Криптографические протоколы

Лекция 2

Атаки на протоколы

Деркач Максим Юрьевич

December 1, 2020

Ссылки

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/

Определения

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 проткола, в том числе:

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

Определения

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

Классификация атак по типу направленности

1. атаки направленные на криптографические алгортмы;
2. атаки направленные на криптографические методы;
3. атаки направленные на криптографические протколы.

Классификация противников/атакующих

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 пассивые 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 существование злоумышленника, считая, что общаются непосредственно друг с другом.
   Пример: протокол Диффи-Хеллмана
   Подтипы: **Атака подмены (Impersonation)** - попытка подменить одного пользователя другим. Нарушитель, выступая от имени одной из сторон и полностью имитируя ее действия, получает в ответ сообщения определенного формата, необходимые для подделки отдельных шагов протокола.

Основные классы атак на протоколы

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 на основе новизны (freshness attack)** - в протоколах передачи ключей данная атака часто применяется для повторного навязывания уже использованного ранее сеансового ключа;
   Атака отражением (Reflection Attack) Задержка передачи сообщения (Forced Delay) - перехват противником сообщения и навязывание его в более поздний момент времени.

Основные классы атак на протоколы

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 сенасе по видом сообщения другого типа.
   Пример: протоколы Wide-Mouth Frog, Деннинга-Сако, Yahalom, Отвея-Рисса (Lect. 7)

Основные классы атак на протоколы

4. **Комбинированная атака (Interleaving Attack)** - подмена или другой метод обмана, использующий комбинацию данных из ранее выполненных протоколов, в том числе протоколов, ранее навязанных противником.
   Пример: NSPK (Lect. 5)
   Подтипы: **Атака параллельного сеанса (Parallel Session Attack)** - класс атак, в котором злоумышленник инициируеет несколько одновременных сеансов протокола с целью использования сообщений из одного сеанса в другом.

Основные классы атак на протоколы

5. **Атака с известным сеаносвым ключом (Known Key Attack)**:
   данная атака заключается в попытке получения информации о долговременном ключе или любой другой ключевой информации, позволяющей восстанавливать сеансовые ключи для других сеансов протокола.
6. **Атака с известным разовым ключом (Short Term Secret Attack)**:
   Классы атак, в котором злоумышленник получает доступ к временным секретам, используемых в протоколах.

Основные классы атак на протоколы

7. **Атака с неизвестным общим ключом (Unknown Key Share Attack)**:
   Класс атак на протоколы с атака, при которой нарушитель C открывает два сеанса с A и B, выступая в первом случае от имени B, хотя последний может ничего не знать об этом. При этом в результате будет сформирован общий ключ между A и B, причем A будет уверен, что сформировал общий ключ с B, а B будет уверен, что сформировал общий ключ с C. Сам ключ может быть не известен C. Пример: NSPK (Lect. 5)

Основные классы атак на протоколы

8. **Атака с использованием специально подобранных текстов (Known Key Attack)**:
   атака на протоколы типа «запрос — ответ», при которой противник по определенному правилу выбирает запросы с целью получить информацию о долговременном ключе доказывающего.

Основные классы атак на протоколы

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.