Open Thesis / Project

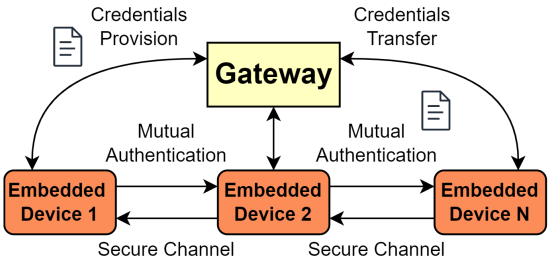
Future-Proofing Implicit Certificates: Ensuring Post-Quantum Security in IoT

Thesis Type

Master Project / Master Thesis

Motivation

Modern Internet of Things (IoT) systems need to rely on security now more than ever, but simply reusing already established security public key infrastructures (PKI) is challenging. These infrastructures often rely on complex protocols, such as TLS, which can be resource-demanding and unsuitable for constrained devices. In the world of cybersecurity, implicit certificates are a sophisticated cryptographic concept. They have gained popularity thanks to their efficiency and scalability and offer a unique approach to managing authentication and security. They differ from traditional explicit certificates in that they allow each entity to have its own certificate and calculate public keys on the go, ultimately requiring smaller certificate sizes.
Although implicit certificate schemes have been effective for networked embedded systems, latest research has revealed that they are not post-quantum secure. This is because these schemes rely on elliptic curves, which makes them vulnerable to quantum attacks. Our aim is to verify these strong claims and look for potential solutions. The goal set with this thesis will include a strong emphasis on protocol analysis, but also the implementation and testing on wireless embedded systems to replicate real-world cases.



Goals and Tasks

Within this context, students can explore several directions and perform different tasks, such as:

- Use the current research paper [1] on the post-quantum security of implicit certificates as a starting ground for understanding the main concepts and motivational goals;
- Replicate some of the presented research claims and work on exploring potential solutions;
- Gain an understanding of our current implicit certificate reference model and integrate it into a wireless embedded system;
- Evaluate the potential security extensions using either a formal or informal security analysis and perform performance analysis on the implemented wireless embedded system.

[1] http://bit.ly/impl-cert-postquantum-publ

Target Group

- Students of ICE/Telematics;
- Students of Computer Science;
- Students of Software Engineering.

Required Prior Knowledge

- Solid skills in C programming;
- Experience with embedded systems;
- Understanding of basic security concepts.

Contact Person

- Dipl.-Ing. Fikret Basic
  basic@tugraz.at
- Assoc.Prof. Carlo Alberto Boano
  cboano@tugraz.at

4480 – Institute of Technical Informatics (ITI)

Low-Power Embedded Networked Systems (LENS) Group
Group leader: Assoc.Prof. Carlo Alberto Boano