Team Nexus:

Adonias Lopez Payan

Henna Girish Gohil

**Application Properties:**

We are developing a messenger app that allows a user to send messages to a single recipient. The messenger app will be developed under the Android JDK and we will use TextSecure server for our backend/server. We will be using TextSecure Protocol for authentication. OpenSSL will be used to implement Transport Layer Security 1.2 (TLS) to handle the security layer and establishes connection between the server and client. Furthermore, we will use MySQL database to store credentials of the users and messages. LetsEncypt will be used to create key pairs to authorize certificates being passed.

**Assets and Stakeholders:**

The stakeholder for this project will be the user of the app. The asset of the stakeholder is the message being sent through the sever to another client (recipient).

**Adversarial Model:**

* **Outside Attacks:**
  + We will incorporate end-to-end encryption to combat eavesdropping from outside attackers.
  + To limit the effectiveness of a brute force attack, the private-key size is going to be set to 2048-bit.
* **Inside Attacks:**
  + We will use endpoint authentication to combat Man-in-the-Middle (MitM) attacks. OpenSSL will allow us to use TLS to implement an authentication process for both messengers using mutual certificate authority.

**Possible Vulnerabilities:**

Possible vulnerabilities of our system can consist of a workstation hijacking and DDOS attacks. Our app cannot guarantee security from someone stealing the device and gaining the messages that have been decrypted from the client side. In addition, no mechanisms will be set up to protect the dignity and availability of the server.

**Possible Related Previous Work:**

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

**Complete Description of Solution:**