KTH ROYAL INSTITUTE
OF TECHNOLOGY

Secure and Privacy Preserving Vehicular Communication Systems: Identity and Credential Management Infrastructure

Mohammad Khodaei
Networked Systems Security Group (NSS)

November 29, 2016

Vehicular Communication (VC) Systems

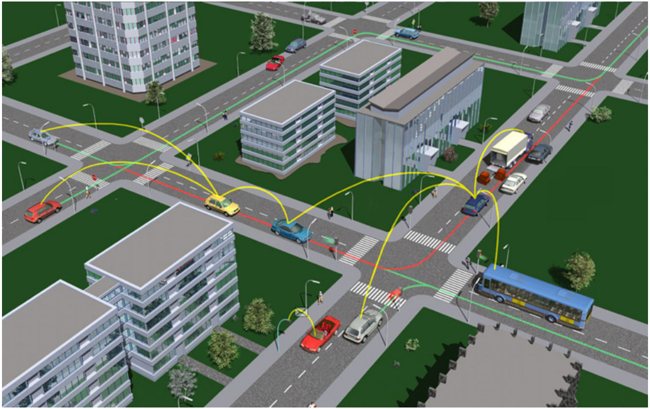
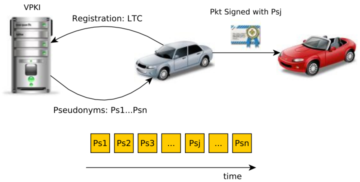


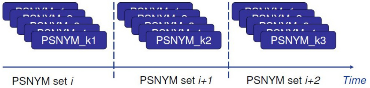
Figure: Photo Courtesy of the Car2Car Communication Consortium (C2C-CC)

Security and Privacy for VC Systems[1]

Basic Requirements

- Message authentication & integrity
- Message non-repudiation
- Access control
- Entity authentication
- Accountability
- Privacy protection



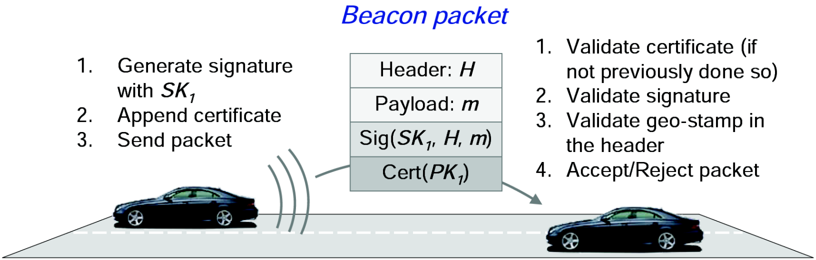


Vehicular Public-Key Infrastructure (VPKI)

- Pseudonymous authentication
- Trusted Third Party (TTP):
  - Certification Authority (CA)
  - Issues credentials & binds users to their pseudonyms

[1] P. Papadimitratos, et al. "Securing Vehicular Communications - Assumptions, Requirements, and Principles," in ESCAR, Berlin, Germany, pp. 5-14, Nov. 2006.
P. Papadimitratos, et al. "Secure Vehicular Communication Systems: Design and Architecture," in IEEE Communications Magazine, vol. 46, no. 11, pp. 100-109, Nov. 2008.

Security and Privacy for VC Systems (cont'd)



- Sign packets with the private key, corresponding to the current valid pseudonym
- Verify packets with the valid pseudonym
- Cryptographic operations in a Hardware Security Module (HSM)

Problem Statement and Motivation

The design of a VPKI

- Resilience
- Stronger adversarial model (than fully-trustworthy entities)
  - User privacy protection against *“honest-but-curious”* entities
  - User privacy enhancement and service unlinkability (inference of service provider or time)
- Pseudonym acquistion policies
  - How should each vehicle interact with the VPKI, e.g., how frequently and for how long?
  - Should each vehicle itself determine the pseudonym lifetime?
- Operation across multiple domains, thus a scalable design
- Efficiency and robustness

Security and Privacy Requirements for the VPKI Protocols

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

Adversarial Model

External adversaries

Internal adversaries

Stronger adversarial model

Protection against *honest-but-curious* VPKI entities

- Correct execution of protocols but motivated to profile users
- Concealing pseudonym provider identity and acquisition time, and reducing pseudonyms linkability (inference based on time)

Multiple VPKI entities could collude

Secure VC System

- Root Certification Authority (RCA)
- Long Term CA (LTCA)
- Pseudonym CA (PCA)
- Resolution Authority (RA)
- Lightweight Directory Access Protocol (LDAP)
- Roadside Unit (RSU)
- Trust established with RCA, or through cross certification

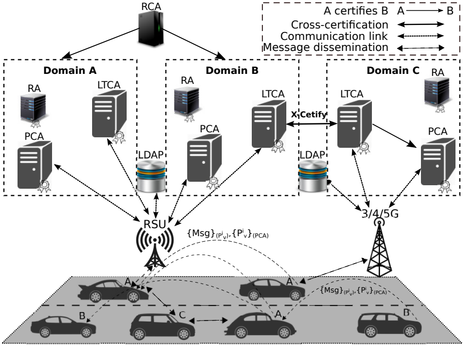


Figure: VPKI Overview

System Model

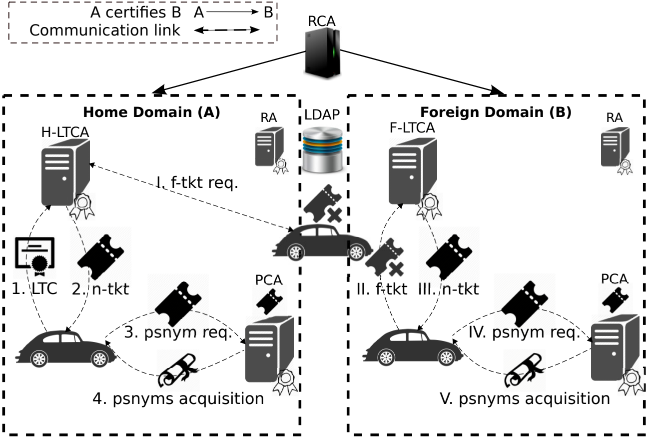


Figure: VPKI Architecture

Experimental Setup (#1)

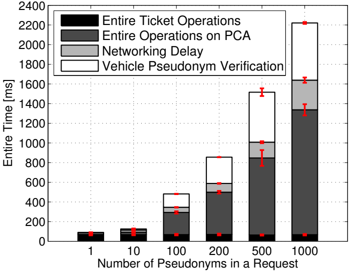
- **VPKI testbed**
  - Implementation in C++
  - OpenSSL: Transport Layer Security (TLS) and Elliptic Curve Digital Signature Algorithm (ECDSA)-256 according to the standard
- **Network connectivity**
  - Varies depending on the actual OBU-VPKI connectivity
  - Reliable connectivity to the VPKI (e.g., RSU, Cellular, opportunistic WiFi)

Table: Servers and Clients Specifications

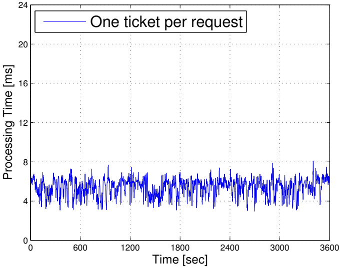
	LTCA	PCA	RA	Clients
VM Number	2	5	1	25
Dual-core CPU (Ghz)	2.0	2.0	2.0	2.0
BogoMips	4000	4000	4000	4000
Memory	2GB	2GB	1GB	1GB
Database	MySQL	MySQL	MySQL	MySQL
Web Server	Apache	Apache	Apache	-
Load Balancer	Apache	Apache	-	-
Emulated Threads	-	-	-	400

- **Use cases**
  - Pseudonym provision
  - Performing a DDoS attack

Client and LTCA Performance Evaluation



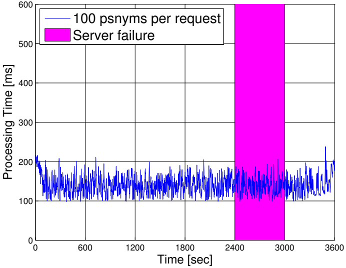
Client processing time



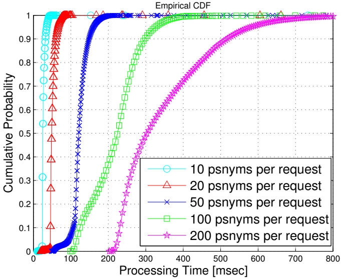
LTCA performance

- 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
- Obtaining 200 pseudonyms: F_x(t=500)=0.9 or Pr{t$\leq$500}=0.9

Experimental Setup (#2)

Table: Mobility Traces Information

	TAPASCologne	LuST
Number of vehicles	75,576	138,259
Number of trips	75,576	287,939
Duration of snapshot (hour)	24	24
Available duration of snapshot (hour)	2 (6-8 AM)	24
Average trip duration (sec.)	590.49	692.81
Total trip duration (sec.)	44,655,579	102,766,924

- **Main metric**
  - End-to-end pseudonym acquisition latency from the initialization of ticket acquisition protocol till successful completion of pseudonym acquisition protocol

Table: Servers & Clients Specifications

	LTCA	PCA	Client
Number of entities	1	1	1
Dual-core CPU (Ghz)	2.0	2.0	2.0
BogoMips	4000	4000	4000
Memory	2GB	2GB	1GB
Database	MySQL	MySQL	MySQL

- N.B. PRESERVE Nexcom boxes specs: dual-core 1.66 GHz, 2GB Memory

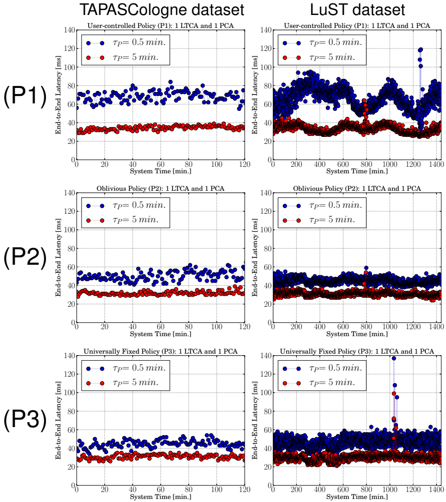
End-to-end Latency for P1, P2, and P3

Choice of parameters:

- Frequency of interaction and volume of workload to a PCA
- Γ=5 min., τ_P=0.5 min., 5 min.

LuST dataset ($\tau_P = 0.5$ *min*):

- P1: $F_x(t = 167\ ms) = 0.99$
- P2: $F_x(t = 80\ ms) = 0.99$
- P3: $F_x(t = 74\ ms) = 0.99$



Summary of Contributions

1. Facilitating multi-domain operation
2. Offering increased user privacy protection
   - Honest-but-curious system entities
   - Eliminating pseudonym linking based on timing information
3. Eradication of Sybil-based misbehavior
4. Proposing multiple generally applicable pseudonym acquisition policies
5. Detailed analysis of security and privacy protocols
6. Extensive experimental evaluation
   - Efficiency, scalability, and robustness
   - Achieving significant performance improvement
   - Modest VMs can serve sizable areas or domain

Original Work

- N. Alexiou, M. Laganà, S. Gisdakis, M. Khodaei, and P. Papadimitratos, *"VeSPA: Vehicular Security and Privacy-preserving Architecture,"* in ACM HotWiSec, Budapest, Hungary, Apr. 2013.
- M. Khodaei, H. Jin, and P. Papadimitratos, *"Towards Deploying a Scalable & Robust Vehicular Identity and Credential Management Infrastructure,"* in IEEE VNC, Paderborn, Germany, Dec. 2014.
- 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.
- M. Khodaei and P. Papadimitratos, *"Evaluating On-demand Pseudonym Acquisition Policies in Vehicular Communication Systems,"* in ACM MobiHoc, Workshop on Internet of Vehicles and Vehicles of Internet (IoV-VoI), Paderborn, Germany, July 2016.
- M. Khodaei, H. Jin, and P. Papadimitratos, *"SECMACE: Scalable and Robust Identity and Credential Management Infrastructure in Vehicular Communication Systems,"* Submitted to the IEEE Transactions on Intelligent Transportation Systems.

Secure and Privacy Preserving Vehicular Communication Systems: Identity and Credential Management Infrastructure

ITRL Conference on Integrated Transport

Mohammad Khodaei
Networked Systems Security Group (NSS)
www.ee.kth.se/nss