Authentichat

GROUP MEMEBERS

Robbie Bridgewater

Dawit Woldegiorgis

Ryan Zavoral

SUMMARY

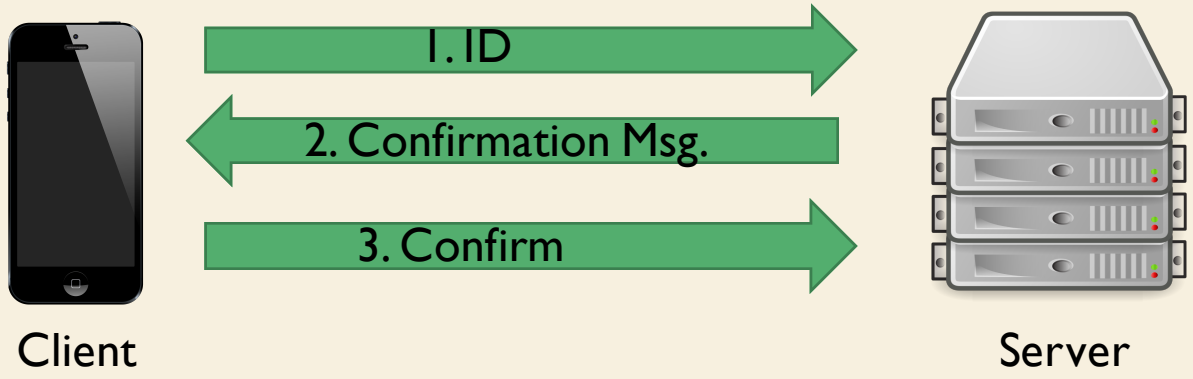
- What is Authentichat?
  - Secure messaging client for iPhone
- How is it special?
  - Physical proximity for establishing connection
  - Private keys for verification
- Why use it?
  - Difficult to impersonate another user
  - Encryption reduces network sniffing risks
  - Authentic chat experience!

SECURITY MODEL

- Identity:
  - Phone Number - Primary
  - Device ID – Secondary
- Communication:
  - Authentication by user (one-time)
  - Private key sharing for establishing secure channel
  - Message encryption
  - Evaluate integrity via encrypted checksum

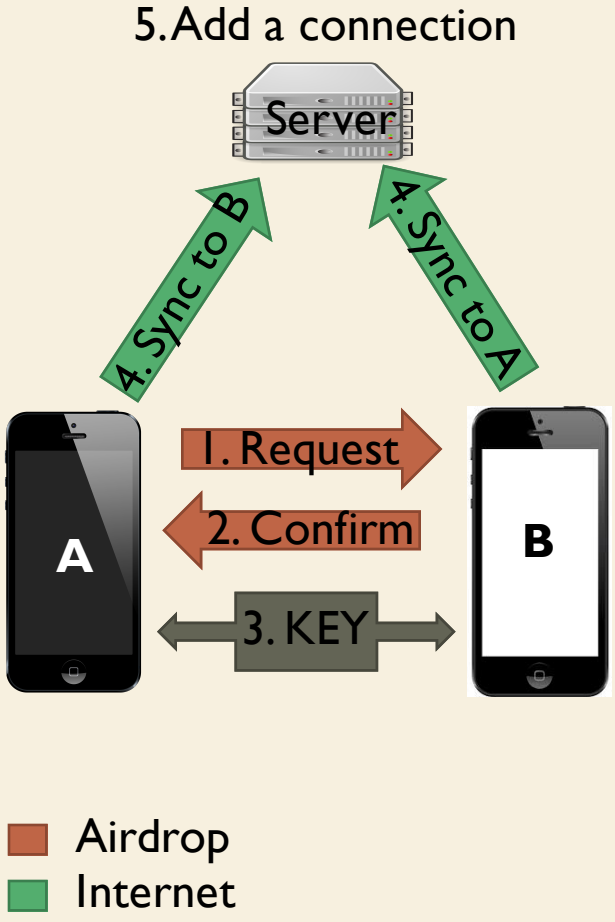
SECURITY MODEL - IDENTITY

- Establishing Identity
  - Confirm via text
  - Reset mechanism

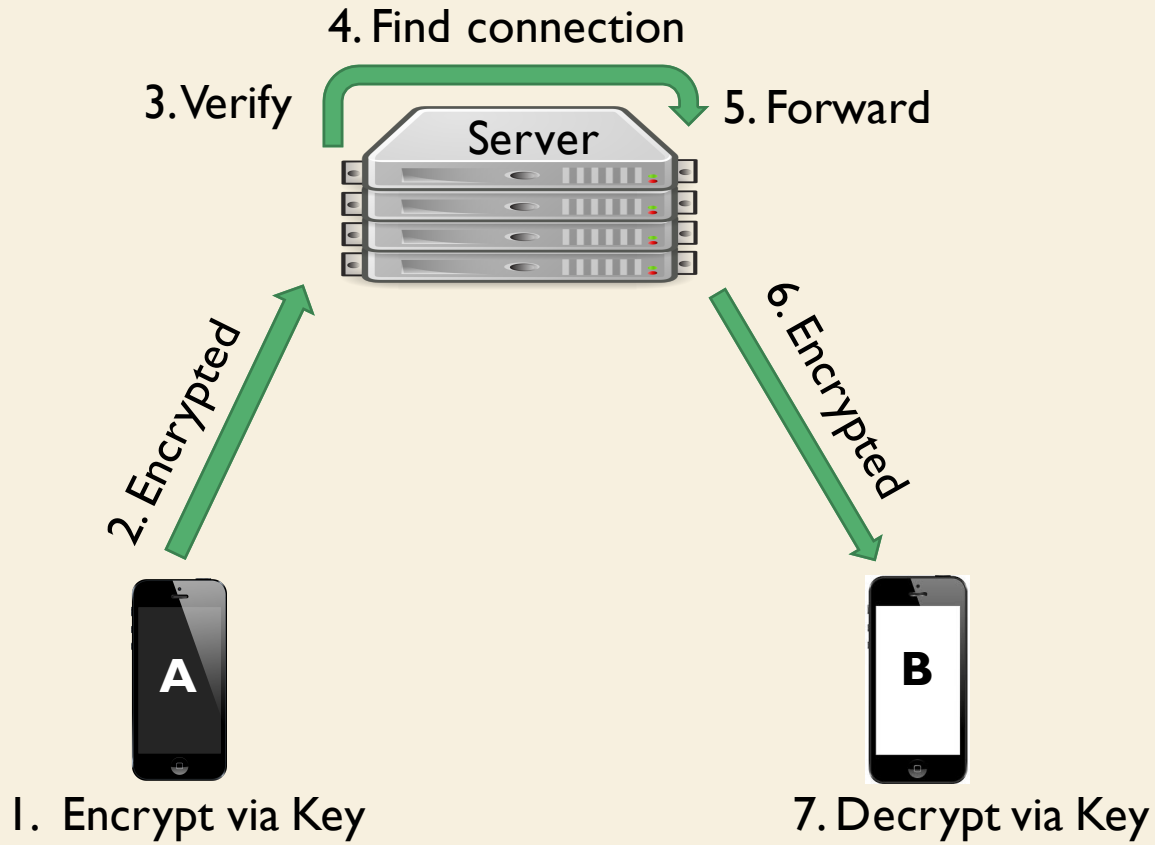


SECURITY MODEL - COMMUNICATION

Establishing Identity



Sending Message



IMPLEMENTATION

- Application source code
  - Swift: backend/frontend
  - Objective C: Wrapper for C++ code (security/low level)
- Messaging API – Sinch
  - Parse web server
- Task division
  - Ryan: Implement security algorithm
  - Robbie: Backend development
  - Dawit: Frontend development & Security penetration testing

REFERENCES

C++ Documentation :
http://www.cplusplus.com/

Objective-C Tutorial and Documentation:
http://www.tutorialspoint.com/ios/ios_objective_c.htm

Swift Documentation:
https://developer.apple.com/swift/

Airdrop Usage with IOS Applications
https://developer.apple.com/library/ios/samplecode/sc2273/Introduction/Intro.html

Symmetric Key Encryption Links
https://en.wikipedia.org/wiki/Symmetric-key_algorithm

Parse Web Server
https://**parse**.com/

Sinch
https://www.sinch.com