V2X Security and Privacy
André Weimerskirch

SANS – Automotive Cybersecurity
2017
32,000 deaths on the road in the US in 2012

Day-1 applications will likely be:
- USA: V2V driver notifications safety applications
- Europe: mobility applications, supported by infrastructure (e.g. temporary highway construction site)

V2V wireless communications for 360° warning applications.
- 300+ m range

Basic Safety Message (BSM)
- Contains position, velocity, acceleration …
- Transmitted up to 10 times per second

Allows receiving unit to predict collisions and warn driver

Source:
https://www.transportation.gov/fastlane/v2v-cars-communicating-prevent-crashes-deaths-injuries
https://icsw.nhtsa.gov/safercar/v2v/
Deployment

- NHTSA released a notice of proposed rulemaking (NPRM) December 2016.
- Cadillac announced deployment of V2V on select 2017 models (CTS).
- Communication might use DSRC and/or LTE-V, but security aspects apply for either communication technology.
V2X Security Concerns

- V2X communication security
- User privacy
  - IEEE 1609.2, SAE J2735 and SCMS Design

- Server security
  - SCMS Design and best-practice implementation

- Vehicle cybersecurity
  - Cybersecurity engineering and proprietary in-vehicle cybersecurity
IEEE 1609.2 and SCMS: Communication Security Overview

To enforce security in V2X systems we need to ensure that:

- A message originates from a trustworthy and legitimate device
- A message was not modified between sender and receiver
- Misbehaving units are removed from the system

**V2V Message Authentication:**
Digital signatures to guarantee integrity

**Root of Trust:** Security Credential Management Server (SCMS) as trust anchor

**Privacy Protection:**
Frequently change certificates to prevent linking BSMs to one-another for tracking purposes

**Performance:** Option to verify-on-demand: only verify messages that will result in driver’s warning
Security Considerations

• Impact on privacy
  – Don’t want the system to be used as a tracking system
  – Prevent eavesdroppers or insiders from collecting Personally Identifiable Information (PII)

• Additional attack surface
  – New wireless interface adds another surface to hack into car (similar to Bluetooth, cellular and Wi-Fi).

• No direct safety impact
  – Unlikely, since (1) system will either be used for notifications only, or (2) since system will be supported by redundant sensors (radar, lidar, camera)
Protect Privacy

• No personal information included in broadcast messages

• Prevent tracking: “Identifiers” at application, network and other levels should be transient and change simultaneously

• Vehicles have \( k \) simultaneously valid BSM certificates,
  – Dynamically choose which certificate to use to sign (e.g. rotate every 5 minutes). More research required to determine proper change strategies.
  – Baseline number of certs \( k = 20 \) per week (but car makers can choose to use more certificates per week)
Security Credential Management System (SCMS)

- Privacy against insiders and outsiders
  - Separation of SCMS duties and information
  - No information stored within SCMS that links certificates to a particular device, vehicle or owner
  - Location Obscurer Proxy (LOP) acts as anonymizer proxy
- Minimize effort of device
- Efficient and privacy-preserving revocation
Shift Effort from Device to Server: Butterfly Keys

• Generating a lot of keys for requests is a burden at the OBE side
  – It might not need all of them
  – It needs to store the private keys
  – Increases request size and risk that request doesn’t make it through the network
• Device generates a private/public seed value and expansion function
• Server expands public seed to create many public keys (without knowing the corresponding private keys)
• Server does most of the work, but only device knows the private keys
Revocation

• Two ways of revocation
  – Publish certificate revocation lists (CRL) to devices
  – Deny renewal of certificates
• Vehicles need to be provisioned with a minimum number of certificates in case they are turned off for some time and turned on in an area with no coverage
  – If you have, say, a month’s worth of certs, you can misbehave for a month
• Revocation by CRL must be supported to reduce potential disruption within system
• Revocation by denying renewal of certificates will be implemented on top
  ➢ Need efficient, privacy-preserving revocation
Efficient Revocation: Linkage Values

• Remember: each device holds 20 certificates per week, more than 1,000 certificates per year
• Revoke all $n$ of a device’s certificates with just one entry on the CRL
• Backwards unlinkability
  – If a device is revoked, its privacy for past events is still protected
• After revocation, privacy cannot be protected
V2X Pilot Programs

NHTSA sponsored pilot programs
- Connected vehicle technology will play a major role in the DOT Smart City Challenge: [https://www.transportation.gov-smartcity](https://www.transportation.gov-smartcity)

- There will be an SCMS to serve all pilot programs
- Cybersecurity and privacy has been identified as a major point of interest
Cybersecurity

- Research results suggest that cybersecurity in vehicles becomes a safety issue
  - E.g., successful penetration via Bluetooth and cellular connections
- DSRC would be another wireless interface
- DSRC supports a safety system

Sources:

Several Highly Publicized Automotive Hacks

Hacker Says Attacks On 'Insecure' Progressive Insurance Dongle In 2 Million US Cars Could Spawn Road Carnage

Corey Thuen has been braving the snow and sub-zero temperatures of Idaho nights in recent weeks, though any passerby would have been perplexed by a man, laptop in hand, tinkering with his aptly-named 2013 Toyota Tundra at such an ungodly hour.
Cybersecurity Concern

1. The DSRC unit/function comes with the same security considerations as every wireless interface (e.g. cellular, WiFi, Bluetooth)
   - The same mitigation mechanisms apply

2. It is very likely that DSRC input will be used as an additional sensor to complement camera, radar, lidar, etc.
   - DSRC output would have an impact to the vehicle’s driving behavior
   - DSRC is the only wireless interface that has an impact to the vehicle’s driving behavior.
Network Topology

Separate DSRC unit via gateway/filter from ADAS/Powertrain

1. In Telematics unit
2. In Connected Gateway
3. In separate unit

*Note:* it’s probably not a good idea to place the DSRC unit directly in the ADAS or Powertrain network segment (or anywhere where traffic does not first pass a gateway).
Standard Cybersecurity Solutions

- Secure Platform
  - Secure boot
  - Software separation
  - Hardened OS
  - Interface firewall/filter
  - Secure communication (CAN, IP)
  - Deactivate and/or protect all debug interfaces
  - Encrypted and authenticated storage for all sensitive data (store key in secure boundary)
- Ability to update **firmware over-the-air**, to fix security flaws
- Consider **anomaly detection** and continuously improve security
- Proper **cybersecurity engineering** and implementation process
Lear’s Connected Gateway

Secure Boot

Vehicle VM
- Adaptive AutoSar
- Vehicle Abstractation API
- Network Anomaly Detection
- Diagnostics
- Power Mgmt
- Flasher
- Secure Boot

Security VM
- Linux
- Certificate Management
- Cryptography
- Logging
- Secure Boot

Application VM's
- VM or LXC
- VM or LXC
- VM or LXC
- Linux VM
- V2X/V2I
  - Safety Applications
  - Traffic Efficiency
  - Infotainment
- LDM
  - ETSI DENM, CAM
- US Standard
  - BSM-I, BSM-II, SPAI, MAP, TIM
- Vehicle Abstraction API
- Event Mgr.
- Call Talker
- Web Server
- System Monitor
- GPS-MON
- WiFi AP/Client
- eCall

Hypervisor / Software Container
- Secure Boot

Run’s on separate micro if legacy vehicle protocols needed (e.g. CAN) or for security purposes.
Forged DSRC Output

- DSRC output (from V2X unit to in-vehicle units) can be forged
  - DSRC is the only wireless interface that has a potential impact to vehicles’ behavior

1. Forged over-the-air DSRC messages
   - Mitigated by local and global V2X misbehavior detection. This will never detect all forged messages immediately though.

2. Compromised V2X unit
   - Proper cybersecurity mechanisms avoid that V2X unit has the power to directly impact vehicle’s behavior (firewall/filter, etc.)
   - But compromised V2X unit can provide forged information (e.g. about broken-down vehicle in driving lane) to vehicle ADAS/powertrain

- For either case, a resilient safety application is required that can handle false DSRC output
  - This is not only required for cybersecurity but also for reliability and safety
Safety and Plausibility Checks

- Plausibility safety checks are necessary and support cybersecurity
  - For instance, if camera and DSRC provide conflicting data, the safety algorithm needs to be able to handle the situation.
  - Cybersecurity needs to be included in the consideration. Security confidence levels for sensor input (camera > radar, lidar > DSRC) can be used.

- There are interesting questions in the safety & security domain
  - For instance, what is if DSRC input implies an immanent crash but camera or radar cannot verify the information because there is no line-of-sight?
Conclusions

- V2X security compromises (1) communication security & privacy as well as (2) in-vehicle cybersecurity.

- V2X in-vehicle cybersecurity has the potential to quickly advance vehicle cybersecurity.

- The in-vehicle cybersecurity can be approached with (1) traditional mechanisms and (2) additional security mechanisms.

- DSRC is a great example where safety and security engineers must collaborate intensely.
Dr. André Weimerskirch
VP Cyber Security
Lear Corporation

Southfield, Michigan, USA
Email: aweimerskirch@lear.com