МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«Южно-Уральский государственный университет (национальный исследовательский университет)»
Высшая школа электроники и компьютерных наук
Кафедра системного программирования

Разработка расширения протокола XMPP для согласования ключей шифрования с аутентификацией

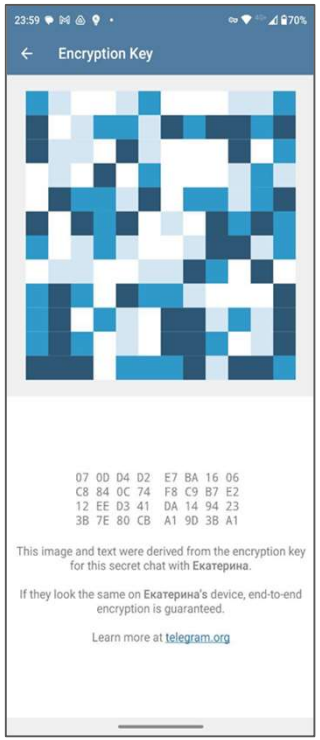
Автор:
студентка группы КЭ-433
Е.М. Короткова

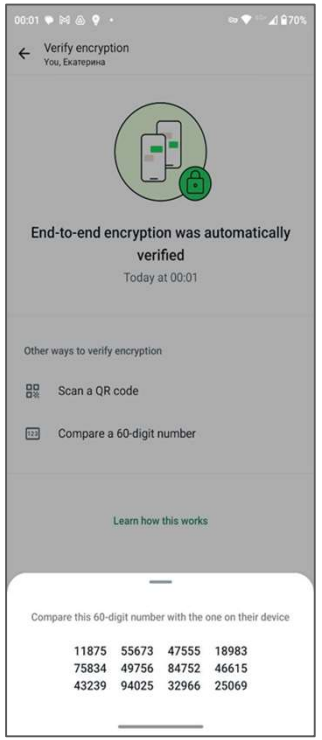
Научный руководитель:
доцент кафедры СП, к.п.н.
О.Н. Иванова

Челябинск, 2024 г.

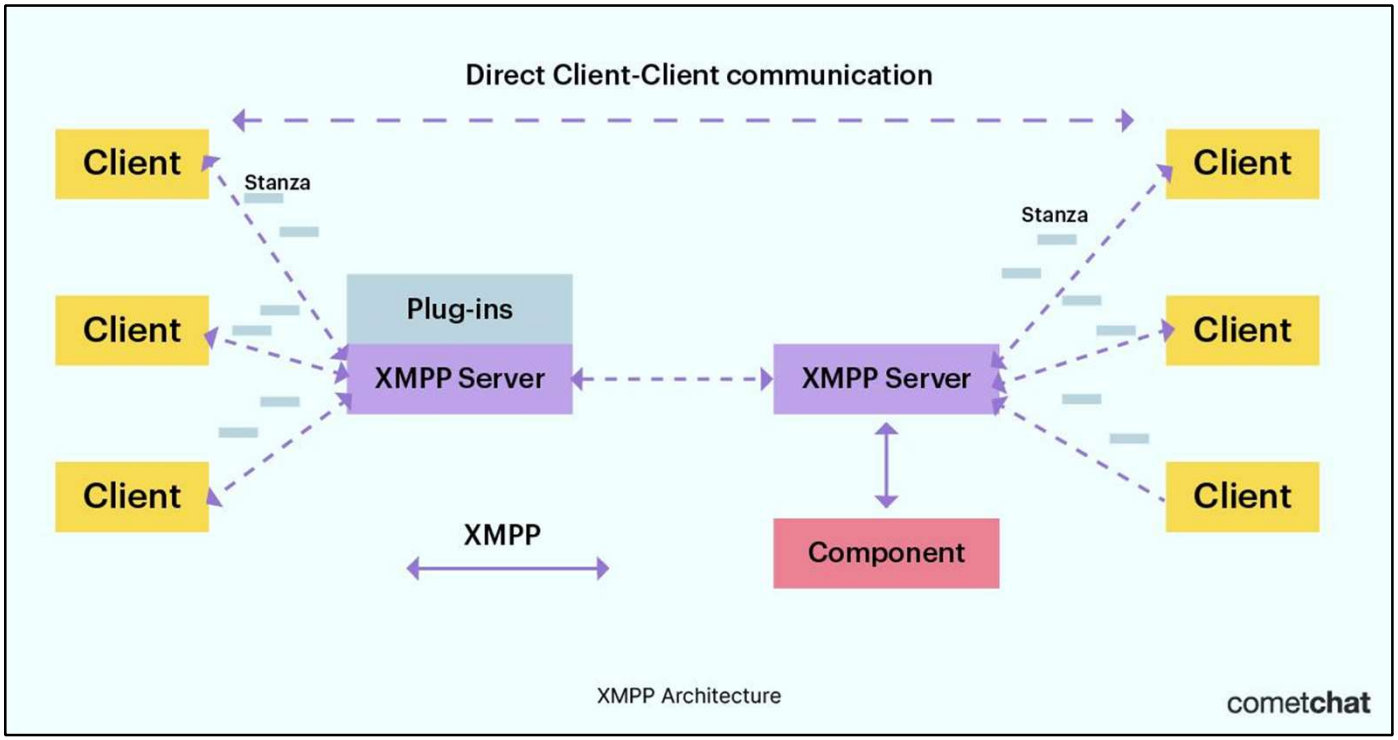
АКТУАЛЬНОСТЬ

- Шифрование является одним из основных элементов безопасности данных
- Проблема идентификации собеседников не решена ни в одном популярном мессенджере (Telegram, WhatsApp, Signal и др.)
- Пользователи пренебрегают ручной проверкой
- Была поставлена задача сделать идентификацию пользователей удобной и безопасной с помощью протокола согласования публичных ключей
- Для опытной реализации был выбран протокол XMPP





ПРОТОКОЛ XMPP



ЦЕЛЬ И ЗАДАЧИ

Цель:

Разработка расширения протокола XMPP для согласования ключей шифрования с аутентификацией

Задачи:

1. Провести анализ предметной области
2. Разработать алгоритм аутентификации пользователей и верификации их устройств
3. Написать текст документации протокола XEP
4. Разработать прототип реализации протокола
5. Реализовать протокол XEP на iOS-клиенте приложения
6. Протестировать работу протокола между клиентами

ПРОТОКОЛЫ КОНЕЧНОГО ШИФРОВАНИЯ XMPP

- Три основных схемы шифрования XMPP: Off-the-Record, OpenPGP и OMEMO Encryption

Протокол	OTR	OpenPGP	OMEMO
Forward secrecy	☑	✕	☑
Многоконечное шифрование	✕	☑	☑
Поддержка offline	✕	☑	☑
Синхронизация чатов между устройствами	✕	☑	☑

1

АНАЛИЗ АНАЛОГОВ

Метод	Суть	Недостатки
TLS	Создает специальный канал для передачи данных. Идентификация узла осуществляется за счет сертификатов.	Требует дополнительного времени и ресурсов.
Сравнение цифровых отпечатков	Верификация устройств происходит путем сравнения их уникальных цифровых отпечатков.	Долгий и трудоемкий процесс для пользователя.
OTR: проверка общим вопросом	Верификация устройства происходит ответом на вопрос, который дает владелец.	Не достаточная безопасность, вовлечение пользователей.

Слайд 6

1 @ekaterina.korotkova@redsolution.ru мне кажется этот слайд не нужен, мы уже сказали на 2 слайде как это делают в телеграме. Если хочешь я этот вопрос тебе подкину с места, чтобы не тратить время от доклада.
Andrew Nenakhov; 17.06.2024

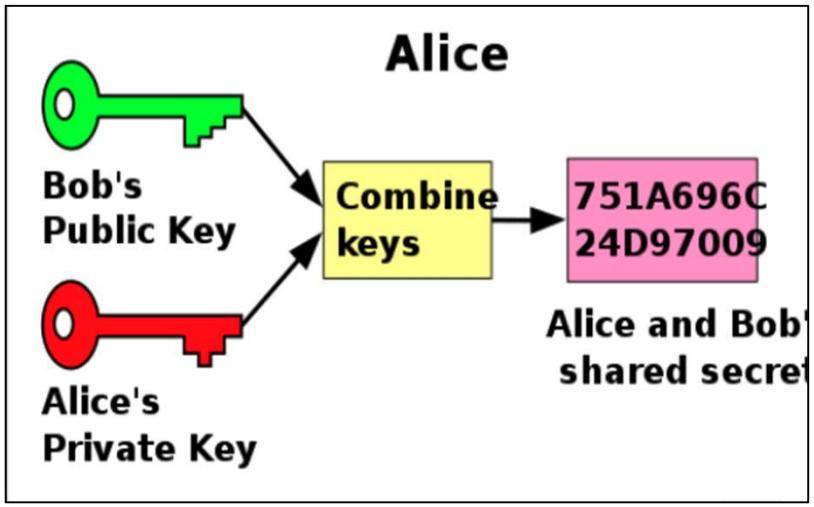
ФУНКЦИОНАЛЬНЫЕ ТРЕБОВАНИЯ

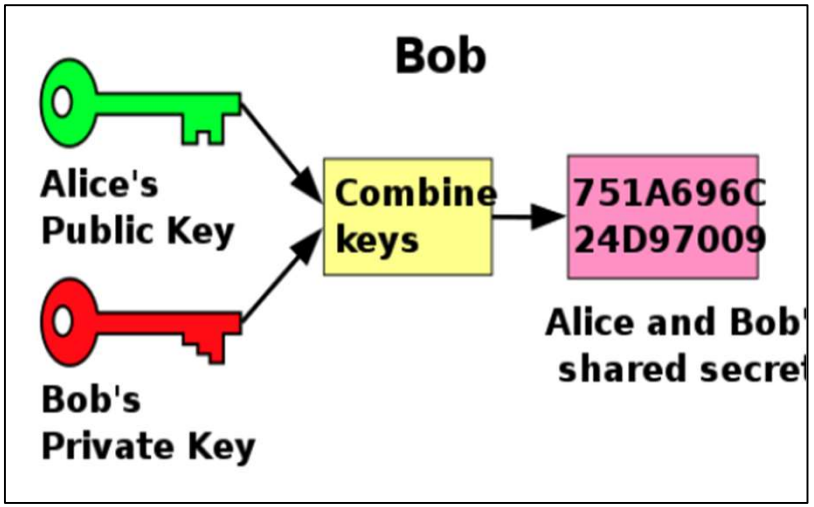
1. Протокол должен быть устойчив к атаками типа MITM.
2. Секретные данные должны передаваться в зашифрованном виде.
3. Данные, которые можно перехватить и/или изменить, должны передаваться подписанными.
4. Процесс аутентификации должен проходить автоматически, с минимальным включением пользователя.
5. Количество передач данных вне канала должно быть минимальным.

НЕФУНКЦИОНАЛЬНЫЕ ТРЕБОВАНИЯ

1. Протокол должен корректно работать между различными клиентами приложения.
2. Оповещение обеих сторон о неудачной сессии верификации.
3. Корректная работа протокола при наличии у пользователя нескольких устройств.
4. Протокол должен поддерживать устройства в offline.

ПРОТОКОЛ ДИФФИ-ХЕЛЛМАНА





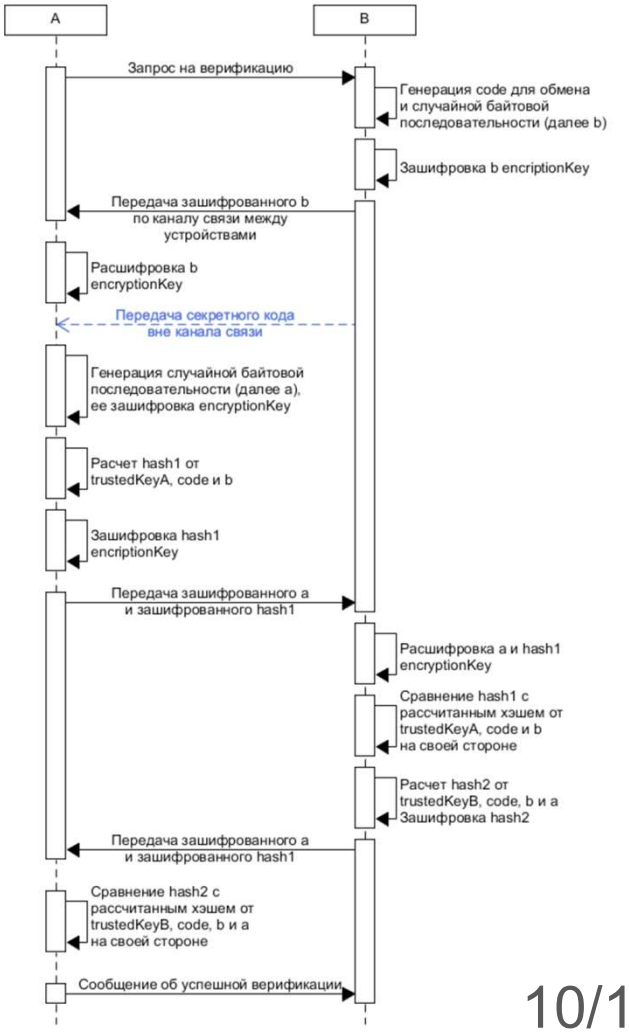
- Обеспечивает надежное шифрование
- Не обеспечивает аутентификацию собеседников

1. Diffie W., Hellman M. E. New Directions in Cryptography (англ.) // IEEE Transactions on Information Theory / F. Kschischang — IEEE, 1976. — Vol. 22, Iss. 6. — P. 644—654.

АЛГОРИТМ ПРОТОКОЛА

Этапы алгоритма:

1. A→B: Запрос на верификацию
2. B→A: Согласие на верификацию
3. 👤B→👤A: Передача секретного кода вне канала связи
4. A→B: Передача вычисленного хэша от данных, известных только обеим сторонам
5. B: Проверка полученного хэша
6. B→A: Передача вычисленного хэша от данных, известных только обеим сторонам
7. A: Проверка полученного хэша
8. A→B: Передача информации об успешной верификации



СРЕДСТВА РЕАЛИЗАЦИИ

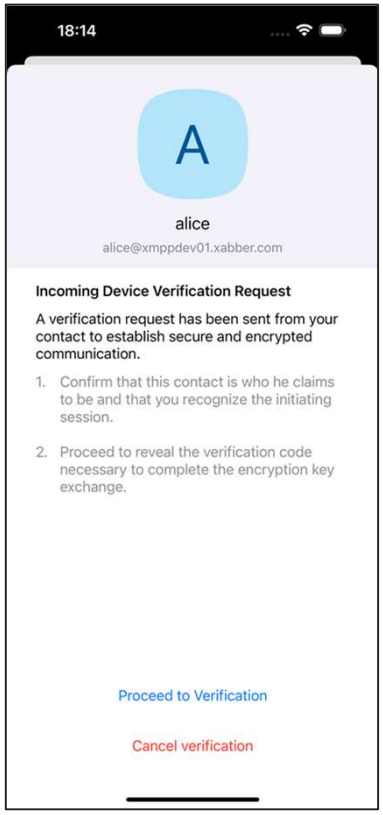
Реализация прототипа:

- Язык программирования Python 3.8
- Среда разработки PyCharm 2024.1.2
- Библиотека aioxmpp

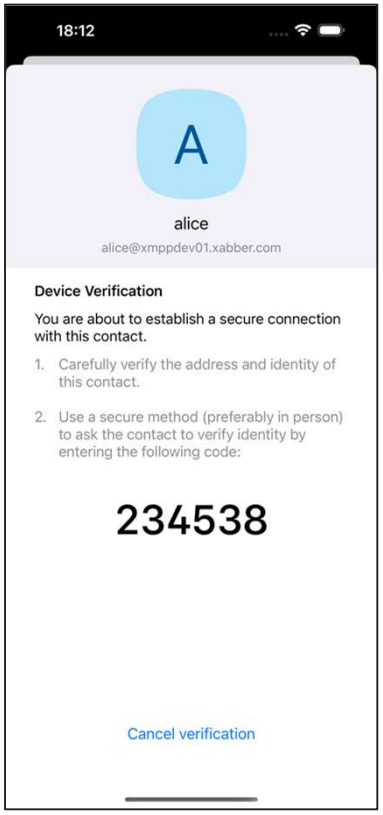
Реализация протокола на iOS-клиенте:

- Язык программирования Swift 5.10
- Среда разработки Xcode 15.2
- Фреймворк XMPPFramework
- Криптографическая эллиптическая кривая Curve25519
- Алгоритм шифрования AES в режиме CBC

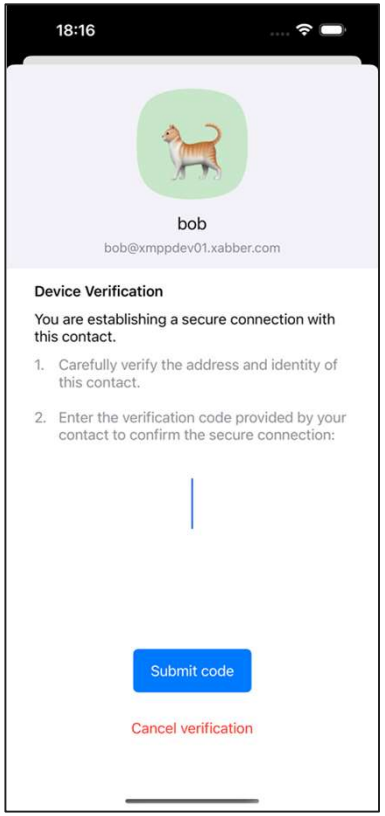
ПРОЦЕСС ВЕРИФИКАЦИИ



🐈 Боб получает запрос



🐈 Боб генерирует код



👩 Алиса вводит код на своем устройстве

ТЕСТИРОВАНИЕ

Тестирование версий продукта для различных платформ показало, что протокол работает корректно, обеспечена совместимость между версиями как для одной платформы (iOS-iOS, web-web), так и между разными платформами.

АКТ О ВНЕДРЕНИИ

redsolution
IT-решения для бизнеса

ООО «Редсолюшн»
http://www.redsolution.ru
info@redsolution.ru

454080, Россия, г. Челябинск
ул. Сони Кривой, 67-а, офис 5/1
тел: +7 351 750 5004

16 июня 2024 г.
исх. № 06-01

АКТ О ВНЕДРЕНИИ

Данный акт удостоверяет, что разработанный в Южно-Уральском государственном университете студенткой группы КЭ-433 Коротковой Е.М. протокол расширения XMPP для аутентификации ключей шифрования (XEP: Authenticated Key Exchange) был реализован в программных продуктах компании «Редсолюшн» на платформах iOS и Web.

Данный протокол позволил создать программное обеспечение, удобным образом решающее актуальную проблему аутентификации собеседника и предотвращения атак типа "человек посередине" (Man-in-the-Middle, MitM), которая до настоящего момента не имела удовлетворительного решения. На сегодняшний день, протокол используется в следующих программных продуктах:

- Xabber for iOS — версия XMPP-клиента Xabber для платформы iOS. Реализация была выполнена Коротковой Е.М.
- Xabber for Web — версия XMPP-клиента Xabber для использования в браузерах. Реализация была выполнена прочими разработчиками компании.

Тестирование версий продукта для различных платформ показало, что протокол работает корректно, обеспечена совместимость между версиями как для одной платформы (web-web, iOS-iOS), так и между различными платформами (web-iOS, iOS-web).

Директор ООО «Редсолюшн» Ненахов А. В.

М.П. redsolution

ЗАКЛЮЧЕНИЕ

В рамках данной работы был разработан протокол XEP-TRUST: Authenticated Key Exchange. При этом были решены нижеизложенные задачи.

1. Произведен обзор литературы и существующих алгоритмов.
2. Разработан алгоритм, используемый в протоколе.
3. Подготовлен текст документации протокола XEP.
4. Разработан прототип.
5. Реализован протокол на iOS-клиенте Xabber.
6. Протестирована работа протокола между клиентами приложения.

На данный момент готовится публикация протокола аутентификации.