МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г. ЧЕРНЫШЕВСКОГО»
(СГУ)

Кафедра теоретических основ компьютерной безопасности и криптографии

Разработка системы мгновенного обмена сообщениями на основе криптографического протокола Off-the-Record Messaging

АВТОРЕФЕРАТ

дипломной работы

студентки 6 курса 631 группы
специальности 10.05.01 Компьютерная безопасность
факультета компьютерных наук и информационных технологий
Альденовой Эльмиры Нурлановны

Научный руководитель
доцент, к.п.н. _____ А. С. Гераськин
18.01.2019 г.

Заведующий кафедрой
д. ф.-м. н., доцент _____ М. Б. Абросимов
18.01.2019 г.

Саратов 2019

ВВЕДЕНИЕ

В условиях современного информационного общества компьютерные технологии настолько укоренились в нашей жизни, что полностью изменили способы обмена информацией, которые мы используем для общения с друзьями, членами семьи и деловыми партнерами. Несмотря на то, что электронная почта становится все более мобильной, большое количество людей пользуется системами мгновенного обмена сообщениями (мессенджерами). В отличие от электронной почты сообщения в мессенджерах передаются мгновенно в режиме реального времени [1].

Одной из главных целей криптографии является защита тайны передаваемых сообщений. Свойство безопасности схем шифрования, как правило, описывается в виде семантической безопасности, которая гарантирует, что злоумышленник не может получить хотя бы частичную информацию о зашифрованном сообщении. Другими словами, знание зашифрованного текста не показывает дополнительной информации о сообщении, которое может быть из него извлечено.

Понятие семантической безопасности оказалось очень полезным в большом количестве приложений. Однако семантическая безопасность не защищает схему шифрования от принудительных атак. Если злоумышленник перехватит зашифрованный текст, а затем попытается заставить отправителя раскрыть секретный ключ или какие-либо случайные параметры, используемые при шифровании, то любые данные, показанные отправителем и согласующиеся с зашифрованным текстом, должны открыть и истинное сообщение.

Многие схемы шифрования имеют только один набор возможных входов для зашифрованного текста. Это свойство шифрования может быть проблематичным, например, в приложениях электронного голосования [2].

Целью данной работы является программная реализация системы мгновенного обмена сообщениями.

Для достижения поставленной цели были сформулированы следующие задачи:

1) определить основные свойства отрицаемого шифрования;

2) изучить криптографический протокол Off-the-Record;

3) ознакомиться с существующими программными продуктами;

4) реализовать систему мгновенного обмена сообщениями, использующую протокол Off-the-Record.

Дипломная работа состоит из введения, 3 разделов, заключения, списка использованных источников и 1 приложения. Общий объем работы – 67 страниц, из них 41 страница – основное содержание, включая 43 рисунка, список использованных источников из 13 наименований.

КРАТКОЕ СОДЕРЖАНИЕ

В разделе 1 «Отрицаемое шифрование» рассмотрено понятие отрицаемого шифрования, связанное с задачей обеспечения стойкости шифрования информации в условиях возможности так называемых атак с принуждением. Данный вид атак подразумевает наличие у злоумышленника инструментов воздействия на отправителя и (или) получателя сообщений, которые вынуждают участников взаимодействия (корреспондентов) раскрыть параметры процесса шифрования, например, ключ шифрования и случайные параметры, использованные в процессе шифрования [3].

В подразделе 1.1 «Протокол Off-the-Record Messaging» подробно изучается криптографический протокол Off-the-Record Messaging (OTR). Ключевыми понятиями данного протокола являются прямая секретность (perfect forward secrecy) и отрицаемая аутентификация (deniable authentication).

Совершенная прямая секретность позволяет защититься от атак в случае раскрытия долговременного ключа тем, что для каждой сессии создается новый ключ общего доступа. Отрицаемая аутентификация относится к возможности двух сторон взаимодействия доказать, что именно они являются авторами каждого отправленного сообщения, причем третья сторона не сможет определить, кто именно отправил сообщение [6].

Для передачи сообщений участники протокола OTR должны установить общий секретный ключ, а для обеспечения совершенной прямой секретности ключи должны постоянно обновляться. Подробно данные составляющие протокола OTR представлены в пункте 1.1.1 «Обмен ключами» рассматривается обмен ключами.

В пункте 1.1.2 «Обмен сообщениями» представлена часть протокола OTR, реализующая непосредственно передачу сообщений. Чтобы предоставить возможность отрицаемой аутентификации, протокол OTR для аутентификации сообщений использует вместо цифровых подписей коды HMAC – это тип

кодов для аутентификации сообщений, включающий криптографическую хэш-функцию и секретный ключ [10].

Хотя обмен ключами в OTR довольно хорош в теории, он обладает и недостатками. Предполагается, что участники взаимодействия знают открытые ключи друг друга до того, как происходит обмен ключами, поскольку в противном случае возможно проведение атаки «человек посередине». Если некоторый собеседник начинает переписку, используя известный открытый ключ, то приложение находит совпадение в хранилище, и аутентификация происходит автоматически. Если же такого ключа в хранилище нет, например, в случае первого взаимодействия между пользователями, то предлагается подтвердить подлинность ключа [8]. В пункте 1.1.3 «Протокол миллионеров-социалистов» приведен протокол, позволяющий пользователям проверить подлинность собеседника, используя какой-то общий секрет, причем данный секрет не разглашается напрямую по каналу связи.

Протокол Off-the-record messaging является протоколом сквозного шифрования (end-to-end encryption). Сквозное шифрование гарантирует, что информация шифруется отправителем, а расшифровывается только его получателем [11]. В разделе 2 «Обзор существующих программных продуктов» рассмотрены бесплатные программные продукты, поддерживающие сквозное шифрование.

В подпункте 2.1 «Signal» изучена и протестирована работа мессенджера Signal, в подпункте 2.2 «Wire» - мессенджера Wire, а в подпункте 2.3 «Riot» - приложения Riot.

В подпункте 2.4 «Сравнение программных продуктов» проведено сравнение результатов тестирования рассмотренных продуктов. При изучении работы продуктов было уделено много внимания на то, как реагируют приложения на изменение ключей при переустановке программы одним из пользователей. Так Signal блокирует отправку и показывает уведомление о том, что у собеседника теперь другие ключи. Только после верификации новых

ключей Signal разрешает опять отправлять сообщения. Riot также информирует пользователей об изменении ключей, а при попытке отправки сообщения показывает предупреждение о том, что в чате есть пользователь, не прошедший процесс верификации. Хуже всего в этом плане показал себя Wire, он совершенно никаким образом не уведомляет пользователей об изменении ключей, поэтому пользователи должны сами проверять данный факт, чтобы быть уверенными, что разговор защищен сквозным шифрованием.

Если рассматривать процесс верификации, то из представленных приложений приятно выделяется Signal со своим встроенным сканером QR-кодов. Wire и Riot же просто показывают ключи, которые пользователем нужно посимвольно сравнивать. Однако стоит сказать, что Signal жестко привязывает к номеру телефона одно устройство, когда Wire и Riot поддерживают список устройств у каждой учетной записи [12].

В разделе 3 «Программная реализация системы обмена сообщениями» наглядно продемонстрирована разработанная программа. В ходе проделанной работы была реализована система мгновенного обмена сообщениями, использующая протокол OTR. Программа написана на языке C# в среде разработки Visual Studio. Для взаимодействия между различными машинами были использованы сокеты для непосредственной передачи сообщений между пользователями, а также база данных SQL, расположенная в облачном сервисе Azure.

Программа состоит из девяти основных классов: FormLogSign, FormFriends, FormDialog, UserBL, MessagesBL, OTRPrivateSession, SessionKeysGenerator, OTRCryptoEngine, Helpers.

Интерфейс программы реализован с помощью классов FormLogSign, FormFriends, FormDialog: FormLogSign отвечает за форму для входа и регистрации учетных записей, FormFriends – за форму для добавления пользователей в список друзей, а FormDialog – непосредственно за окно, где участники разговора ведут переписку.

В классе UserBL реализованы методы, отвечающие за логику учетных записей, например, метод, который получает на вход логин и пароль и проверяет, есть ли в базе данных запись, соответствующая входным параметрам. С помощью класса MessagesBL происходит добавление и извлечение из базы данных текстов сообщений, которыми обмениваются пользователи.

Класс OTRPrivateSession содержит основную логику протокола Off-the-Record Messaging, а именно аутентификацию с помощью протокола SMP, обмен ключами и их обновление, обмен сообщениями. В классе SessionKeysGenerator вычисляются сессионные ключи для шифрования и сессионные MAC-ключи, а класс OTRCryptoEngine генерирует пары открытых и закрытых ключей и вычисляет общий ключ. В классе Helpers собраны вспомогательные методы, например, методы по преобразованию сообщений в массив байт для передачи по каналу связи.

ЗАКЛЮЧЕНИЕ

В теоретической части данной работы были рассмотрены атаки с принуждением и отрицаемое шифрование, обеспечивающее стойкость в условиях возможности подобных атак.

Также был подробно разобран криптографический протокол Off-the-Record Messaging, который удовлетворяет основным свойствам отрицаемого шифрования: совершенной прямой секретности и отрицаемой аутентификации.

Для того, чтобы определить требования к системам мгновенного обмена сообщениями, были изучены существующие программные продукты, проведено сравнение их функциональных возможностей.

В практической части работы была реализована система мгновенного обмена сообщениями на основе криптографического протокола Off-the-Record. Программа представляет собой независимое клиентское приложение, в качестве базы данных выбрана SQL Azure на облачной платформе Microsoft Azure.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 Манукова, Е. Ю. Использование сервисов мгновенного обмена сообщениями в современной массовой коммуникации [Электронный ресурс] / Е. Ю. Манукова, М. В. Захарова : Материалы V Международной научной конференции «Современная филология». Самара, 2017. С. 85-88. URL: https://moluch.ru/conf/phil/archive/234/12011/ (дата обращения: 10.01.2019). Загл. с экрана. Яз. рус.

2 Canetti, R. Deniable Encryption [Электронный ресурс] / R. Canetti, C. Dwork, M. Naor, R. Ostrovsky : Advances in Cryptology, CRYPTO 1997, Lecture Notes in Computer Science. 15 с. URL: http://www.wisdom.weizmann.ac.il/~naor/PAPERS/deniable.pdf (дата обращения 26.11.2018). Загл. с экрана. Яз. англ.

3 Вайчикаускас, М. А. Классификация принуждающих атак и схем отрицаемого шифрования [Электронный ресурс] / М. А. Вайчикаускас, Я. А. Мондикова : Материалы конференции «Региональная информатика (РИ-2016)». СПб, 2016. 599 с. URL: http://spoisu.ru/files/ri/ri2016/ri2016_materials.pdf (дата обращения 28.11.2018). Загл. с экрана. Яз. рус.

4 Морозова, Е. В. Способы отрицаемого шифрования с разделяемым ключом [Электронный ресурс] / Е. В. Морозова, Я. А. Мондикова, Н. А. Молдовян // Информационно-управляющие системы. 2013. № 6. С. 73-78.

5 Молдовян, Н. А. Отрицаемое шифрование на основе блочных шифров [Электронный ресурс] / Н. А. Молдовян, А. Р. Биричевский, Я. А. Мондикова // Информационно-управляющие системы. 2014. № 5. С. 80-86.

6 Jefferys, K. Loki: Конфиденциальные транзакции, децентрализованное общение [Электронный ресурс] / K. Jefferys, S. Harman, J. Ross, P. McLean : Техническая документация, версия 3. 2018. URL: https://loki.network/wp-content/uploads/2018/10/WhitepaperV3Russian.pdf (дата обращения 29.11.2018). Загл. с экрана. Яз. рус.

7 Borisov, N. Off-The-Record Wire Protocol Documentation [Электронный ресурс] / N. Borisov, I. Goldberg : Техническая документация, версия 1. 2013. URL: https://bugs.otr.im/lib/libotr/blob/master/Protocol-v1.txt (дата обращения 15.11.2018). Загл. с экрана. Яз. англ.

8 Alexander, C. Improved user authentication in off-the-record messaging [Электронный ресурс] / C. Alexander, I. Goldberg // Proceedings of the 2007 ACM workshop on Privacy in electronic society. 2007. С. 41-47.

9 Borisov, N. Off-the-record communication, or, why not to use PGP [Электронный ресурс] / N. Borisov, I. Goldberg, E. Brewer // Proceedings of the 2004 ACM workshop on Privacy in the electronic society. 2004. С. 77-84.

10 Di Raimondo, M. Secure off-the-record messaging [Электронный ресурс] / M. Di Raimondo, R. Gennaro, H. Krawczyk // Proceedings of the 2005 ACM workshop on Privacy in the electronic society. 2005. С. 81-89.

11 Communicating with Others [Электронный ресурс] / Surveillance Self-Defense [Электронный ресурс] : [сайт]. URL: https://ssd.eff.org/en/module/communicating-others (дата обращения: 26.12.2018). Загл. с экрана. Яз. англ.

12 Mujaj, A. A Comparison of Secure Messaging Protocols and Implementations [Электронный ресурс] / A. Mujaj // Университет Осло [Электронный ресурс] : [сайт]. URL: https://www.mn.uio.no/ifi/english/research/groups/psy/completedmasters/2017/Aulon_Mujaj/aulon_mujaj_msc_comparison_secure_messaging_protocols_implementations_2017.pdf (дата обращения: 29.12.2018). Загл. с экрана. Яз. англ.

13 Stedman, R. A user study of off-the-record messaging [Электронный ресурс] / R. Stedman, K. Yoshida, I. Goldberg] // Proceedings of the 4th symposium on Usable privacy and security. 2008. С. 95-104.