KTH Electrical Engineering

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

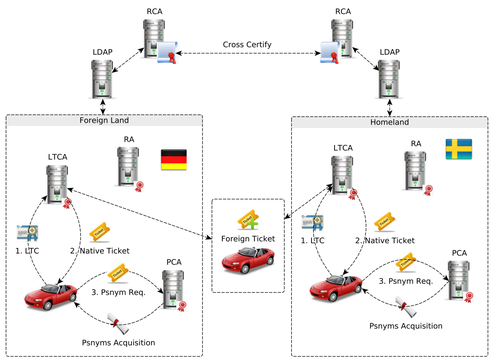
Assumptions

- 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)
  - Trust with the help of a Root Certification Authority (RCA)
- ***"Honest-but-curious"*** VPKI entities

Objectives

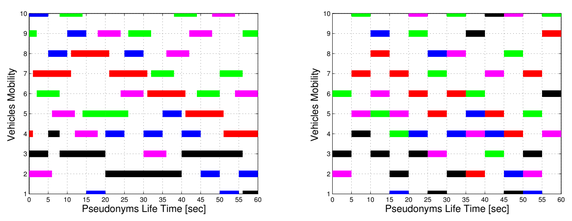
- Enhanced trustworthiness with ***"honest-but-curious"*** VPKI entities
- Improved protection and extended functionality
- Full-blown *standard-compliant* implementation, extensive experimental evaluation
- Significant performance improvements
- Robust and scalable VPKI

VPKI Architecture



- Multi-domain organization
- Cross-domain operations
- Privacy protection
  - Conditional anonymity
- Pseudonymous credential management system
  - Authentication, Authorization and Accounting
- Service discovery
- Emphasis on efficiency

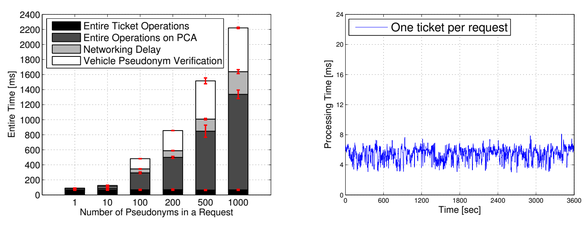
Pseudonym Lifetime Policy



Flexible non-overlapping pseudonyms — Fixed non-overlapping pseudonyms

- Uniform pseudonym lifetime for issuers in a domain
- No distinction among obtained pseudonyms set, thus no linkability

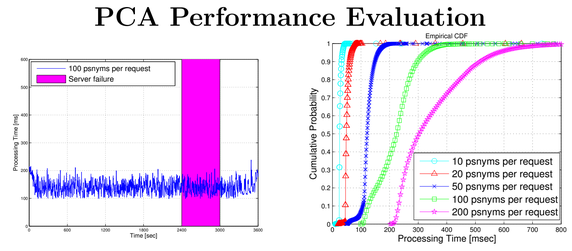
Client and LTCA Performance Evaluation



Client Processing Time — LTCA Performance

- Delay to obtain pseudonyms
- LTCA response time to issue a ticket

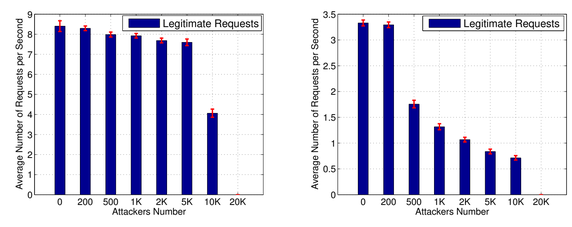
PCA Performance Evaluation



Issuing 100 Pseudonyms per Request — PCA Performance under different configuration

- PCA response time, including a *crash* failure
- Efficient provision for pseudonyms, with different configurations

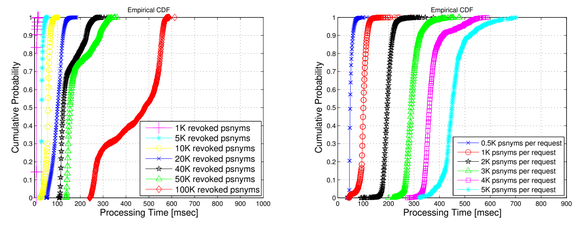
VPKI Servers under DDoS Attack



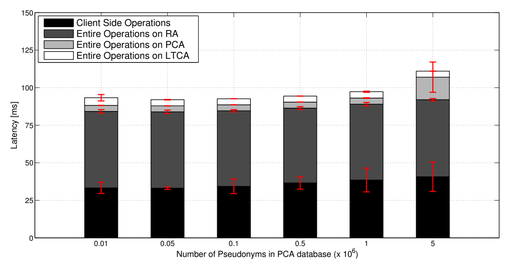
LTCA Performance — PCA Performance

- An LTCA is more resistant to DDoS than a PCA

Performance Evaluation for Pseudonym Revocation (CRL[a] or OCSP[b]) and Resolution



Fetching CRL — Performing OCSP Operation



Entities Response Time to Resolve & Revoke a Pseudonym

- For 50K CRL: F_x(t=280)=0.9 or Pr{t≤280}=0.9
- For 5K OCSP: F_x(t=500)=0.9 or Pr{t≤500}=0.9
- On average 100 ms. to resolve & revoke a pseudonym

[a]CRL: Certificate Revocation List
[b]OCSP: Online Certificate Status Protocol

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

[1] M. Khodaei, H. Jin, and P. Papadimitratos. **"Towards Deploying a Scalable & Robust Vehicular Identity and Credential Management Infrastructure,"** IEEE VNC, Paderborn, Germany, Dec. 2014.

[2] **Preparing Secure Vehicle-to-X Communication Systems (PRESERVE) Project**. Security Requirements of Vehicle Security Architecture. URL: http://preserve-project.eu/.

PRESERVE
preparing secure v2x communication systems