Об одном протоколе выработки общего ключа

Алексей Нестеренко

29 марта 2012 г.

Мотивация

Обеспечение защищенного канала связи
Протоколы выработки общего ключа (key agreement)

- Отсутствие рекомендованных/стандартизированные решений.
- TLS — решение де-факто. Вопрос, хорошее ли?
- Отсутствие требований к тому, что должно быть/хочется иметь.
- Не всегда ясно, как реализовывать протоколы так, чтоб они были стойкими.
- Отсутствие вариативности при решении конкретных задач.

Существующее множество решений

Математические модели: схемы Диффи-Хеллмана, семейство схем MTI, схемы Блома.

Уровень реализации:

- транспортный уровень IKE, Oakley (IPSec), EAP-TLS (IEEE 802.11 WiFi).
- прикладной уровень: TLS, SSH.

Механизм аутентификации: цифровая подпись (удостоверяющие центры), симметричные ключи (предварительное распределение), доверенные центры (схемы Нидхема-Шрёдера, Kerberos).

Перечень пожеланий к стойкости протокола

1. Сложность компрометации вырабатываемого ключа.
2. Сложность определения долговременных ключей.
3. Защита от чтения вперед/назад.
4. Защита при компрометации долговременных ключей.
5. Подтверждение ключа.
6. Защита от навязывания ключа другому абоненту.
7. Защита от выработки ключа с третьим участником протокола.
8. Защита владельца скомпрометированного ключа (key compromise impersonation).

Новый протокол: основные характеристики

Цель	Выработка общего ключа шифрования.
Уровень	Прикладной уровень (поверх TCP).
Схема	Схема Диффи-Хеллмана.
Группа	Группа точек эллиптической кривой над $\mathbb{F}_p$.
Длина вырабатываемого ключа	256 бит.
Аутентификация (долговременные ключи)	Ключи ЦП, ГОСТ Р 34.10.
Количество пересылаемых сообщений	6.
Блочное шифрование	Алгоритм ГОСТ 28147-89.
Анализ	начиная с 2007 г. по н.вр.
Апробация	Модуль сервера Apache (2008 г.), сервер на основе e-poll (2012 г.).

Новый протокол: первый этап

Обмен параметрами, выработка идентификаторов сеанса

Клиент (I_a)		Сервер (I_b)
$N_a \in_R$,		
$text_1 = AlgList \|\| Cert_a$,	$\xrightarrow{m_1}$	
$s_1 = Sign_a(h_1 \|\| N_a \|\| I_a \|\| text_1 \|\| I_b)$,		
$m_1 = (h_1 \|\| N_a \|\| I_a \|\| text_1 \|\| s_1)$.		
		$N_b \in_R$,
		$text_2 = RetList \|\| Cert_b$,
	$\xleftarrow{m_2}$	$s_2 = Sign_b(h_2 \|\| N_a \|\| I_a \|\| text_1 \|\| I_b \|\| N_b \|\| text_2)$,
		$m_2 = (h_2 \|\| N_b \|\| text_2 \|\| s_2)$.

Новый протокол: второй этап I

Выработка и подтверждение ключа.

$$k_a, R_a = Kex(),$$
$$s_3 = Sign_a(h_3||N_a||N_b||I_a||I_b||R_a), \quad \xrightarrow{m_3}$$
$$m_3 = (h_3||R_a||s_3).$$

$$k_b, R_b = Kex(), \quad Q = [k_b]R_a,$$
$$K_{ab} = Kdf(Q, N_a, N_b, \ldots),$$
$$\xleftarrow{m_4} \qquad text_3 \in_R, \quad ET_1 = Enc(X_{ab}, text_3),$$
$$s_4 = Sign_b(h_4||N_a||N_b||I_a||I_b||R_a||R_b||text_3),$$
$$m_4 = (h_4||R_b||ET_1||s_4).$$

$$\text{Kex}() = \{k, R\}, \quad R = [k]P = \underbrace{P + \cdots + P}_{k}.$$

Новый протокол: второй этап II

$$Q = [k_a]R_b,$$
$$K_{ab} = Kdf(Q, N_a, N_b, \ldots),$$
$$text_3 = Enc(X_{ab}, ET_1),$$
$$text_4 \in_R, \quad ET_2 = Enc(X_{ab}, text_4),$$
$$s_5 = Sign_a(h_5||N_a||N_b||I_a||I_b||R_a||R_b||text_3||text_4),$$
$$m_5 = (h_5||ET_2||s_5).$$

$$\xrightarrow{m_5}$$

$$\xleftarrow{m_6}$$

$$text_5 = \text{готов к приему/передаче данных}$$
$$s_6 = Sign_b(h_6||N_a||N_b||I_a||I_b||R_a||R_b||text_3||text_4||text_5),$$
$$m_6 = (h_6||text_5||s_6).$$

на втором этапе можно выполнять протокол: запрос/ответ, например, HTTPS.

Анализ: отличительные особенности протокола

- Уникальные идентификаторы для каждого сеанса.
- Разная длина сообщений.
- Единственная передача данных.
- *Двусторонняя аутентификация* и наличие кода целостности/аутентификации в каждом сообщении.
- Наличие кода целостности/аутентификации.
- Включение всех переданных ранее данных в код аутентификации.
- Подтверждение выработанного ключа: вариант блочное шифрование + цифровая подпись.

Анализ: выполнение требований

Стойкость протокола: трудоемкость решения задачи DL в группе точек эллиптической кривой

Выбор параметров кривых: сложность сравнима с сложностью атаки на блочный шифр.

Защита от чтения вперед/назад	да
Защита при компрометации долговременных ключей	да
Защита от выработки ключа с третьим участником протокола	да
Отсутствие навязывания ключевых значений	да
Защита владельца скомпрометированного ключа	да

Заключение

Предложения в ТК-26.

- Необходима нормативная база/стандартизированное решение для протоколов ОРК.
- Целесообразно стандартизировать перечень из нескольких протоколов.
- Возможно, необходимо регламентировать требования к реализации протоколов.
- Предложенный протокол может быть включен в указанный перечень.