Security & Privacy for Vehicular Communication Systems:

The Key to Intelligent Transportation

Mohammad Khodaei and Panos Papadimitratos
Networked Systems Security Group, NSE-EES, KTH
www.ee.kth.se/nss

Vehicular Communication (VC) System

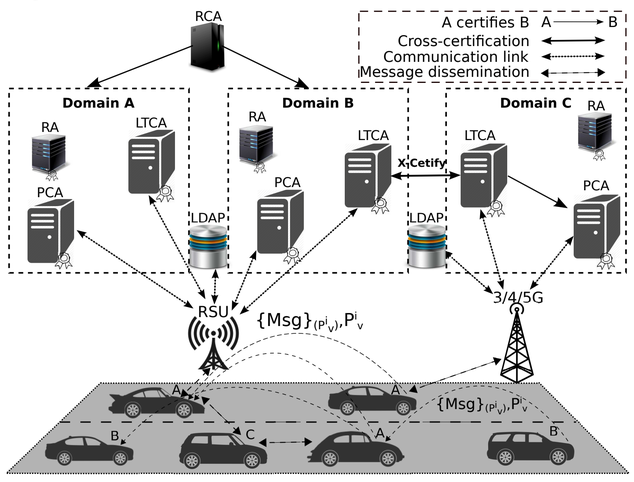

Figure 1: Vehicular Public-Key Infrastructure (VPKI) Architecture [1, 2]

Identity and credential management challenges:

- Security and privacy protection, with emphasis on efficiency and scalability
- Multi-domain organization
- Cross-domain operations and service discovery
- Preventing linkability based on the timing information
- ***"Honest-but-curious"*** VPKI entities

Security System Entities

- 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 CA (RCA)**

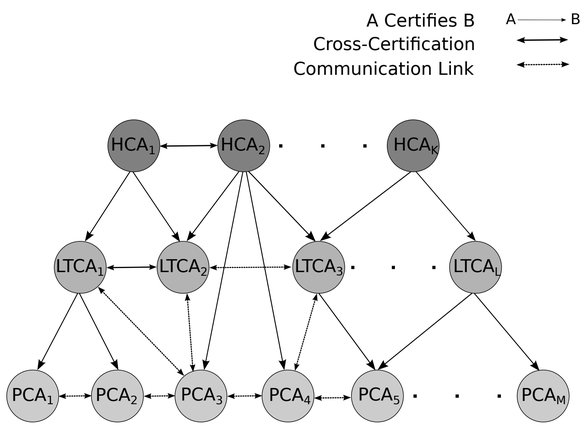

Figure 2: Hierarchical Organization of the VC Security Infrastructure [3]

Security & Privacy Requirements

- Authentication and communication integrity, and confidentiality
- Authorization and access control
- Non-repudiation, accountability and eviction (revocation)
- Anonymity (conditional)
- Unlinkability
- Thwarting Sybil-based attacks
- Availability

SECMACE Overview

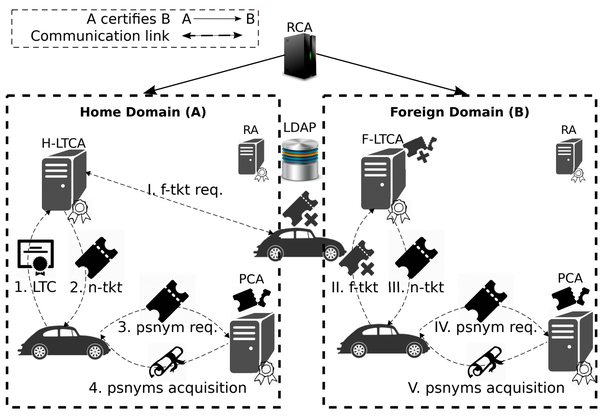

Figure 3: Pseudonym Acquisition Overview in the Home and Foreign Domains [1, 4]

Pseudonym Acquisition Policy

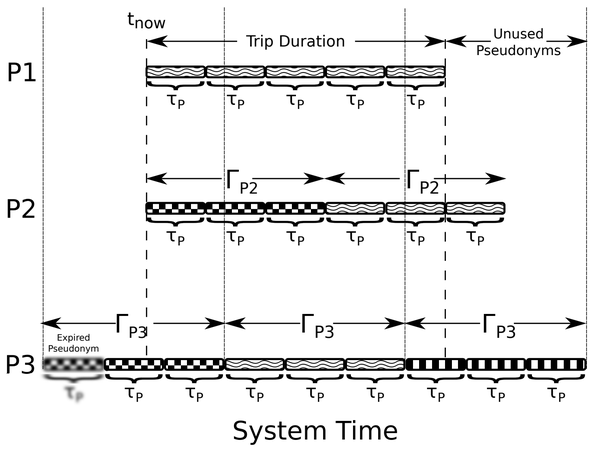

Figure 4: A Schematic Comparison of P1, P2, and P3 [2]

- P1: User-controlled (user-defined) policy
- P2: Oblivious policy
- P3: Universally fixed policy

SECMACE Evaluation

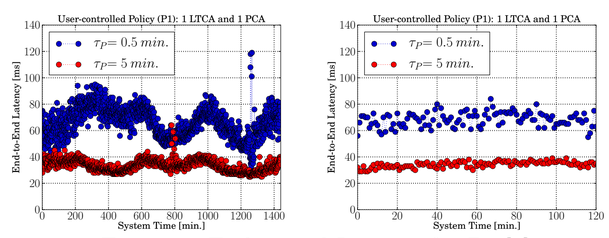

Figure 5: End-to-end Latency for P1 [2]

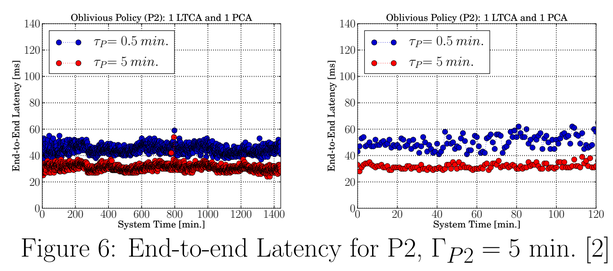

Figure 6: End-to-end Latency for P2, $\Gamma_{P2} = 5$ min. [2]

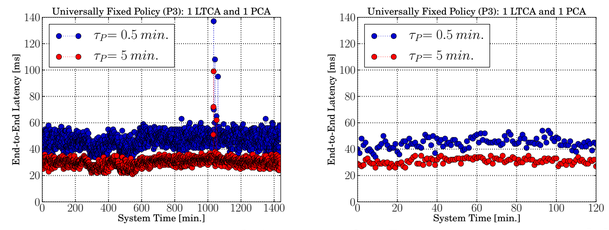

Figure 7: End-to-end Latency for P3, $\Gamma_{P3} = 5$ min. [2]

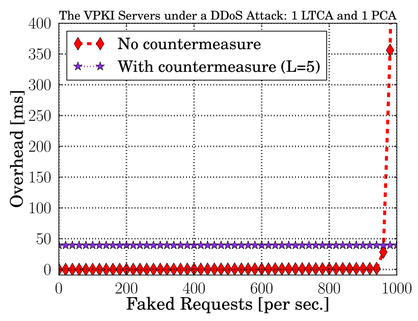

Figure 8: SECMACE under a DDoS Attack [1]

Privacy Analysis

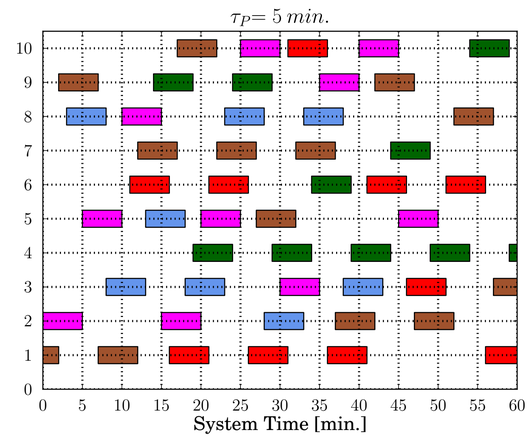

Figure 9: User-controlled (user-defined) Policy [1]

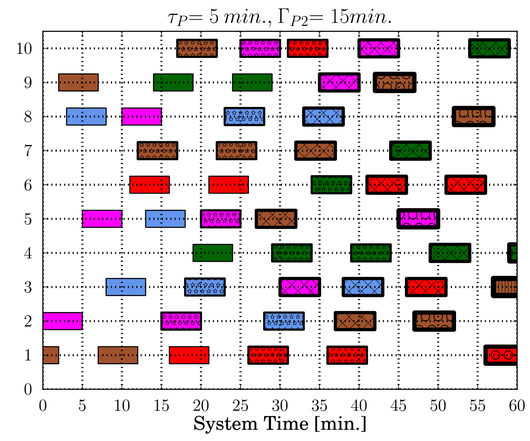

Figure 10: Oblivious Policy [1]

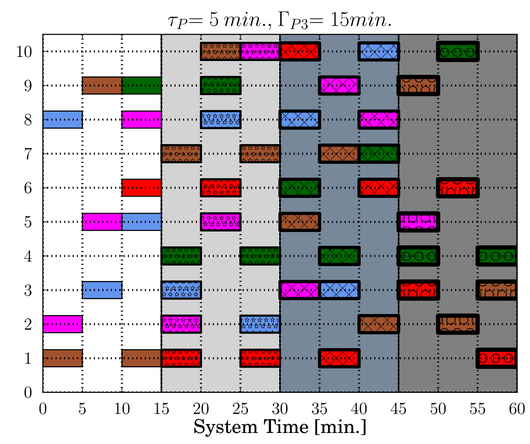

Figure 11: Universally Fixed Policy [1]

Remaining Challenges

- High availability and dynamic scalability
- Traceability based on timing information
- Efficient, scalable, and resilient mechanism for certificate revocation list distribution
- Formal analysis of the protocols
- Integration with PRESERVE [5] testbed

References

[1] M. Khodaei, H. Jin, and P. Papadimitratos, **"SECMACE: Scalable and Robust Identity and Credential Management Infrastructure in Vehicular Communication Systems,"** accepted in IEEE Transactions on Intelligent Transportation Systems.

[2] M. Khodaei and P. Papadimitratos, **"Evaluating On-demand Pseudonym Acquisition Policies in Vehicular Communication Systems,"** in Proceedings of the First International Workshop on Internet of Vehicles and Vehicles of Internet, Paderborn, Germany, pp. 7–12, July 2016.

[3] M. Khodaei and P. Papadimitratos, **"The Key to Intelligent Transportation: Identity and Credential Management in Vehicular Communication Systems,"** IEEE VT Magazine, vol. 10, no. 4, pp. 63–69, Dec. 2015.

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

[5] **"Preparing Secure Vehicle-to-X Communication Systems - PRESERVE."** [Online]. Available: http://www.preserve-project.eu/