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

Разработка безопасного мобильного мессенджера

АВТОРЕФЕРАТ
дипломной работы

студента 6 курса 631 группы
специальности 10.05.01 Компьютерная безопасность
факультета компьютерных наук и информационных технологий
Цуканова Ильи Дмитриевича

Научный руководитель
к.п.н, доцент _____ 22.01.2024 г. А. С. Гераськин

Заведующий
кафедрой д. ф.-м. н.,
доцент _____ 22.01.2024 г. М. Б. Абросимов

Саратов 2024

ВВЕДЕНИЕ

В настоящее время существует множество средств коммуникации: почтовые службы и службы доставки, телефонная и видео связь и, безусловно, самая многофункциональная и распространенная — связь посредством интернета. Все больше людей используют мобильные устройства для обмена сообщениями. Однако, с ростом популярности мобильных мессенджеров возникает ряд проблем, связанных с безопасностью и конфиденциальностью переписки. В условиях использования общедоступных Wi-Fi сетей, такие проблемы становятся особенно актуальными, поскольку данные пользователей могут быть украдены или подвергнуты другим видам злоупотреблений. Например, в 2022 году количество атак на частных лиц увеличилось на 44%. На обычных пользователей пришлось 17% от числа всех атак. Традиционно основной вектор атаки — это различные приемы социальной инженерии, которые использовались в 93% случаев. Для проведения таких атак злоумышленники создавали фишинговые сайты (56%), отправляли вредоносные письма по электронной почте (39%), искали жертв в социальных сетях (21%) и мессенджерах (18%). Согласно последним исследованиям, список наиболее безопасных мессенджеров выглядит так:

- Signal
- Wickr
- Viber
- Telegram
- Confide
- Slack
- IMessage
- WhatsApp

В тройку самых безопасных мессенджеров вошли Signal, Wickr и Viber, который опередил Telegram. Мессенджер Signal по-прежнему получает высокую 4 оценку экспертов за качество протоколов шифрования, наличие

двухфакторной идентификации, шифрование по умолчанию и готовность к раскрытию персональных данных. Цель данной дипломной работы состоит в разработке защищенного мобильного мессенджера, который будет обеспечивать высокий уровень безопасности и конфиденциальности переписки в условиях использования одной Wi-Fi сети. Для достижения этой цели необходимо решить следующие задачи:

- Изучить существующие методы и алгоритмы шифрования и аутентификации данных в мобильных мессенджерах.
- Разработать архитектуру защищенного мобильного мессенджера.
- Реализовать прототип мессенджера с использованием выбранных методов шифрования и аутентификации.
- Провести тестирование разработанного прототипа для оценки его безопасности и эффективности.
- Сделать выводы о возможности применения разработанного мессенджера в реальных условиях и предложить пути его усовершенствования.

Дипломная работа состоит из введения, 3 разделов, заключения, списка использованных источников и 1 приложения. Общий объем работы – 79 страниц, из них 55 страниц – основное содержание, включая 37 рисунков и 0 таблиц, список использованных источников из 15 наименований.

КРАТКОЕ СОДЕРЖАНИЕ

Глава 1 Теоретическая часть

1.1 Требования безопасности к безопасному мобильному мессенджеру

Эта глава описывает требования безопасности, которые включают в себя ряд мер и условий, необходимых для обеспечения конфиденциальности, целостности и доступности передаваемых данных. В контексте мобильных мессенджеров и приложений, такие требования становятся особенно важными, учитывая чувствительность информации, которая обменивается через эти каналы.

1. Шифрование данных: Одним из основных требований является использование сильного шифрования для защиты передаваемых данных от несанкционированного доступа. Это включает в себя как шифрование в покое, так и во время передачи данных по сети.

2. Аутентификация: Требуется обеспечить возможность проверки подлинности участников коммуникации, чтобы исключить возможность подделки сообщений и атак типа man-in-the-middle.

3. Защита от вредоносных вмешательств: Канал связи должен быть защищен от вредоносных вмешательств, таких как внедрение вредоносного кода или атаки на протоколы связи.

4. Управление ключами: Необходимо обеспечить безопасное управление ключами шифрования, включая их генерацию, хранение и обмен между участниками коммуникации.

5. Соблюдение стандартов безопасности: Канал связи должен соответствовать современным стандартам безопасности, таким как использование протоколов шифрования, рекомендуемых криптографических алгоритмов и т.д.

6. Устойчивость к атакам: Канал связи должен быть способен обнаруживать и предотвращать попытки атак, такие как перехват сообщений, внедрение вредоносного кода и другие виды злоупотреблений.

Эти требования помогают построить безопасный канал связи, который обеспечивает конфиденциальность и защиту пользовательских данных.

Основная цель данного подраздела - определить требования к безопасности защищенного канала связи, которые будут использоваться в дальнейшей разработке защищенного мессенджера.

1.2 Анализ существующих мобильных мессенджеров и их уязвимостей

В этом подразделе проводится анализ существующих мобильных мессенджеров, включая как коммерческие, так и с открытым исходным кодом, таких как: WhatsApp, Telegram, Signal, Element, Wire, Tox. Рассматриваются их функциональность и особенности в области безопасности данных, а также выявляются уязвимости.

WhatsApp - это популярное приложение для обмена сообщениями, использует принцип "end-to-end" шифрования сообщений для обеспечения безопасности данных. Однако, возникает необходимость более глубокого изучения безопасности и шифрования данных, а также протоколов конфиденциальности, применяемых в данном мессенджере.

Telegram - это другой популярный мессенджер, который также использует шифрование данных для обеспечения безопасности сообщений. Однако, в работе обсуждаются возможные уязвимости, связанные с использованием Telegram, такие как возможность перехвата сообщений и утечки данных.

Таким образом, анализ существующих мобильных мессенджеров и их уязвимостей позволяет выявить особенности и проблемы в области безопасности данных, связанные с использованием различных мессенджеров. Это позволяет разработчикам учитывать эти проблемы при создании новых мессенджеров и обеспечивать более высокий уровень безопасности и конфиденциальности данных.

Основная цель данного подраздела - выявить уязвимости существующих мессенджеров и определить, какие методы шифрования и аутентификации используются в них.

В результате анализа было выявлено, что большинство мессенджеров используют шифрование "end-to-end", но при этом могут быть уязвимы к атакам

типа "Man-in-the-middle".

1.3 Описание протоколов шифрования и методов обеспечения безопасности в организации канала связи

В данном подразделе представлено описание различных протоколов шифрования и методов обеспечения безопасности в организации канала связи, таких как шифрование "end-to-end", аутентификация, цифровые подписи и другие.

Основная цель данного подраздела - описать различные методы шифрования и аутентификации, которые могут быть использованы для обеспечения безопасности защищенного канала связи.

В результате исследования было выявлено, что использование шифрования "end-to-end" и двухфакторной аутентификации является наиболее эффективным способом обеспечения безопасности канала связи.

Глава 2 Обзор технологий для разработка безопасного мобильного мессенджера

Обзор технологий для разработки безопасного мобильного мессенджера включает в себя рассмотрение различных инструментов, платформ и методов, которые могут быть использованы для создания мобильных приложений с учетом требований безопасности, эффективности и кроссплатформенной совместимости.

1. .NET Multi-platform App UI (MAUI): Рассматривается кроссплатформенный фреймворк от компании Microsoft, который позволяет разрабатывать нативные мобильные и десктопные приложения с использованием языка программирования C# и языка разметки XAML. MAUI обеспечивает возможность создания приложений под различные операционные системы, такие как Android, iOS, macOS и Windows.

2. WebSocket и шифрование ГОСТ Р34.12-2015: Рассматривается использование технологии WebSocket для обеспечения двусторонней связи между клиентскими устройствами и серверами, а также применение шифрования ГОСТ Р34.12-2015 (Кузнечик) для защиты передаваемых данных. Для обмена данными между клиентскими приложениями предлагается

использовать WebSocket, а для защиты данных, отправляемых по сети, предлагается использовать шифрование ГОСТ Р34.12-2015 (Кузнечик).

Таким образом, обзор технологий для разработки мобильных приложений включает в себя изучение кроссплатформенных фреймворка .NET MAUI, а также рассматриваются такие технологии, как: AES-256 шифрование, ГОСТ Р34.12-2015 «Кузнечик» и технология QR-код.

Основная цель данной главы - описать существующие технологии, которые могут быть использованы для разработки защищенного мессенджера.

В результате исследования было выявлено, что использование протоколов шифрования, аутентификации и цифровых подписей является наиболее эффективным способом обеспечения безопасности защищенного канала связи.

Глава 3 Практическая часть

В данной главе описывается практическая реализация защищенного мессенджера с использованием выбранных методов шифрования и аутентификации. Рассматриваются основные модули и функциональность мессенджера. Также продемонстрирован интерфейс приложения, который продемонстрирован на Рисунке 1, возможность создать чат с другим пользователем и отправить сообщение в чате.

Рисунок 1 - Интерфейс приложения

Важным аспектом практической части работы является использование WebSocket для обмена данными между клиентскими приложениями. Это позволяет обеспечить быстрое и безопасное соединение между клиентом и сервером, минимизировать возможности для атак и повысить безопасность. Для

шифрования данных было использовано ГОСТ Р34.12-2015 (Кузнечик) шифрование, которое обеспечивает высокий уровень безопасности и конфиденциальности переписки. Каждому пользователю предоставляется свой уникальный ключ для шифрования и дешифрования сообщений, что обеспечивает дополнительный уровень безопасности.

В работе также было уделено внимание защите метаданных, таких как информация о времени отправки сообщений, идентификаторы отправителей и получателей, и другие подобные данные. Защита метаданных помогает предотвратить отслеживание пользователей и обеспечить приватность пользовательской активности.

В целом, практическая часть работы демонстрирует возможность создания защищенного мобильного мессенджера с использованием современных технологий и методов шифрования, что может быть полезно для пользователей, которые ценят безопасность своей переписки, а также для предприятий, которые нуждаются в обеспечении безопасного общения коллег во время работы.

Основная цель данной главы - реализовать защищенный мессенджер, который будет обеспечивать высокий уровень безопасности и конфиденциальности переписки.

В результате исследования был разработан прототип защищенного мессенджера.

ЗАКЛЮЧЕНИЕ

В процессе работы мы изучили способы организации безопасных каналов связи и разобрали на чем основывается передача данных в популярных мессенджерах. Были представлены примеры взломов и уязвимостей этих мессенджеров.

Можно сделать вывод, что организация безопасного канала связи в условиях одной WI-FI сети с использованием шифрования «Кузнечиком» является, хоть и не удобным с точки зрения дальности передачи данных, но более безопасным способом обмена данными, так как не используются сервера для хранения каких-либо данных и мета-данных, а также для перехвата данных нужно либо быть в данной сети и иметь ключ для расшифрования перехваченных сообщений, либо получить доступ к одному из устройств. Но даже при получении доступа к одному устройству, можно будет получить доступ только к ограниченному количеству сообщений.

Таким образом, данная работа имеет практическую значимость и может быть полезна для пользователей, которые ценят безопасность своей переписки, а также для людей, работающих на предприятиях, которые нуждаются в обеспечении общения коллег во время работы и быть уверенными в безопасности беседы.