Open Thesis / Project

Are Implicit Certificates still Necessary? The Future of IoT Security

Thesis Type

Bachelor Thesis, Seminar Project,
Master Project / Master Thesis

Motivation

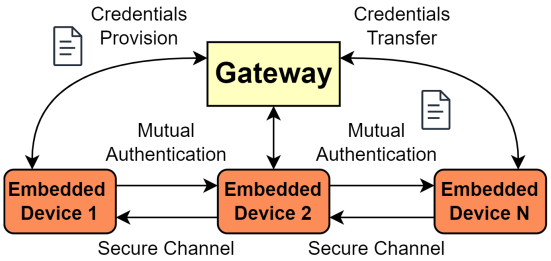
In recent years, research has increasingly focused on enhancing implicit certificates, particularly the Elliptic Curve Qu-Vanstone (ECQV) scheme. Implicit certificates offer a significant advantage, shorter signatures, making them ideal for resource-constrained IoT devices that must store and exchange numerous certificates. However, despite their potential, several challenges persist:

- Decentralized Issuance - Can third parties issue certificates independently at a local level?
- Reputability Concerns - Traditional public key possession does not inherently prove ownership by the original requester.

With the emergence of more powerful IoT devices, we must reevaluate the role of implicit certificates:

- Do they still offer a significant advantage over explicit certificates?
- In which direction should future research on implicit certificates evolve?

If you are interested in cryptographic security for IoT and want to contribute to shaping the future of certificate-based authentication, this thesis topic offers a look at an alternative opportunity!



Goals and Tasks

Within this context, students can explore several directions depending on the scope of the thesis:

- Review the available literature on implicit certificates and their use with embedded devices, understanding the main challenges.
- Replicate some of the research claims, such as [1], and work on exploring potential integrations;
- Gain an understanding of both the latest implicit and explicit certificate reference models and integrate them into an embedded system;
- Evaluate the potential security extensions using either a formal or informal security analysis and perform performance analysis on an implemented wireless networked system.

[1] Liu et al., "Extension of elliptic curve Qu-Vanstone certificates and their applications", Journal of Information Security and Applications, 2022.

Target Group

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

Required Prior Knowledge

- Skills in C programming;
- Understanding of security concepts;
- Experience with embedded systems is a plus.

Contact Person

- Dr. Fikret Basic
  basic@tugraz.at

4480 – Institute of Technical Informatics (ITI)

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