An Overview of Automotive Cybersecurity

Conference Paper · October 2015

DOI: 10.1145/2808414.2808423

CITATIONS
15

READS
2,969

1 author:

Andre Weimerskirch
University of Michigan
17 PUBLICATIONS **470** CITATIONS

SEE PROFILE

An Overview of Automotive Cybersecurity: Challenges and Solution Approaches

André Weimerskirch

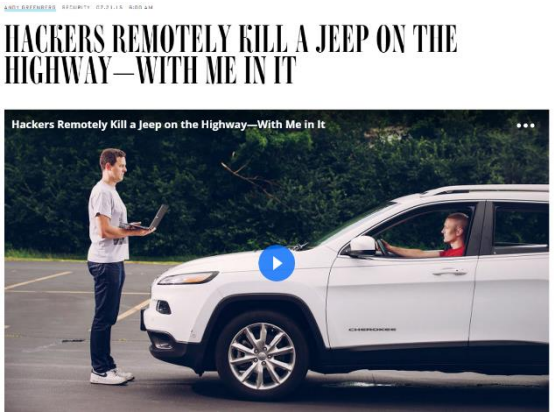
University of Michigan

TrustED 2015 – Trustworthy Embedded Devices
October 16, 2015

MOTIVATION

Introduction

- **Denial-phase should be over: Several teams demonstrated that it is possible to hack critical traffic systems**



SECURITY 1/15/2015 @ 10:51AM | 41,750 views

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

+ Comment Now + Follow Comments

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.

CAR HACKED ON 60 MINUTES

No real security on the Internet -- even the military is under daily assault - says the man the Defense Department hired to make the web more secure

2015	COMMENTS	FACEBOOK	TWITTER	STUMBLE	MORE
FEB 06	6	1.5K	786		

UMTRI

Traffic Light Controller Security

- Several teams were able to hack into traffic light controller systems, highway signs, and traffic surveillance cameras [e.g. Halderman et al.]
- No (direct) safety-critical vulnerabilities, so far
  - It is not possible to turn all lights to green
  - It might be possible to annoy people to such a degree that they start ignoring traffic laws
- Vulnerabilities due to unprotected networks, missing security standards, lack of awareness, unclear responsibilities
- Potential risk unclear

Green Lights Forever

Michigan computer science researchers have demonstrated security flaws that exist in traffic control systems now in use throughout the country, leaving them vulnerable to manipulation or attack.

UMTRI

Aftermarket Devices

- Every car sold in the US since 1996 has to have an on-board diagnostics port (OBD2)
- Recent reports indicate that OBD2 dongles can be hacked
  - Not really a surprise
- Once an attacker has access to the OBD2 port, the attacker can inject messages that modify the behavior of the vehicle
  - E.g. deactivate brakes, depending on car model

UMTRI

Automotive

- Luckily never happend in the field so far
- [Checkoway et al.] and [Miller and Valasek] demonstrated that by injecting packets to the OBD2 port, it is possible to disable brakes, turn-off head-lights, and take-over steering (for cars equipped with a parking assistant)
- [Checkoway et al.] demonstrated that it is possible to remotely hack into car via remote telematics connection.
- [Miller and Valasek] demonstrated that it is possible to hack into a car via Internet.
  - Once they hack into the telematics or infotainment unit, the attacks are similar to the previous ones via OBD2
- A mobile device attached to a vehicle infotainment system can inject malicious code.
- Even an MP3 song downloaded from Internet, burned on a CD and insert to the infotainment unit can inject malicious code and change the vehicle behavior.

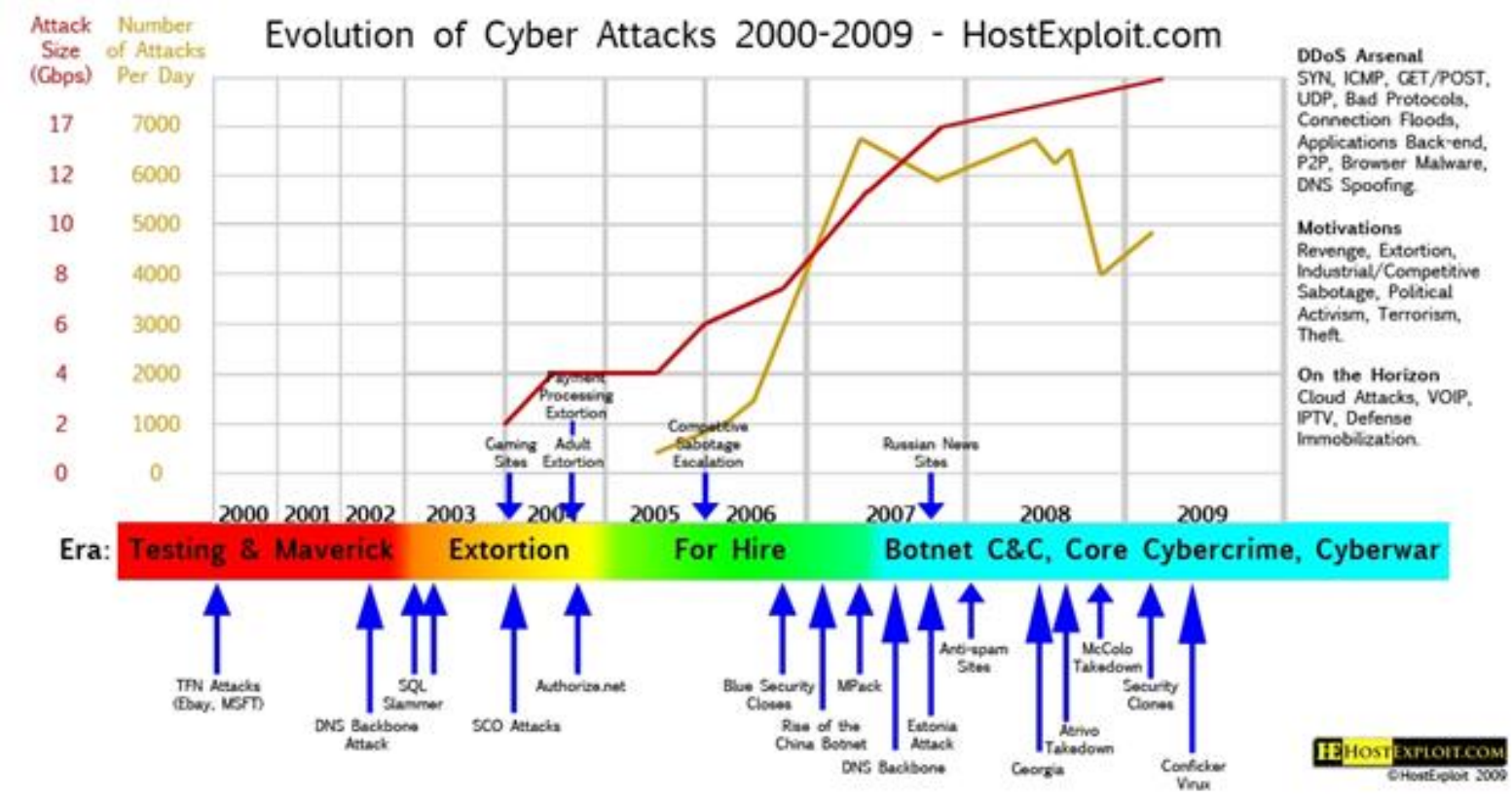
Source: Center for Automotive Embedded Systems Security

Miller attempts to rescue the Jeep after its brakes were remotely disabled, sending it into a ditch. ANDY GREENBERG/WIRED

UMTRI

CYBERSECURITY RISKS

History of Internet Cyber Attacks



- If transportation cyber security follows path of Internet, we might see real-world automotive cyber attacks

UMTRI

Should we be concerned?

- There isn‘t much incentive to hack into a car in order to harm the passengers
- *No need to be concerned?*
- The motivation of hackers might eventually root from financial motivation. Once a hacker figures out how to hack into a vehicle for financial reasons, it‘s a small step (or even accident) to abuse it in other ways.

Financial Damage

Vehicles are already hacked today every day:

- Counterfeit black market is a gigantic problem
  - Up to $45 billion damage
- Odometer rollback
  - 6 billion Euro damage per year in Germany
- Chip tuning
  - Damage due to warranty fraud

Source: http://www.ebay.com

Source: http://www.ebay.com

UMTRI

Theft

- Increasingly based on “magic boxes“
  - Disclaimer: Probably many hoaxes around!

Infrastructure

- Central infotainment server could be hacked and modified to push out malware to all vehicles
- Attacker searches entire Internet IPv4 address space for vulnerable vehicles, and then attacks those
  - Using ZMap [zmap.io] , searching the entire IPv4 address space takes less than 5 minutes

UMTRI

Today and Near Future: Advanced Driver Assistance Systems

- ADAS provide features such as adaptive cruise control (ACC), pre-crash systems, and automated parking.
- These systems allow electronics to take control of the vehicle (e.g. steering for automatic parking or lane assistance, and accelerating and breaking for ACC)

The new BMW is the world's first self-parking car

Source: http://www.mirror.co.uk/news/technology-science/technology/new-bmw-7-series-self-parks-5555297

- If these systems can be remotely controlled or if the behavior can be modified, there are obvious threats.

Near Future: Connected Vehicles

- Vehicle-to-vehicle (V2V) communication via wireless interface
- Day-1 applications will be a driver safety notification
- V2X could be used as additional sensor for ADAS
- Every vehicle will come with a standardized wireless interface with a range of at least 300m
- If the V2V wireless interface can be compromised, malware can potentially spread rapidly

Future: Automated Vehicles

- Combines many ADAS/control application features (e.g. radar and camera based driver assistance systems) and connected vehicles technologies (wireless communication)
- Combines the risks that are coming with ADAS and connected vehicle technology:
  - Input from sensors could be manipulated (e.g. to make car believe of a threat)
  - Control systems could be directly manipulated (e.g. to remotely control brakes and steering)
  - Driver might not be able to take control if necessary

Researcher Hacks Self-driving Car Sensors

By Mark Harris
Posted 4 Sep 2015 | 19:00 GMT

Share | Email | Print | Reprint

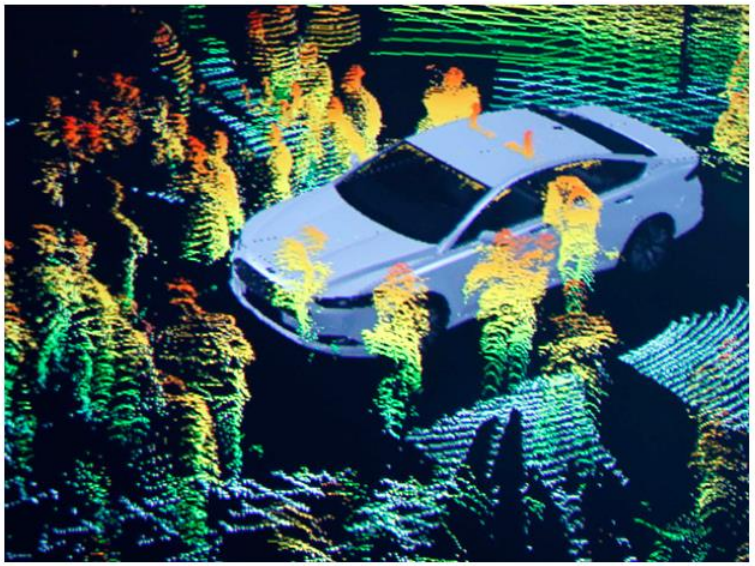


Photo: Jeff Kowalsky/Corbis

UMTRI

Who would ever attack vehicles?

- Already today for financial gain:
  - Odometer manipulation
  - Chip-tuning
- To collect privacy sensitive data
- Attacks on functional safety will probably follow Internet history
  - Curiosity and “fame“
  - Targeted paid attacks
  - Organized actions

  } Driven by illegal business models
- Note: The majority of safety-critical attacks probably do not even target safety but are “accidents“ of flawed attacks with a financial background.

What's special about cars?

- More than 50 million lines of code
- 50+ electronic control units (ECUs)
- Several miles of wire
- Wireless and wired interfaces
- Safety critical systems
- Lifetime of a vehicle at least 10 years, life-cycle much slower than IT and entertainment.

- But also increasingly similar to other embedded systems and PCs: embedded Linux, Windows, Bluetooth, software updates, etc.

- Common vulnerabilities will increasingly apply to vehicles
- Common countermeasures can be applied as well

SOLUTION APPROACHES

Security Solutions: Defense in Depth

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*

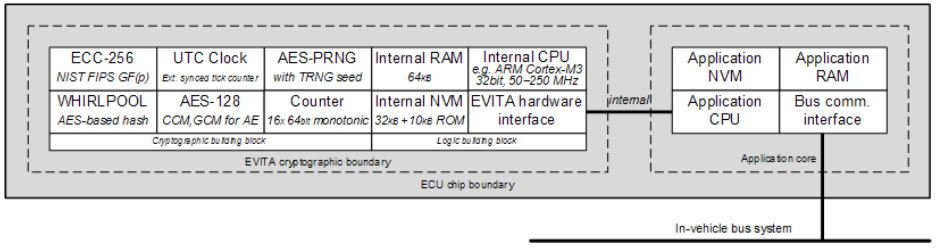
Back-end

Legend:
Common
Coming
R&D

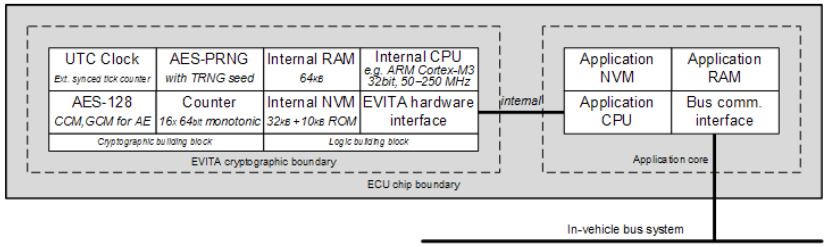
Hot Topics: Secure Hardware

- Basis for many security applications
- EVITA Full: V2X (one per car)
- HSM - EVITA Medium: for advanced ECUs (gateway, head-unit, engine control)
  - Available 2014/2015
- SHE - EVITA Light: for sensors, actuators, …
  - Already available

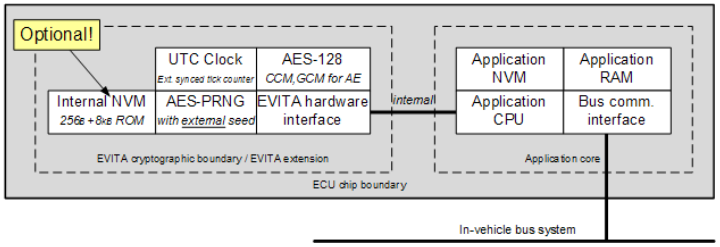
*(a) **Full** version for V2X and large ECU level*



*(b) **Medium** version for standard ECU level*



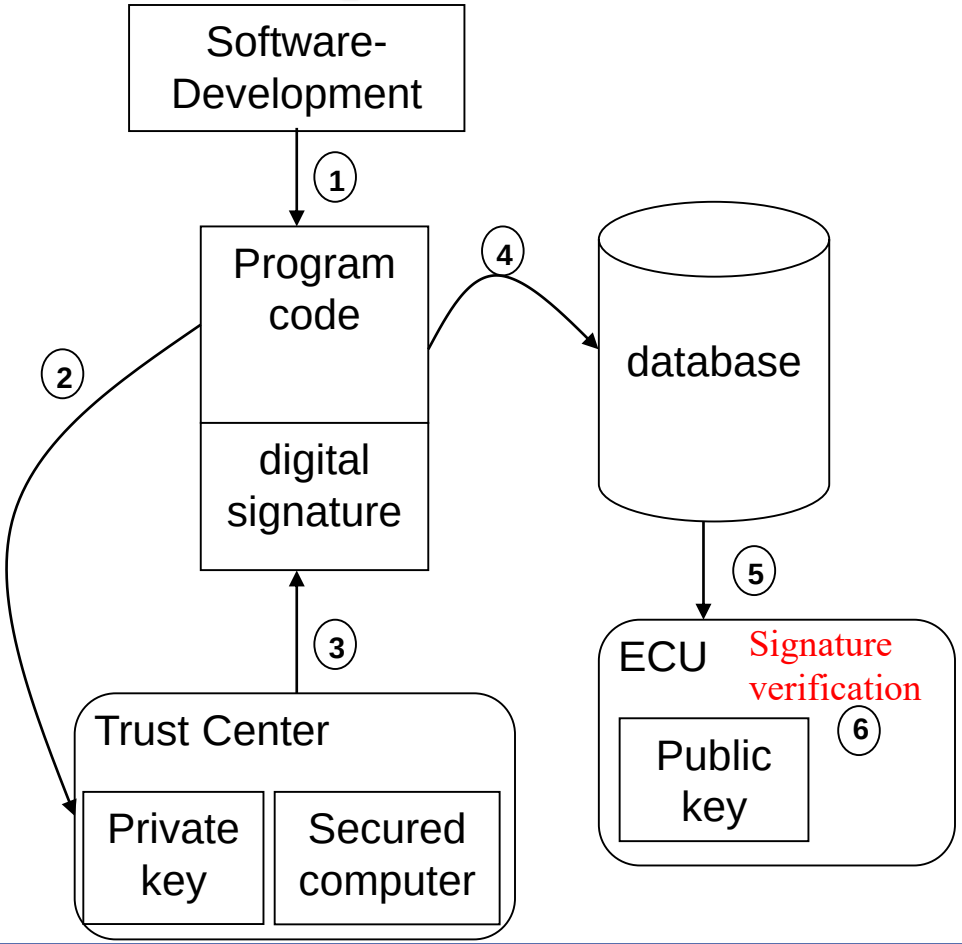
*(c) **Light** version for sensor/actuator ECU level*



UMTRI

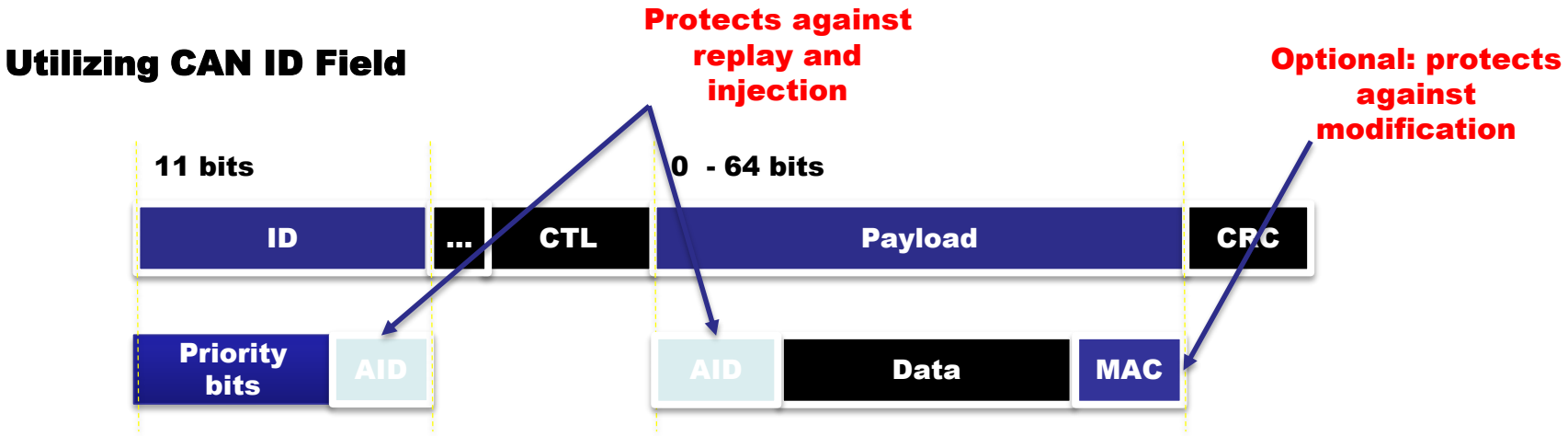
Hot Topics: Secure Software Update

- There is a need to load/update software over-the-air in a secure manner
  - Fix safety issues
  - Introduce new features
- (More or less) understood for infotainment and already offered
- Details not well understood for non-infotainment ECUs
  - E.g., how to update 50 components?



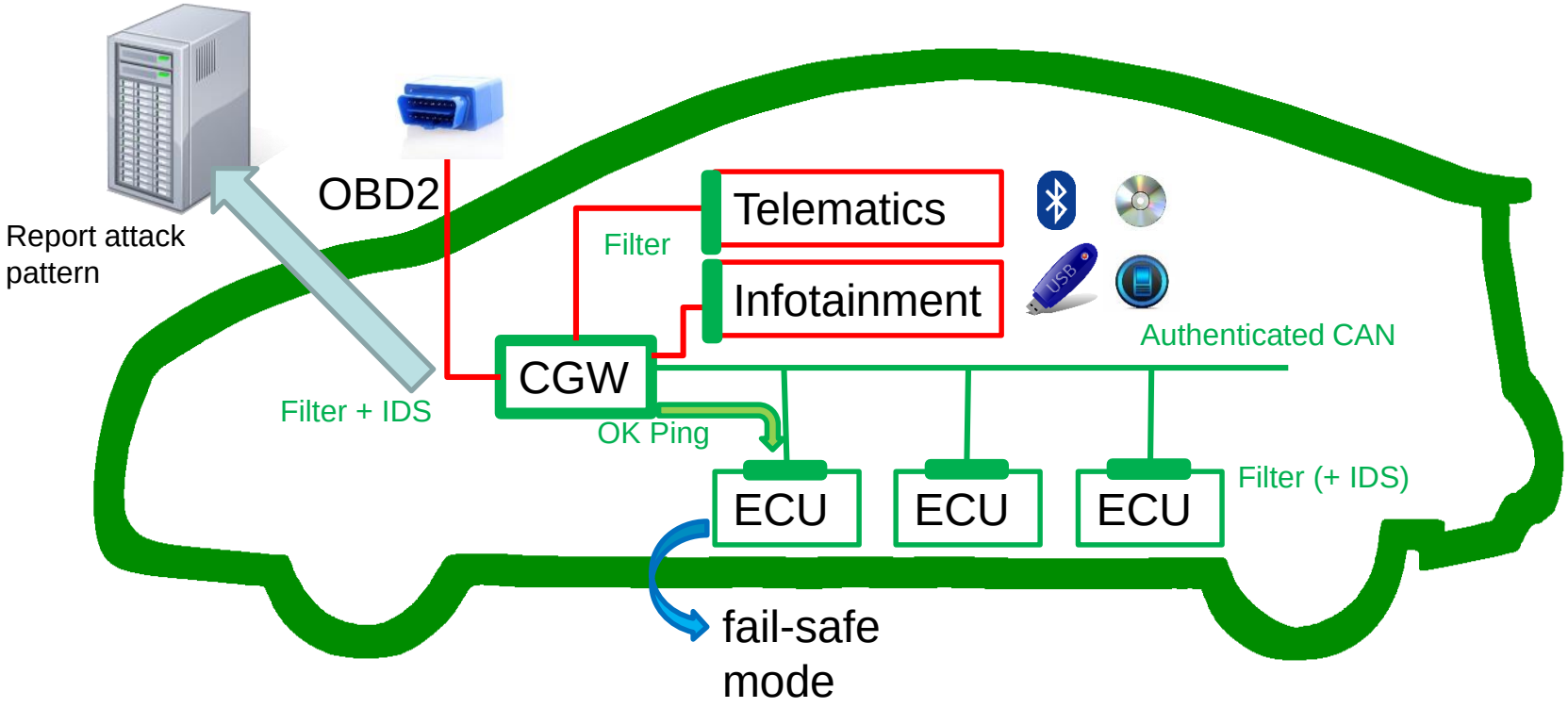
Hot Topics: Authenticated CAN

- Prevent packet injection and manipulation, e.g.
  - Protect against forged sensor data
  - Component theft protection / immobilizer
  - Authenticated ECU-to-ECU communication
- Identifier Anonymized CAN
  - Use sender authentication (instead of message authentication) to save bytes in payload



UMTRI

Hot Topics: Separated Architecture, Firewall and IDS



- Especially useful with a central gateway architecture that separates safety-critical network segments from external interfaces
- Protects safety-critical systems if infotainment system has been compromised
- Protects vehicle electronics from attacks via OBD2, or from a compromised OBD2 (e.g. insurance) dongle

Firewall and IDS

- Detect and log attack attempts
- Possibly react after successful intrusion attack to stop attack early (e.g. separate any communication between safety-critical network segments)
- UMTRI is working on test platform and framework

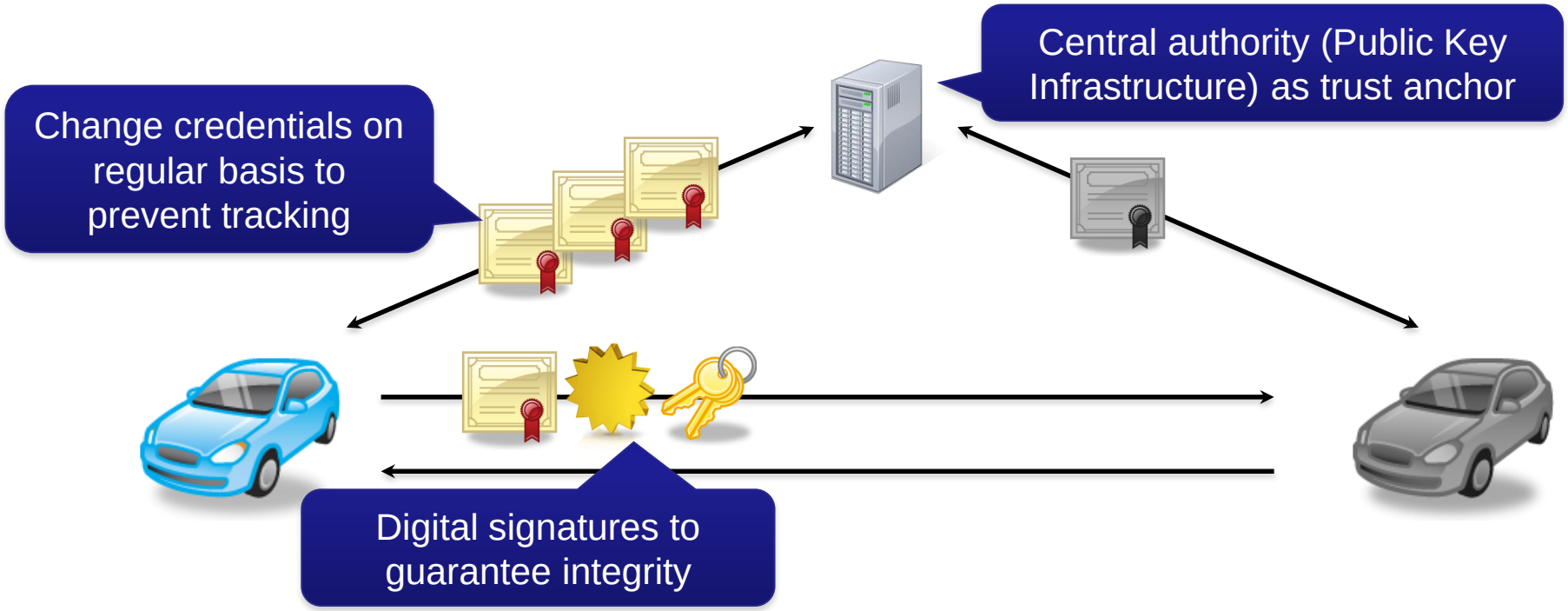
Hot Topics: Connected Vehicle Security

- 32,000 deaths on the road in the US in 2012
- Significant reduction may be possible from V2V wireless communications for 360º warning applications.
  - 300 m range, 802.11-derived medium access
  - Basic Safety Message (BSM): Location, velocity, steering angle…
  - Allows receiving unit to predict collisions
  - Warn driver, driver action can prevent or reduce impact of collision
- USDOT (NHTSA) announced Feb. 3rd, 2014, to move on with the process of mandating this system for inclusion in new light vehicles

Connected Vehicles

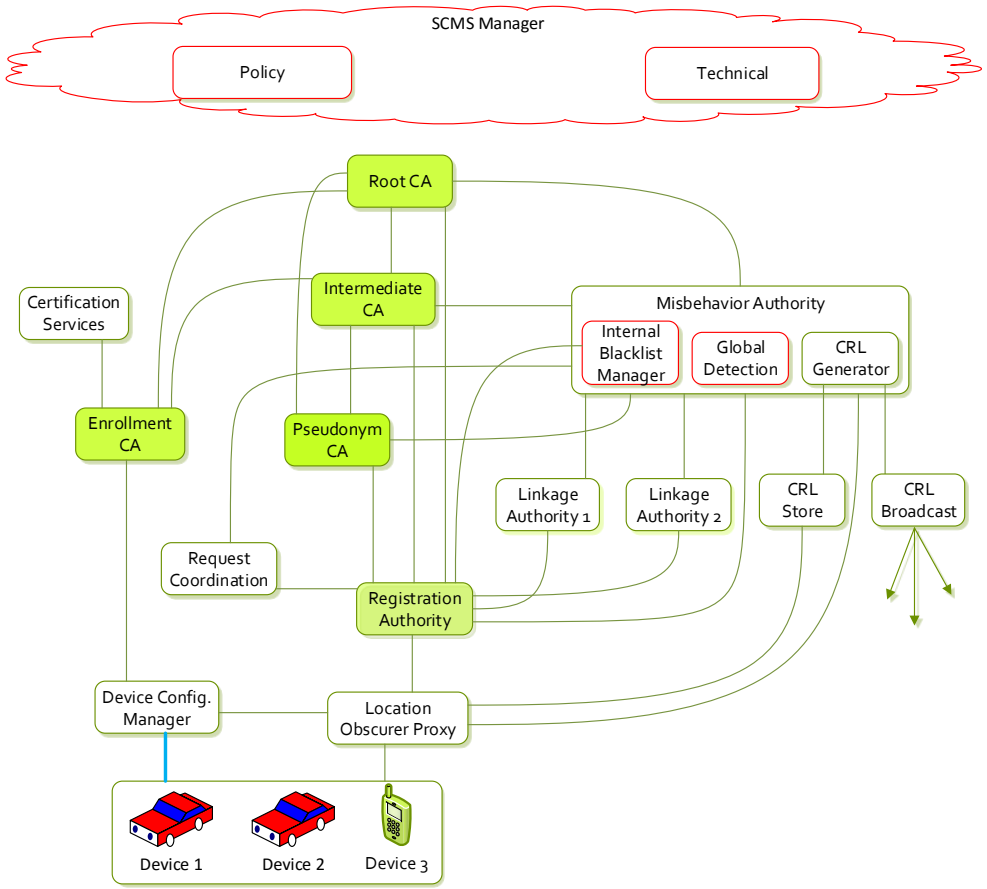
To enforce security in V2X systems we need to ensure that

- **a message originates from a trustworthy and legitimate device**
- **a message was not modified between sender and receiver**



UMTRI

SCMS Overview



- Privacy against insiders and outsiders
  - Separation of SCMS duties and information: a single SCMS component cannot link any two certificates to same device (no tracking)
  - No information stored within SCMS that links certificates to a particular device, vehicle or owner
  - Registration Authority (RA) shuffles all requests from device
  - Location Obscurer Proxy (LOP) acts as anonymizer proxy
- Butterfly keys to minimize effort of device
- Efficient privacy-preserving revocation

UMTRI

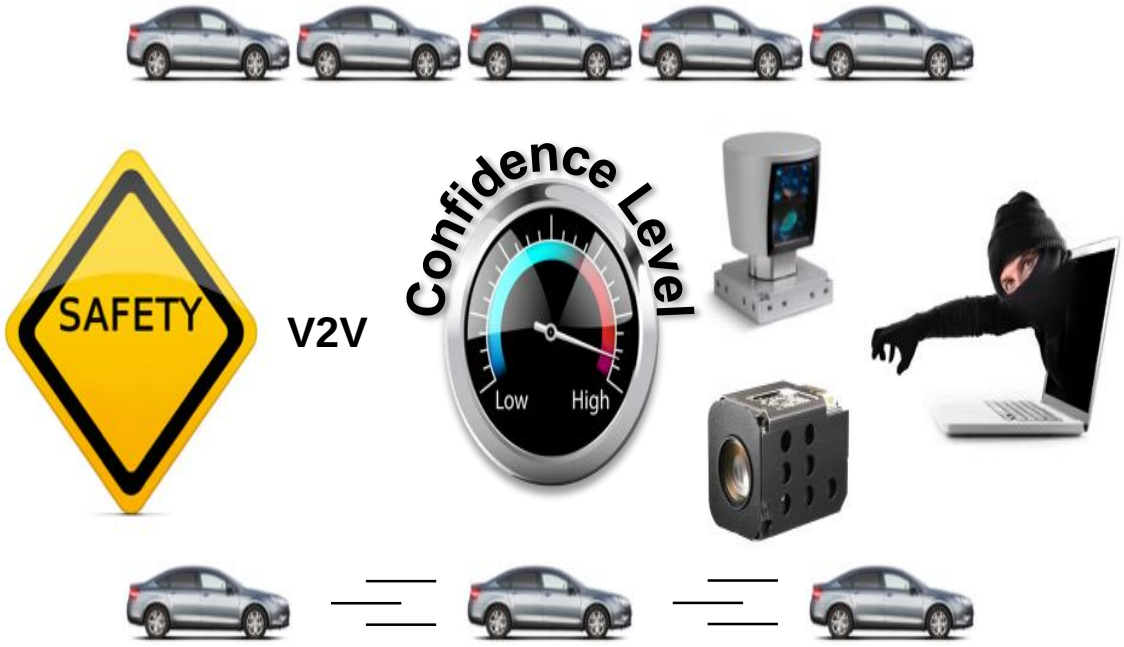
Safety Pilot Model Deployment

- Conducted by UMTRI
- More than 2,800 vehicles equipped with DSRC wireless communication devices in a concentrated geographic area (Ann Arbor)
- Equipped roadside units.
- Full-blown cybersecurity tested.

UMTRI

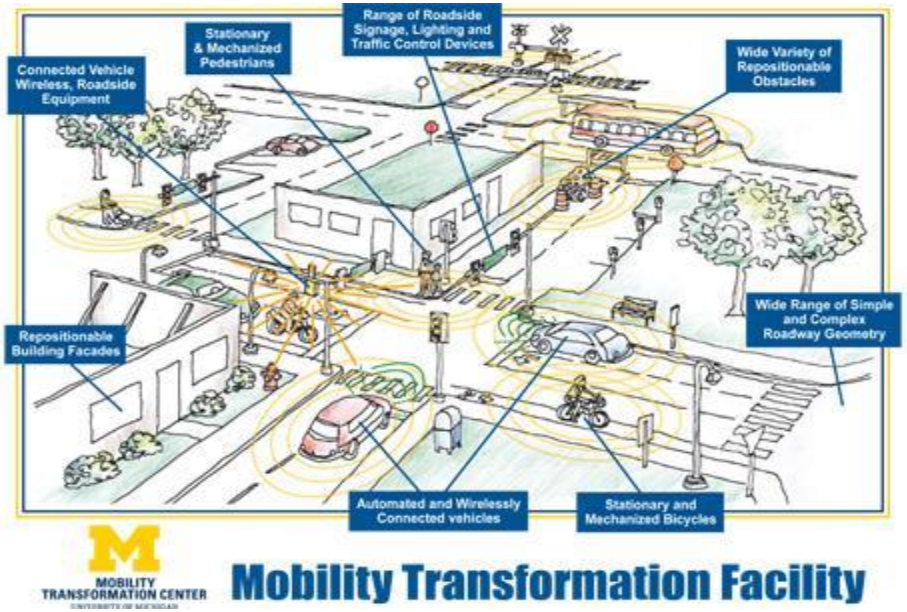
Hot Topics: Automated Cars

- Safe platoon
  - Redundant sensors
- Secure platoon
  - Redundant sensors and confidence levels
- On-going work whether cybersecurity is limiting factor



UMTRI

Mobility Transformation Center and M City



MTC

- 20,000 *secure* connected vehicles in South East Michigan
- 2,000 *secure* automated vehicles in Ann Arbor by 2021

- Public-private partnership of car makers, suppliers, chip makers, insurance companies, MDOT, etc.
- Cybersecurity identified as cross-layer topic

UMTRI

Conclusions

- Automotive cybersecurity is real
  - Attackers will likely not target safety but seek financial profit.
  - Attackers might accidentally impact safety.
  - If automotive cybersecurity follows the Internet history, we will see attack waves in the future.
- Automotive cybersecurity is unique
- There is no one size fits all cybersecurity solution, but a good security design follows a defense-in-depth strategy
- Future technologies will require new cybersecurity solutions

Contact

Dr. André Weimerskirch

2901 Baxter Road, Ann Arbor, MI 48109
Email: andrewmk@umich.edu
Office: 734-936-1046
Mobile: 734-474-5255

UMTRI