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

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
- Thrusting Sybil-based attacks
- Availability

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

S2: Pseudonym Acquisition for a Large-scale Scenario

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)

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

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 16GB of memory

Figure 7: Average end-to-end latency.

S3: VPKIaaS Performance

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