SECMACE: Scalable and Robust Identity and Credential Management Infrastructure in Vehicular Communication Systems

M. Khodaei, H. Jin and P. Papadimitratos
Networked Systems Security Group (NSS)

In IEEE Transactions on Intelligent Transportation Systems (April 2018)
Outline

Secure Vehicular Communication (VC) Systems

Problem Statement
System Model
Security and Privacy Analysis
Performance Evaluation
Summary of Contributions and Future Steps
Vehicular Communication (VC) Systems

Figure: Photo Courtesy of the Car2Car Communication Consortium (C2C-CC)
Security and Privacy for VC Systems

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

---


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)
State-of-the-art

Standardization and harmonization efforts

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

Projects

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

Proposals

- V-Token, CoPRA, SCMS , SEROSA, PUCA
Outline

Secure Vehicular Communication (VC) Systems

Problem Statement
System Model
Security and Privacy Analysis
Performance Evaluation
Summary of Contributions and Future Steps
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 acquisition 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
Outline

Secure Vehicular Communication (VC) Systems
Problem Statement

**System Model**

Security and Privacy Analysis
Performance Evaluation
Summary of Contributions and Future Steps
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

A certifies B

Communication link

RCA

Home Domain (A)

F-LTCA

1. LTC

2. n-tkt

3. psnym req.

4. psnyms acquisition

Foreign Domain (B)

H-LTCA

I. f-tkt req.

II. f-tkt

III. n-tkt

RA

LDAP

PCA

IV. psnym req.

V. psnyms acquisition

Figure: VPKI Architecture
Pseudonym Acquisition Policies

User-controlled policy (P1)

Oblivious policy (P2)

Universally fixed policy (P3)

\( \tau_{P1} \) \( \tau_{P2} \) \( \tau_{P3} \)

System Time

\( t_{\text{start}} \) \( t_{\text{end}} \) Trip Duration

Unused Pseudonyms

Expired Pseudonym
Vehicle Registration and Long Term Certificate (LTC) Update

1. $L K_v, L k_v$

2. $(L K_v)_{\sigma_{L K_v}} , N, t$

3. $Cert(LTC_{ltca}, L K_v)$

4. $L T C_v, N + 1, t$
Ticket Acquisition Protocols

Protocol 1 Ticket Request (from the LTCA)

1: procedure \( \text{REQ} \text{TICKET}(P_x, \Gamma_{P_x}, t_s, t_e, t_{date}) \)
2: \hspace{1cm} if \( P_x = P1 \) then
3: \hspace{2cm} (\( t_s, t_e \)) ← (\( t_s, t_e \))
4: \hspace{2cm} else if \( P_x = P2 \) then
5: \hspace{3cm} (\( t_s, t_e \)) ← (\( t_s, t_s + \Gamma_{P2} \))
6: \hspace{2cm} else if \( P_x = P3 \) then
7: \hspace{3cm} (\( t_s, t_e \)) ← (\( t_{date} + \Gamma_{P3} \), \( t_{date} + \Gamma_{P3}^{i+1} \))
8: \hspace{2.5cm} end if
9: \hspace{1cm} \( \zeta \leftarrow (Id_{\text{tkt}-\text{req}}, H(Id_{PCA} || Rnd_{\text{tkt}}), t_s, t_e) \)
10: \hspace{1cm} (\( \zeta \))\(_{\sigma_v} \leftarrow \text{Sign}(Lk_v, \zeta) \)
11: \hspace{1cm} return ((\( \zeta \))\(_{\sigma_v} \), \( \text{LTC}_V \), \( N \), \( t_{now} \))
12: end procedure

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

Protocol 2 Issuing a Ticket (by the LTCA)

1: procedure ISSUE\text{TICKET}((\( msg \))\(_{\sigma_v} \), \( \text{LTC}_V \), \( N \), \( t_{now} \))
2: \hspace{1cm} Verify(\( \text{LTC}_V, (msg)_{\sigma_v} \))
3: \hspace{2cm} ILK_{tkt} ← H(\( \text{LTC}_V || t_s || t_e || Rnd_{ILK_{tkt}} \))
4: \hspace{2cm} \( \zeta \leftarrow (SN, H(Id_{PCA} || Rnd_{tkt}), ILK_{tkt}, Rnd_{ILK_{tkt}}, \)
5: \hspace{2cm} t_s, t_e, Exp_{tkt} \)
6: \hspace{2cm} (\( tk_t \))\(_{\sigma_{ltca}} \leftarrow \text{Sign}(Lk_{ltca}, \zeta) \)
7: \hspace{1cm} return ((\( tk_t \))\(_{\sigma_{ltca}} \), \( N + 1 \), \( t_{now} \))
8: end procedure

- “ticket identifiable key” (ILK\(_{tkt}\)) binds a ticket to the corresponding LTC
- Preventing a compromised LTCA from mapping a different LTC during resolution process
Pseudonyms Acquisition Protocols

Protocol 3 Pseudonym Request (from the PCA)

1: procedure REQPSNYMS($t_s, t_e, (tkt)_{\sigma_{ltca}}$)
2: for $i:=1$ to $n$ do
3: Begin
4: Generate($K^i_V, k^i_V$)
5: $(K^i_V)_{\sigma_{k^i_V}}$ ← Sign($k^i_V, K^i_V$)
6: End
7: psnymReq ← $(Id_{req}, Rnd_{tkt}, t_s, t_e, (tkt)_{\sigma_{ltca}}, ((K^1_V)_{\sigma_{k^1_V}}, \ldots, (K^n_V)_{\sigma_{k^n_V}}), N, t_{now})$
8: return psnymReq
9: end procedure

Run over TLS with unidirectional (server-only) authentication

Protocol 4 Issuing Pseudonyms (by the PCA)

1: procedure ISSUEPSNYMS(psnymReq)
2: psnymReq → $(Id_{req}, Rnd_{tkt}, t_s, t_e, (tkt)_{\sigma_{ltca}}, ((K^1_V)_{\sigma_{k^1_V}}, \ldots, (K^n_V)_{\sigma_{k^n_V}}), N, t_{now})$
3: Verify($LTC_{ltca}, (tkt)_{\sigma_{ltca}}$)
4: $H(Id_{this-PCA}||Rnd_{tkt}) \overset{?}{=} H(Id_{PCA}||Rnd_{tkt})$
5: $[t_s, t_e] \overset{?}{=} ([t_s, t_e])_{tkt}$
6: for $i:=1$ to $n$ do
7: Begin
8: Verify($K^i_V, (K^i_V)_{\sigma_{k^i_V}}$)
9: $IK_{pi} \leftarrow H(IK_{tkt}||K^i_V||t^i_s||t^i_e||Rnd_{IK^i_V})$
10: $\zeta \leftarrow (SN^i, K^i_V, IK_{pi}, Rnd_{IK^i_V}, t^i_s, t^i_e)$
11: $(P^i_V)_{\sigma_{pca}} \leftarrow \text{Sign}(Lk_{pca}, \zeta)$
12: End
13: return $\{(P^1_V)_{\sigma_{pca}}, \ldots, (P^n_V)_{\sigma_{pca}}\}, N+1, t_{now}$
14: end procedure

“pseudonym identifiable key” ($IK_{pi}$) binds a pseudonym to the corresponding ticket

Preventing a compromised PCA from mapping a different ticket during resolution process
Ticket and Pseudonym Acquisition

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

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

3. $tkt, N + 1, t$

4. $tkt, Rnd_{256}, t_{s'}, t_{e'}, \{(K^1_v)_{\sigma_{k^1_v}}, \ldots, (K^n_v)_{\sigma_{k^n_v}}\}, N', t$

5. $Cert(LTC_{pca}, P^i_v)$

6. $\{P^1_v, \ldots, P^n_v\}, N' + 1, t$
Roaming User: Foreign Ticket Authentication

1. LDAP Req.

2. LDAP Search

3. LDAP Res.

4. $H(F-LTCA_{ID} \parallel R_{nd_{256}}), t_s, t_e, LTC_v, N, t$

5. Cert($LTCA_{ltca}, f-tkt$)

6. $f-tkt, N + 1, t$
Native Ticket and Pseudonym Acquisition in the Foreign Domain

1. $f\text{-}tkt, H(PCA_{ID}||Rnd'_{256}), Rnd_{256}, N, t$

2. $\text{Cert}(LTC_{ltca}, n\text{-}tkt)$

3. $n\text{-}tkt, N + 1, t$

4. $n\text{-}tkt, Rnd'_{256}, t_{s'}, t_{e'}, \{(K^1_v)_{\sigma_{k_v}}, \ldots, (K^n_v)_{\sigma_{k_v}}\}, N', t$

5. $\text{Cert}(LTC_{pca}, P^i_v)$

6. \{$P^1_v, \ldots, P^n_v\}, N' + 1, t$
Pseudonym Revocation and Resolution

1. $P_i, N, t$

2. Update CRL

3. $tkt, N + 1, t$

4. $SN_{tkt}, N', t$

5. Resolve $LTC_v$

6. $LTC_v, N' + 1, t$
Outline

Secure Vehicular Communication (VC) Systems
Problem Statement
System Model

Security and Privacy Analysis
Performance Evaluation

Summary of Contributions and Future Steps
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 $H(PCA_{id} \parallel Rnd_{256}), t_s, t_e, LTC_v$ to the H-LTCA
  - PCA verifies if $[t'_s, t'_e] \subseteq [t_s, t_e]$

- Thwarting Sybil-based misbehavior
  - LTCA never issues valid tickets with overlapping lifetime (for a given domain)
  - A ticket is bound to a specific PCA
  - PCA keeps records of ticket usage
Linkability based on Timing Information of Credentials

- Non-overlapping pseudonym lifetimes from eavesdroppers’ perspective
- P1 & P2: Distinct lifetimes per vehicle make linkability easier (requests/pseudonyms could act as user ‘fingerprints’)
- P3: Uniform pseudonym lifetime results in no distinction
Outline

Secure Vehicular Communication (VC) Systems
Problem Statement
System Model
Security and Privacy Analysis
Performance Evaluation
Summary of Contributions and Future Steps
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)

### Table: Servers and Clients Specifications

<table>
<thead>
<tr>
<th></th>
<th>LTCA</th>
<th>PCA</th>
<th>RA</th>
<th>Clients</th>
</tr>
</thead>
<tbody>
<tr>
<td>VM Number</td>
<td>2</td>
<td>5</td>
<td>1</td>
<td>25</td>
</tr>
<tr>
<td>Dual-core CPU (Ghz)</td>
<td>2.0</td>
<td>2.0</td>
<td>2.0</td>
<td>2.0</td>
</tr>
<tr>
<td>BogoMips</td>
<td>4000</td>
<td>4000</td>
<td>4000</td>
<td>4000</td>
</tr>
<tr>
<td>Memory</td>
<td>2GB</td>
<td>2GB</td>
<td>1GB</td>
<td>1GB</td>
</tr>
<tr>
<td>Database</td>
<td>MySQL</td>
<td>MySQL</td>
<td>MySQL</td>
<td>MySQL</td>
</tr>
<tr>
<td>Web Server</td>
<td>Apache</td>
<td>Apache</td>
<td>Apache</td>
<td>-</td>
</tr>
<tr>
<td>Load Balancer</td>
<td>Apache</td>
<td>Apache</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Emulated Threads</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>400</td>
</tr>
</tbody>
</table>

- **Use cases**
  - Pseudonym provision
  - Performing a DDoS attack
Experimental Setup (cont’d)

**Table:** Mobility Traces Information

<table>
<thead>
<tr>
<th></th>
<th>TAPAS Cologne</th>
<th>LuST [5]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of vehicles</td>
<td>75,576</td>
<td>138,259</td>
</tr>
<tr>
<td>Number of trips</td>
<td>75,576</td>
<td>287,939</td>
</tr>
<tr>
<td>Duration of snapshot (hour)</td>
<td>24</td>
<td>24</td>
</tr>
<tr>
<td>Available duration of snapshot (hour)</td>
<td>2 (6-8 AM)</td>
<td>24</td>
</tr>
<tr>
<td>Average trip duration (sec.)</td>
<td>590.49</td>
<td>692.81</td>
</tr>
<tr>
<td>Total trip duration (sec.)</td>
<td>44,655,579</td>
<td>102,766,924</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th></th>
<th>LTCA</th>
<th>PCA</th>
<th>Client</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of entities</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Dual-core CPU (Ghz)</td>
<td>2.0</td>
<td>2.0</td>
<td>2.0</td>
</tr>
<tr>
<td>BogoMips</td>
<td>4000</td>
<td>4000</td>
<td>4000</td>
</tr>
<tr>
<td>Memory</td>
<td>2GB</td>
<td>2GB</td>
<td>1GB</td>
</tr>
<tr>
<td>Database</td>
<td>MySQL</td>
<td>MySQL</td>
<td>MySQL</td>
</tr>
</tbody>
</table>

- 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
- $\Gamma = 5$ min., $\tau_P = 0.5$ min., 5 min.

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

- P1: $F_X(t = 167 \text{ ms}) = 0.99$
- P2: $F_X(t = 80 \text{ ms}) = 0.99$
- P3: $F_X(t = 74 \text{ ms}) = 0.99$
Latency Comparison for Different Policies

**Figure:** End-to-end latency comparison for different policies (Tapas Dataset)
Pseudonym Utilization, LuST Dataset for P2 & P3

P2: Oblivious Policy

P3: Universally Fixed Policy
The VPKI Servers under a DDoS Attack

Figure: Overhead to obtain pseudonyms, LuST dataset with P1 (\(\tau_P = 5\) min.)
Performance Evaluation for Ticket and Pseudonym Acquisition

Obtaining a Certificate Revocation List (CRL)

Online Certificate Status Protocol (OCSP) validation

- Ticket Acquisition: $F_x(t=4\text{ms})=0.95$ or $\Pr\{t \leq 4\text{ms}\}=0.95$.
- Pseudonym Acquisition: $F_x(t=52\text{ms})=0.95$ or $\Pr\{t \leq 52\}=0.95$. 
Performance Evaluation for Pseudonym Revocation (CRL or OCSP)

Obtaining CRL from a PCA: LuST dataset

- 10K revoked pseudonyms
- 25K revoked pseudonyms
- 50K revoked pseudonyms
- 100K revoked pseudonyms

Cumulative Probability

End-to-End Latency [sec.]

OCSP Validation with 1 PCA: LuST dataset

- 1 pseudonym per request
- 100 pseudonyms per request
- 500 pseudonyms per request

End-to-End Latency [ms]

System Time [min.]

Obtaining a CRL

OCSP validation
On average 100 ms to resolve & revoke a pseudonym
Comparison with Other Implementations

**Table:** Latency for issuing 100 pseudonyms (without communication delay)

<table>
<thead>
<tr>
<th>System</th>
<th>$\text{Delay}_{\text{PCA}}$</th>
<th>$\text{CPU}_{\text{PCA}}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>VeSPA [6]</td>
<td>817 ms</td>
<td>3.4 GHz</td>
</tr>
<tr>
<td>SEROSA [7]</td>
<td>650 ms</td>
<td>2.0 GHz</td>
</tr>
<tr>
<td>PUCA [8]</td>
<td>1000 ms</td>
<td>2.53 GHz</td>
</tr>
<tr>
<td>PRESERVE PKI (Fraunhofer SIT) [9]</td>
<td>$\approx$ 4000 ms</td>
<td>N/A</td>
</tr>
<tr>
<td>C2C-CC PKI (ESCRYPT) [3]</td>
<td>393 ms</td>
<td>N/A</td>
</tr>
<tr>
<td>SECMACE</td>
<td>260 ms</td>
<td>2.0 GHz</td>
</tr>
</tbody>
</table>
Outline

Secure Vehicular Communication (VC) Systems
Problem Statement
System Model
Security and Privacy Analysis
Performance Evaluation

Summary of Contributions and Future Steps
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
Future Steps

VPKI enhancements

- 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

Efficient distribution of revocation information

- How to disseminate pseudonyms validity information without interfering with vehicles operations?
Bibliography I


Bibliography II


SECMACE: Scalable and Robust Identity and Credential Management Infrastructure in Vehicular Communication Systems

M. Khodaei, H. Jin, and P. Papadimitratos
Networked Systems Security Group (NSS)
www.ee.kth.se/nss

In IEEE Transactions on Intelligent Transportation Systems
(April 2018)