Lehrstuhl für Sicherheit in der Informatik
Prof. Dr. Claudia Eckert

Fraunhofer AISEC

Announcement: Student job in cooperation with Fraunhofer AISEC, Garching

Secure Messenger based on the Signal Messaging Protocol and Attribute Based Usage Control

Motivation and Topic

Several of the currently available messengers already provide sophisticated security measures including forward secrecy, end-to-end encryption and mutual authentication.

In this project, the goal is to build a messenger using such a protocol (specifically the Signal Messaging Protocol[1]) with additional attribute based usage control (LUCON[2]). In the messenger, users will be able to mark messages with attributes that classify the content of the message. Depending on the labels of a message, LUCON rules will control what can be done with the message. Examples for rules could be “message lifetime 60min”, “message will be deleted after reading”, or “message can only be received if recipient is authenticated”. The rules should be enforced directly in the client, or in the intermediate server.

If you enjoy self-driven research & development in this area, we currently have an opening for a research assistant position. The monthly working time is 40 hours, but can be de-/increased on request.

Required skills

- Programming Android Applications (Java) and programming in general (Java)
- Linux experience for setting up a backend
- Experience in writing unit tests and integration tests is a nice-to-have
- Experience in network security (particularly security principles) is a nice-to-have
- Experience in (practical) cryptography is a nice-to-have
- Fluency in German or English

Contact

Fraunhofer Institute for Applied and Integrated Security (AISEC)
Dennis Titze
Email: dennis.titze@aisec.fraunhofer.de
Phone: +49 89 322-9986-114

[1] https://signal.org/docs/

[2] https://industrial-data-space.github.io/trusted-connector-documentation/docs/usage_control/#introduction-to-lucon/