Evaluating On-demand Pseudonym Acquisition Policies in Vehicular Communication Systems

Mohammad Khodaei and Panos Papadimitratos

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

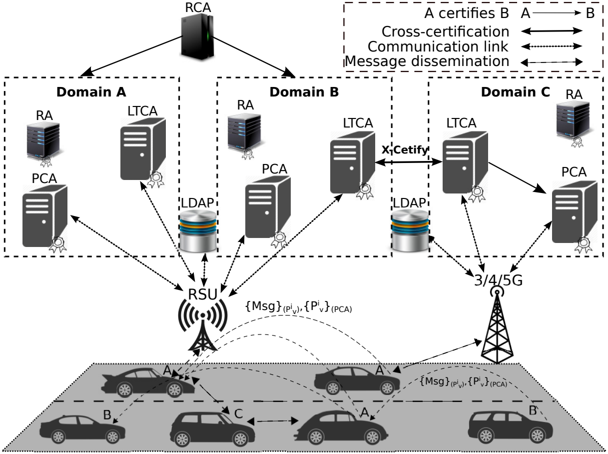
July 5, 2016

Outline

Outline

Secure Vehicular Communication (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



State of the art

Standardization and Harmonization

IEEE 1609.2 [1], ETSI [2] and C2C-CC [3]: VC related specifications for privacy-preserving architectures

Projects

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

Vehicular Public Key Infrastructure (VPKI)

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

Acquisition of short-term credentials, *pseudonyms*

- *How should each vehicle interact with the VPKI, e.g., how frequently and for how long?*
- *Should each vehicle itself determine the pseudonym lifetime?*

Pseudonym Refilling Strategies

Preloading schemes

- Preloading vehicles with required pseudonyms for a long period

On-demand schemes

- More frequent vehicles interactions with the VPKI servers, e.g., once or multiple times per day

Pseudonyms validity intervals

- Overlapping
- Non-overlapping

Strategies / Metrics	Preloading & Overlapping	Preloading & Nonoverlapping	On-demand & Overlapping	On-demand & Nonoverlapping
Storage size	large	large	small	small
Pseudonym quantity	fixed & low volume	fixed & high volume	varying	varying
Pseudonym lifetime	long	short	varying	varying
V-VPKI communication frequency	low	low	high	high
Communication overhead	low	low	high	high
Efficient pseudonym utilization	**very low**	**very low**	**high**	**high**
Pseudonym revocation	difficult & challenging	difficult & challenging	no need (lower risk)	no need (lower risk)
Pseudonym vulnerability window	wide	wide	narrow	narrow
Resilience to Sybil-based misbehavior	×	✓	×	✓
User privacy protection (probability of linking sets of pseudonyms based on timing information)	**privacy protection: high (probability of linking: low)**	**privacy protection: low (probability of linking: high)**	**privacy protection: high (probability of linking: low)**	**privacy protection: low (probability of linking: high)**
User privacy protection (duration for which a pseudonym provider can trivially link sets of pseudonyms for the same vehicle; the longer the duration, the higher the chance to link sets of pseudonyms)	**privacy protection: low (long duration)**	**privacy protection: low (long duration)**	**privacy protection: high (short duration)**	**privacy protection: high (short duration)**
Effect on safety application operations	low	low	high	high
Deployment cost (e.g. RSU)	low	low	high	high
Proposals & schemes	C2C-CC [3], PRESERVE [4], CAMP VSC3 [5]	SeVeCom [6], Safety Pilot [7]	SRAAC [8], V-tokens [9], CoPRA [10]	VeSPA [11], SEROSA [12], SR-VPKI [13], PUCA [14]

Problem Statement

On-demand acquisition with non-overlapping pseudonym lifetimes

(i) improved security, i.e., resilience to Sybil-based misbehavior, (ii) user privacy protection, i.e., shorter periods with linkable pseudonyms, and (iii) efficiency, i.e., no over-provisioning

Contributions

- Proposing three generally applicable policies
- Evaluating overall VPKI performance, i.e., *end-to-end latency*
  - Leveraging two large-scale mobility datasets

Stronger adversarial model

Increased 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)

Outline

1. Secure VC System
2. System Overview
3. Pseudonym Acquisition Protocols
4. Performance Evaluation
5. Conclusion

System Model

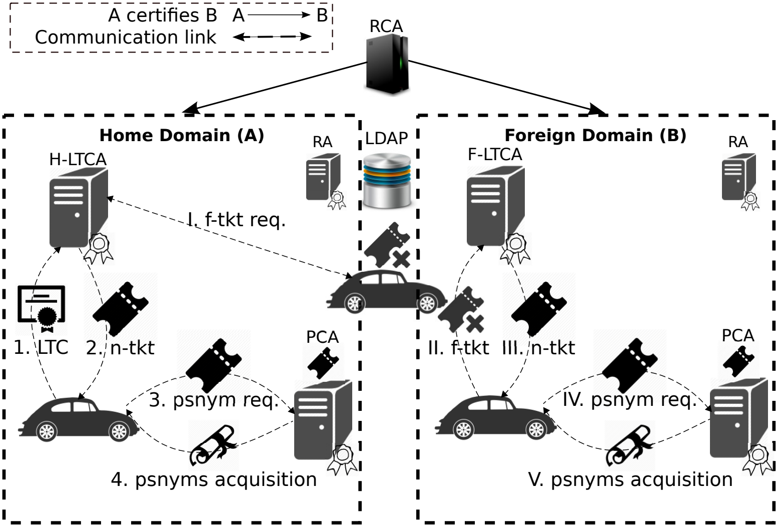
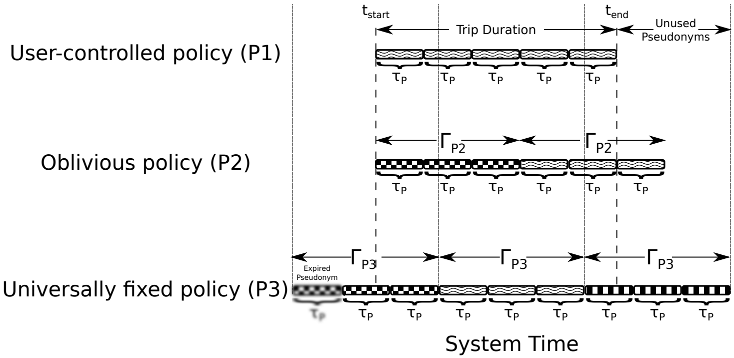


Figure: VPKI Architecture

Pseudonym Acquisition Policies



- P1 & P2: Requests could act as user *"fingerprints"*; the exact time of requests and all subsequent requests until the end of trip could be unique, or one of few
- P3: Requesting intervals fall within *"universally"* fixed interval Γ_{P3}, and pseudonyms are aligned with PCA clock

Outline

Ticket Acquisition Protocols

Protocol 1 Ticket Request (from the LTCA)

procedure ReqTicket($P_x, \Gamma_{Px}, t_s, t_e, t_{date}$)
  if $P_x = P1$ **then**
    $(t_s, t_e) \leftarrow (t_s, t_e)$
  else if $P_x = P2$ **then**
    $(t_s, t_e) \leftarrow (t_s, t_s + \Gamma_{P2})$
  else if $P_x = P3$ **then**
    $(t_s, t_e) \leftarrow (t_{date} + \Gamma^{i}_{P3}), t_{date} + \Gamma^{i+1}_{P3})$
  end if
  $\zeta \leftarrow (Id_{tkt\text{-}req}, H(Id_{PCA} \| Rnd_{tkt}), t_s, t_e)$
  $(\zeta)_{\sigma_v} \leftarrow Sign(Lk_v, \zeta)$
  return $((\zeta)_{\sigma_v}, \text{LTC}_v, N, t_{now})$
end procedure

- Run over Transport Layer Security (TLS) with mutual authentication

Protocol 2 Issuing a Ticket (by the LTCA)

procedure IssueTicket($(msg)_{\sigma_v}, \text{LTC}_v, N, t_{now}$)
  Verify($\text{LTC}_v, (msg)_{\sigma_v}$)
  $IK_{tkt} \leftarrow H(\text{LTC}_v \| t_s \| t_e \| Rnd_{IK_{tkt}})$
  $\zeta \leftarrow (SN, H(Id_{PCA} \| Rnd_{tkt}), IK_{tkt}, Rnd_{IK_{tkt}}, t_s, t_e, Exp_{tkt})$
  $(tkt)_{\sigma_{ltca}} \leftarrow Sign(Lk_{ltca}, \zeta)$
  return $((tkt)_{\sigma_{ltca}}, N + 1, t_{now})$
end procedure

- *"ticket identifiable key"* (IK_{tkt}) binds a ticket to the corresponding Long Term Certificate (LTC)
- Preventing a compromised LTCA from mapping a different LTC during resolution process

Pseudonyms Acquisition Protocols

Protocol 3 Pseudonym Request (from the PCA)

procedure $\textsc{ReqPsnyms}(t_s, t_e, (tkt)_{\sigma_{ltca}})$
  for i:=1 to **n do**
    Begin
      Generate(K_v^i, k_v^i)
      $(K_v^i)_{\sigma_{k_v^i}} \leftarrow$ Sign(k_v^i, K_v^i)
    End
  $psnymReq \leftarrow (Id_{req}, Rnd_{tkt}, t_s, t_e, (tkt)_{\sigma_{ltca}}, \{(K_v^1)_{\sigma_{k_v^1}}, ..., (K_v^n)_{\sigma_{k_v^n}}\}, N, t_{now})$
  return *psnymReq*
end procedure

- Run over TLS with unidirectional (server-only) authentication

Protocol 4 Issuing Pseudonyms (by the PCA)

procedure $\textsc{IssuePsnyms}(psnymReq)$
  $psnymReq \rightarrow (Id_{req}, Rnd_{tkt}, t_s, t_e, (tkt)_{\sigma_{ltca}}, \{(K_v^1)_{\sigma_{k_v^1}}, ..., (K_v^n)_{\sigma_{k_v^n}}\}, N, t_{now})$
  Verify$(LTC_{ltca}, (tkt)_{\sigma_{ltca}})$
  $H(Id_{this\text{-}PCA} \| Rnd_{tkt}) \stackrel{?}{=} H(Id_{PCA} \| Rnd_{tkt})$
  $[t_s,\ t_e] \stackrel{?}{=} ([t_s, t_e])_{tkt}$
  for i:=1 to **n do**
    Begin
      Verify$(K_v^i, (K_v^i)_{\sigma_{k_v^i}})$
      $IK_{P^i} \leftarrow H(IK_{tkt} || K_v^i || t_s^i || t_e^i || Rnd_{IK_v^i})$
      $\zeta \leftarrow (SN^i, K_v^i, IK_{P^i}, Rnd_{IK_v^i}, t_s^i, t_e^i)$
      $(P_v^i)_{\sigma_{pca}} \leftarrow Sign(Lk_{pca}, \zeta)$
    End
  return $(\{(P_v^1)_{\sigma_{pca}}, \ldots, (P_v^n)_{\sigma_{pca}}\}, N{+}1, t_{now})$
end procedure

- *"pseudonym identifiable key"* (IK_{P^i}) binds a pseudonym to the corresponding ticket
- Preventing a compromised PCA from mapping a different ticket during resolution process

Outline

Experimental Setup

- **VPKI testbed**
  - Implementation in C++
  - OpenSSL: TLS and Elliptic Curve Digital Signature Algorithm (ECDSA)-256 according to the standard [1]
- **Network connectivity**
  - Varies depending on the actual OBU-VPKI connectivity
  - Reliable connectivity to the VPKI (e.g., RSU, Cellular, opportunistic WiFi)
- **Main metric**
  - *End-to-end pseudonym acquisition latency* from the initialization of protocol 1 till successful completion of protocol 4

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

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

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

Choice of parameters:

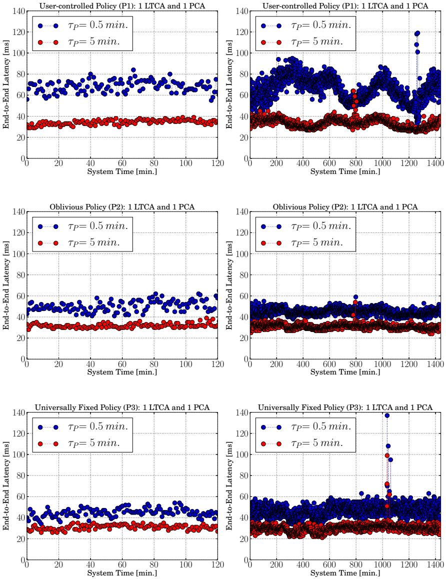
- Frequency of interaction and volume of workload to a PCA
- Γ=5 min., τ_P=0.5 min., 5 min.

Table: Latency Statistics for each Policy (Γ=5 min., τ_P=0.5 min.)

	TAPAS-P1	TAPAS-P2	TAPAS-P3	LuST-P1	LuST-P2	LuST-P3
Maximum (ms)	426	268	4254	504	248	3408
Minimum (ms)	17	26	18	15	25	20
Average (ms)	69	50	45	69	45	47
Std. Deviation	26	17	23	30	12	21
Variance	708	295	535	895	138	449
$\Pr\{t \leq x\} = 0.99$ (ms)	153	109	70	167	80	74

LuST dataset:

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



Outline

Conclusion and Future Work

Conclusion

- Efficient, secure, and privacy-preserving VPKI
- Timing information cannot harm user privacy
- Modest VMs can serve sizable areas or domain with very low delays

Future Work

- Investigation of pseudonym utilization with various configurations ($\Gamma_{P2/P3}$ and τ_P)
- Evaluation of the level of privacy, i.e., unlinkability, based on the timing information of the pseudonyms for each policy
- Evaluation of actual networking latency, e.g., OBU-RSU
- Rigorous analysis of the security and privacy protocols

Bibliography

[1] IEEE P1609.2/D12, "Draft Standard for Wireless Access in Vehicular Environments," Jan. 2012.

[2] T. ETSI, "ETSI TS 103 097 v1. 1.1-Intelligent Transport Systems (ITS); Security; Security Header and Certificate Formats, Standard, TC ITS, 2013."

[3] Car-to-Car Communication Consortium (C2C-CC), http://www.car-2-car.org/.

[4] "Preparing Secure Vehicle-to-X Communication Systems - PRESERVE," http://www.preserve-project.eu/.

[5] W. Whyte *et al.*, "A Security Credential Management System for V2V Communications," in *IEEE VNC*, Boston, Dec. 2013.

[6] P. Papadimitratos *et al.*, "Secure Vehicular Communication Systems: Design and Architecture," *IEEE CommMag*, vol. 46, no. 11, pp. 100–109, Nov. 2008.

[7] "U.S. Department of Transportation (DoT). Safety Pilot Model Deployment." http://safetypilot.umtri.umich.edu/.

[8] L. Fischer *et al.*, "Secure Revocable Anonymous Authenticated Inter-vehicle Communication (SRAAC)," in *ESCAR*, Berlin, Germany, Nov. 2006.

[9] F. Schaub *et al.*, "V-tokens for Conditional Pseudonymity in VANETs," in *IEEE WCNC*, NJ, USA, Apr. 2010.

[10] N. Bißmeyer *et al.*, "CoPRA: Conditional Pseudonym Resolution Algorithm in VANETs," in *IEEE WONS*, Banff, Canada, Mar. 2013.

[11] N. Alexiou *et al.*, "VeSPA: Vehicular Security and Privacy-preserving Architecture," in *ACM HotWiSec*, Budapest, Hungary, Apr. 2013.

[12] S. Gisdakis *et al.*, "SEROSA: SERvice Oriented Security Architecture for Vehicular Communications," in *IEEE VNC*, Boston, MA, USA, Dec. 2013.

[13] M. Khodaei *et al.*, "Towards Deploying a Scalable & Robust Vehicular Identity and Credential Management Infrastructure," in *IEEE VNC*, Paderborn, Germany, Dec. 2014.

[14] D. Förster *et al.*, "PUCA: A Pseudonym Scheme with User-Controlled Anonymity for Vehicular Ad-Hoc Networks (VANET)," in *IEEE VNC*, Paderborn, Germany, Dec. 2014.

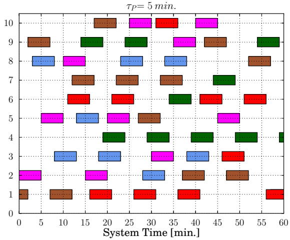
Evaluating On-demand Pseudonym Acquisition Policies in Vehicular Communication Systems

Mohammad Khodaei and Panos Papadimitratos

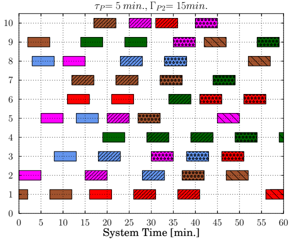
Networked Systems Security Group (NSS)
www.ee.kth.se/nss

July 5, 2016

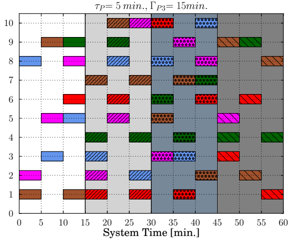
Linkability based on Timing Information of Credentials



User-controlled policy (P1)



Oblivious policy (P2)



Universally fixed policy (P3)

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