Towards Deploying a Scalable & Robust Vehicular Identity and Credential Management Infrastructure

M. Khodaei, H. Jin, and P. Papadimitratos

Networked Systems Security Group
www.ee.kth.se/nss

Royal Institute of Technology (KTH)
Stockholm, Sweden

December 3, 2014

Outline

Outline

Background

Projects

SEVECOM, EVITA, PRECIOSA, OVERSEE, DRIVE-C2X, PRESERVE, CAMP-VSC3

Standarization and Harmonization

IEEE 1609.2, ETSI and C2C-CC: Vehicular Communication (VC) related specifications for privacy-preserving architectures

Vehicular Public-Key Infrastructure (VPKI)

- Cornerstone for all these efforts
- Consensus on the need and basic characteristics

Background (Cont'd)

Inference of service provider or service time

- C2C-CC [1], PRESERVE [2], SCMS [3]
- CoPRA [4] linking pseudonyms to the real-identity
- VeSPA [5, 6], SEROSA [7]
- V-Token [8] learns the real identity of V-Token's owner

Sybil-based misbehavior not precluded by VPKI

- C2C-CC [1], PRESERVE [2], SCMS [3]
- VeSPA [5, 6], SEROSA [7]
- **One remedy**
  - Non-overlapping pseudonym lifetimes
  - Downside: easier linkability

Contributions

Stronger adversarial model

Increased protection against *honest-but-curious* VPKI entities

- No inference of service provider or time
- Correct execution of protocols, but motivated to profile users

Eradication of Sybil-based misbehavior

VPKI design that ensures a compromised vehicle cannot obtain multiple pseudonyms valid simultaneously

Extensive & detailed experimental evaluations

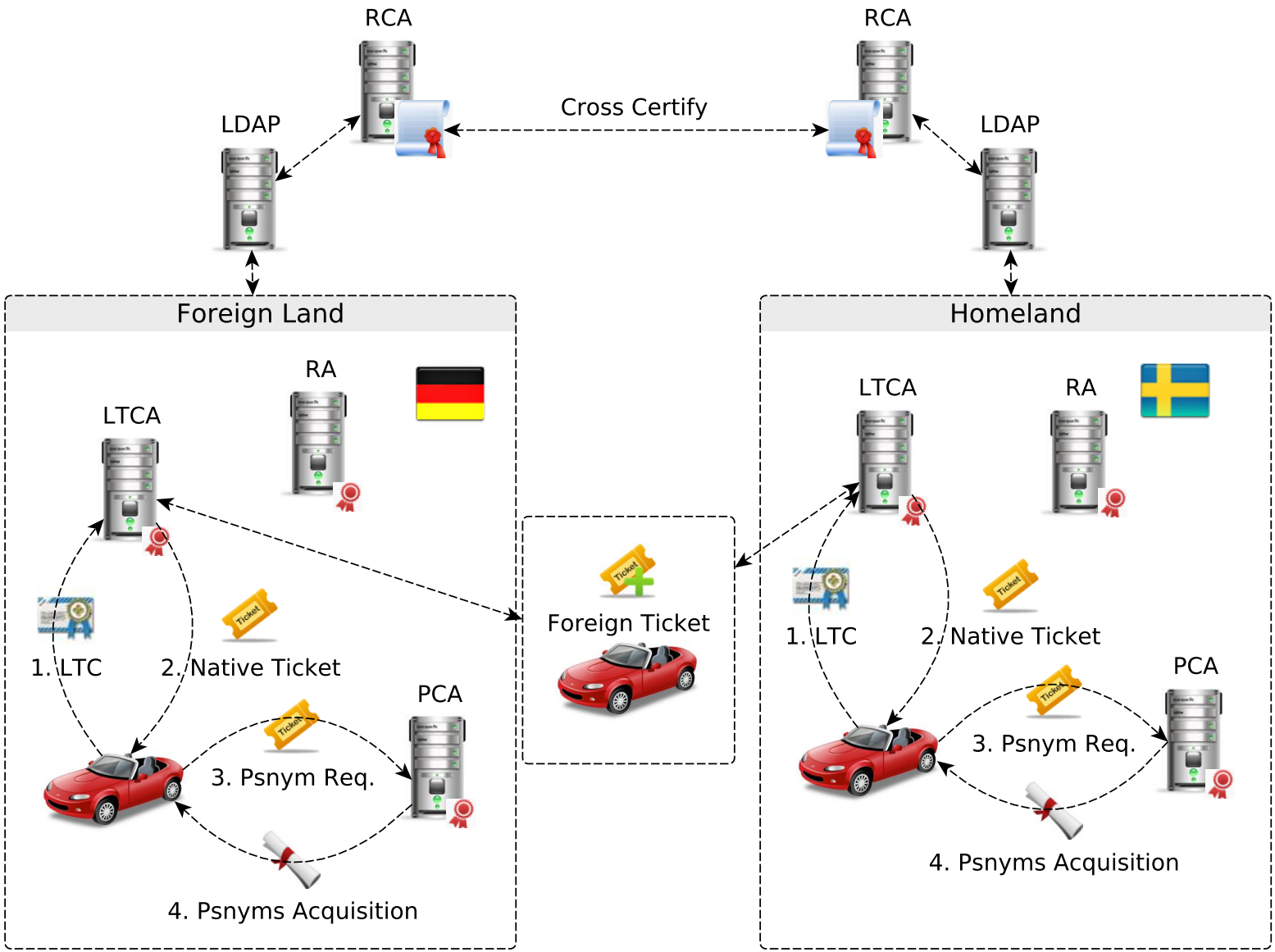
- Full-blown VC *standard-compliant* implementation of VPKI
- Significant performance improvement
  - Multi-domain operation
  - Efficiency
  - Scalability

System Outline

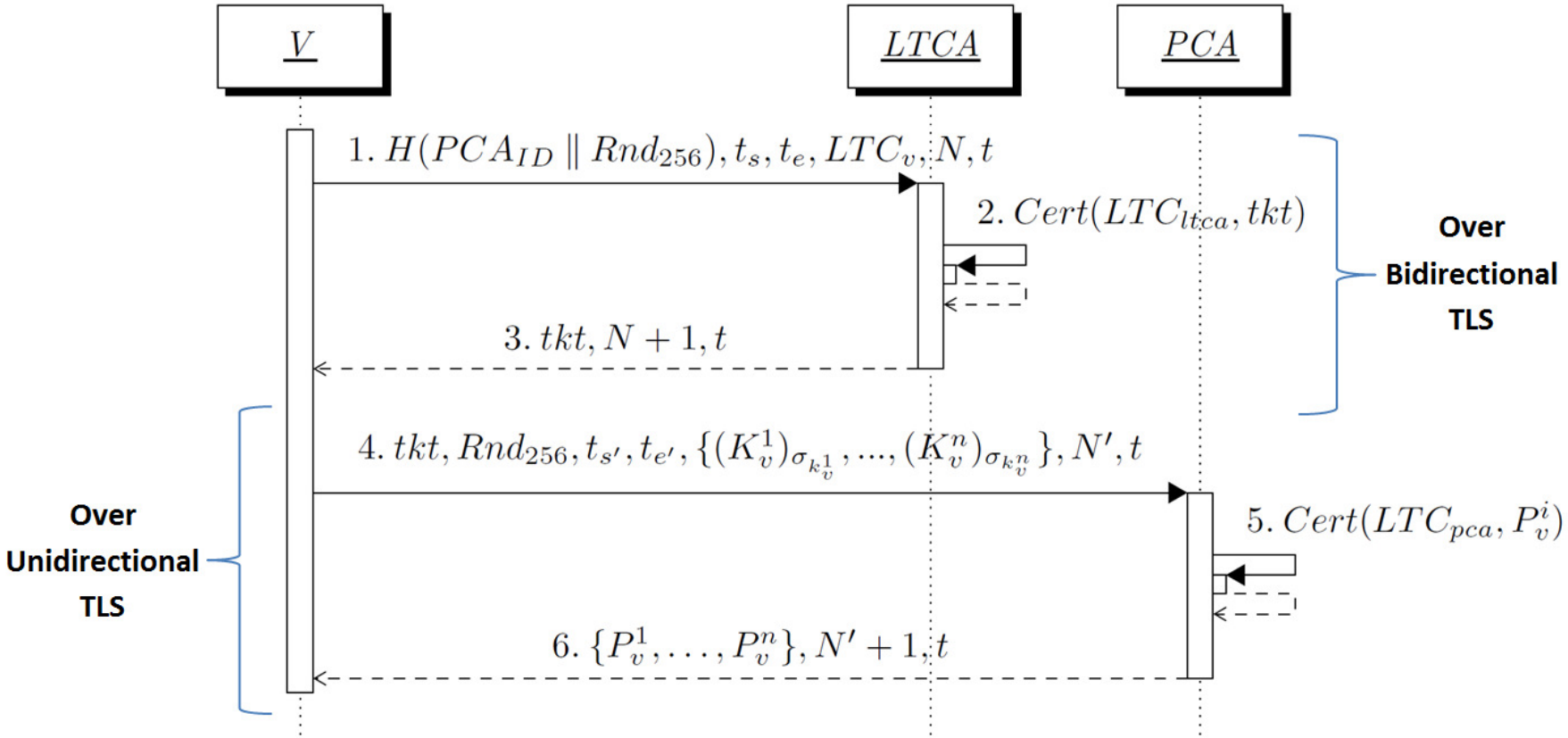
- Vehicles registered with one **Long Term Certification Authority (LTCA)** (home domain)
- **Pseudonym Certification Authority (PCA)** servers in one or multiple domains
- Vehicles can obtain pseudonyms from any **PCA** (in home or foreign domains)
- Trust with the help of a **Root Certification Authority (RCA)**
- Trust associations of PCAs and LTCAs through **Lightweight Directory Access Protocol (LDAP)** services
- Resolve a pseudonym with the help of a **Resolution Authority (RA)**

Outline

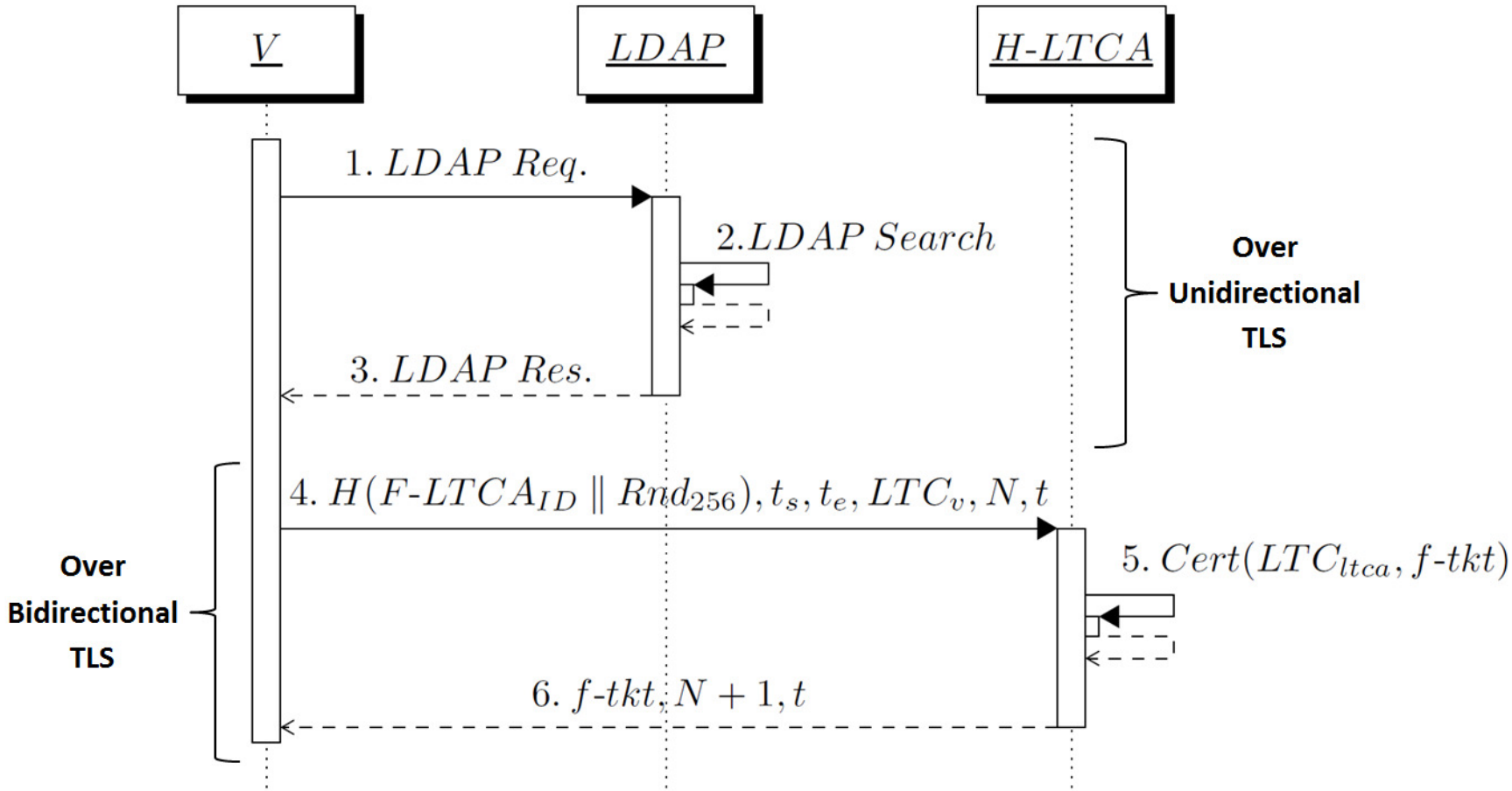
VPKI Architecture



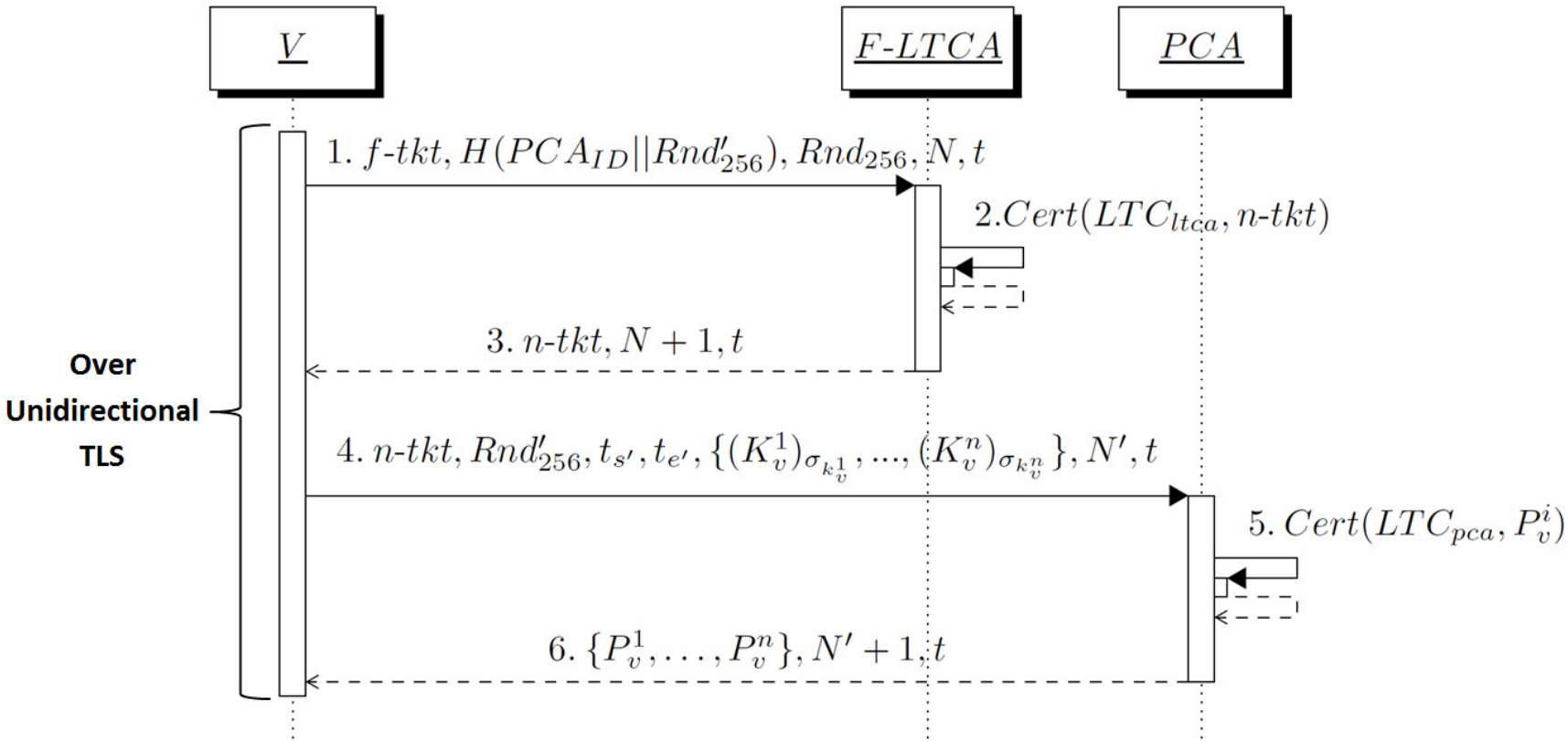
Ticket and Pseudonym Acquisition



Roaming User: Foreign Ticket Authentication



Native Ticket and Pseudonym Acquisition in the Foreign Domain

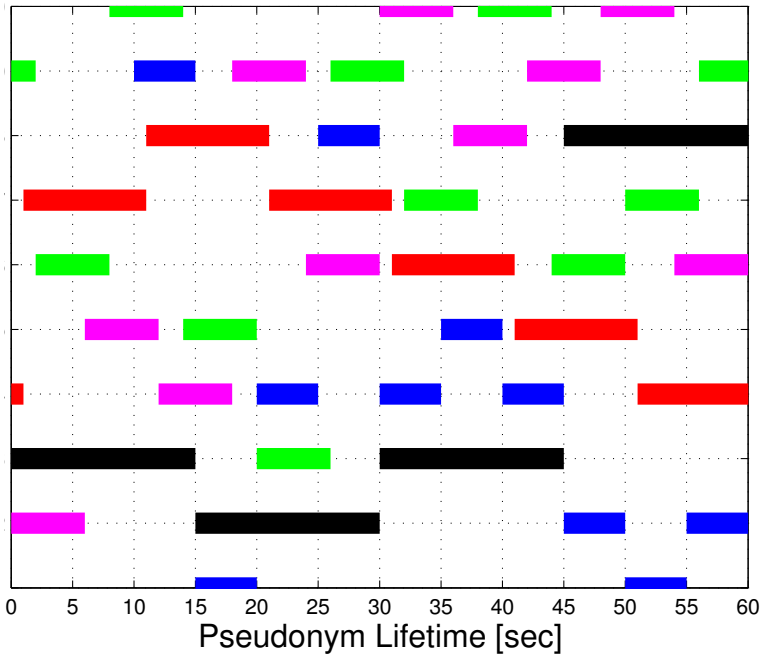


Outline

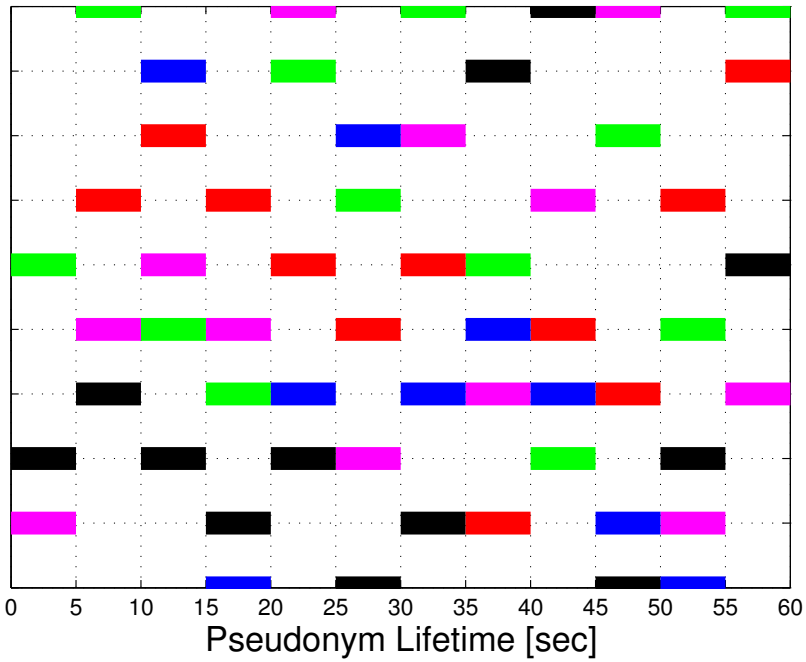
Security Analysis

- **Communication integrity, confidentiality, non-repudiation**
  - Certificates, TLS and digital signatures
- **Authentication and authorization**
  - LTCA performs Authentication, Authorization and Accounting (AAA)
  - PCA grants the service
  - Security Association through LDAP
- **Concealing pseudonym providers, foreign identity providers and actual pseudonym acquisition period**
  - Sending $H(PCA_{id} \| Rnd_{256})$, t_s, t_e, LTC_v to the home LTCA
  - PCA verifies if $[t'_s,\ t'_e] \subseteq [t_s,\ t_e]$
- **Thwarting Sybil-based misbehavior**
  - LTCA keeps the records of the issued tickets
  - A ticket is bound to a specific PCA
  - PCA keeps records of ticket usage

Ticket & Pseudonym Lifetime Policy



Flexible lifetimes



Fixed lifetimes

- Non-overlapping pseudonym lifetimes from eavesdroppers' perspective
- Distinct lifetimes per vehicle make linkability easier
- Uniform pseudonym lifetime in a domain
- No distinction among obtained pseudonyms set, thus less probable to link pseudonyms

Outline

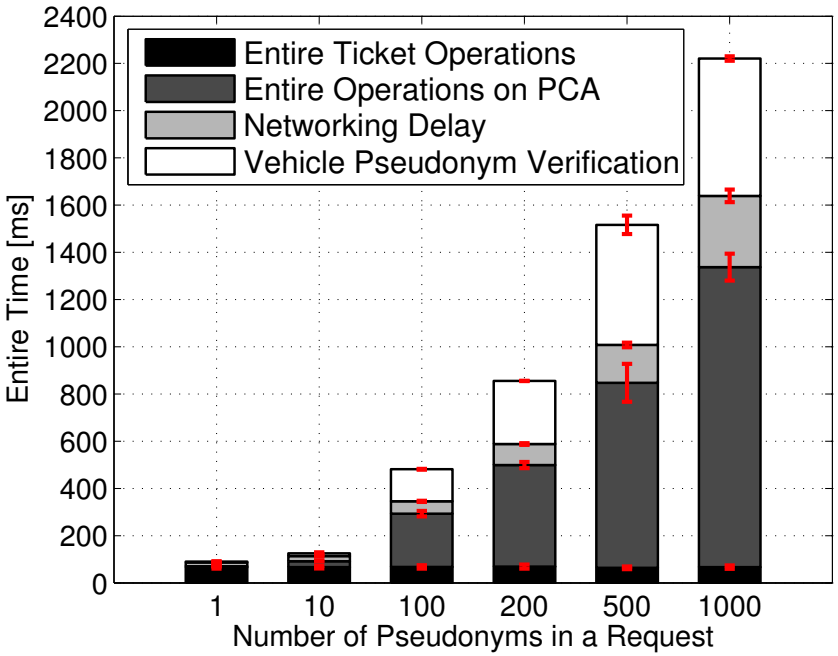
Server and Client Specifications

	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

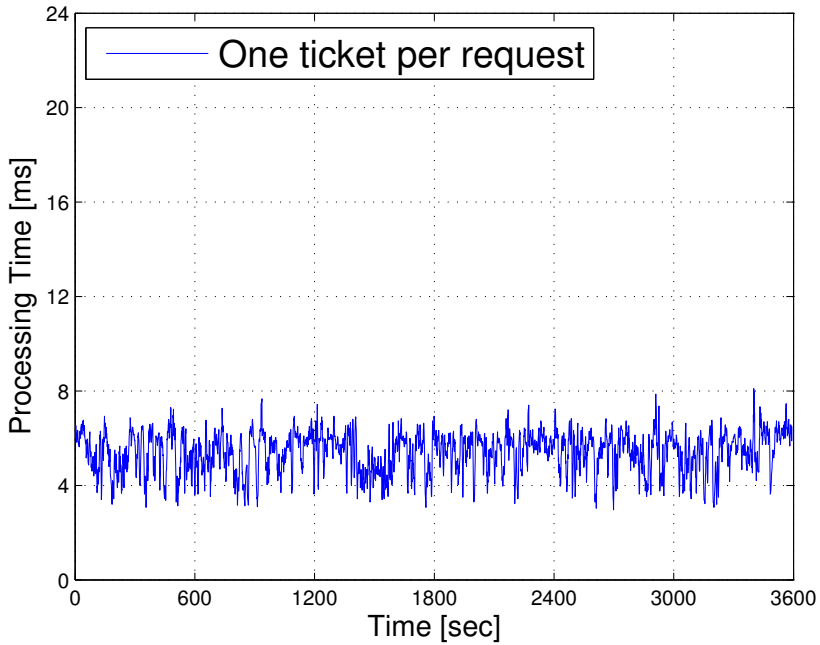
Use cases:

- Pseudonym provision
- Pseudonym resolution & revocation
- Performing DDoS attack

Client and LTCA Performance Evaluation



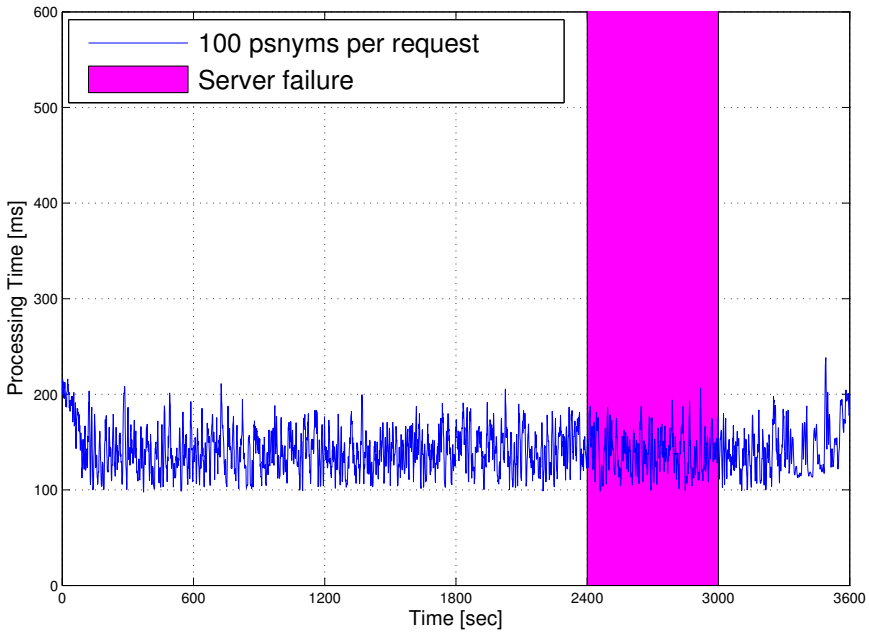
Client processing time



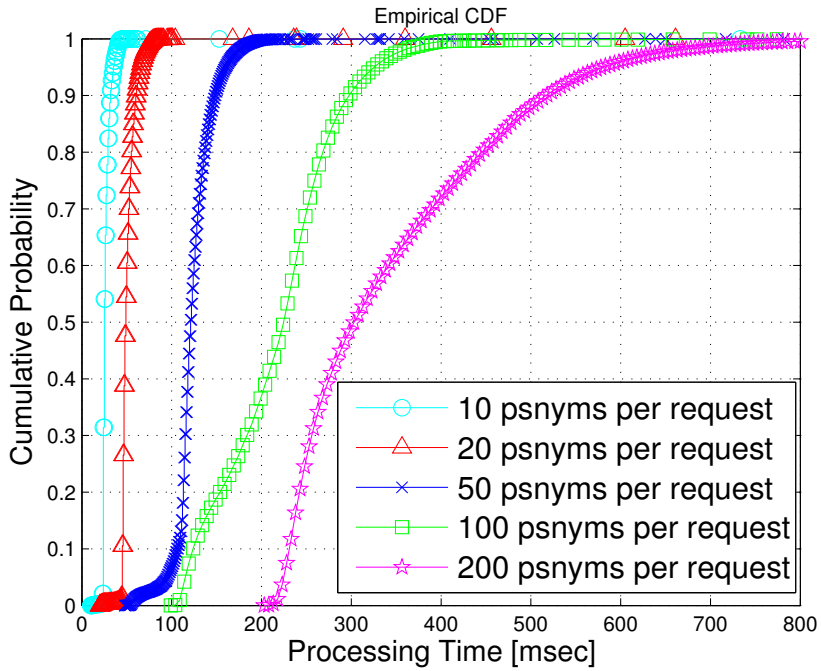
LTCA performance

- Delay to obtain pseudonyms
- LTCA response time to issue a ticket

PCA Performance Evaluation



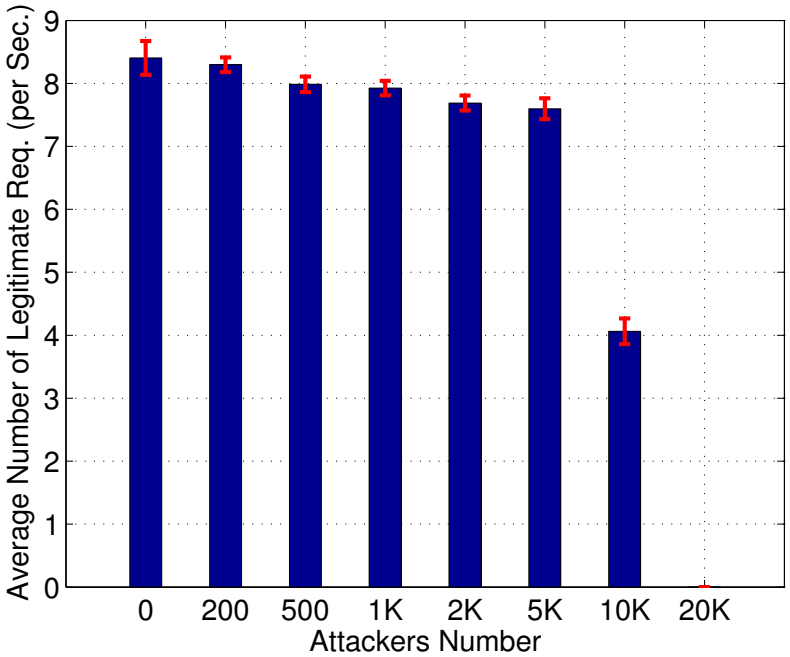
Issuing 100 pseudonyms per request



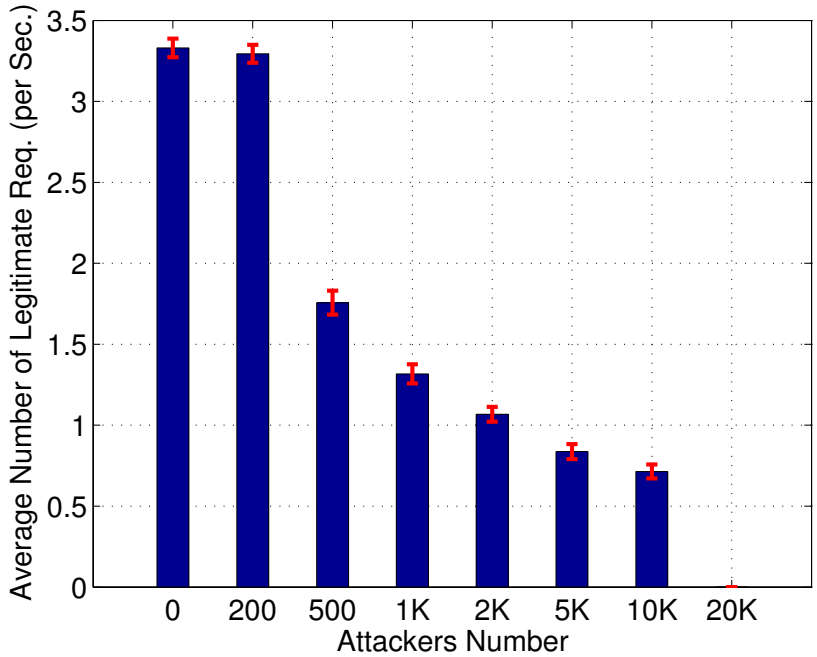
PCA performance under different configuration

- PCA response time, including a *crash* failure
- Efficient provision for pseudonyms, with different configurations

VPKI Servers under DDoS Attack



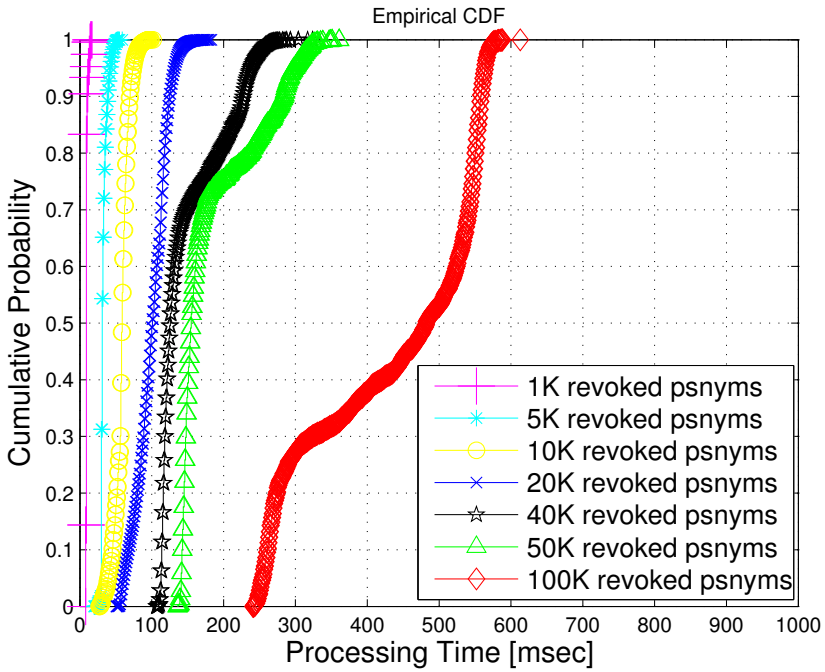
LTCA performance



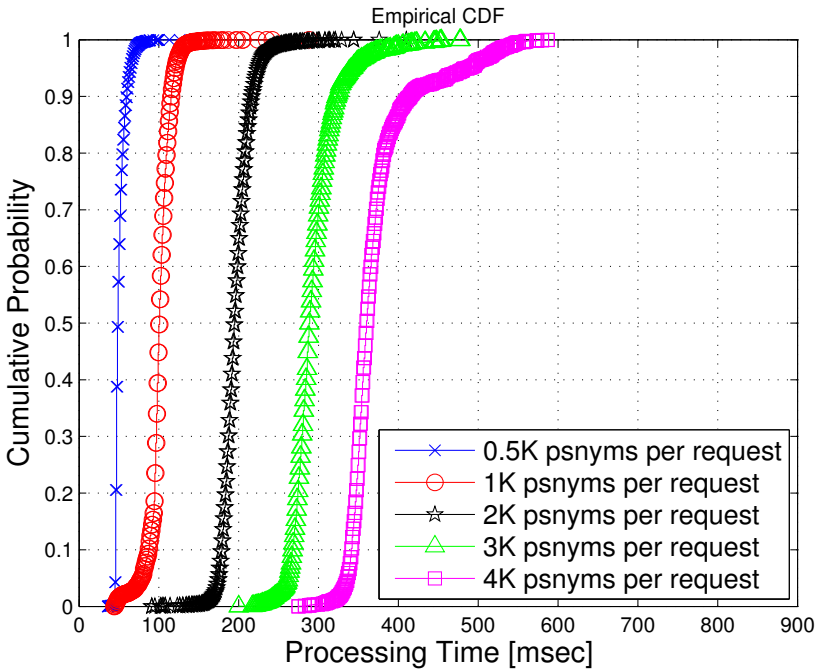
PCA performance

- 10K legitimate vehicles, requesting 100 pseudonyms every 10 minutes
- Up to 20K attackers, sending requests every 10 seconds
- An LTCA is more resistant to DDoS than a PCA

Performance Evaluation for Pseudonym Revocation (CRL[1] or OCSP[2]) and Resolution



Obtaining a CRL



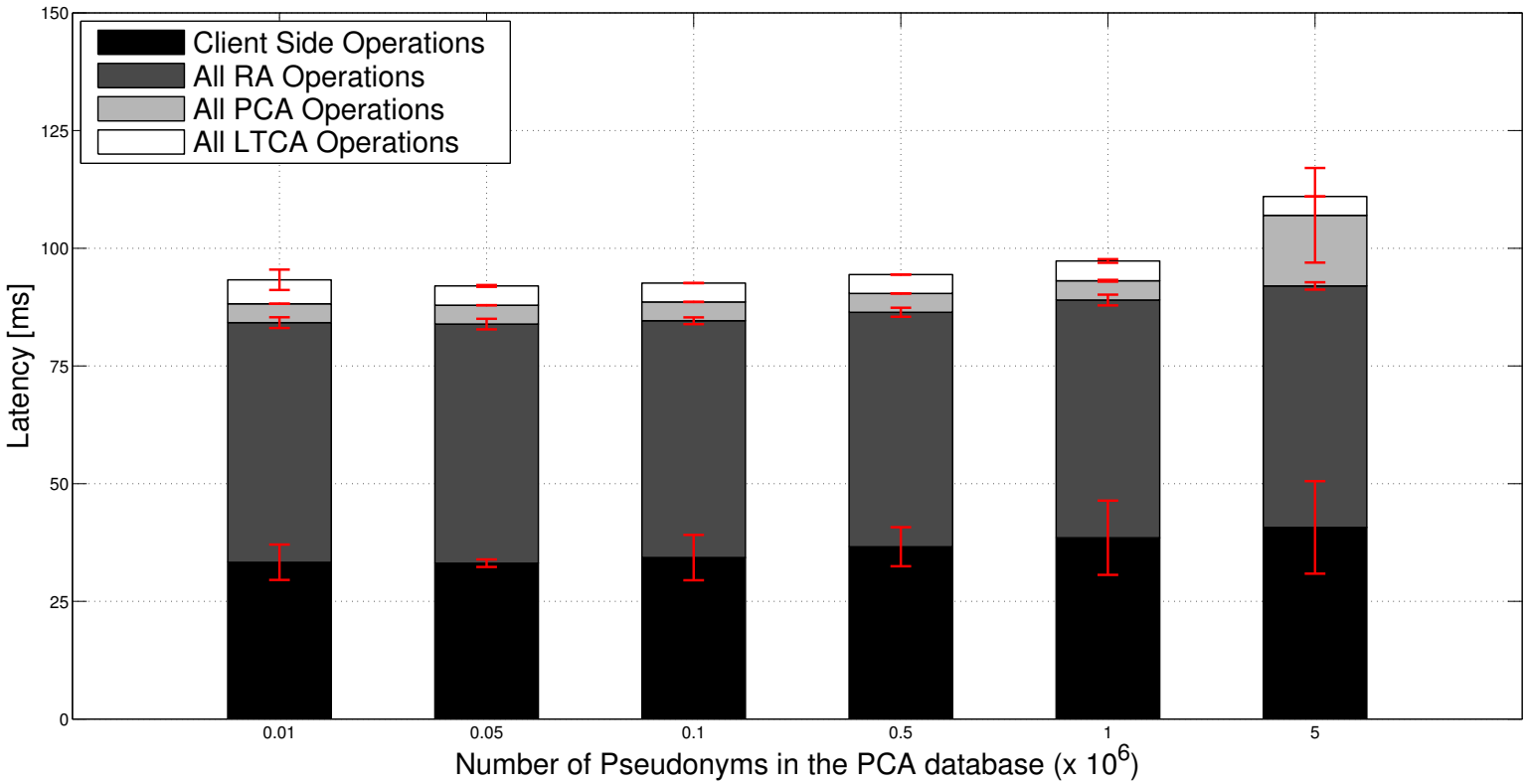
OCSP validation

- For 50K CRL: $F_x(t{=}280){=}0.9$ or $\Pr\{t{\leq}280\}{=}0.9$
- For 4K OCSP: $F_x(t{=}400){=}0.9$ or $\Pr\{t{\leq}400\}{=}0.9$

[1] CRL: Certificate Revocation List

[2] OCSP: Online Certificate Status Protocol

Entities Response Time to Resolve & Revoke a Pseudonym



- On average 100 ms to resolve & revoke a pseudonym

Outline

Conclusion

- Strong adversarial model: *honest-but-curious* VPKI entities
- Prevention from Sybil-based misbehavior
- Reduction of pseudonym linkability, thus message linkability
- Extensive evaluation of a full-blown VC *standard compliant* VPKI
  - Very significant performance improvement over prior systems

Bibliography

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

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

[3] W. Whyte, A. Weimerskirch, V. Kumar, and T. Hehn, "**A security credential management system for V2V communications**," in *IEEE VNC*, Boston, MA, USA, Dec. 2013.

[4] N. Bißmeyer, J. Petit, and K. M. Bayarou, "**Copra: Conditional pseudonym resolution algorithm in VANETs**," in *IEEE WONS*, Banff, Canada, Mar. 2013.

[5] 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.

[6] N. Alexiou, S. Gisdakis, M. Laganà, and P. Papadimitratos, "**Towards a Secure and Privacy-preserving Multi-service Vehicular Architecture**," in *D-SPAN*, Madrid, Spain, Jun. 2013.

[7] S. Gisdakis, M. Laganà, T. Giannetsos, and P. Papadimitratos, "**SEROSA: SERvice Oriented Security Architecture for Vehicular Communications**," in *IEEE VNC*, Boston, MA, USA, Dec. 2013.

[8] F. Schaub, F. Kargl, Z. Ma, and M. Weber, "**V-tokens for Conditional Pseudonymity in VANETs**," in *IEEE WCNC*, NJ, USA, Apr. 2010.

Questions and Discussion

Thank you!

khodaei@kth.se