



UNITED STATES
DEPARTMENT OF TRANSPORTATION

COLLABORATIVE V2V SECURITY RESEARCH UPDATE

ITS-JPO Public Workshop
September 24, 2013

Mike Lukuc, NHTSA Research

Overview

This presentation provides an overview of collaborative V2V security research performed over the past year in the following areas:

1. Security Credential Management System (SCMS) Design (7 OEMs)
2. Misbehavior Detection (8 OEMs)
3. Over-the-Air Security Credential Management (8 OEMs)



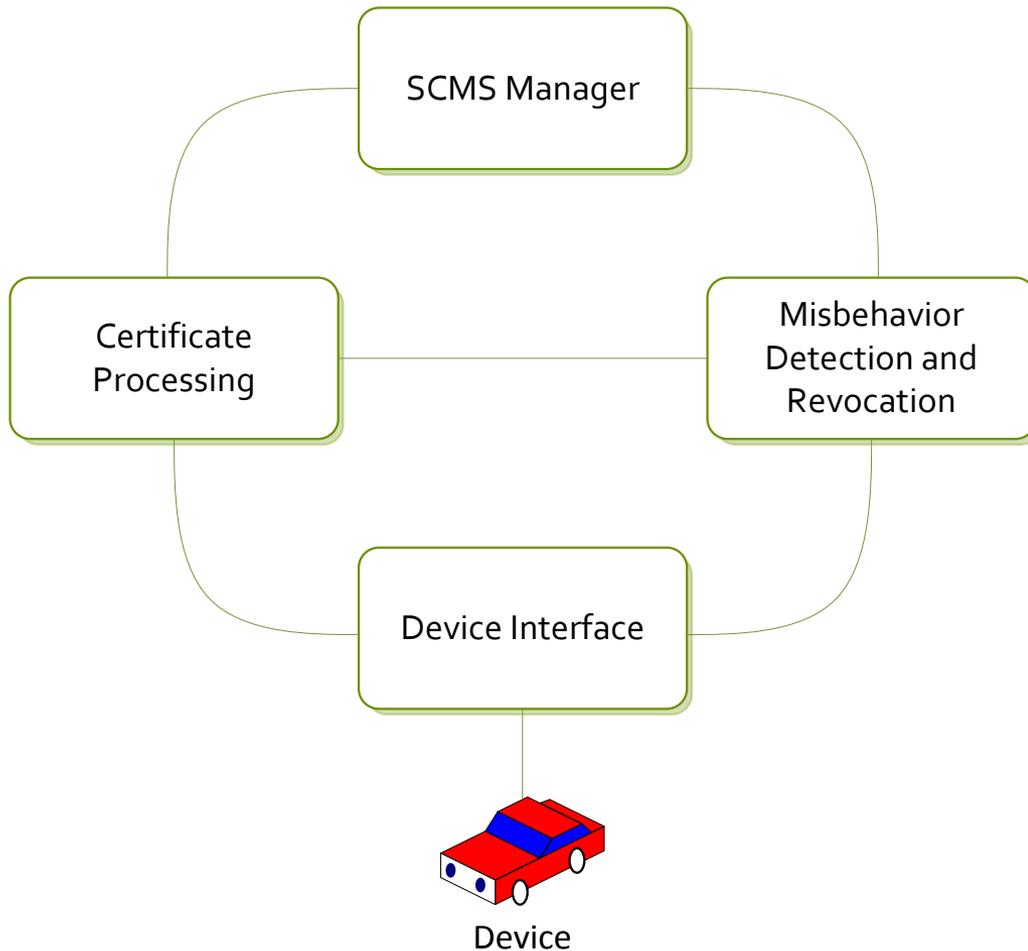
Motivation for V2V Security

- V2V safety applications can alert the driver and help prevent crashes by issuing different safety warnings, e.g.:
 - Forward Collision Warning (FCW)
 - Intersection Movement Assist (IMA)
 - Electronic Emergency Brake Light (EEBL)
- Basic Safety Messages (BSM) broadcast over-the-air (OTA) include information on current position, velocity, heading, etc.
- In cooperative safety systems, the received BSMs must have integrity and authentication
- Current design solution:
 - Digital signature of BSM (ECDSA-256) for integrity and authentication
 - BSM includes digital certificate issued by a Public-Key-Infrastructure (PKI), the SCMS for chain of trust
 - No encryption of BSMs, as they are useful for everyone in the vicinity (including non-safety applications)

High Level Requirements

- Privacy (OEM privacy goals)
 - Prevent SCMS from collecting information that could identify a person or motor vehicle, directly or indirectly (PII)
 - Prevent trip tracking by outsiders: frequent change in pseudonym certificates (short term 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
 - Certificate revocation needs to be integrated to mitigate misbehavior

High Level SCMS Technical Structure



Main Operations:

1. Device Initialization
2. Certificate Provisioning
3. Misbehavior Detection and Revocation

Design Optimization and Cost Analysis of Connected Vehicle Security System

(CAMP V2V-Vehicle Communication Security Studies Project under a Cooperative Agreement with USDOT)

Period of Performance: April 3, 2013 – January 3, 2014

Activities:

- Define reference security model and baseline OBE requirements ✓
- Develop cost model for the SCMS (underway)
- Perform cost analysis on reference security model (underway)
- Analyze potential simplifications to the SCMS (underway)
- Perform connectivity cost analysis, consider epidemic distribution (underway)
- Perform sensitivity analysis (Not Started)
- Provide design recommendations for V2V Security System (underway)
- Identify technical solutions for linking enrollment certificates to batches of devices to aid defect investigations (outside of SCMS) ✓

Primary Deliverables to USDOT:

- Cost model
- V2V Security Design Recommendations Report

Assumptions for Reference Security Model

Starting point for the assessment:

- Full deployment model of SCMS
- Separation: 26 organizations running non-central components
 - Registration Authority
 - Pseudonym Certificate Authority
 - Enrollment Certificate Authority
 - Device Configuration Manager
- 20 certificates / week, 3 years' worth (500 kB)
- Daily CRL distribution, CRL size limited to 400 kB
- Full CRLs (no delta CRL)
- Epidemic Distribution
- First-hand seeders get CRLs through, for example, dealer RSEs or satellite distribution

Cost Model Overview

- Step 1a: Determine number of cert. provisioning / year
- Step 1b: Determine number of certificates / year

#Certs

- Step 2: List out all possible crypto operations
- Step 3: Partition crypto ops: HSMs and GP-CPU's
- Step 4: Use safety-margin factors and Moore's law
- Step 5: Calculate number of HSMs and servers
- Step 6: Calculate total costs for crypto ops

Crypto

- Step 7: Compile database operations
- Step 8: Price database operations

Database

- Step 9: Add operational and other general costs

Operational/
General
costs

Expert Reviews of the SCMS Design

- Ongoing detailed technical reviews from security experts as part of this project, including:
 - Scott Vanstone (CertiCom / TrustPoint / University of Waterloo)
 - Stephen Farrell (Tolerant Networks / IETF Security Area Director)
- No major concerns have been identified
- Minor technical design improvements
- Improvements to presentation of information in the CAMP VSC3 SCMS document

Next steps – CAMP

(CAMP V2V-Vehicle Communication Security Studies Project)

- Complete Cost Model
- Complete cost analysis for reference model
- Start sensitivity analysis

Potential future Activities (2014)

(CAMP V2V-Vehicle Communication Security Studies Project)

- Assess cost estimations using a security supplier's design implementation
- Preliminary assessment of applicability of the SCMS for V2I/I2V
- Proof-of-concept backend implementation, testing with OBEs
- Simulations and testing for CRL dissemination using epidemic distribution

Misbehavior Detection (MBD) Research

(CAMP V2V-Interoperability Project)

- Misbehavior Reporting and Detection
 - Researching both Local and Global MBD
 - Exploring detection schemes (one or more) which could potentially be suitable for initial deployment
 - Considering communication protocol and/or data elements
- Specific activities to include:
 - Analyzing attack models from former projects
 - Identifying potential Global MBD approaches
 - Aligning Local and Global MBD approaches
 - Defining report formats to support potential approaches
 - Performing simulations of promising approaches
- Coordination between various research teams

Model Deployment Over-the-Air Security Credential Management Testing

(CAMP V2V-Model Deployment Project)

- Sixteen integrated light vehicles performed over-the-air security credential management during Phase 2 of the Safety Pilot Model Deployment
- Forty-seven vehicles used short term certificates preloaded on USB drives (same as in Phase 1)
- Further detail will be provided in the Safety Pilot Model Deployment Integrated Light Vehicle Presentation this afternoon

For questions, please contact:

Mike Lukuc

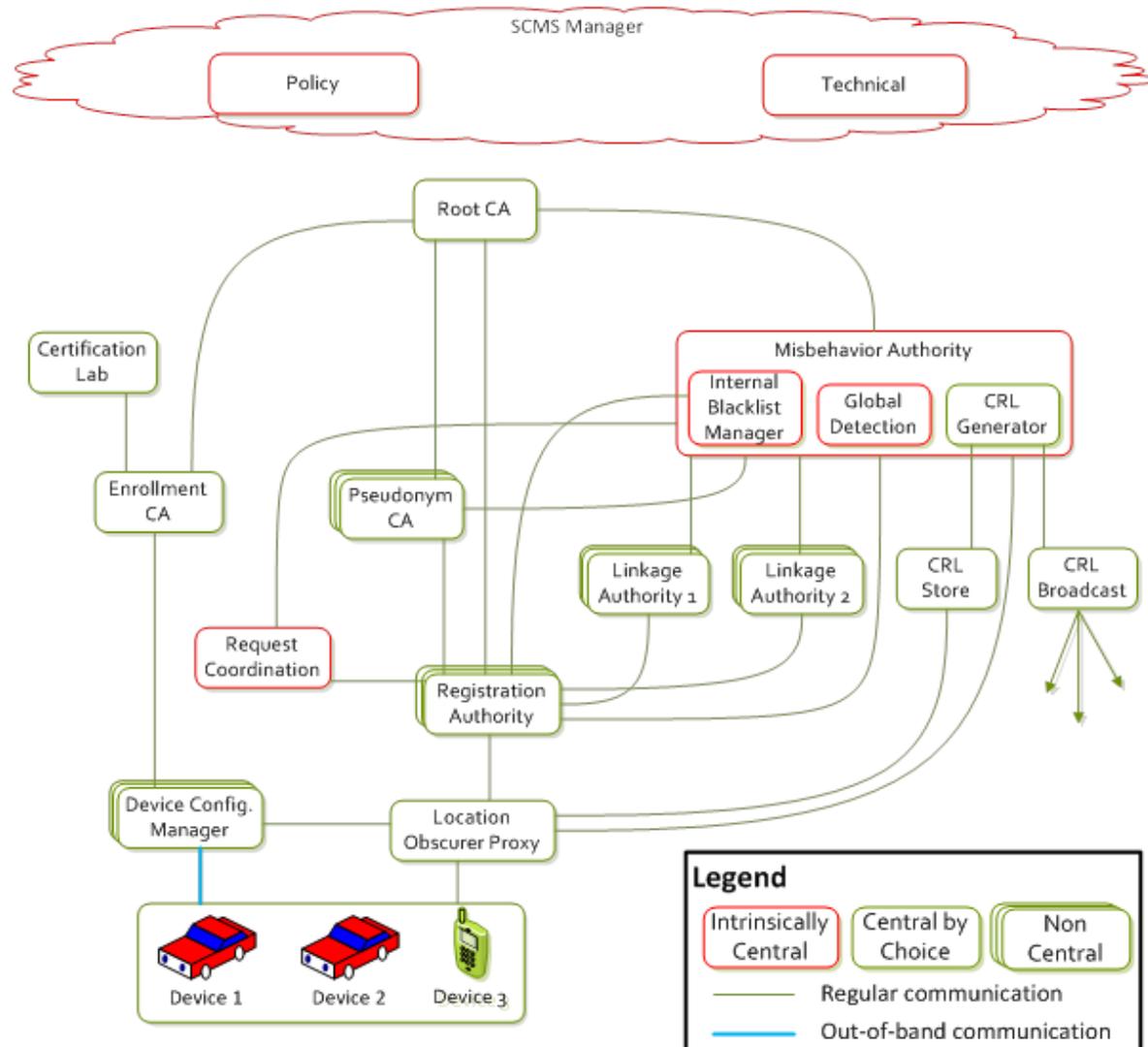
NHTSA Research

mike.lukuc@dot.gov



BACK-UP SLIDES

SCMS – Initial Deployment Model



SCMS - Full Deployment Model

