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

Mohammad Khodaei and Panos Papadimitratos
Networked Systems Security Group

www.ee.kth.se/nss
Vehicular Communication (VC)

PHOTO COURTESY OF THE CAR-TO-CAR COMMUNICATION CONSORTIUM (C2C-CC)
Vehicular Communication Applications

Safety

Warning: Accident at (x,y,z)

Warning: Accident at (x,y,z)

Efficiency

Warning: Congestion at (x,y,z)

Traffic Update: Congestion at (x,y,z); Use alternate route

RSU
Vehicular Communication Applications (cont’d)

Efficiency

Warning: Emergency vehicle approaching in area (X,Y,Z);

Warning: Ambulance approaching at (x,y,z)

Slow down and yield
Security and Privacy for VC – Why?

Safety (?)

Warning: Accident at \((x,y,z)\)

Efficiency (?)

Warning: Congestion at \((x,y,z)\)

Traffic Update: Congestion at \((x,y,z)\); Use alternate route
Security and Privacy for VC – Why? (cont’d)

Efficiency (?)

Warning: Emergency vehicle approaching in area (X,Y,Z);

Warning: Ambulance approaching at (x,y,z)

Slow down and yield
Security and Privacy for VC – Why? (cont’d)

Privacy (?)

A at location
\((x_1, y_1, z_1)\)
at time \(t_1\)

A communicates with \(B\)

①

Eavesdropper

②

A enters the parking lot at time \(t_3\)

A downloads data from server \(X\)

A refuels at time \(t_2\)
and location
\((x_2, y_2, z_2)\)
Security and Privacy for VC Systems

Vehicular Public-Key Infrastructure (VPKI)

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


Pseudonym Refilling & Authentication

Pseudonymous Authentication:
1. Generate signature with $SK_1$
2. Append certificate
3. Send packet

Beacon packet
- Header: $H$
- Payload: $m$
- $\text{Sig}(SK_1, H, m)$
- $\text{Cert}(PNYM_K_1)$

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

References:
VPKI Overview

Root Certification Authority (RCA)

Long-Term (CA)

Pseudonym CA (PCA)

Resolution Authority (RA)

Lightweight Directory Access Protocol (LDAP)

A certifies B

Communication link

Message dissemination

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.
Pseudonym Acquisition Overview

A certifies B
Communication link

Home Domain (A)

1. LTC
2. n-tkt
3. psnym req.
4. psnyms acquisition

Foreign Domain (B)

1. f-tkt req.
2. H-LTCA
3. RA
4. LDAP
5. PCA
6. F-LTCA
7. RA
8. n-tkt
9. psnym req.
10. psnyms acquisition

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.
End-to-End Delay to Obtain Pseudonyms
Vehicular Testbed at KTH

V2X Security Subsystem (VSS)

- Dual-core 1.66 GHz
- 2 GB Memory
- 100 MB Ethernet
- USB 2.0 Controller

Functions

- Hitachi communication stack
- CAM & DENM generator
- Security processing of messages (sign, verify)
- Crypto acceleration (AES, ECDSA, …)
- Secure storage
Related Publications


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

Mohammad Khodaei and Panos Papadimitratos
Networked Systems Security Group

www.ee.kth.se/nss