Scaling Pseudonymous Authentication for Large Mobile Systems

ACM WiSec'19, May 17, 2019

Mohammad Khodaei, Hamid Noroozi, and Panos Papadimitratos

Networked Systems Security Group

www.eecs.kth.se/nss

Vehicular Communication Systems (VCS)

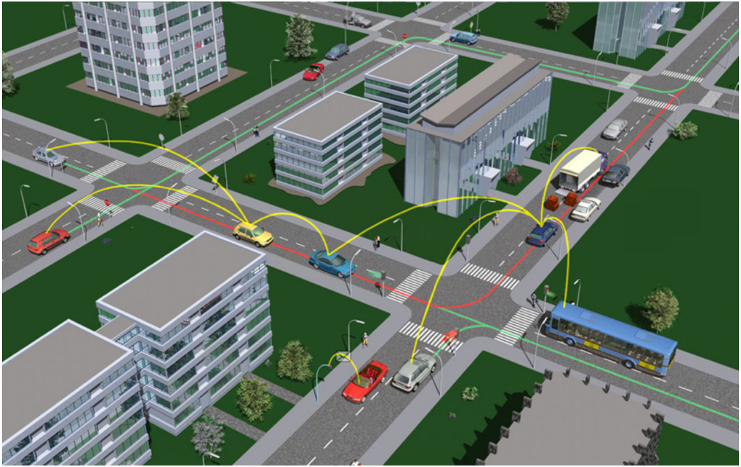
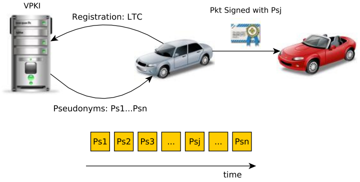


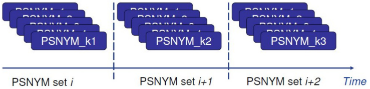
Illustration: C2C-CC

VCS Security and Privacy

Basic Requirements

- Authentication & integrity
- Non-repudiation
- Authorization & access control
- Anonymity (conditional)
- Unlinkability (longer-term)
- Accountability

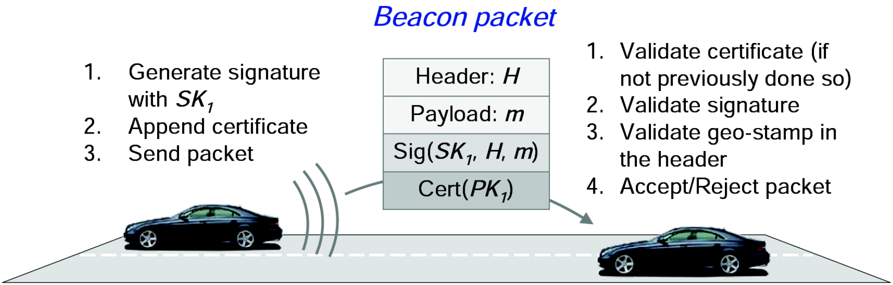




Vehicular Public-Key Infrastructure (VPKI)

- Ephemeral pseudonymous credentials
- Long-term credentials (Long Term Certificates (LTCs))

VCS Security and Privacy (cont'd)



Beacon packet

1. Generate signature with SK_1
2. Append certificate
3. Send packet

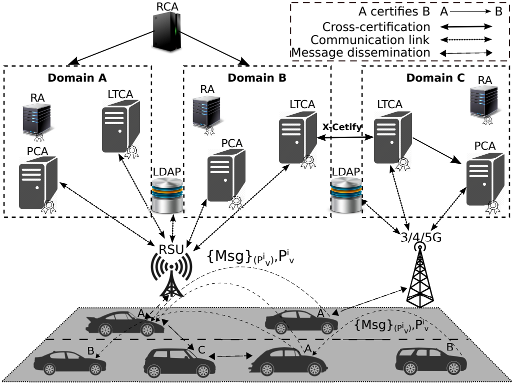
Header: H
Payload: m
Sig(SK_1, H, m)
Cert(PK_1)

1. Validate certificate (if not previously done so)
2. Validate signature
3. Validate geo-stamp in the header
4. Accept/Reject packet

- Vehicle-to-Vehicle (V2V)/Vehicle-to-Infrastructure (V2I) (V2X) message communications are digitally signed
- Messages are signed with the private key corresponding to the currently valid pseudonym
- Cryptographic operations in a Hardware Security Module (HSM)

VCS Security and Privacy (cont'd)

- Vehicular Public-Key Infrastructure (VPKI)
- Root CA (RCA)
- Long Term CA (LTCA)
- Pseudonym CA (PCA)
- Resolution Authority (RA)
- Lightweight Directory Access Protocol (LDAP)
- Roadside Unit (RSU)



- Vehicles registered with one LTCA (home domain)
- One or more PCA servers per domains
- Vehicles can obtain pseudonyms from any PCA (home or foreign domains)
- RCA or cross-certification
- Deanonymize (resolve pseudonyms) with the help of an RA

VPKI Challenges; Motivation

Traditional PKI vs. Vehicular PKI

- Dimensions (5 orders of magnitude more credentials)
- Complexity and constraints
    - Balancing act: security, privacy, and efficiency
        - *Honest-but-curious* VPKI entities
        - Performance constraints: safety- and time-critical operations (rates of 10 safety beacons per second)
    - Multiple and diverse entities, global deployment, long-lived entities
    - Cost-driven platform resource constraints
- Mechanics of revocation
    - Highly dynamic environment
    - Short-lived pseudonyms, multiple per entity
    - Need for efficient and timely distribution of Certificate Revocation Lists (CRLs)
    - Strong privacy protection prior to revocation events

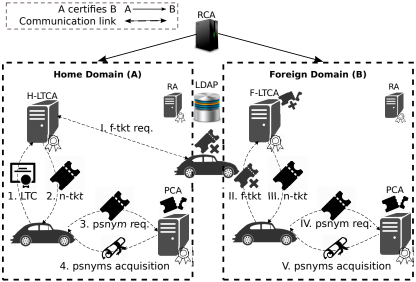
Adversarial Model

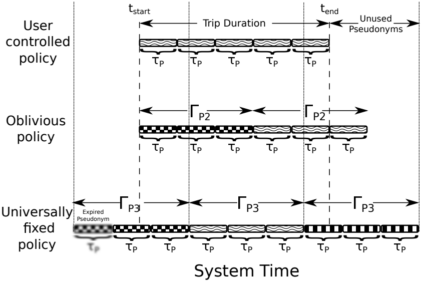
- Honest-but-curious service providers
- Faulty PCAs could:
  - Issue multiple sets of (simultaneously valid) pseudonyms
  - Issue a set of pseudonyms for a non-existing vehicle
  - 'Incriminate' vehicles (users) during a pseudonym resolution process
- Faulty LTCAs could:
  - 'Incriminate' vehicles (users) during the resolution process
  - Issue fake authorization tickets for pseudonym acquisition process
- A faulty RA can continuously initiate a pseudonym validation process towards inferring user sensitive information

Adversarial Model (cont'd)

- Multiple VPKI entities (servers) could collude
- Malicious (compromised) VCS entities
    - Interval adversaries, i.e., On-Board Units (OBUs) could
        - Repeatedly request multiple simultaneously valid pseudonyms, attempting to become 'Sibyl nodes'
        - Mount a clogging Denial of Service (DoS) attack against the VPKI servers
    - External adversaries, i.e., unauthorized entities, could try to:
        - Mount a clogging DoS attack against the VPKI servers

System Model and Assumptions





Pseudonym acquisition overview in the home and foreign domains.

Pseudonym Acquisition Policies.

- P1 & P2: Requests could be user “fingerprints”: exact times of requests throughout the trip
- P3: Request intervals falling within “universally” fixed intervals Γ_{P3}; pseudonym lifetimes aligned with the PCA clock

M. Khodaei, H. Jin, and P. Papadimitratos. “*SECMACE: Scalable and Robust Identity and Credential Management Infrastructure in Vehicular Communication Systems.*” IEEE Transactions on ITS 19(5) 1430-1444

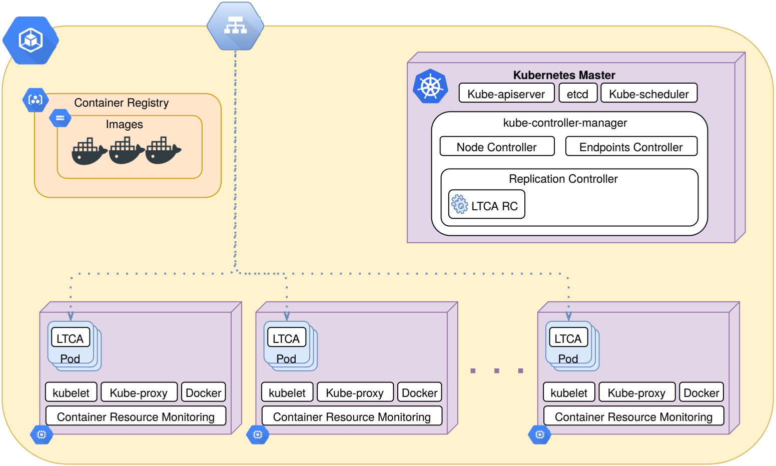
Objectives

- Design, analyse, implement and evaluate the VPKI
    - Management of credentials: provisioning, revocation, resolution
    - Standard-compliant implementation
- Resilience to *honest-but-curious* and *malicious* VPKI entities
- Eradication of Sybil-based misbehavior (without degrading performance)
- Handling of unexpected demanding loads, while being cost-effective
- Scalability
- Efficient revocation and resolution

VPKI as a Service (VPKIaaS)

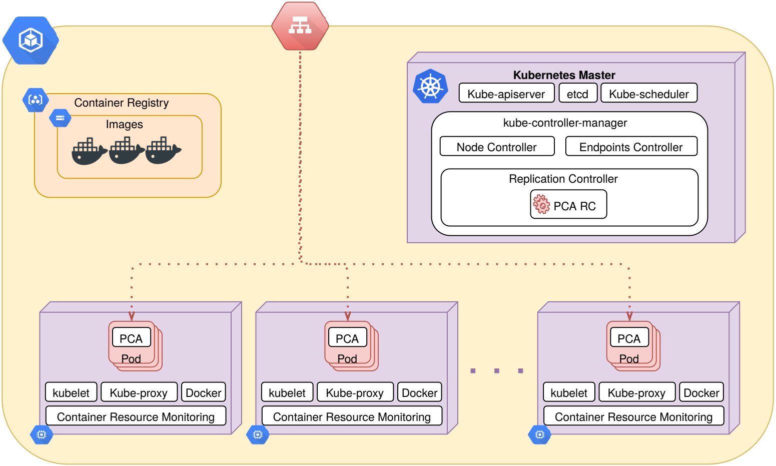
- Refactoring the source code of a state-of-the-art VPKI
- Fully automated procedures of deployment
- Migration to the cloud, e.g., Google Cloud Platform (GCP), Amazon Web Service (AWS), Microsoft Azure
- Health and load metrics used by an orchestration service to scale in/out accordingly
- Eradication of Sybil-based misbehavior when deploying multiple replicas without diminishing the efficiency of the pseudonym acquisition process
- Functionality enhancements

VPKI as a Service (VPKIaaS) Architecture



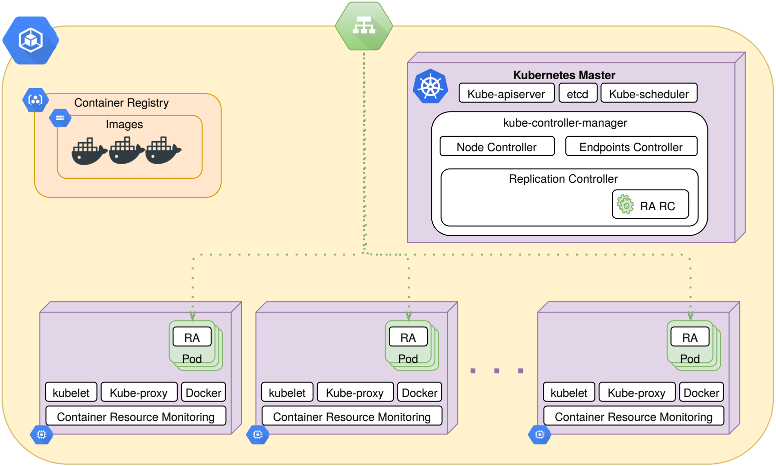
High-level Overview of VPKIaaS Architecture on the Cloud

VPKI as a Service (VPKIaaS) Architecture



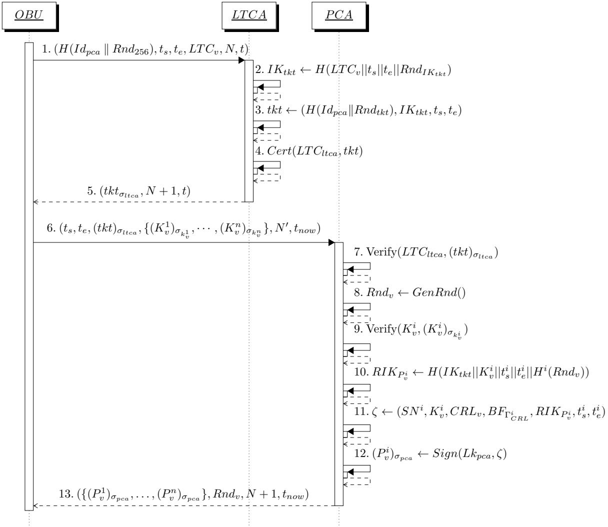
High-level Overview of VPKIaaS Architecture on the Cloud

VPKI as a Service (VPKIaaS) Architecture



High-level Overview of VPKIaaS Architecture on the Cloud

Pseudonym Acquisition Process



OBU

$LTCA$

PCA

1. $(H(Id_{pca} \parallel Rnd_{256}), t_s, t_e, LTC_v, N, t)$

2. $IK_{tkt} \leftarrow H(LTC_v || t_s || t_e || Rnd_{IK_{tkt}})$

3. $tkt \leftarrow (H(Id_{pca} \| Rnd_{tkt}), IK_{tkt}, t_s, t_e)$

4. $Cert(LTC_{ltca}, tkt)$

5. $(tkt_{\sigma_{ltca}}, N+1, t)$

6. $(t_s, t_e, (tkt)_{\sigma_{ltca}}, \{(K_v^1)_{\sigma_{k_v^1}}, \cdots, (K_v^n)_{\sigma_{k_v^n}}\}, N', t_{now})$

7. $\text{Verify}(LTC_{ltca}, (tkt)_{\sigma_{ltca}})$

8. $Rnd_v \leftarrow GenRnd()$

9. $\text{Verify}(K_v^i, (K_v^i)_{\sigma_{k_v^i}})$

10. $RIK_{P_v^i} \leftarrow H(IK_{tkt} || K_v^i || t_s^i || t_e^i || H^i(Rnd_v))$

11. $\zeta \leftarrow (SN^i, K_v^i, CRL_v, BF_{\Gamma_{CRL}^i}, RIK_{P_v^i}, t_s^i, t_e^i)$

12. $(P_v^i)_{\sigma_{pca}} \leftarrow Sign(Lk_{pca}, \zeta)$

13. $(\{(P_v^1)_{\sigma_{pca}}, \ldots, (P_v^n)_{\sigma_{pca}}\}, Rnd_v, N+1, t_{now})$

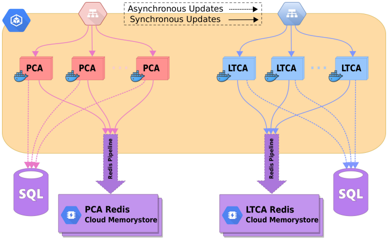
VPKIaaS Memorystore with Redis and MySQL

LTCA Sybil Attack Mitigation

- Checking if a ticket was issued to the requester
- Updating the Redis database if not
- Invoking the ticket issuance procedure

PCA Sybil Attack Mitigation

- Checking if pseudonyms were issued to (the requester of) a given ticket
- Updating the Redis database if not
- Invoking the pseudonym issuance procedure



Ticket	Is Used
V1-T1	0
V1-T2	1
V2-T1	1
V3-T1	0

Certificate	Ticket Exp.
V1	T1
V2	T2
V3	T3
V4	T4

VPKIaaS Memorystore with Redis & MySQL

Ticket Request Validation (by the LTCA)

Ticket Request Validation (by the LTCA using Redis)

```
procedure ValidateTicketReq($SN^i_{LTC}, tkt^i_{start}, tkt^i_{exp}$)
    $(value^i) \leftarrow$ RedisQuery($SN^i_{LTC}$)    ▷ Checking if a ticket was issued to the requester during that period
    if $value^i == NULL$ OR $value^i <= tkt^i_{start}$ then    ▷ If not or does not overlaps with the previously recorded entry
        RedisUpdate($SN^i_{LTC}, tkt^i_{exp}$)    ▷ Updating the entry with the new ticket expiration time
        $Status \leftarrow IssueTicket(\ldots)$    ▷ Invoking ticket issuance procedure
        if $Status == False$ then    ▷ Failure during the ticket issuance process
            RedisUpdate($SN^i_{LTC}, value^i$)    ▷ Reverting $SN^i_{LTC}$ to $value^i$
            return $(False)$    ▷ Ticket issuance failure
        else
            return $(True)$    ▷ Ticket issuance success
        end if
    else
        return $(False)$    ▷ Suspected Sybil attack
    end if
end procedure
```

Pseudonym Request Validation (by the PCA)

Pseudonym Request Validation (by the PCA using Redis)

```
procedure ValidatePseudonymReq($SN^i_{tkt}$)
    $(value^i) \leftarrow$ RedisQuery($SN^i_{tkt}$)    ▷ Checking if pseudonyms were issued to the requester for a given ticket
    if $value^i == NULL$ OR $value^i == False$ then    ▷ If the key does not exist or the value is false (i.e., unused)
        RedisUpdate($SN^i_{tkt}, True$)    ▷ Updating the database, setting value to true (i.e., used)
        $Status \leftarrow IssuePsnyms(\dots)$    ▷ Invoking pseudonym issuance procedure
        if $Status == False$ then    ▷ Failure during the pseudonym issuance process
            RedisUpdate($SN^i_{tkt}, False$)    ▷ Reverting $SN^i_{tkt}$ to False
            return $(False)$    ▷ Pseudonym issuance failure
        else
            return $(True)$    ▷ Pseudonym issuance success
        end if
    else
        return $(False)$    ▷ Suspected Sybil attack
    end if
end procedure
```

Pseudonym Issuance Validation Process

Pseudonym Issuance Validation Process (by the RA)

$$V_j : P_v^i \leftarrow (SN^i, K_v^i, IK_{P_v^i}, t_s^i, t_e^i) \tag{1}$$

$$V_j : \zeta \leftarrow (P_v^i) \tag{2}$$

$$V_j : (\zeta)_{\sigma_v} \leftarrow Sign(P_v^j, \zeta) \tag{3}$$

$$V_j \rightarrow \text{RA} : (Id_{req}, (\zeta)_{\sigma_v}, t_{now}) \tag{4}$$

$$\text{RA} : \text{Verify}(P_v, (\zeta)_{\sigma_v}) \tag{5}$$

$$\text{RA} : \zeta \leftarrow (P_v^i) \tag{6}$$

$$\text{RA} : (\zeta)_{\sigma_{ra}} \leftarrow Sign(Lk_{ra}, \zeta) \tag{7}$$

$$\text{RA} \rightarrow \text{PCA} : (Id_{req}, (\zeta)_{\sigma_{ra}}, \text{LTC}_{ra}, N, t_{now}) \tag{8}$$

$$\text{PCA} : \text{Verify}(LTC_{ra}, (\zeta)_{\sigma_{ra}}) \tag{9}$$

$$\text{PCA} : (tkt, Rnd_{IK_{P_v^i}}) \leftarrow \text{Resolve}(P_v^i) \tag{10}$$

$$\text{PCA} : \chi \leftarrow (SN_{P^i}, tkt_{\sigma_{ltca}}, Rnd_{IK_{P_v^i}}) \tag{11}$$

$$\text{PCA} : (\chi)_{\sigma_{pca}} \leftarrow Sign(Lk_{pca}, \chi) \tag{12}$$

$$\text{PCA} \rightarrow \text{RA} : (Id_{res}, (\chi)_{\sigma_{pca}}, N{+}1, t_{now}) \tag{13}$$

$$\text{RA} : \text{Verify}(LTC_{pca}, \chi) \tag{14}$$

$$\text{RA} :(SN_{P^i}, tkt_{\sigma_{ltca}}, Rnd_{IK_{P_v^i}}){\leftarrow}\chi \tag{15}$$

$$\text{RA} : \text{Verify}(LTC_{ltca}, tkt_{\sigma_{ltca}}) \tag{16}$$

$$\text{RA} :(H(Id_{PCA} \| Rnd_{tkt}), IK_{tkt}, t_s^i, t_e^i, Exp_{tkt}){\leftarrow}tkt \tag{17}$$

$$\text{RA} : H(IK_{tkt}||K_v^i||t_s^i||t_e^i||Rnd_{IK_{P_v^i}}) \stackrel{?}{=} IK_{P_v^i} \tag{18}$$

Security and Privacy Analysis

- ✓ Communication integrity, confidentiality, and non-repudiation
  - Certificates, TLS and digital signatures
- ✓ Authentication, authorization and access control
  - LTCA is the *policy decision and enforcement point*
  - PCA grants the service
  - Security association discovery through LDAP
- ✓ Concealing PCAs, F-LTCA, actual pseudonym acquisition period
  - Sending $H(PCA_{id} \| Rnd_{256}), t_s, t_e, LTC_v$ to the H-LTCA
  - PCA verifies if $[t'_s, t'_e] \subseteq [t_s, t_e]$
- ✓ Thwarting Sybil misbehavior
  - LTCA never issues valid tickets with overlapping lifetime (for a given domain)
  - Tickets are bound to specific PCAs
  - PCA keeps records of ticket usage
  - Suspicious requests instantaneously validated via the Redis Memorystore
  - Redis on a single thread; pipeline guaranteed to sequentially execute commands

Security and Privacy Analysis (cont'd)

- ✓ Single deviant PCA issuing multiple simultaneously valid pseudonyms, or issuing pseudonyms without any valid ticket
  - The RA efficiently validates pseudonyms without harming user privacy

- ✓ High availability and fault-tolerance
  - Benign failure: the Kubernetes master can kill the running (faulty) Pod and create a new Pod
  - High loads: the Kubernetes master scales out the Pods

- ✓ Distributed DoS (DDoS) attacks on the VPKIaaS system
  - Network-level protection; puzzles

Experimental Setup

VPKI testbed

- Implementation in C++, OpenSSL for cryptographic protocols & primitives, TLS and Elliptic Curve Digital Signature Algorithm (ECDSA)-256 (ETSI [TR-102-638] and IEEE 1609.2).
- FastCGI to interface Apache web-server; we use XML-RPC & Google Protocol Buffers

VPKIaaS system

- Built and pushed Docker images for LTCA, PCA, RA, MySQL, and Locust, *an open source load testing tool*, to the Google Container Registry
- Google Kubernetes Engine (GKE) v1.10.11
- Configured a cluster of five Virtual Machines (VMs) (n1-highcpu-32), each with 32 vCPUs and 28.8GB of memory

VPKIaaS Memorystore

- Redis; in-memory key-value data store
- MySQL

Experiment Parameters

Parameters	Config-1	Config-2
Total number of vehicles	1000	100, 50,000
Hatch rate	1	1, 100
Interval between requests	1000-5000 ms	1000-5000 ms
pseudonyms per request	100, 200, 300, 400, 500	100, 200, 500
LTCA memory request	128 MiB	128 MiB
LTCA memory limit	256 MiB	256 MiB
LTCA CPU request	500 m	500 m
LTCA CPU limit	1000 m	1000 m
LTCA HPA	1-40; CPU 60%	1-40; CPU 60%
PCA memory request	128 MiB	128 MiB
PCA memory limit	256 MiB	256 MiB
PCA CPU request	700 m	700 m
PCA CPU limit	1000 m	1000 m
PCA HPA	1-120; CPU 60%	1-120; CPU 60%

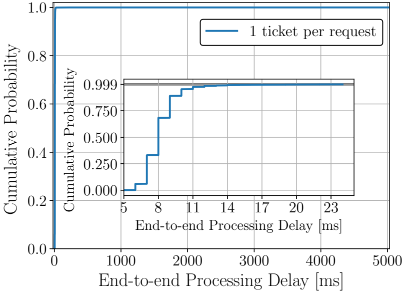
- Config-1: normal vehicle arrival rate; every 1-5 sec, a new vehicle joins the system, requesting 100-500 pseudonyms
- Config-2: flash crowd scenario; on top of Config-1, 100 new vehicles join the system every 1-5 sec, requesting 100-200 pseudonyms

Experimental Setup (cont'd)

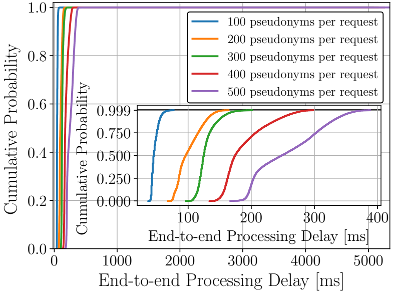
- **Network connectivity**
  - Varies depending on the actual OBU-VPKI connectivity
  - Reliable connectivity to the VPKI (e.g., RSU, Cellular, opportunistic WiFi)
- **Metrics**
  - End-to-end pseudonym acquisition latency from the initialization of ticket acquisition protocol till successful completion of pseudonym acquisition protocol
  - High availability, robustness, reliability, dynamic-scalability
- **Use cases**
  - Large-scale pseudonym provision
  - VPKIaaS with Flash Crowd Load Pattern
  - Dynamic scalability of the VPKIaaS

- **Remark**
  - Pseudonyms issued with non-over-lapping intervals, to mitigate Sybil-based misbehavior
  - Average daily commute 10-30 minutes (actual urban vehicular mobility dataset), or 1 hour (according to the US DoT)
  - Obtaining 100 and 500 pseudonyms per day implies pseudonym lifetimes of 14.4 minutes or 3 minutes respectively, covering 24 hours trip duration
  - Requesting pseudonyms based on Config-2, i.e., VPKIaaS system would serve 720,000 vehicles joining the system within an hour

Performance Evaluation



(a) CDF of end-to-end latency to issue a ticket

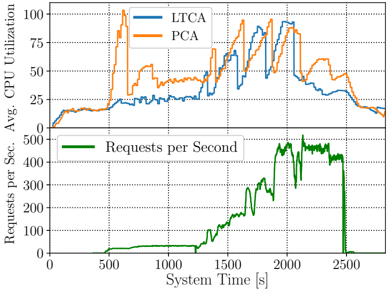


(b) CDF of end-to-end processing delay to issue pseudonyms

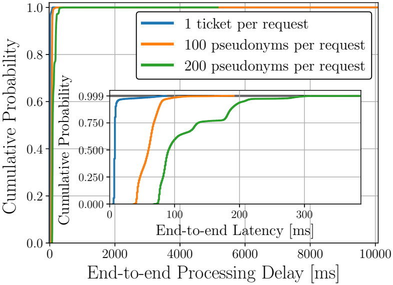
Large-scale pseudonym acquisition (based on Config-1):

- End-to-end Latency for ticket: $F_x(t = 24\, ms) = 0.999$.
- Batch of 100 pseudonyms per request: 99.9% of the vehicles are served within less than 77 ms ($F_x(t = 77\, ms) = 0.999$)
- Batch of 500 pseudonyms per request: $F_x(t = 388\, ms) = 0.999$

Performance Evaluation (cont'd)



(c) CPU utilization and number of requests per second (100 pseudonyms per request)

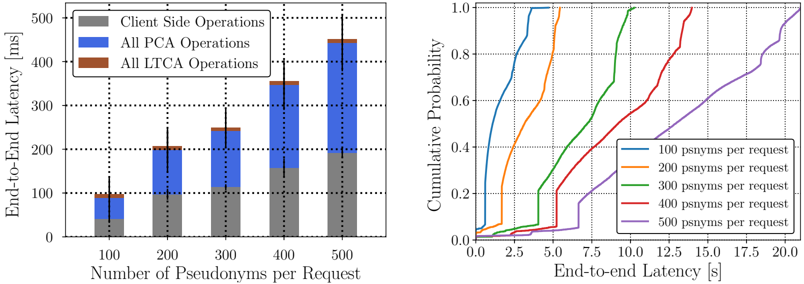


(d) CDF of processing latency to issue tickets and pseudonyms

VPKIaaS system in a flash crowd situation (based on Config-2):

- CPU utilization hits a 60% threshold, services scale out, CPU utilization drops
- Latency to issue a single ticket is: $F_x(t = 87\ ms) = 0.999$
- Batch of 100 pseudonyms per request: $F_x(t = 192\ ms) = 0.999$
- 'normal' conditions vs. flash crowd: latency for a single ticket from 24 ms to 87 ms; latency for issuing 100 pseudonyms from 77 ms to 192 ms

Performance Evaluation (cont'd)

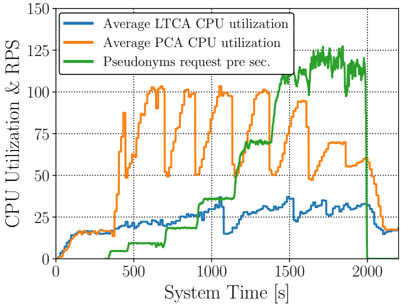


(e) Average e2e latency to obtain pseudonyms **(f)** CDF of e2e latency, observed by clients (including the networking latency)

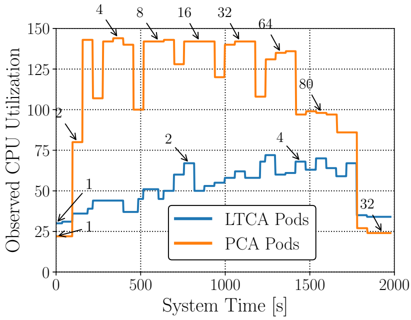
VPKIaaS system with flash crowd load pattern (based on Config-2):

- *All* vehicles obtained a batch of 100 pseudonyms within less than 4,900 ms
- ***Note:*** *The CR manuscript refers to improvement over prior implementation achieved by a standalone implementation [10]: latency for issuing a pseudonym ≈4ms. The same figure for the VPKIaaS system is 0.56 ms (56 ms to issue 100 pseudonyms). The performance overall is captured by Figs. 4-7, which depict data for the VPKIaaS system.*

Performance Evaluation (cont'd)



(g) Number of active vehicles and CPU utilization



(h) Dynamic scalability of VPKIaaS system

Reliability and dynamic scalability of the VPKIaaS system (based on Config-2):

- Each vehicle requests 500 pseudonyms (CPU utilization observed by HPA)
- Synthetic workload generated using 30 containers, each with 1 vCPU and 1GB of memory

Summary

- Refactored a state-of-the-art VPKI source code, with fully automated procedures of deployment and migration to the cloud
- Health and load metrics used by an orchestration service to scale in/out accordingly
- Eradicated Sybil-based misbehavior when deploying multiple replicas of a microservice, without diminishing the efficiency of the pseudonym acquisition
- Enhanced features
- Providing extensive experimental evaluation

Summary (cont'd)

- Practical framework, issues on-demand pseudonyms for large-scale vehicular communication systems
- Highly efficient, scalable, and resilient
- Viable solution for deploying secure and privacy-protecting vehicular communication systems
- Investigating further adversarial behavior by the VPKI entities
- Investigating the performance of cryptographic operations on the Cloud-HSMs

Bibliography I

[1] P. Papadimitratos, V. Gligor, and J.-P. Hubaux, “Securing Vehicular Communications-Assumptions, Requirements, and Principles,” in *ESCAR*, Berlin, Germany, Nov. 2006.

[2] P. Papadimitratos *et al.*, “Secure Vehicular Communication Systems: Design and Architecture,” *IEEE Communications Magazine*, vol. 46, no. 11, pp. 100–109, Nov. 2008.

[3] ——, “Vehicular Communication Systems: Enabling Technologies, Applications, and Future Outlook on Intelligent Transportation,” *IEEE Communications Magazine*, vol. 47, no. 11, pp. 84–95, Nov. 2009.

[4] G. Calandriello, P. Papadimitratos, J.-P. Hubaux, and A. Lioy, “On the Performance of Secure Vehicular Communication Systems,” *IEEE Transactions on Dependable and Secure Computing (TDSC)*, vol. 8, no. 6, pp. 898–912, Nov. 2011.

[5] Security-WG5, “Security & Certification: Trust Models for Cooperative Intelligent Transport System (C-ITS), An analysis of the possible options for the design of the C-ITS trust model based on Public Key Infrastructure in Europe,” https://smartmobilitycommunity.eu/sites/default/files/Security_WG5An1_v1.1.pdf, C-ITS Platform WG5.

[6] ——, “Security & Certification: Revocation of Trust in Cooperative-Intelligent Transport Systems(C-ITS),” https://smartmobilitycommunity.eu/sites/default/files/Security_WG5An2_v1.0.pdf, C-ITS Platform WG5.

[7] 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.

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

[9] ——, “Evaluating On-demand Pseudonym Acquisition Policies in Vehicular Communication Systems,” in *ACM IoV-VoI*, Paderborn, Germany, July 2016.

[10] 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 (TITS)*, vol. 19, no. 5, pp. 1430–1444, May 2018.

[11] W. Whyte, A. Weimerskirch, V. Kumar, and T. Hehn, “A Security Credential Management System for V2V Communications,” in *IEEE VNC*, Boston, MA, Dec. 2013.

Bibliography II

[12] V. Kumar, J. Petit, and W. Whyte, “Binary Hash Tree based Certificate Access Management for Connected Vehicles,” in *ACM WiSec*, Boston, USA, July 2017.

[13] “V2V Communications: Readiness of V2V Technology for Application,” Aug. 2014, National Highway Traffic Safety Administration, DOT HS 812 014.

[14] “Vehicle Safety Communications Security Studies: Technical Design of the Security Credential Management System,” https://bit.ly/2CA1WbV, July 2016.

[15] M. Raya, P. Papadimitratos, I. Aad, D. Jungels, and J.-P. Hubaux, “Eviction of Misbehaving and Faulty Nodes in Vehicular Networks,” *IEEE Journal on Selected Areas in Communications (JSAC)*, vol. 25, no. 8, pp. 1557–1568, Oct. 2007.

[16] M. Khodaei and P. Papadimitratos, “Efficient, Scalable, and Resilient Vehicle-Centric Certificate Revocation List Distribution in VANETs,” in *ACM WiSec*, Stockholm, Sweden, June 2018.

[17] M. A. Simplicio Jr, E. L. Cominetti, H. K. Patil, J. E. Ricardini, and M. V. M. Silva, “ACPC: Efficient Revocation of Pseudonym Certificates using Activation Codes,” *Elsevier Ad Hoc Networks*, July 2018.

[18] J. R. Douceur, “The Sybil Attack,” in *ACM Peer-to-peer Systems*, London, UK, Mar. 2002.

[19] H. Noroozi, M. Khodaei, and P. Papadimitratos, “DEMO: VPKIaaS: A Highly-Available and Dynamically-Scalable Vehicular Public-Key Infrastructure,” in *ACM WiSec*, Stockholm, Sweden, June 2018.

[20] ETSI, “Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Definitions,” ETSI Tech. TR-102-638, Jun. 2009.

[21] IEEE-1609.2, “IEEE Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages,” Mar. 2016.

Scaling Pseudonymous Authentication for Large Mobile Systems

ACM WiSec'19, May 17, 2019

Mohammad Khodaei, Hamid Noroozi, and Panos Papadimitratos

Networked Systems Security Group

www.eecs.kth.se/nss