The relevance of cyber-security to functional safety of connected and automated vehicles

André Weimerskirch

University of Michigan
Transportation Research Institute (UMTRI)
February 12, 2014
Introduction

- Automotive cyber security and privacy is increasingly mentioned in the media
- Several research teams now demonstrated that they are able to hack a car and also how to hack it
- Question: when is the first car in the field hacked?
If transportation cyber security follows path of Internet, we will see real-world automotive cyber attacks within 5 years.
Attacks on Safety

- Luckily never happened so far
- [Checkoway et al.] and [Miller and Valasek] demonstrated that it is possible to disable brakes, turn-off head-lights, and take-over steering (for cars equipped with a parking assistant)
- [Checkoway et al.] also demonstrated, that it is possible to remotely hack into car via telematics connection.
  - It is possible to hack into a car from a remote location.
  - A mobile device attached to a vehicle infotainment system, or even a CD played in an infotainment system, can inject malicious code.
Advanced Driver Assistance Systems

- ADAS provide features such as adaptive cruise control (ACC), pre-crash systems, and automatic parking.
- These systems allow electronics to take control of the vehicle (e.g. steering for automatic parking, steer-by-wire, electronic acceleration and breaking for ACC)
- If these systems can be remotely controlled or if the behavior can be modified, there are obviously threats.
Infrastructure

- Traffic signals can be manipulated via traffic center
  - Imagine a hacker closing all bridges and tunnels to Manhattan
- Central infotainment server could be hacked and modified to push out malware to all vehicles
How is automotive data security similar to regular PCs?

- Modern cars include 100 million lines of code
  - Industry average is about one security flaw per 1,000 lines of code
- Cars use a variety of wired and wireless interfaces and most communication mechanisms are standardized
  - Cars can be considered a data center
Why is data security in vehicles special?

- Safety critical: a hacked PC will not physically harm the user
- The attacker might have physical access to the car, be it just for a minute
- The traditional model of finding vulnerabilities does not work in cars: honeypots to attract attackers and analyze attacks are impossible to implement
- Cost restrictions of additional electronics in cars are far more strict
Security Solutions

In-vehicle

- Secure applications and secure access
- Application Layer: integrity of applications
- Operating System: secure operating environment
- Hardware Layer: support for higher layers
- Architecture

Secure platform development

- Secure diagnostics
- Secure software update
- secure boot
- Hardened OS
- Secure OS
- Micro-kernel
- Virtualization
- Secure boot
- Theft protection
- Secure data and key storage (e.g., for odometer)
- Secure in-vehicle communication
- Dedicated central gateway
- Firewall and intrusion detection system

Legend:
Common
Starting
R&D

Back-end
Security Efforts

- European Union funded research
  - EVITA, PRESERVE, OVERSEE
- European car makers are active and publish ideas
  - SHE and HSM automotive security controllers
  - Academic workshops
  - Join EU funded research
- SAE cyber security committee with input from US car makers and DOT
- Security standards for connected vehicle communication
  - IEEE and ETSI
Near-Term Future: Connected Vehicles

- US DOT announced “its decision to begin taking the next steps toward implementing V2V technology in all new cars and trucks.”
- Day-1 applications will be a driver safety notification based on V2V.
- Risk analysis showed that successful attacks do not pose a safety threat in early deployment stages.
  - However, too many false warnings will motivate people to turn off the system.
Security Design Idea

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

Digital signatures to guarantee integrity

Central authority (Public Key Infrastructure) as trust anchor

Change credentials on regular basis to prevent tracking
Privacy

- No outside attacker is able to easily track nodes
- No inside attacker with access to a single component is able to track nodes
Future: Automated Vehicles

- Combines many ADAS/control application features (e.g. radar and camera based driver assistance systems) and connected vehicles (wireless communication)
- Combines the risks that are coming with ADAS and connected vehicle technology:
  - Input from sensors can be manipulated (e.g. to make car believe of a threat)
  - Control systems can be directly manipulated (e.g. to remotely control brakes and steering)
  - Wireless interfaces might be mandated in each car, and implementations often introduce vulnerabilities
Automated vehicles come in stages
- DOT defines 5 levels from „Non-Automated“ to „Full Self Driving Automation“

A comprehensive security requirements analysis for each level is required

Then proper electronics architecture, best practice, and “functional safety for security“ standards can be developed for each level
- Includes “Level 0 - non-automated“ vehicles
- Includes in-vehicle electronics and communication, inter-vehicle communication, infrastructure security, and vehicle-infrastructure communication.
Dr. André Weimerskirch

2901 Baxter Road, Ann Arbor, MI 48109
Email: andrewmk@umich.edu
Office: 734-936-1046
Mobile: 734-474-5255
Appendix I: De-Facto Security Standards

- **Hersteller Initiative Software (HIS): Security Module / Secure Flashloader**
  - German car makers
  - Used by many OEMs
- **HIS: Feature Activation**
  - Defined by BMW
- **HIS: Secure Hardware Extension (SHE)**
  - Available as HIS specification 1.1 (needs to be requested from HIS)
  - Microcontrollers available
- **Bosch: automotive Hardware Security Module (HSM)**
  - Microcontrollers are supposed to be available 2014/2015
- **European Union funded projects**
  - EVITA: secure hardware
  - OVERSEE: secure in-vehicle application and communications platform
  - PRESERVE: vehicle-to-vehicle communication ASIC
- **ETSI and IEEE: vehicle-to-vehicle safety application security**
  - Driven by Car-to-Car Communication Consortium (C2C-CC) and CAMP
  - Active in ITS/V2V communication security specification
Appendix II: Automotive Security History

- Since 1980s: introduction of remote key unlock and electronic immobilizers
  - Since then cat-and-mouse game between OEMs and organized groups
- Since 1990s: odometer manipulation to increase used car sales price
  - Became much easier with the introduction of electronic odometers
- Since 1990s: chip-tuning to increase engine power
- 2010: Security and privacy attack on tire pressure monitoring system (TPMS) to identify vehicles and generate false in-vehicle warnings [Rouf et al.]
- 2010: demonstration how to manipulate behavior of vehicle via diagnosis interface [Koscher et al.]
- 2011: demonstration how to hack into a car via telematics, wireless interfaces, USB, and CD [Checkoway et al.]
- 2013: publication of all details to manipulate behavior of vehicle via diagnosis interface [Miller and Valasek]