KTH Electrical Engineering

The Key to Intelligent Transportation:

Identity and Credential Management for Vehicular Communication Systems

Mohammad Khodaei and Panos Papadimitratos
Networked Systems Security Group
Royal Institute of Technology, Stockholm, Sweden
www.ee.kth.se/nss

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

- Privacy
- Resilience
- Revocation of (pseudonymous) credentials
- Non-technical and operational uncertainty

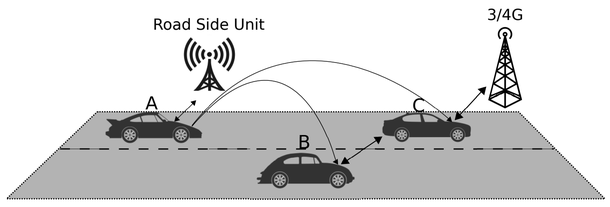
Assumptions

- 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

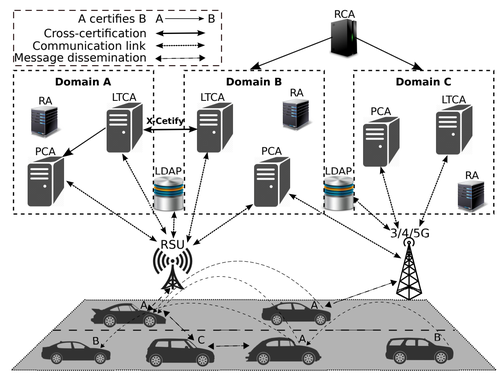
Secure and Privacy-protecting V2X Communication



Vehicle A:
1. Generate and sign message
2. Encapsulate message
3. Broadcast $\{Msg\}_{(P^i_v)}, \{P^i_v\}_{(PCA)}$

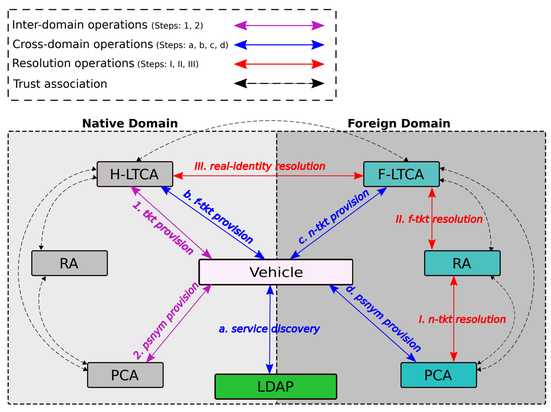
Vehicles B & C:
1. Validate the pseudonym, $\{P^i_v\}_{(PCA)}$
2. Verify the signature
3. Validate message content
4. Accept/reject the message
5. Re-broadcast

VPKI Architecture

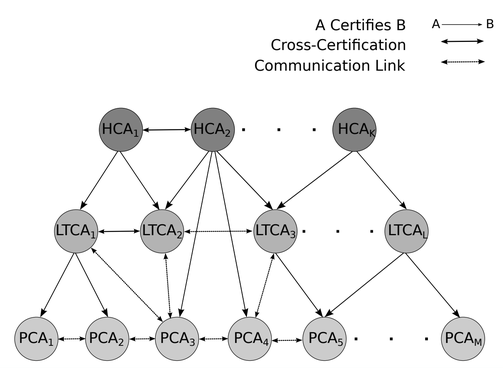


- Multi-domain organization
- Cross-domain operations
- Privacy protection
  - Conditional anonymity
- Pseudonymous credential management system
  - Authentication, Authorization and Accounting
- Service discovery
- Emphasis on efficiency and scalability

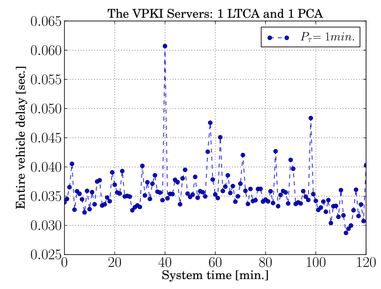
Multi-domain Operations



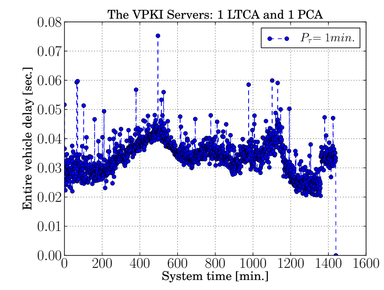
Hierarchical Organization of the VC Security Infrastructure



VPKI Delay for Real Mobility Traces

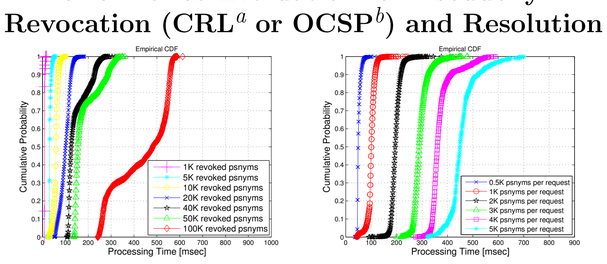


Tapas-Cologne dataset

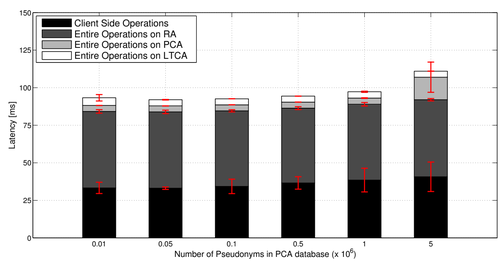


LuST dataset

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

References

[1] M. Khodaei, and P. Papadimitratos. **"Identity and Credential Management in Vehicular Communication Systems,"** IEEE VT Magazine, Dec. 2015 (to appear).

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

[3] S. Uppoor, O. Trullols-Cruces, M. Fiore, and J. M. Barcelo-Ordinas, **"Generation and Analysis of a Large-scale Urban Vehicular Mobility Dataset,"** IEEE Transactions on Mobile Computing, vol. 13, no. 5, pp. 1061–1075, 2014.

[4] L. Codeca, R. Frank, and T. Engel, **"Lust: a 24-hour Scenario of Luxembourg City for Sumo Traffic Simulations,"** in SUMO User Conference 2015-Intermodal Simulation for Intermodal Transport, Berlin, Germany, May, 2015.

[5] P. Papadimitratos, A. L. Fortelle, K. Evenssen, R. Brignolo, and S. Cosenza, **"Vehicular Communication Systems: Enabling Technologies, Applications, and Future Outlook on Intelligent Transportation,"** IEEE Communication Magazine., vol. 47, no. 11, pp. 84-95, Nov. 2009.

[6] IEEE P1609.2/D12, **"Draft Standard for Wireless Access in Vehicular Environments,"** Jan. 2012.

[7] **Car-to-Car Communication Consortium (C2C-CC).** [Online]. Available: http://www.car-2-car.org/