A Security Credential Management System (SCMS) for Vehicle-to-Vehicle Communications

Thorsten Hehn (CAMP VSC3 / Volkswagen Group of America)
Motivation

• V2V system can alert the driver (thus help prevent crashes) by issuing different safety warnings, e.g.:
  • Forward Collision Warning (FCW)
  • Intersection Movement Assist (IMA)
  • Electronic Emergency Brake Light (EEBL)
• Messages include information on current position, velocity, etc.
• Messages received over the air: integrity and authentication required

• CAMP VSC3 Choice:
  • Unencrypted messages with signature based on asymmetric cryptography (ECDSA-256)
  • Certificates (incl. public key) issued by a Public-Key-Infrastructure (PKI)
Contradicting requirements

• Privacy (OEM privacy goals)
  • Prevent SCMS from collecting Personally Identifiable Information (PII)
  • Prevent trip tracking by outsiders: frequent change in pseudonym certificates
  • Prevent trip tracking by SCMS insiders: separation of duties and information such that trip tracking is only possible by a collusion of several SCMS components

• Trustworthy messages
  • Incoming messages must be verifiable
  • Misbehaving units need to be removed
Basic Overview

To Enrollment Certificate Authority: Prove Eligibility
Receive ONE enrollment certificate

Certificate Provisioning

To Registration Authority: Show Enrollment Cert
Receive SET of pseudonym certificates

Participate in V2V

Current Assumptions on pseudonym certificates:
• 3000 pseudonym certificates
• 20 valid per week
• Frequent change of pseudonym certificate (e.g. every 5 minutes)
Full SCMS Structure

SCMS Manager

Policy

Technical

Root CA

Intermediate CA

Pseudonym CA

Request Coordination

Registration Authority

Device Config. Manager

Location Obscuer Proxy

Certification Lab

Enrollment CA

Device 1

Device 2

Device 3

Legend

Intrinsically Central

Not Intrinsically Central

Regular communication

Out-of-band communication

Internal Blacklist Manager

Global Detection

CRL Generator

CRL Store

CRL Broadcast
Enrollment CA

- Certification Lab
- Intermediate CA
- Pseudonym CA
- Request Coordination
- Registration Authority
- Device Config. Manager
- Location Obscuer Proxy

- Root CA
- Enrollment CA
- Misbehavior Authority
  - Internal Blacklist Manager
  - Global Detection
  - CRL Generator
  - Linkage Authority 1
  - Linkage Authority 2
  - CRL Store
  - CRL Broadcast

Legend:
- In Intrinsically Central
- Not Intrinsically Central
- Regular communication
- Out-of-band communication
Linkage Authority
Privacy by Design, an OEM perspective

• Privacy from attacks by an SCMS insider
  • Introduce extra SCMS components, e.g. 2\textsuperscript{nd} LA, LOP, etc.
  • Don’t link certificates to VIN

• Separate operation of SCMS components:
  Two or more components should not be run by the same organization without “proper” separation
  \textbf{if}
  the combined information held by the components would allow the organization to track\textsuperscript{*} a vehicle

*predict next pseudonym certificate based on current one or find out whether two certificates belong to the same device
Use case: Enrollment

Legend
- Directly acts in this use case
- Provides information before execution
Use case: Certificate Provisioning

- Request Coordination
- Certification Lab
- Enrollment CA
- Pseudonym CA
- Intermediate CA
- Root CA
- Registration Authority
- Device Config. Manager
- Location Obscurer Proxy
- Misbehavior Authority
  - Internal Blacklist Manager
  - Linkage Authority 1
  - Linkage Authority 2
  - Global Detection
  - CRL Generator
  - CRL Store
  - CRL Broadcast

Legend:
- Directly acts in this use case
- Provides information before execution

Device 1, Device 2, Device 3
Current Activities

- SCMS and V2I: which changes are required to support V2I use cases?
- Definition of the protocols within the backend as well as between OBE and backend
- Working towards a pre-deployment implementation