Deploying a Vehicular Credential Management System: Challenges Ahead

Mohammad Khodaei, Hongyu Jin and Panos Papadimitratos
Networked Systems Security Group
Royal Institute of Technology, Stockholm, Sweden

Abstract
Several years of academic and industrial research efforts have converged to a common understanding on fundamental security building blocks for the upcoming Vehicular Communication (VC) systems. There is growing consensus towards deploying a Vehicular Public-Key Infrastructure (VPKI) enabling pseudonymous authentication. Basic concepts of this envisioned architecture have been long known, they have been refined more recently, and standardization efforts have progressed. However, there are still significant technical issues that remain unresolved. Existing proposals for instantiating the VPKI either lack specific definitions of functionality, or they are not sufficiently rigorous in terms of security or privacy protection. Equally important, there is limited experimental work that establishes their efficiency and scalability. We are concerned with exactly these issues and challenges. We leverage the common VPKI approach and contribute an enhanced system with precisely defined, novel features that improve its resilience and the user privacy protection. In particular, we depart from the common assumption that the VPKI entities are fully trusted and improve user privacy in the face of an "honest-but-curious" security infrastructure.

Challenges
- VPKI concepts known for long
- Work out all components in details
- Analyze the security of the VPKI
- Evaluate its robustness and performance

Assumptions
- Literature and standards (IEEE 1609, ETSI)
  - Vehicles registered with one Long Term Certification Authority (LTCA) (home domain)
  - Pseudonym Certification Authority (PCA) servers in one or multiple domains
  - Vehicles can obtain pseudonyms from any PCA (home or foreign domains)
  - Treat with the help of a Root Certification Authority (RCA)
- "Honest-but-curious" VPKI entities

Objectives
- Enhanced trustworthiness with "honest-but-curious" VPKI entities
- Improved protection and extended functionality
- Full-blown standard-compliant implementation, extensive experimental evaluation
- Significant performance improvements
- Robust and scalable VPKI

Contributions
- Achieving a four-fold performance improvement over the state-of-the-art VPKI
- Extensive evaluation of a full-blown VC standard compliant VPKI
- An efficient multi-domain credential management infrastructure for the VC domain

References

VPKI Architecture

Performance Evaluation for Pseudonym Revocation (CRL or OCSP) and Resolution

Pseudonym Lifetime Policy

Client and LTCA Performance Evaluation

PCA Performance Evaluation

References