Hello world!

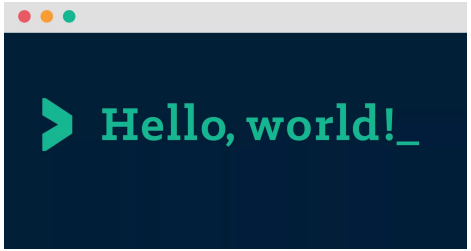
Jiří Horák, Adam Ivora, Ivan Mitruk

Content

- Intro
- Provided services
- Future plans
- Security
- Communication

Introduction

- Hello world! is an instant messaging application similar to WhatsApp
- It’s name comes from simple program used to illustrate syntax of programming language
- It’s primarily made for tech-savvy people or tech enthusiasts, who wants simple and safe way to communicate

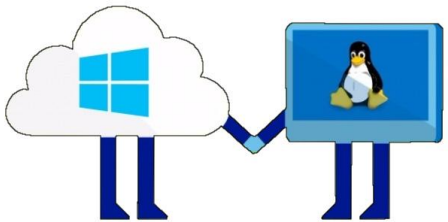


Provided services

- Registration of new users
- Login as an existing user
- Ability to find other users
- Safe way to communicate with other users

Future plans

- Expand to other operating systems (only linux for now)
- Simple graphical interface (only text based for now)
- Add group chats (only person to person communication for now)

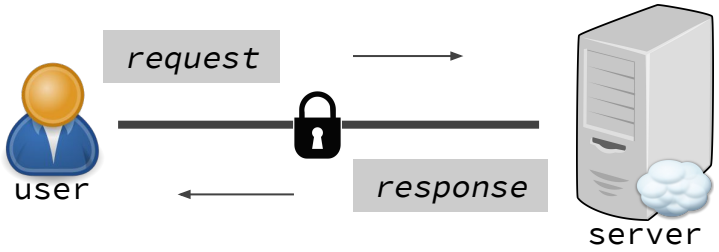


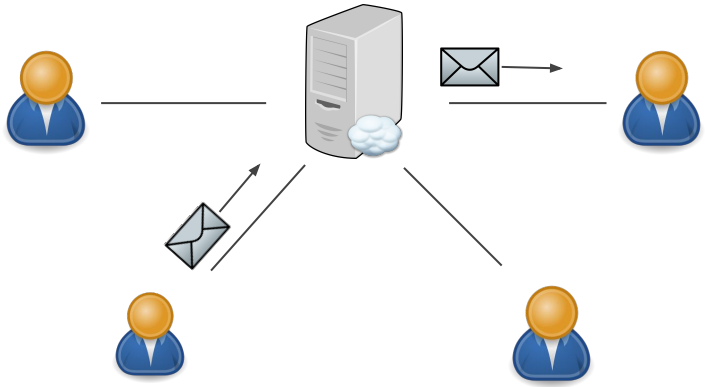
Security

- RSA 2048
  - secure channel establishment
  - derivation of cipher keys
- AES 128
  - message encryption
- SHA 512
  - hashing (MAC)
- X3DH key agreement protocol
  - initial symmetric key
- Double ratchet
  - for deriving new symmetric key each time message is sent

Communication

- Communication with server is in a form of requests and responses (request and responses have predefined syntax)
- Users exchange messages through server (one hop network)





Thank you for your time

Have a nice day!