

Криптографические протоколы

Лекция 2

Атаки на протоколы

Деркач Максим Юрьевич

November 12, 2019

http://journals.tsu.ru/pdm2/&journal_page=archive&id=1139&article_id=18544
<https://habr.com/ru/post/475218/>
<https://prosecco.gforge.inria.fr/personal/bblanche/proverif/>

Определение 1

Атака - попытка проведения анализа сообщений протокола и(или) выполнения непредусмотренных протоколом действий в целях нарушения работы протокола и(или) получения информации, составляющей секрет участников протокола.

Атака успешна, если нарушена безопасность протокола, в том числе:

- ▶ срыв выполнения протокола;
- ▶ получение секретной информации нарушителем;
- ▶ нарушение аутентификации сторон.

Определение 2

Компрометация протокола - это ситуация, когда протокол не способен достичь тех целей, для которых он предназначен, причем противник получает преимущество только путем манипуляции протоколом.

Классификация атак по типу направленности

1. атаки направленные на криптографические алгоритмы;
2. атаки направленные на криптографические методы;
3. атаки направленные на криптографические протоколы.

Противники подразделяются на следующих два класса

- ▶ пассивные противники - они могут перехватывать сообщения, пересылаемые участниками протокола, и анализировать их;
- ▶ активные противники - они могут делать то же, что и пассивные противники, а также:
 1. модифицировать или удалять перехваченные сообщения;
 2. генерировать новые сообщения и посылать их участникам протокола;
 3. выдавать себя за участников протокола.

Основные классы атак на протоколы

1. Атака посередине (MitM):

Класс атак, в котором злоумышленник ретранслирует и изменяет сообщения, проходящие между участниками протокола, причем последние не знают о существовании злоумышленника, считая, что общаются непосредственно друг с другом.

Пример: протокол Диффи-Хеллмана

Подтипы: **Атака подмены (Impersonation).**

2. Атака с повторной передачей (Replay Attack):

Класс атак, в котором злоумышленник записывает сообщения, проходящие в одном сеансе протокола, а далее повторяет их в новом, выдавая себя за одного из участников нового сеанса.

Пример: Бесключевой протокол Шамира (Lect. 7)

Подтипы: **Атака отражением (Reflection Attack),**

Задержка передачи сообщения (Forced Delay).

3. Атака подмены типа (Type Flaw Attack):

Класс атак, в котором злоумышленник используя переданные сообщения в легальном сеансе протокола, конструирует новое сообщение и передает его в новом сеансе по виду сообщения другого типа.

Пример: протоколы Wide-Mouth Frog, Деннинга-Сако, Yahalom, Отвея-Рисса (Lect. 7)

4. Атака параллельного сеанса (Parallel Session Attack):

Класс атак, в котором злоумышленник инициирует несколько одновременных сеансов протокола с целью использования сообщений из одного сеанса в другом.

Пример: NSPK (Lect. 5)

Подтипы: **Комбинированная атака (Interleaving Attack).**

5. **Атака с известным сеансовым ключом (Known Key Attack)**

6. **Атака с известным разовым ключом (Short Term Secret Attack):**

Классы атак, в котором злоумышленник получает доступ к временным секретам, используемых в протоколах.

7. **Атака с неизвестным общим ключом (Unknown Key Share Attack):**

Класс атак на протоколы с аутентификацией ключа, в которых злоумышленник получает возможность доказать одной из сторон владение ключом/секретом.

Пример: NSPK (Lect. 5)

8. Атака с использованием специально подобранных текстов (Known Key Attack)

9. Атака на основе связывания (Binding Attack):

Для криптографических протоколов, построенных на основе асимметричных шифрсистем, основной уязвимостью является возможность осуществления подмены открытого ключа одного из участников на другой открытый ключ с известной противнику секретной половиной этого ключа. В частности, это позволяет противнику узнавать содержание зашифрованных сообщений, отправляемых данному участнику.

