VPKIaaS: A Highly-Available and Dynamically-Scalable Vehicular Public-Key Infrastructure

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

Vehicular Communication (VC) System

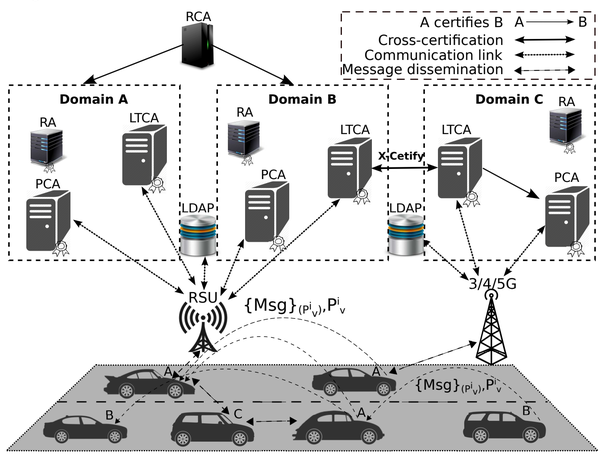


Figure 1: Vehicular Public-Key Infrastructure (VPKI) Architecture [1, 3]

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 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** (in home or foreign domains)
- Trust across domains with the help of a **Root CA (RCA)** or cross-certification

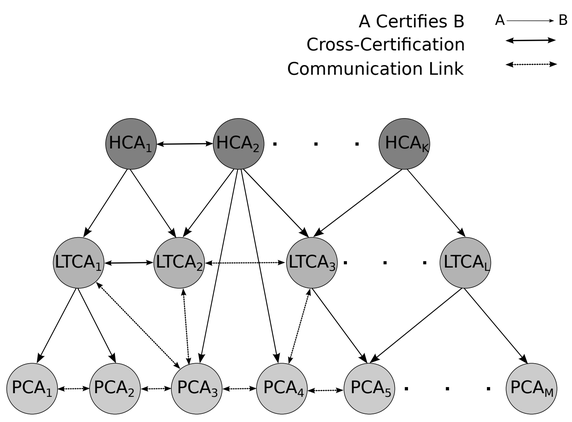


Figure 2: Hierarchical Organization of the VC Security Infrastructure [4].

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

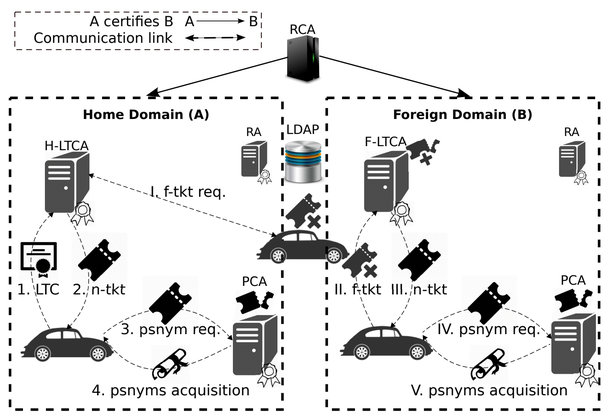


Figure 3: Pseudonym Acquisition Overview in Home and Foreign Domains [1, 5].

VPKI as a Service (VPKIaaS)

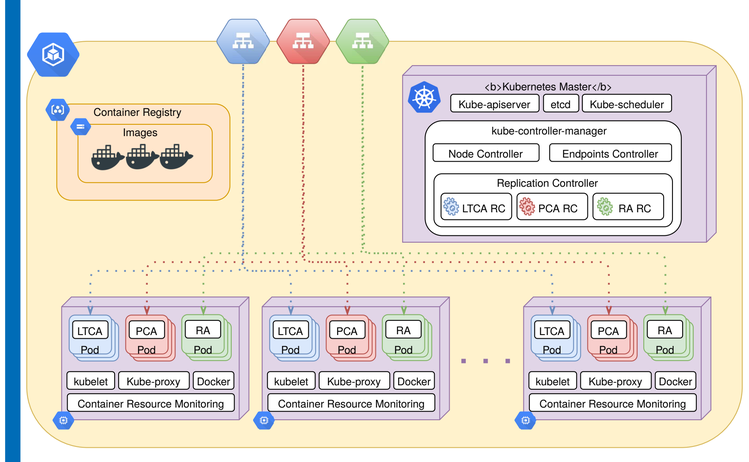
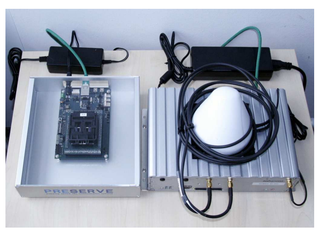


Figure 4: A high-level VPKIaaS architecture.

Experimental Setup



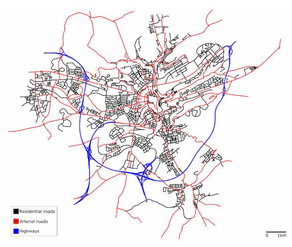


Figure 5: Nexcom vehicular OBUs boxes from the PRESERVE project [7] and LuST Topology [6].

- Nexcom boxes: Dual-core 1.66 GHz, 1GB memory, which support IEEE 802.11p
- LuST scenario: rush hours (7-9 am and 5-7 pm)

Google Cloud Platform

- Google Kubernetes Engine v1.9.6
- A cluster of three Virtual Machines (VMs), each with 8 vCPUs and 10GB of memory
- A cluster of four VMs (in another data center), each with 10 vCPUs and 10GB of memory

S1: Pseudonym Acquisition by an OBU

- One OBU to be a Roadside Unit (RSU), connected to the VPKI via Ethernet
- Another OBU requests pseudonyms from the VPKI via the "RSU" over IEEE 802.11p

S2: Pseudonym Acquisition for a Large-scale Scenario

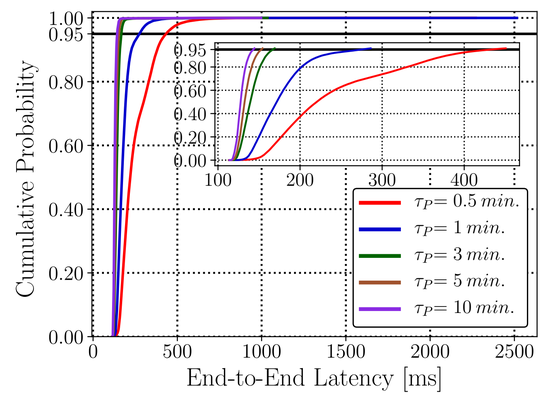


Figure 6: End-to-end latency for pseudonym acquisition.

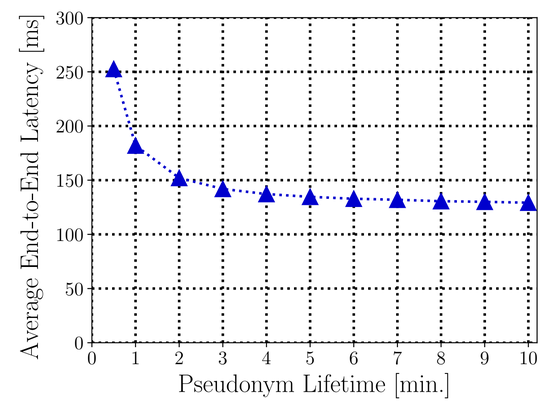


Figure 7: Average end-to-end latency.

S3: VPKIaaS Performance

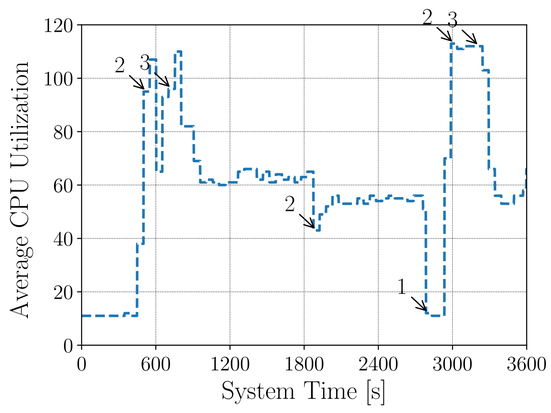


Figure 8: Dynamic scalability of the VPKIaaS.

Remaining Challenges

- Single point of contact to store/retrieve data
- Asynchronous data storage could yield providing more than one set of pseudonyms per ticket, thus Sybil-based misbehavior

References

[1] M. Khodaei, H. Jin, and P. Papadimitratos, **"SECMACE: Scalable and Robust Identity and Credential Management Infrastructure in Vehicular Communication Systems,"** IEEE Transactions on Intelligent Transportation Systems, vol. 19, no. 5, 1430–1444, May 2018.

[2] M. Khodaei, A. Messing, and P. Papadimitratos. 2017. **"RHyTHM: A Randomized Hybrid Scheme To Hide in the Mobile Crowd,"** In IEEE Vehicular Networking Conference (VNC), Torino, Italy, Nov. 2017.

[3] 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.

[4] 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.

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

[6] L. Codeca and et al. 2015. **"Luxembourg SUMO Traffic (LuST) Scenario: 24 Hours of Mobility for Vehicular Networking Research,"** IEEE VNC. Kyoto, Japan.

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