Implementation and Study of a Man in the Middle Attack on the Signal Private Messenger

Introduction

The Signal protocol has become ubiquitous in private messaging, with applications like Whatsapp, Facebook Messenger and Signal [1] [2] [3] being built on it to provide forward secrecy for their end-to-end encryption. But the protocol does not give any guarantee w.r.t whom a user is communicating with after fetching the cryptographic data from the untrusted server [4]. To exclude Man in the Middle (MiTM) & impersonation attacks, the conversation endpoints must verify each other's identity [5].

But what does staging such an attack entail? Answering this question and studying the associated challenges is the goal of this project. We will be working with the open-source Signal Android Client as the target [6].

Tentative Tasks

- Familiarize yourself with the Signal Protocol and application.
- Research which tools may be used to build a MiTM-proxy.
- Determine which assumptions must be met and modify the Android client to meet them.
- Implement the attack.
- Come up with and test out different scenarios and determine the difficulties and how to overcome them.
- Write the thesis.

Preferred Skillset

- Strong programming skills.
- Prior experience with Android programming, Java and Kotlin beneficial.
- Familiarity with Git or strong willingness to learn.
- Interest in understanding and breaking security protocols.
- Knowledge of Network Security concepts and technologies.

Advisors

- Christelle Gloor
- Prof. Adrian Perrig

References

[1] M. Marlinspike, "Whatsapp's signal protocol integration is now complete," [Online]. Available: https://signal.org/blog/whatsapp-complete/. [Accessed 16 02 2023].

[2] M. Marlinspike, "Facebook messenger deploys signal protocol for end-to-end encryption," [Online]. Available: https://signal.org/blog/facebook-messenger/. [Accessed 16 02 2023].

[3] Signal, "Signal technical information," [Online]. Available: https://signal.org/docs/. [Accessed 16 02 2023].

[4] Signal, "Signal X3DH specification," [Online]. Available: https://signal.org/docs/specifications/x3dh/. [Accessed 16 02 2023].

[5] M. Marlinspike, "Safety number updates," [Online]. Available: https://signal.org/blog/verified-safety-number-updates/. [Accessed 16 02 2023].

[6] Signal, "Signal Android Github," [Online]. Available: https://github.com/signalapp/Signal-Android. [Accessed 16 02 2023].