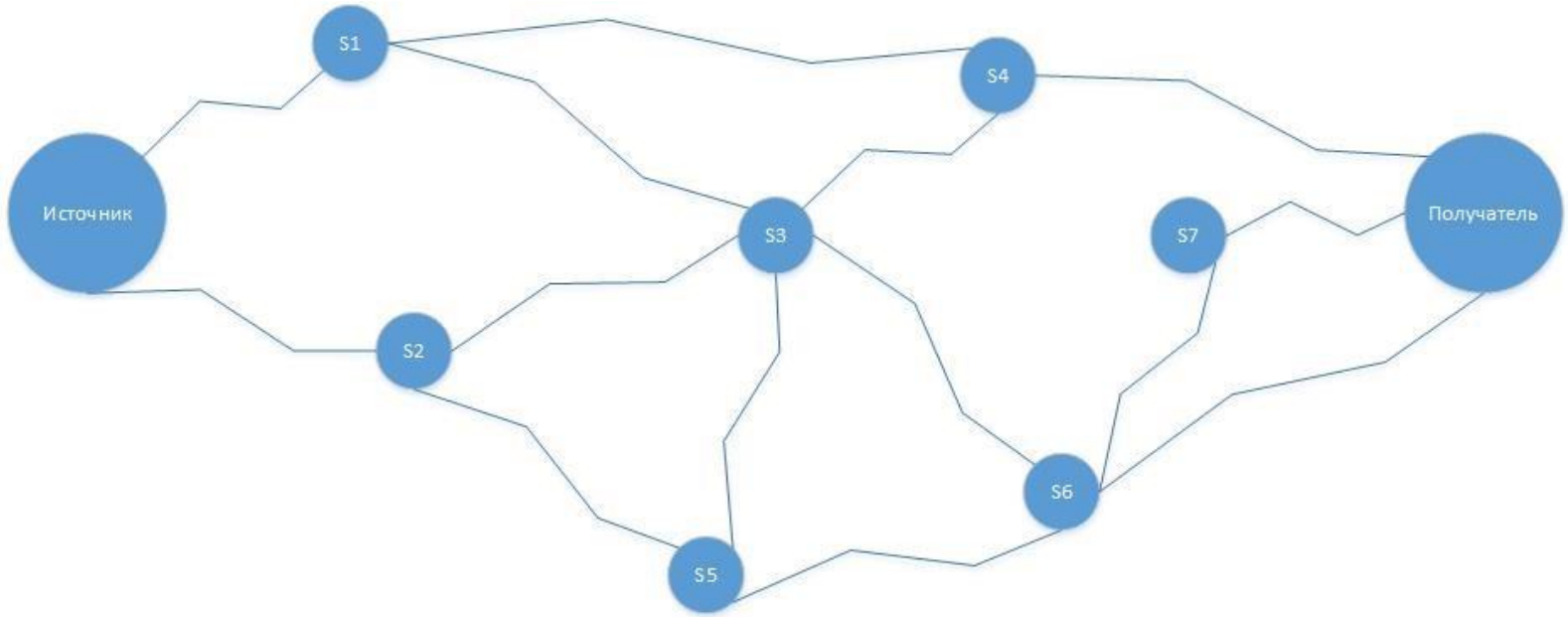
$D_A = D_B$ - аутентификатор канала связи

E ≠ 0 = $(e_1, .. e_n)$ – предварительный ключ

k = $\sum_{i=1}^{n} e_i d_i \ mod \ 2^m$ – сеансовый ключ

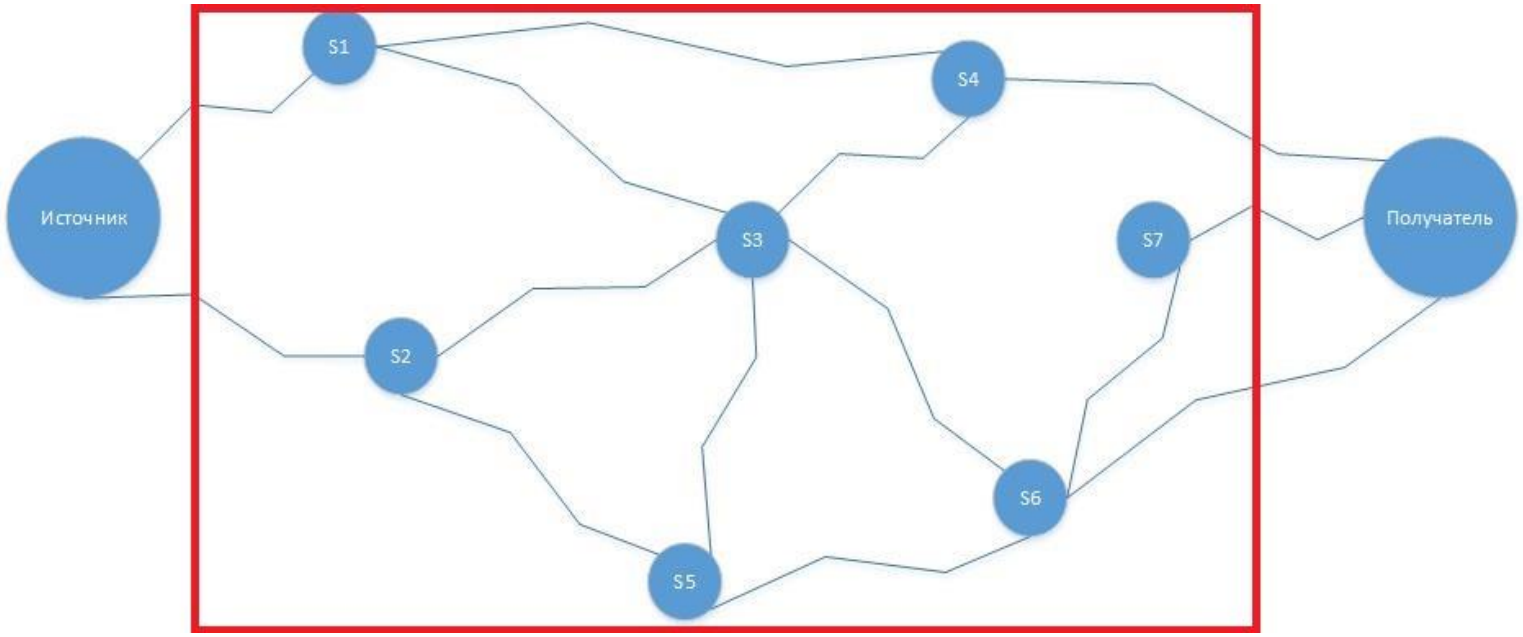
n < m; n ≥ 2

Модель Долева-Яо



- Модель включает в себя симметричную и асимметричную модели шифрования
- MITM-атака реализуется за счет слабости аутентификации

Возможности противника



- Противник не имеет доступа к носителям и устройству шифрования отправителя и получателя
- Противник не может угадывать случайные числа, выбранные из достаточно большого множества

$$k_{AB} = k_{BA} = \sum_{i=1}^{n} e_i d_i \ mod\ 2^m \ (1)$$

Обозначим E = $share_1(k)$;

D = $share_2(k)$;

Формула (1) – восстановления секрета в структуре доступа

P = {{A, B}, {A, B, C}}

N = {{A, C}, {B, C}, {A}, {B}, {C}, {Ø}}

Утверждение 1: Пусть множество ключей, которое можно получить формулой (1) обладает свойством $k_1, k_2 \ldots k_{2^m}, k_i \neq k_j, i \neq j$, тогда

$$\begin{cases} H(k_{AB} \mid \{E, D\}) = 0 \\ H(k_{AB} \mid \{E\}) = H(k_{AB}) - \delta \end{cases}$$

$$\delta < H(k_{AB})$$

Пересечение предварительных и сеансовых ключей

K = $\{k_1 \ldots, k_m\}$ - сеансовые ключи

|K| = 2^m - *мощность множества K*

E = $(e_1 \ldots, e_n)$ – предварительные ключи

|E| = 2^n - *мощность множества E*

$$\emptyset = K \cap E \quad (2)$$

Из утверждения 1 и (2) следует, что предварительный ключ можно передавать в открытую в канале связи.

С точки зрения СРС и утверждения 1 вес информации (2) - δ

Протокол создания симметричного ключа при пассивном противнике

1. $A \to B : E = \{e_1 ... e_n\} \neq 0$
2. $A : k_{AB} = \sum e_i d_i \bmod 2^m$
3. $B : k_{BA} = \sum e_i d_i \bmod 2^m$

Протокол создания симметричного ключа при активном противнике

Усиление протокола:

$H_{d_e}(S)$ – ключевая хэш-функция, d_e – предыдущий успешно сгенерированный сеансовый ключ по формуле k = $\sum_{i=1}^{n} e_i d_i \ mod \ 2^m$

Противник не может построить H_{d_e}, не зная ключа d_e — Утверждение 1.

Протокол создания симметричного ключа при активном противнике

1. $A \to B : E = \{e_1 ... e_n\} \| H^A_{d_e}(E)$
2. $B : H^B_{d_e}(E);\quad если \quad H^B_{d_e}(E) \neq H^A_{d_e}(E) \quad то \quad стоп$
3. $A : k_{AB} = \sum e_i d_i \bmod 2^m;\quad H^A_{d_e}(k_{AB})$
4. $B : k_{BA} = \sum e_i d_i \bmod 2^m;\quad H^B_{d_e}(k_{BA})$
5. $A \to B : H^A_{d_e}(k_{AB})$
6. $B : если \quad H^A_{d_e}(k_{AB}) = H^B_{d_e}(k_{BA}) \quad то \quad d_e \leftarrow k_{BA} \quad иначе \quad стоп$
7. $B \to A : Ok$
8. $A : Если \quad Ok \quad то \quad d_e \leftarrow k_{AB}$

Протокол передачи сообщения при активном противнике

1. $A \to B: f_k(S) \| H_k^A(S)$
2. $B: f_k^{-1}(S)$
3. $B:$ если $H_k^B(S) = H_k^A(S)$, то ОК

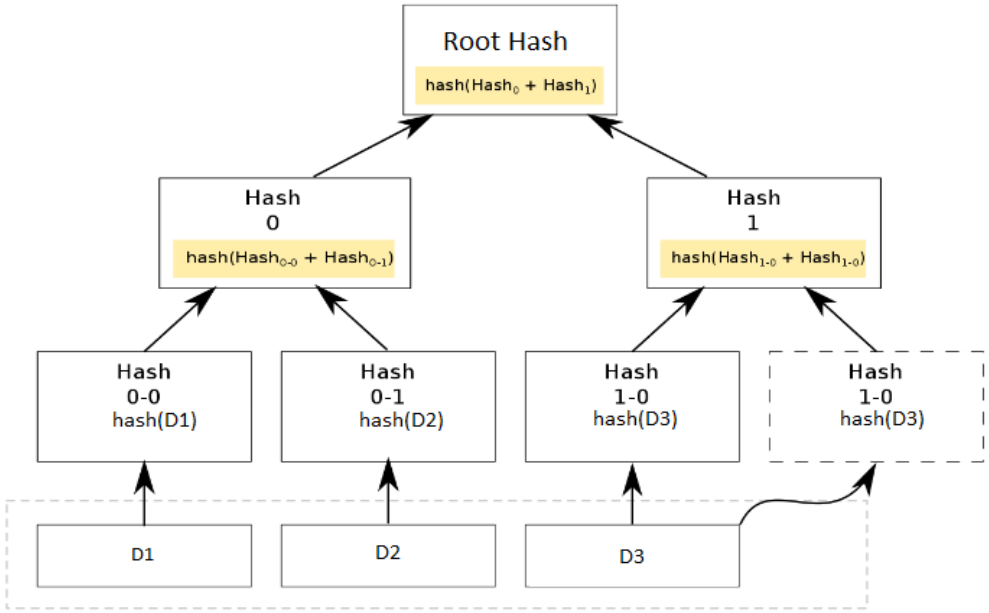
Процедура встраивания общей памяти в модель секретной связи

Вне канала связи:

1. Создаем общую память D_A=D_B. Сохраняем на устройствах. Защищаем от внешних изменений.
2. Создаем первоначальные предварительный и сеансовый ключи.
3. Создаем первоначальный хэш.

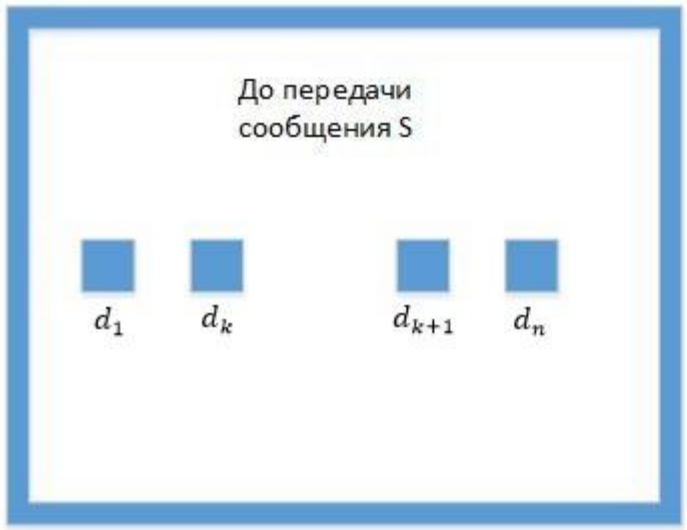
Контроль целостности общей памяти

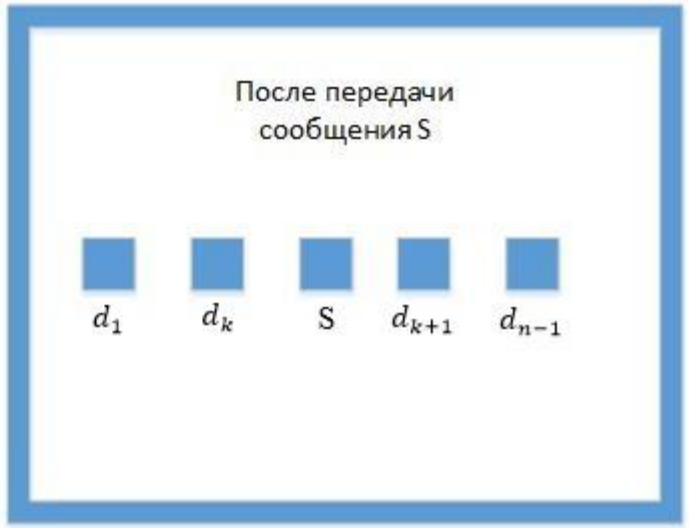
1. Построение дерева Дамгарда-Меркла (RDM)



2. Доказательство Меркла
3. С применением двустороннего протокола для отправителя и получателя построения RDM_x; x = {A, B} и доказательства Меркла обеспечивается целостность общей памяти.

Динамическая общая память





где $d_1..d_k$ - статическая компонента общей памяти

$d_{k+1}..d_n$ - динамическая компонента общей памяти, представленная в виде очереди

Динамическая общая память

Изменение общей памяти и RDM проводит к автоматическому изменению $k_{AB} = k_{BA} = \sum_{i=1}^{n} e_i d_i \ mod \ 2^m$ на следующих шагах генерации ключа, не передавая при этом предварительный ключ E = $(e_1,.. \ e_n)$

Классификация протоколов по IETF

Протокол	Свойство G_i														
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
TLS	×	×	×				×			×	×		×		
TLS-v1.1	×	×	×				×			×	×		×		
TLS-SPR	×	×	×				×			×	×		×		
TLS-sharedkeys	×	×	×				×			×	×		×		

Выводы

Предложенные протоколы:

- безопасны по отношению к пассивному и активному противнику в канале связи;
- удовлетворяют требованиям безопасных аутентифицированных протоколов обмена ключами;
- ограничены в повсеместном применении;
- могут использоваться в теории управления объектами, управлении на производстве, TLS протоколах и др. сферах;
- с использованием динамической общей памяти удается снять одну из проблем симметричной криптографии – генерация и передача симметричного ключа.

Контактная информация

Сорокин Илья Игоревич,
магистрант

Электронная почта:
night7117@mail.ru

Телефон:
+7 930 746-55-16

Сайт:
www.izi.vlsu.ru

Александров Алексей Викторович,
науч. руководитель

Электронная почта:
alex_izi@mail.ru

Телефон:
+7 999 710-16-36

Сайт:
www.izi.vlsu.ru