Threat Model 153

Chase Maguire, Kauana dos Santos, Kush Patel

May 2019

1 Preparation

Below, we go through some of the definitions

1.1 Asset

Our asset is our application, SafeChat. It is an app that facilitates anonymous chatting, using Firebase, NodeJS, and React Native. The messages will aim to be secure, so that only the sender and the recipient can see these messages. The sender and recipient will be able to "find" each other through the app, so that they can start the chat in the first place.

1.2 Threat Agent

The threat agent is who would want to exploit our assets. While in a broader sense, a moral dilemma occurs through pure anonymous chatting, we do not care about this, for the scope of the class. So, our threat agent would be anyone who wants to read chats. They could use this information to dox, exploit, or blackmail. Though the specifics may depend on the context of their goals, and whatever they could get their hands on, the main point is that they want these anonymous messages.
Encrypted messages could be broken through large amounts of brute force, however.

1.3 Attack Surface

Our attack vectors, will be in the following places.

1. Through the network (Sniffing packets, MITM)
2. The device itself (If the device is compromised, the user should still be guaranteed security)
3. User input (through login services, or through messages)

1.4 Likelihood

The likelihood of an attack happening and succeeding will be astronomically low. Since we are not a fortune 500, any serious attack will never happen. We do however, will have to run simulated attacks on our own system, and to find the flaws in the system as well.
However, we will need to be conscious of the network sniffers. We cannot detect these, so security of messages will be very important.

1.5 Impact

The potential damage is small. We're planning to store messages for only delivery systems, and considering burning the messages and sending a read reciept right after. The smaller impact, and possibly only other case is the one where the attacker gains access, through decryption or any other kind of listening attack. They would only gain access to both of the compromised users chats.

2 Objective

To create a platform on which two people can find each other, and begin a secure and private chat

2.1 Platform

We will be using React Native for the user side of the applicaiton. It will communicate with a Firebase server. The server will handle account creation, chat setup, and message passing. The user will register with an email, username, and password. The only public information is the username, and it is how users will setup chats with each other.

2.2 Security

We will most likely be using Virgil security as our encryption library. It integrates well with Javascript and Firebase. The server will not store any messages, and we are currently considering burning the messages upon read, and sending a read receipt, so that they don't remain on the users device. We will be using end to end encryption.
The list of what Virgil uses is here
https://developer.virgilsecurity.com/docs/sdk-and-tools

Template

Built by following:
https : *//github.com/OWASP/CheatSheetSeries/blob/master/cheatsheets/Threat_Modeling_Cheat_Sheet.md*