Name for project

COMP4109 Group Project

Adam Payzant 101082175 Kelvin Ratsamany William So Anders Sonstenes

January 23, 2021

1 Introduction

For this project, we will be implementing a secure messaging and video app.

2 Background

In the modern messaging space, all mainstream options have at least a few failings or tradeoffs that fail the goal of absolute security. SMS (conventional texting) is highly susceptable to transmission interception, does not transmit securely, and is easily traced back to the sender/recipient. [1] Apple's iMessage offers end-to-end encryption (which means the message is sent encrypted and can only be unencrypted by the recipient), but the messages are still stored on Apple's servers and are only usable on Apple devices. In 2021, WhatsApp changed their privacy policy to allow more sharing of user data towards Facebook, which can include some messages. [2] Even the posterchild of secure messaging apps, Signal, has tradeoffs as data still goes through their servers, can be stored on their servers, and prevents anonymity by requiring a phone number. [3]

Based on these failings, our app aims to mitigate them by following these principles:

1. Message Security - A message should be encrypted before sending and can only by the recipient upon recieving the message
2. Safe Storage - Messages should be stored in safe way and should strive to gurantee complete deletion upon request
3. Anonymity - Users should be anonymous in the eyes of the system. This increases user safety by increasing the work factor to attack an individual

Each of these principles are vital for a number of reasons. Message security is vital as there is no practical way to gurantee secure transmission over the internet. When sending unsecure data, a Man-in-the-Middle Attack, an attack where data in transit is intercepted, read, then send to the intended target, can easily collect user information. [4] Message security can be achieved by using a public-key encryption method, where the data is encrypted using the recipient's public key, and only decrypted by the recipient's secret private key. This will mitigate any attacks occuring during data transmission. Safe Storage is critical as attacks can still occur after the message has been recieved. Storing messages unencrypted posing the risk of that storage service being broken into, and allows an attack to collect the contents. In addition, even if the stored data is encrypted, it may not provide sufficient work factor, meaning an attack must take more effort than the data is worth, to actually be considered secure. [5] Not to mention, while an encryption method today may be considered secure, in 5 years the method may no longer be considered to be a sufficient work factor. Finally, anonymity is vital to making a secure messaging system. Making users anonymous in the eyes of the system adds yet another layer of security should the system be breached. Doing so increases the work required for an attacker to pinpoint a user's identity, making a security breach less damaging.

3 System Descrption

4 Implementation Plan

[1] https://www.popularmechanics.com/technology/security/a29789903/what-is-sms/

[2] https://www.androidpolice.com/2021/01/12/whatsapps-new-terms-of-service-are-a-facebook-or-die-ultimatum/

[3] https://nakedsecurity.sophos.com/2020/05/22/signal-secure-messaging-can-now-identify-you-without-a-phone-number/

[4] https://www.csoonline.com/article/3340117/what-is-a-man-in-the-middle-attack-how-mitm-attacks-work-and-how-to-prevent-them
html

[5] van Oorschot, Paul C. *Computer Security and the Internet: Tools and Jewels.* Springer, 25 Sept 2019

Bibliography