Министерство образования и науки Российской Федерации

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г. ЧЕРНЫШЕВСКОГО»

Кафедра теоретических основ компьютерной безопасности и криптографии

Приложение обмена сообщениями для операционной системы Android

АВТОРЕФЕРАТ

дипломной работы

студента 6 курса 631 группы

специальности 10.05.01 Компьютерная безопасность

факультета компьютерных наук и информационных технологий

Болоховцева Никиты Олеговича

Научный руководитель

доцент, к.ф.-м.н. _____ А.В. Жаркова

31.12.2016 г.

Заведующий кафедрой

профессор, к.ф.-м.н. _____ В.Н. Салий

31.12.2016 г.

Саратов 2017

ВВЕДЕНИЕ

Безопасность личных данных всегда была актуальной проблемой. Одной из важнейших вещей, нуждающихся в надежной защите, является переписка. Множество людей по всему миру используют мобильные приложения как для личного, так и для делового общения. Последние годы конкуренция на рынке мессенджеров очень высока. Доступный Интернет у каждого в смартфоне позволил мессенджерам стать самыми часто используемыми приложениями. Проанализировав самые популярные из мобильных мессенджеров на устойчивость к различным угрозам, можно прийти к выводу, что многие из них не обеспечивают надежной защиты. В большинстве из них вся переписка хранится на удаленных серверах в незашифрованном виде и в любой момент может быть прочитана или передана. Конечно, некоторые приложения осуществляют шифрование данных клиент-клиент, но существует еще множество угроз, например, таких как чтение данных сервис-провайдерами, перехват текущего ключа шифрования, неподлинная личность собеседника и т.д.

Целью данной дипломной работы является разработка и реализация приложения обмена сообщениями с криптографической защитой информации под операционную систему Android. Для достижения поставленной цели требуется решить следующие задачи:

- рассмотреть алгоритмы и протоколы для организации обеспечения безопасности личной переписки;
- проанализировать некоторые существующие мессенджеры;
- изучить специфику разработки приложений под платформу Android.

Дипломная работа состоит из введения, 7 разделов, заключения, списка использованных источников и 2 приложений. Общий объем работы – 128 страниц, из них 63 страницы – основное содержание, включая 17 рисунков и 1 таблицу, список использованных источников из 24 наименований.

КРАТКОЕ СОДЕРЖАНИЕ

В разделе 1 «Необходимые определения и сведения» приводятся основные понятия и сведения, используемые в работе, такие как криптография, открытый текст, шифрование, криптограмма, дешифрование, ключ, шифр замены, шифр перестановки, композиционные графы, блочные шифры замены, симметричные и асимметричные шифры, блочное шифрование, блочный шифр, итерационный ключ, развертывания ключа, идентификатор доступа, идентификация, аутентификация, хеш-функция, электронная подпись, криптосистема, система вычетов по модулю n, взаимно простые числа, первообразный корень по модулю n, ассоциативность, абелева группа, кольцо, поле.

Использование шифрования данных – одна из наиболее важных вещей в безопасности мобильных мессенджеров. Многие мобильные устройства не обладают сверхмощным процессором и большим количеством памяти, а данные должны шифроваться быстро. Это делает нецелесообразным применять в реализации мессенджеров некоторые из алгоритмов шифрования. В разделе 2 «Алгоритмы шифрования» рассматриваются некоторые алгоритмы шифрования, такие как алгоритм симметричного шифрования DES, асимметрические криптосистемы и стандарт шифрования ГОСТ Р 34.12-2015.

В настоящее время в связи с обширным развитием сетевых технологий аутентификация используется повсеместно. В мобильных мессенджерах чаще всего используется аутентификация по многоразовым паролям. В разделе 3 «Протоколы аутентификации» рассматриваются и анализируются различные варианты аутентификации, применяемые в том числе на мобильных устройствах, такие как аутентификация по многоразовым паролям, с помощью протокола аутентификации Kerberos, аутентификация на основе шифрования с открытым ключом, используя многофакторную аутентификацию, с помощью SMS или биометрических данных, с использованием протокола CHAP.

В мессенджерах с клиент-клиент шифрованием перед установлением связи абонентам необходимо как-то обменяться криптографическими ключами. Обычно ключи хранятся и (или) генерируются серверами мессенджера. Соответственно, если сервер будет взломан злоумышленниками (или будет принужден к раскрытию ключей властями), то шифрование не поможет. Многие популярные мессенджеры полагаются на центральный сервер для генерации и распределения ключей шифрования, а в отдельных случаях еще и для их хранения. В разделе 4 «Протоколы распределения ключей» рассматриваются некоторые протоколы распределения ключей, такие как протокол Диффи-Хеллмана, протокол Нидхема-Шрёдера, протокол Отвея-Рииса, а также рассматриваются некоторые атаки на протоколы распределения ключей.

В приложениях обмена сообщениями хеш-функции обычно используются для вычисления хеш-кода пароля, который в дальнейшем хранится на сервере. Это делается для того, чтобы, перехватив хеш-код пароля по каналу связи или прочитав с сервера, злоумышленник не смог восстановить первоначальный пароль. Некоторые хеш-функции, такие как MD5, SHA-1, ГОСТ Р 34.11-2012 рассматриваются в разделе 5 «Хеш-функции».

Идея создания сервиса обмена короткими текстовыми сообщениями возникла еще в 1984 году, а первое SMS-сообщение было отправлено в 1992 в сотовой сети Vodafone. Сегодня для личной переписки используются различные мессенджеры, которые для связи используют Интернет. Уже привычный метод SMS становится все менее популярным. За последние несколько лет появилось множество приложений, позволяющих пользователям не просто переписываться между собой текстом, но и общаться по видеосвязи, обмениваться файлами, создавать групповые чаты и прочее. В разделе 6 «Некоторые существующие мессенджеры» рассматриваются некоторые популярные мобильные мессенджеры и их уязвимости.

В ходе проделанной работы было разработано и реализовано приложение обмена сообщениями под операционную систему Android, в том числе с

использованием отечественных стандартов шифрования ГОСТ Р 34.12-2015 и хеш-функции ГОСТ Р 34.11-2012, которое состоит из двух частей – клиентской и серверной. Приложение-клиент написано на языке Java в среде разработки Eclipse с использованием AndroidSDK. Для тестирования использовался Android Virtual Device. Также был установлен локальный сервер Apache, в котором запросы обрабатываются на языке PHP. Для хранения истории сообщений и данных для аутентификации используется MySqlServer. Разработанное приложение описывается в разделе 7 «Программная реализация приложения обмена сообщениями». Также в этом разделе сравниваются некоторые существующие мессенджеры по наличию end-to-end шифрования и открытого протокола. Листинг программы-сервера приведен в приложении А, программы-клиента – в приложении Б.

ЗАКЛЮЧЕНИЕ

В последнее время мессенджеры часто используются в мобильных устройствах. С их помощью ведется переписка, как для личного, так и для делового общения, отправляются различные данные, осуществляются звонки. Безопасность передачи и хранения данных – один из важнейших факторов мобильных мессенджеров, который дает им преимущество перед обычными SMS сообщениями.

В ходе данной дипломной работы были рассмотрены различные алгоритмы и протоколы для разработки приложения обмена сообщениями, в том числе блочный шифр «Кузнечик», протокол аутентификации CHAP, протокол распределения ключей Диффи-Хеллмана и функция хеширования из отечественного стандарта ГОСТ Р 34.11-2012. Также были рассмотрены некоторые существующие мессенджеры и изучена специфика разработки под платформу Android. В результате проведенной работы было разработано и реализовано приложение обмена сообщениями под операционную систему Android, которое состоит из двух частей – клиентской и серверной. Приложение-клиент написано на языке Java в среде разработки Eclipse с использованием AndroidSDK. Также был установлен локальный сервер Apache, в котором запросы обрабатываются на языке PHP. Для хранения истории сообщений и данных для аутентификации используется MySqlServer. Использовать данное приложение можно на устройствах Android версии 4.1 и выше.

В ходе дипломной работы в разработанном приложении, в частности, реализован протокол аутентификации CHAP, алгоритм шифрования «Кузнечик» из отечественного стандарта ГОСТ Р 34.12-2015, протокол распределения ключей Диффи-Хеллмана, отечественная хеш-функция ГОСТ Р 34.11-2012, а также наложены ограничения на некоторые действия, например, требования к паролю пользователя и отсутствие у других пользователей возможности проверки заданного логина на регистрацию в системе.

Таким образом, все поставленные задачи были полностью решены, цель работы достигнута.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 Салий, В. Н. Криптографические методы и средства защиты информации : учеб. пособие [Электронный ресурс] / В. Н. Салий. Саратов : 2012. 41 с. Загл. с экрана. Яз. рус.

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

3 Сборник руководящих документов по защите информации от несанкционированного доступа [Электронный ресурс]. М. : 1998. Загл. с экрана. Яз. рус.

4 Федеральный закон «Об электронной подписи» от 06.04.2011 № 63-ФЗ [Электронный ресурс] // КонсультантПлюс [Электронный ресурс]. URL: http://www.consultant.ru/document/cons_doc_LAW_112701/ (дата обращения: 17.10.2016). Загл. с экрана. Яз. рус.

5 Баричев, С. Г. Основы современной криптографии [Электронный ресурс] / С. Г. Баричев, В. В. Гончаров, Р. Е. Серов. М. : Горячая линия-Телеком, 2011. 175 с. Загл. с экрана. Яз. рус.

6 Шнайер, Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си / Б. Шнайер. М. : Издательство ТРИУМФ, 2003. 816 с.

7 Шаханова, М. В. Современные технологии информационной безопасности : учебно-методический комплекс [Электронный ресурс] / М. В. Шаханова. М. : Проспект, 2015. 216 с. Загл. с экрана. Яз. рус.

8 Асимметричные криптосистемы шифрования [Электронный ресурс] // Your Private Network [Электронный ресурс]. URL: http://ypn.ru/197/asymmetric-encryption-system/2/ (дата обращения: 14.10.2016). Загл. с экрана. Яз. рус.

9 ГОСТ Р 34.12-2015. Информационная технология. Криптографическая защита информации. Блочные шифры [Электронный ресурс] // Технический комитет по стандартизации «Криптографическая защита информации» (ТК 26)

[Электронный ресурс]. URL: https://tc26.ru/standard/gost/GOST_R_3412-2015.pdf (дата обращения: 18.10.2016). Загл. с экрана. Яз. рус.

10 ГОСТ Р 34.13-2015. Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров [Электронный ресурс] // Технический комитет по стандартизации «Криптографическая защита информации» (ТК 26) [Электронный ресурс]. URL: https://www.tc26.ru/standard/gost/GOST_R_3413-2015.pdf (дата обращения: 18.10.2016). Загл. с экрана. Яз. рус.

11 Анисимов, В. В. Протоколы аутентификации (идентификации) [Электронный ресурс] / В. В. Анисимов // Anisimovkhv [Электронный ресурс]. URL: https://sites.google.com/site/anisimovkhv/learning/kripto/lecture/tema11 (дата обращения: 18.10.2016). Загл. с экрана. Яз. рус.

12 Идентификация и аутентификация [Электронный ресурс] // Научная библиотека [Электронный ресурс]. URL: http://sernam.ru/ss_23.php (дата обращения: 21.10.2016). Загл. с экрана. Яз. рус.

13 Технологии идентификации – CHAP [Электронный ресурс] // Cisco [Электронный ресурс]. URL: http://www.cisco.com/russian_win/warp/public/3/ru/solutions/sec/mer_tech_ident-chap.html/ (дата обращения: 09.09.2016). Загл. с экрана. Яз. рус.

14 Молдовян, Н. А. Введение в криптосистемы с открытым ключом [Электронный ресурс] / Н. А. Молдовян, А. А. Молдовян. М. : БХВ-Петербург, 2005. 285 с. Загл. с экрана. Яз. рус.

15 Семенов, Ю. А. Протокол аутентификации Нидхэма-Шредера в случаях симметричной и асимметричной системы шифрования [Электронный ресурс] / Ю. А. Семенов // CIT Forum [Электронный ресурс]. URL: http://citforum.ru/nets/semenov/6/n_s_p_k.shtml (дата обращения: 03.10.2016). Загл. с экрана. Яз. рус.

16 ГОСТ Р 34.11-2012. Информационная технология. Криптографическая защита информации. Функция хэширования [Электронный ресурс] // ГОСТ Эксперт [Электронный ресурс]. URL: http://gostexpert.ru/data/files/34.11-

2012/70020.pdf (дата обращения: 24.10.2016). Загл. с экрана. Яз. рус.

17 Skype [Электронный ресурс]. URL: https://www.skype.com/ru/ (дата обращения: 28.11.2016). Загл. с экрана. Яз. рус.

18 Telegram Messenger [Электронный ресурс]. URL: https://telegram.org/ (дата обращения: 28.11.2016). Загл. с экрана. Яз. рус.

19 Лихачёв, Н. Telegram удалил 78 публичных каналов об «Исламском государстве» по требованию Apple / Н. Лихачёв // TJournal [Электронный ресурс] : Новое медиа. URL: https://tjournal.ru/p/grugq-telegram (дата обращения: 28.11.2016). Загл. с экрана. Яз. рус.

20 Viber [Электронный ресурс]. URL: http://www.viber.com/ru/ (дата обращения: 28.11.2016). Загл. с экрана. Яз. рус.

21 WhatsApp [Электронный ресурс]. URL: https://www.whatsapp.com/ (дата обращения: 28.11.2016). Загл. с экрана. Яз. рус.

22 ICQ [Электронный ресурс]. URL: https://icq.com/android/ru (дата обращения: 28.11.2016). Загл. с экрана. Яз. рус.

23 Google Hangouts [Электронный ресурс]. URL: https://hangouts.google.com/ (дата обращения: 28.11.2016). Загл. с экрана. Яз. рус.

24 Мобильный протокол MTProto [Электронный ресурс] // Документация Telegram [Электронный ресурс]. URL: https://tlgrm.ru/docs/mtproto (дата обращения: 28.11.2016). Загл. с экрана. Яз. рус.