МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г. ЧЕРНЫШЕВСКОГО»

Кафедра теоретических основ компьютерной безопасности и криптографии

Методы анализа криптографических протоколов

АВТОРЕФЕРАТ
дипломной работы

студента 6 курса 631 группы
специальности 10.05.01Компьютерная безопасность
факультета компьютерных наук и информационных технологий
Завенягина Максима Павловича

Научный руководитель
профессор, д.ф.-м.н., профессор _____ В. А. Молчанов
23.01.2020 г.

Заведующий кафедрой
д. ф.-м. н., доцент _____ М. Б. Абросимов
23.01.2020 г.

Саратов 2019

ВВЕДЕНИЕ

Криптография является одной из важнейших наук в настоящее время. Многим людям часто приходится выполнять действия, использующие криптографию: сделать денежный перевод в банке, расплатиться в магазине за покупки электронной картой или даже просто отправить другу сообщение по сети Internet, используя протокол, обеспечивающий конфиденциальность обмена данными.

Криптографические протоколы являются очень важным направлением криптографии. Реализация современных алгоритмов дает возможность пользователям протоколов без труда обмениваться данными по зашифрованным каналам, подписывать электронные документы одним кликом по кнопке компьютерной мыши, аутентифицироваться на различных сервисах, используя простейший интерфейс, и так далее. Для большинства людей технологии, основанные на криптографии, представляются сложным математическим аппаратом, и они убеждены в том, что полностью защищены от возможных атак злоумышленников. Однако даже самые надежные системы, использующие криптографические средства, могут содержать уязвимости, которыми рано или поздно может воспользоваться злоумышленник.

Целью данной работы является анализ на устойчивость к некоторым видам атак на известные криптографические протоколы, такие как: протокол обмена ключами Диффи-Хеллмана, протокол обмена ключами Шамира, протокол доказательства с нулевым разглашением знания гамильтонова цикла в графе, протокол доказательства с нулевым разглашением знания изоморфизма графов, протокол цифровой подписи на основе схемы Эль Гамаля, протокол цифровой подписи на основе схемы Шнорра.

Основной задачей работы является проверка перечисленных выше протоколов на устойчивость к атакам следующих видов: атака подменой, атака повторным навязыванием сообщения, атака отражением, атака с задержкой передачи сообщения, комбинированная атака, атака с параллельными сеансами,

атака с использованием специально подобранных текстов, атака с использованием злоумышленником своих средств в качестве части телекоммуникационной структуры, а также предложение возможных способов защиты от таких атак [2].

Одной из задач работы является реализация программного продукта, предоставляющего доступный и понятный интерфейс для пользователя, желающего более подробно рассмотреть вышеперечисленные криптографические протоколы и проверить эти протоколы на устойчивость к основным видам атак на криптографические протоколы.

КРАТКОЕ СОДЕРЖАНИЕ

Первый раздел дипломной работы посвящен рассмотрению основных понятий, связанных с криптографическими протоколами. Данный раздел содержит пять подразделов, в первом из которых рассматриваются понятия протокола и криптографического протокола. Во втором подразделе приведена базовая информация для описания процесса шифрования сообщения. Третий подраздел содержит классификации криптографических протоколов, такие как: классификация по числу участников, классификация по используемым криптографическим системам, а также классификация по целевому назначению. В четвертом подразделе приводятся основные математические сведения, необходимые для понимания работы криптографических протоколов. Пятый подраздел содержит описания некоторых вспомогательных алгоритмов, применяемых при реализации криптографических протоколов, такие как: алгоритм Маурера генерации простого числа, тест Миллера-Рабина проверки числа на простоту, алгоритм вычисления дискретного логарифма Гельфонда-Шенкса.

Второй раздел дипломной работы посвящен описанию основных атак на криптографические протоколы. В данном разделе рассматриваются такие атаки, как: атака подменой, атака повторным навязыванием сообщения, атака отражением, атака с задержкой передачи сообщения, комбинированная атака, атака с использованием специально подобранных текстов, а также атака с использованием злоумышленником своих средств в качестве части телекоммуникационной структуры.

В третьем разделе дипломной работы рассматриваются протоколы обмена ключами. Этот раздел содержит два подраздела, первый из которых содержит формальное описание трехэтапного протокола обмена ключами Шамира, а также анализ этого протокола на наличие уязвимостей к следующим атакам: атаке типа «человек посередине», атаке с повторным навязыванием

сообщения. Также в разделе рассматриваются способы модификации протокола для защиты от описанных уязвимостей.

Во втором подразделе приводится формальное описание протокола Диффи-Хеллмана, описание уязвимости этого протокола к атаке типа «человек посередине», а также способ модификации протокола для защиты от такой атаки.

Четвертый раздел работы посвящен описанию протоколов доказательства с нулевым разглашением. В этом разделе описывается основная идея протоколов доказательства с нулевым разглашением, а также раздел содержит два подраздела, в первом из которых приводится формальное описание протокола доказательства знания гамильтонова цикла в графе, а во втором формальное описание протокола доказательства знания изоморфизма графов. Также в этом разделе содержится анализ протоколов доказательства с нулевым разглашением, рассматриваются уязвимости этих протоколов под названиями: «проблема гроссмейстера», «обман, выполненный мафией». Также в разделе рассматриваются способы защиты от некоторых уязвимостей для протоколов доказательства с нулевым разглашением.

Пятый раздел содержит описание протоколов цифровой подписи. В разделе имеются два подраздела, в первом из которых приводится формальное описание протокола цифровой подписи на основе схемы Эль Гамаля. Также первый подраздел содержит подробное описание атаки на основе генерации случайных сообщений с электронными подписями на основе уже имеющейся электронной подписи для схемы Эль Гамаля. Также в этом подразделе приводится способ защиты от такой атаки.

Второй подраздел содержит формальное описание протокола цифровой подписи на основе схемы Шнорра.

Также в пятом разделе рассматриваются уязвимости в некоторых схемах аутентификации, которые используют протоколы цифровой подписи.

Шестой раздел содержит в себе описание реализованного в ходе выполнения дипломной работы программного комплекса, пример описания

входных данных для этой программы, подробное описание интерфейса программы. Также в шестом разделе приводятся примеры работы программы в двух режимах: обычный режим проведения протокола, режим проведения протокола от лица злоумышленника.

Работа программы в обычном режиме проведения протокола описывается на примере реализации протокола обмена ключами Диффи-Хеллмана.

Использование программы в режиме проведения атаки от лица злоумышленника описывается на примере атаки на протокол доказательства с нулевым разглашением знания изоморфизма графов на основе уязвимости под названием «проблема гроссмейстера». А также в разделе описывается пример работы программы при реализации атаки подменой сообщения на протокол аутентификации, использующий электронную подпись на основе схемы Эль Гамаля.

Стоит отметить, что программе на вход подается формальное описание протоколов в текстовом файле, что дает возможность пользователю проверить и другие, не рассматриваемые в рамках данной дипломной работы, криптографические протоколы на наличие уязвимостей к некоторым атакам.

ЗАКЛЮЧЕНИЕ

В результате выполнения работы рассмотрены и проанализированы следующие криптографические протоколы: протокол обмена ключами Диффи-Хеллмана, протокол обмена ключами Шамира, протокол доказательства с нулевым разглашением знания гамильтонова цикла в графе, протокол доказательства с нулевым разглашением знания изоморфизма графов, протокол цифровой подписи на основе схемы Эль Гамаля, протокол цифровой подписи на основе схемы Шнорра. Анализ проводился на предмет наличия уязвимостей у вышеперечисленных протоколов к атакам на криптографические протоколы следующих видов: атака подменой, атака повторным навязыванием сообщения, атака отражением, атака с задержкой передачи сообщения, комбинированная атака, атака с параллельными сеансами, атака с использованием специально подобранных текстов, атака с использованием злоумышленником своих средств в качестве части телекоммуникационной структуры. Также в работе были предложены некоторые способы модификации протоколов для защиты от найденных уязвимостей.

В ходе практической части работы была реализована программа, имеющая простой и доступный интерфейс, поддерживающая возможность наглядной реализации рассмотренных в работе протоколов, добавления в программу новых протоколов в виде формального описания в текстовом файле, реализации рассмотренных атак на криптографические протоколы с помощью возможности перехвата сообщений, пересылаемых между участниками протокола, а также возможности отправки сообщений от лица любого участника протокола.

Программа содержит несколько режимов работы, которые позволяют пользователю рассмотреть со стороны подробно процесс проведения протокола, дают возможность участвовать в проведении протокола со стороны конкретного участника, дают возможность участвовать в проведении протокола со стороны злоумышленника, а также самостоятельно полностью выполнить

все действия протокола от лица каждого из участников. Программа может использоваться в учебном курсе «Криптографические протоколы».

Также в ходе практической части работы с помощью созданной программы были приведены примеры реализации атак на некоторые из рассматриваемых протоколов, такие как: атака на протокол доказательства с нулевым разглашением знания изоморфизма графов на основе уязвимости под названием «проблема гроссмейстера», атака подменой на схему аутентификации с использованием электронной подписи на основе схемы Эль Гамаля.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Миронов, А.М. Криптографические протоколы [Электронный ресурс] / А.М. Миронов // Криптографические протоколы [Электронный ресурс]. - 129 с.- . -URL: http://intsys.msu.ru/staff/mironov/kp.pdf (дата обращения: 18.10.2019). - Загл. с экрана. - Яз. рус.

2. Черемушкин, А.В. Криптографические протоколы: основные свойства и уязвимости [Электронный ресурс] / А.В. Черемушкин // Институт криптографии, связи и информатики, г. Москва, Россия. - 36 с.- . - URL: http://elearning.paradygma.ru/docs/books/Черёмушкин%20Криптопротоколы+.pdf (дата обращения: 18.10.2019). - Загл. с экрана. - Яз. рус.

3. Шнайер, Б. Прикладная криптография [Электронный ресурс] / Б. Шнайер // Протоколы, алгоритмы и исходные тексты на языке С. - 2-е издание. - 610 с. - Загл. с экрана. - Яз. рус.

4. Глухов, М.М. Алгебра [Электронный ресурс] / М.М. Глухов, В.П. Елизаров, А.А. Нечаев // Том 2. - Изд. М.: Гелиос АРВ, 2003. - 415 с. - Загл. с экрана. - Яз. рус.

5. Виноградов, И.М. Основы теории чисел [Электронный ресурс] / М.И. Виноградов. - Под ред. А.З. Рыжкина. - 6-е изд. М.: Государственное издательство технико-теоретической литературы, 1952. - 178 с. - Загл. с экрана. - Яз. рус.

6. Мусатов, Д.В. Сложность вычислений [Электронный ресурс] / Д.В. Мусатов // Конспект лекций. - МФТИ, 2016. - Загл. с экрана. - Яз. рус.

7. Харари, Ф. Теория графов [Электронный ресурс] / Ф. Харари // Изд. М.: Мир, 1973. - 306 с.- . -URL: https://stugum.files.wordpress.com/2014/03/harary-graph-theory.pdf (дата обращения: 21.10.2019). - Загл. с экрана. - Яз. рус.

8. Карпов, Д.В. Теория графов [Электронный ресурс] / Д.В. Карпов // 525 с.- . -URL: https://logic.pdmi.ras.ru/~dvk/graphs_dk.pdf (дата обращения: 04.10.2019). - Загл. с экрана. - Яз. рус.

9. Глухов, М.М. Введение в теоретико-числовые методы криптографии [Электронный ресурс] / М.М. Глухов, И.А. Круглов, А.Б. Пикчур, А.В. Черемушкин // Учебное пособие. - Изд. сПБ.: Лань, 2011. - 396 с. - Загл. с экрана. - Яз. рус.

10. Запечников, С.В. Криптографические протоколы [Электронный ресурс] / С.В. Запечников // Национальный исследовательский ядерный университет МИФИ. - Курс лекций. - Москва, 2018. - 33 с.- . -URL: https://cryptowiki.net/images/c/c7/M17-507_lecture2.pdf (дата обращения: 2.11.2019). - Загл. с экрана. - Яз. рус.

11. Доказательство знания гамильтонова цикла [Электронный ресурс] // URL: http://www.cryptoprotocols.kz/index.php?view=examples&id=29 (дата обращения: 5.11.2019). - Загл. с экрана. - Яз. рус.

12. Алгоритмы электронной цифровой подписи [Электронный ресурс] // Лекционный материал для студентов [Электронный ресурс]- . -URL: https://studopedia.su/19_47275_algoritm-tsifrovoy-podpisi-el-gamalya-EGSA.html (дата обращения: 12.11.2019). - Загл. с экрана. - Яз. рус.

13. Алгоритм цифровой подписи Шнорра [Электронный ресурс] // Лекционный материал для студентов [Электронный ресурс]- . -URL: https://studopedia.org/3-18522.html (дата обращения: 12.11.2019). - Загл. с экрана. - Яз. рус.

14. Албахари, Д. Справочник C# 6.0 [Электронный ресурс] / Д. Албахари, Б. Албахари // Полное описание языка C# 6.0. - 6-е изд. М.: Издательский дом «Вильямс». - 2016. - 1040 с. - Загл. с экрана. - Яз. рус.

15. Руководство по программирования на языке C# [Электронный ресурс] // Практическое руководство [Электронный ресурс]- . -URL: https://msdn.microsoft.com (дата обращения: 14.09.2019). - Загл. с экрана. - Яз. рус.

16. Венбо, М. Современная криптография. Теория и практика [Электронный ресурс] / М. Венбо // Изд. Д. «Вильямс», 2005. - 764 с. - Загл. с экрана. - Яз. рус.

17. Вельшенбах, М. Криптография на C и C++ [Электронный ресурс] / М. Вельшенбах // Учебное пособие. - Изд. М.: Триумф, 2004. - 464с. - Загл. с экрана. - Яз. рус.

18. Никитин, В.Н. Повышение защиты протоколов распределения ключей от атак вторжения в середину канала связи [Электронный ресурс] / В.Н. Никитин, М.М. Ковцур, Д.В. Юркин // Санкт-Питербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича [Электронный ресурс]- . -URL: https://cyberleninka.ru/article/n/povyshenie-zaschity-protokolov-raspredeleniya-klyuchey-ot-atak-vtorzheniya-v-seredinu-kanala-svyazi/viewer (дата обращения: 8.01.2020). - Загл. с экрана. - Яз. рус.

19. Алферов, А.П. Основы криптографии [Электронный ресурс] / А.П. Алферов, А.Ю. Зубов, А.С. Кузьмин, А.В. Черемушкин, 2-е изд. М.: «Гелиос АРВ», 2002. - 480 с. - Загл. с экрана. - Яз. рус.