

# InterMessage

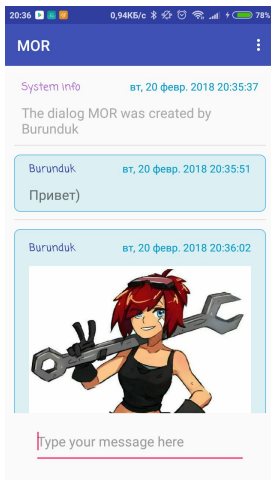
Дмитрий Саютин  
Александр Федоров

Санкт-Петербургский Академический Университет

22.02.2018

- Ситуация А:  
Вы студент и в вашем общежитии кто-то не заплатил за интернет, но сеть wi-fi всё ещё поднята. Как сообщить всему общежитию, что сегодня опять отключили горячую воду?
- Ситуация Б: Вы грибник и поехали группой за грибами в лес, а там нет ни Интернета ни общей сети wi-fi. Но вы не промах и взяли с собой мощный wi-fi роутер. Тогда, чтобы сообщить другим людям, что вы нашли грибную поляну, вам теперь не нужно идти искать их в лесу, надеясь, что поляну за это время не найдут другие грибники.

- Децентрализованный мессенджер работающий в локальной сети



- Многие системы видео-звонков используют возможности peer-to-peer связи (например skype).

- Многие системы видео-звонков используют возможности peer-to-peer связи (например skype).
- Есть некоторое количество мессенджеров в локальной сети (в основном для ПК).

- Многие системы видео-звонков используют возможности peer-to-peer связи (например skype).
- Есть некоторое количество мессенджеров в локальной сети (в основном для ПК).
- А вот децентрализованных в локальной сети уже немного!

- Многие системы видео-звонков используют возможности peer-to-peer связи (например skype).
- Есть некоторое количество мессенджеров в локальной сети (в основном для ПК).
- А вот децентрализованных в локальной сети уже немного!
- Ближайший известный аналог — FireChat.

- В основном ориентирован на публичные комнаты, а не приватные диалоги.



- В основном ориентирован на публичные комнаты, а не приватные диалоги.
- У него только сообщения и картинки.

- В основном ориентирован на публичные комнаты, а не приватные диалоги.
- У него только сообщения и картинки.
- Пытается комбинировать связь через интернет и локальные взаимодействия (в частности при первом запуске нужно подтвердить почту!).

- В основном ориентирован на публичные комнаты, а не приватные диалоги.
- У него только сообщения и картинки.
- Пытается комбинировать связь через интернет и локальные взаимодействия (в частности при первом запуске нужно подтвердить почту!).
- Умеет передавать сообщения ещё и по bluetooth.

- В основном ориентирован на публичные комнаты, а не приватные диалоги.
- У него только сообщения и картинки.
- Пытается комбинировать связь через интернет и локальные взаимодействия (в частности при первом запуске нужно подтвердить почту!).
- Умеет передавать сообщения ещё и по bluetooth.
- Использует чужие устройства для передачи сообщений.

- Работает по WiFi в локальной сети

- Работает по WiFi в локальной сети
- Полное End-To-End шифрование (RSA + AES)

- Работает по WiFi в локальной сети
- Полное End-To-End шифрование (RSA + AES)
- Автоматические цифровые подписи у каждого сообщения

- Работает по WiFi в локальной сети
- Полное End-To-End шифрование (RSA + AES)
- Автоматические цифровые подписи у каждого сообщения
- Поддержка различных типов сообщений (например картинки)



- Работает по WiFi в локальной сети
- Полное End-To-End шифрование (RSA + AES)
- Автоматические цифровые подписи у каждого сообщения
- Поддержка различных типов сообщений (например картинки)
- Другие устройства могут помогать с доставкой сообщений, но только внутри одного чата.

- У каждого человека есть публичный и приватный RSA-ключ.

- У каждого человека есть публичный и приватный RSA-ключ.
- Публичный ключ общеизвестен и является внутренним идентификатором в системе.

- У каждого человека есть публичный и приватный RSA-ключ.
- Публичный ключ общеизвестен и является внутренним идентификатором в системе.
- Как следствие, например, невозможна MITM-атака (система сразу обнаружит попытку подмены адресата).

- У каждого человека есть публичный и приватный RSA-ключ.
- Публичный ключ общеизвестен и является внутренним идентификатором в системе.
- Как следствие, например, невозможна MITM-атака (система сразу обнаружит попытку подмены адресата).
- Так как с помощью RSA можно шифровать только сравнительно короткие сообщения, то мы дополнительно используем AES.

- У каждого человека есть публичный и приватный RSA-ключ.
- Публичный ключ общеизвестен и является внутренним идентификатором в системе.
- Как следствие, например, невозможна MITM-атака (система сразу обнаружит попытку подмены адресата).
- Так как с помощью RSA можно шифровать только сравнительно короткие сообщения, то мы дополнительно используем AES.
- С помощью RSA шифруется AES ключ и дальнейший обмен данными происходит через AES.

- Проблема: так как нет центрального сервера, то нет общей истории сообщений, на каждом клиенте сообщения могут приходить в разном порядке.

## Сеть: логический уровень

- Проблема: так как нет центрального сервера, то нет общей истории сообщений, на каждом клиенте сообщения могут приходить в разном порядке.
- Нужно как-то научиться синхронизировать данные.



- Проблема: так как нет центрального сервера, то нет общей истории сообщений, на каждом клиенте сообщения могут приходить в разном порядке.
- Нужно как-то научиться синхронизировать данные.
- Наблюдение: если кто-то отправил нам в чат несколько сообщений, то вряд ли разумна ситуация если более раннее сообщение не доставилось, а более новое доставилось.

- Проблема: так как нет центрального сервера, то нет общей истории сообщений, на каждом клиенте сообщения могут приходить в разном порядке.
- Нужно как-то научиться синхронизировать данные.
- Наблюдение: если кто-то отправил нам в чат несколько сообщений, то вряд ли разумна ситуация если более раннее сообщение не доставилось, а более новое доставилось.
- Следовательно состояние нашего чата прекрасно описывает некоторый массив целых чисел — сколько сообщений у нас есть от соответствующего человека.

- Давайте для каждого человека в нашем чате поддерживать их массивы, в том виде как мы их видели в последний раз.

- Давайте для каждого человека в нашем чате поддерживать их массивы, в том виде как мы их видели в последний раз.
- Тогда мы более-менее легко можем поддерживать список людей, у которых хотя бы в одном чате недостаточно новый список сообщений.
- Плохая новость: на каждое новое сообщение в чате запускается достаточно много новых синхронизаций.

- Давайте для каждого человека в нашем чате поддерживать их массивы, в том виде как мы их видели в последний раз.
- Тогда мы более-менее легко можем поддерживать список людей, у которых хотя бы в одном чате недостаточно новый список сообщений.
- Плохая новость: на каждое новое сообщение в чате запускается достаточно много новых синхронизаций.
- Хорошая новость: после любой синхронизации хотя бы один массив сведений у какого-то человека увеличивается.

- С физической точки зрения мы используем UDP бродкасты и прямые соединения по TCP.

- С физической точки зрения мы используем UDP бродкасты и прямые соединения по TCP.
- С помощью UDP можно обнаружить других клиентов в той же сети.

- С физической точки зрения мы используем UDP бродкасты и прямые соединения по TCP.
- С помощью UDP можно обнаружить других клиентов в той же сети.
- С помощью TCP происходит непосредственно синхронизация данных между двумя устройствами.



- Все сообщения и информация о пользователях сохраняется на устройстве с помощью SQLite.

- Все сообщения и информация о пользователях сохраняется на устройстве с помощью SQLite.
- Кеширование сообщений

- Проблема: откуда брать людей, которых можно добавить в диалог?

- Проблема: откуда брать людей, которых можно добавить в диалог?
- Решение: Давайте предлагать всех людей, которые сейчас находятся поблизости

- Дмитрий Саютин — сеть, шифрование, цифровые подписи, логика работы приложения.
- Александр Федоров — интерфейс, база данных, а также взаимодействие между собой частей программы

.end()

Вопросы?