Seminar

The future of Kerberos for IoT applications

Wichtiger Hinweis: Diese Arbeit wird am Fraunhofer AISEC betreut.

Kerberos [1] was developed at MIT in the mid-eighties as an authentication and key exchange protocol and currently is still widely used. Since it was developed in times when asymmetric cryptography was in its infancy it relays on symmetric algorithms. Exactly this characteristic of Kerberos makes it especially interesting for IoT applications. Symmetric cryptography is way more efficient and thus more suitable for constrained IoT devices than asymmetric cryptography. In the course of this work the state of the art of Kerberos-like protocols for IoT and related approaches for key exchange using only symmetric cryptography has to summarized and analyzed. Depending on the findings and if the student is interested this work can be carried forward as a master thesis in the next semester.


Contact

Request topic

Advisors

Michael Pehl
Stefan Hristozov (Fraunhofer AISEC)