Encrypted Chat Application

Phase I

Pied Piper

Braulio Flores, Ariel Nguyen

CECS 478

Application Properties

- Application will provide end to end encryption for messages.
- Should time allow, support for image and group messages will be incorporated.
- Application client will be implemented for Android in Java.
- The backend will be implemented as a RESTful server using the LAMP stack.
- Will provide confidentiality using OpenSLL.
- Certificates will be generated through Let's Encrypt.

Assets/Stakeholders

- For our purposes we will define the stakeholder to be the user.
- The asset will be the messages sent by users, and all of the data attached to them.
- By doing this, the user is the priority and the design will always prioritize the safety of user information.

Adversarial Model

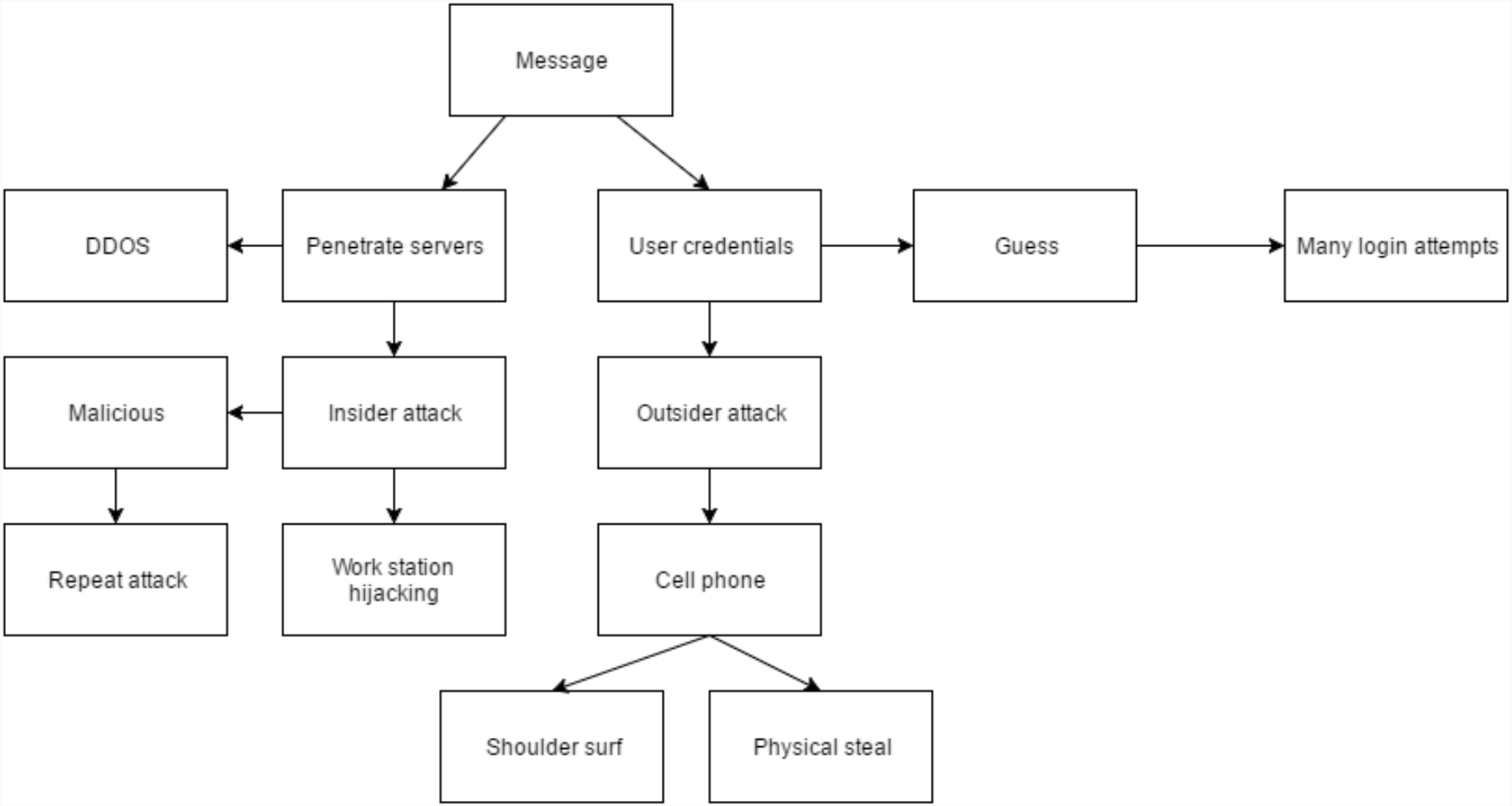
Insider Adversary

- To prevent an insider attack (Man in the Middle), we will use OpenSSL to generate 2048 bit keys.

Outsider Adversary

- To prevent an outsider attack (eavesdropping), we will implement Transport Layer Security (TLS).

Possible Vulnerabilities



Previous Work

WhatsApp

- https://www.whatsapp.com/security/WhatsApp-Security-Whitepaper.pdf

Signal

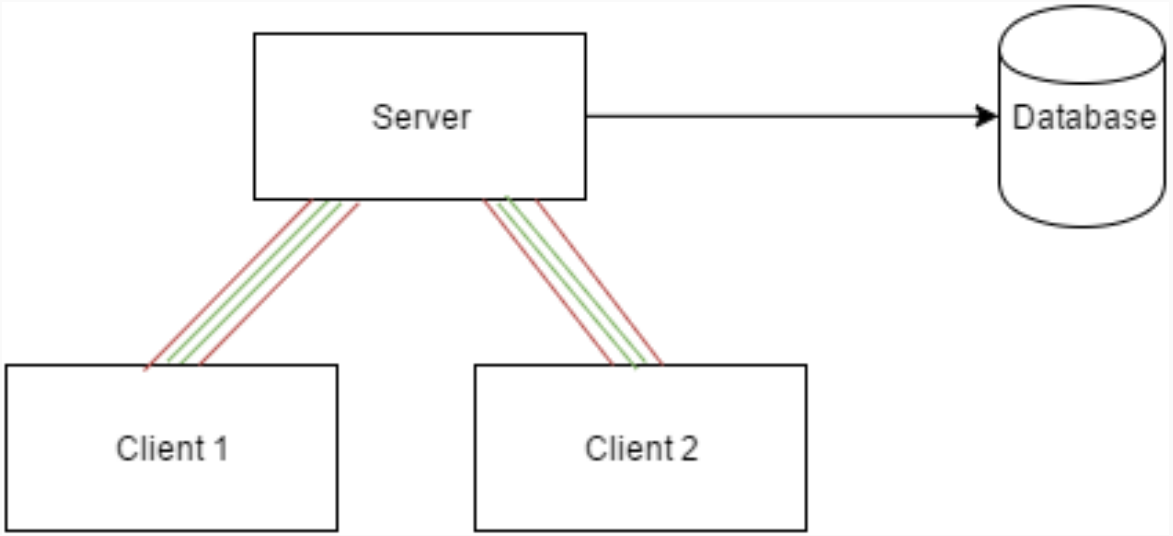
- https://open-whisper-systems.readme.io/

Wickr

- https://www.wickr.com/security/how-it-works

Solution

- Client will connect to server through HTTPS and TLS for secure connections.
- User credentials will be hashed when stored to prevent information from being stolen.
- Server will communicate the public keys and messages encrypted with public and private keys



Analysis

- Our system relies on the assumptions that AES, TLS/SSL, HTTPS, and OpenSSL are computationally secure mechanisms.
- We are not reinventing the wheel, merely building on proven technologies.
- By abiding by their limitations we can guarantee message confidentiality and integrity.
- Confidentiality will be achieved using OpenSSL.
- Integrity will be handled with TLS connections between the client and server.
- Authentication will be achieved by storing user logins and passwords securely.