Abstract

This thesis explores the security challenges within connected infrastructures such as cooperative intelligent transport systems where vehicles and infrastructure has the ability to communicate efficiently via both short-range and cellular technologies. The primary focus is on the vulnerabilities of weak devices with poor randomness and limited computational resources. The research is two-fold: firstly, it investigates the security of efficient signature and authentication schemes in multi-node environments by proposing novel cryprographic schemes; secondly, we assess the feasibility and performance of these cryptographic solutions through proof of concept implementations for IoT and low-powered devices. Theoretical and practical approaches are thus used, with formal security proofs and software implementations primarily in Python. Our goal is to bridge the gap between theoretical cryptography and industry implementation, providing secure and feasible solutions for intelligent connected infrastructures, such as vehicular ad-hoc networks.

The research output was five core papers P_{I} to P_{V}, proposing enhanced schemes used in several different use cases. The schemes in papers P_{I}, P_{II} and P_{V} are proven secure against ephemeral key leakage. In papers P_{I} and P_{II} the original schemes are shown vulnerable in the stronger security models, referred to as cryptanalysis, whereas in paper P_{V} we provide a stronger version of cryptanalysis where the original scheme is shown weak under the current security model. We use in particular three different security enhancement techniques: exponentiation, key split and key refresh mechanisms. These techniques are used in papers $\mathsf{P}_{\mathsf{I}}, \mathsf{P}_{\mathsf{II}}, \mathsf{P}_{\mathsf{III}}$ and P_{V}. However, in core paper P_{IV} we also provide a novel scheme for source hiding - particularly important for privacy in connected vehicle systems - in a multi-party environment using standard re-encryption, mixing and ring signature primitives. In addition to the core papers' results, we also provide an additional proof of security for core paper P_{I}, using the asymmetric pairing setup, whereas the previous proofs are in the symmetric setup. Finally, we also provide as an additional contribution, the performance analysis of all schemes developed and run in laboratory equipment from the Swedish Transport Administration.