Automotive Cybersecurity Map – Today and Tomorrow

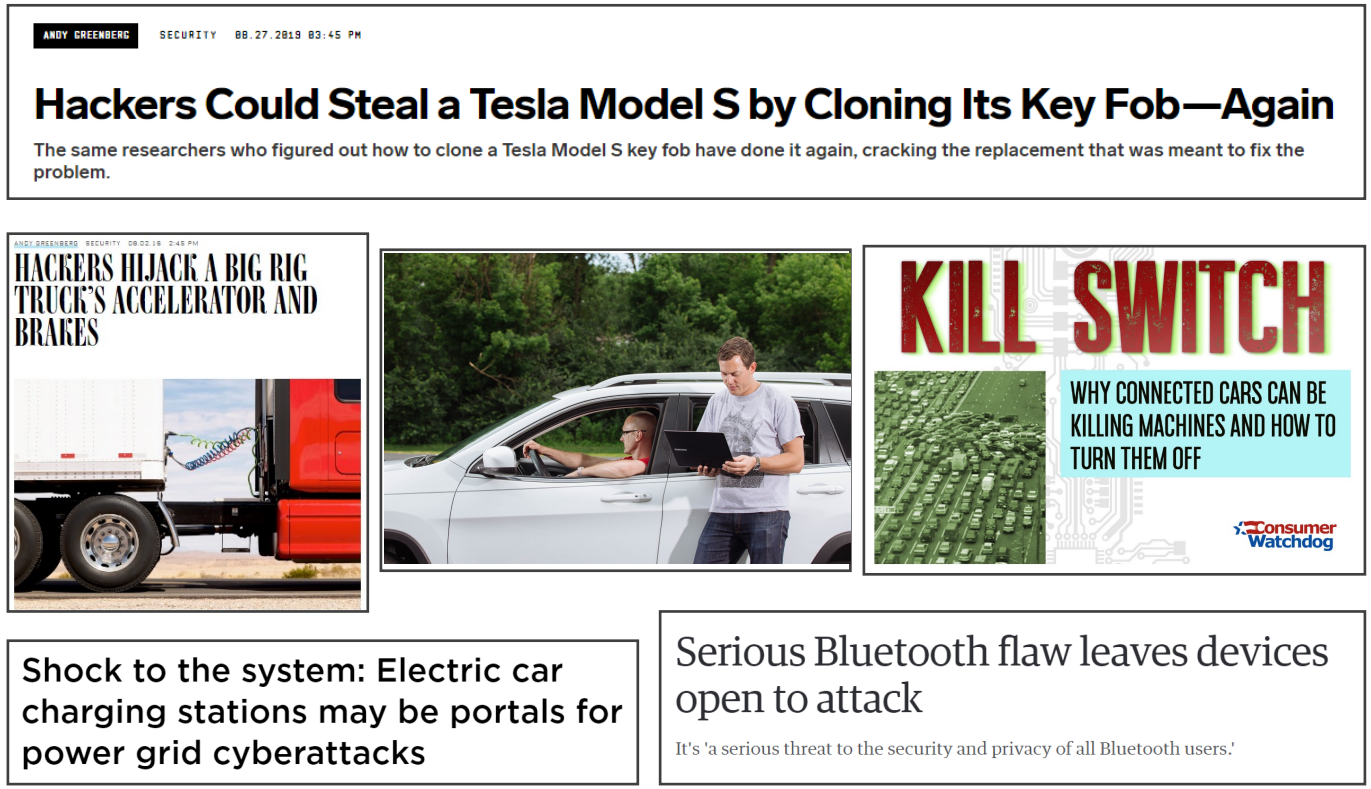
André Weimerskirch

September 14, 2023

Making every drive better™

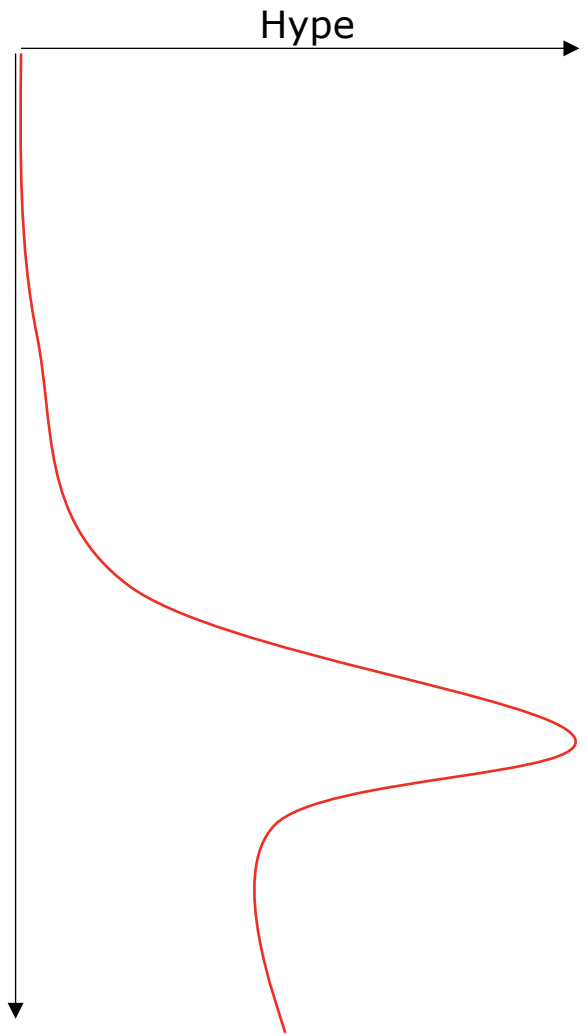
Introduction

- Automotive cybersecurity has been around for 20 years and peaked around 2016.
- Today, there are many initiatives.
- This talk will provide an overview of initiatives, identify gaps, look into the future, and provide some advice.



Automotive Cybersecurity History

- 1980s: Introduction of remote key unlock and electronic immobilizers
  - Since then cat-and-mouse game between car makers and organized groups
- 1990s: Odometer manipulation to increase used car sales price
  - Became much easier with the introduction of electronic odometers
- 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
- 2010: UC San Diego & U Washington demonstrated variety of hacks that required physical access to the vehicle
- 2011: UC San Diego & U Washington demonstrated capability to hack into a vehicle remotely
- 2013: Miller & Valasek demonstrated variety of hacks via physical access to the vehicle
- 2014: Demonstration of hacked aftermarket OBD2 dongles that could potentially affect the vehicle's behavior
- 2015: Miller & Valasek demonstrated capability to hack into a Jeep Cherokee remotely
- 2016: NHTSA Cybersecurity Best Practice (updated 2022)
- 2016: Auto-ISAC Best Practices
- 2022: ISO/SAE 21434 published



Priorities

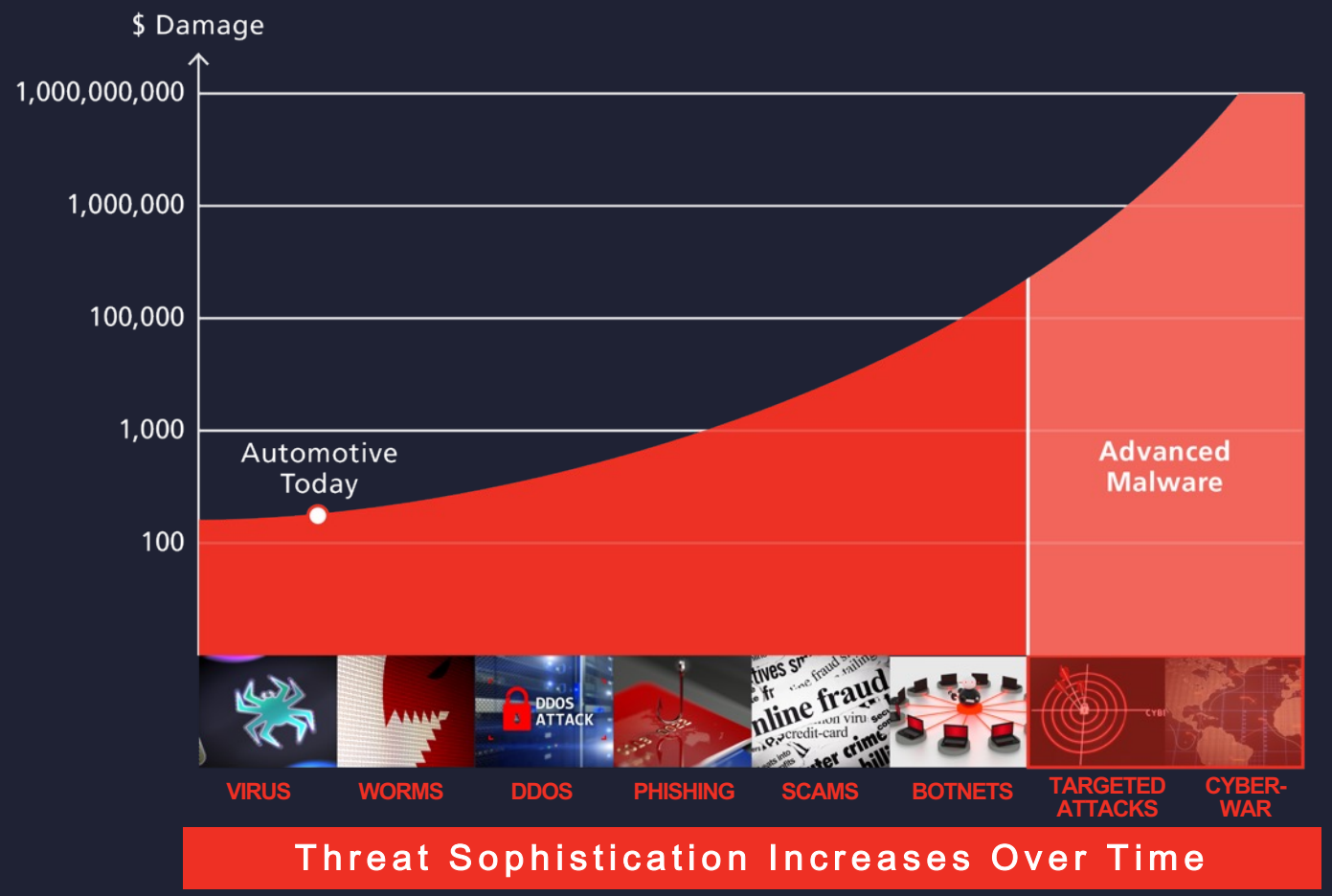
- Originally, automotive security was driven by damages
  - Car theft
  - Mileage manipulation
  - Chip tuning (warranty damages)
  - Protecting business models (copy protection)
- In the 2010‘s, automotive security was pressured by potential mandates, reputation concerns, and liability concerns.
- In the last few years, the hype decreased and expertise heavily increased. This industry is very good around process adherence and the community put together a cybersecurity engineering process requirements standard (SAE/ISO 21434).
- Security has become a planned, controlled and managed discipline. The focus has shifted to:
  1. Secure products, security process adherence, and security compliance
  2. Efficiency: Smart tools, automation

Threat Landscape

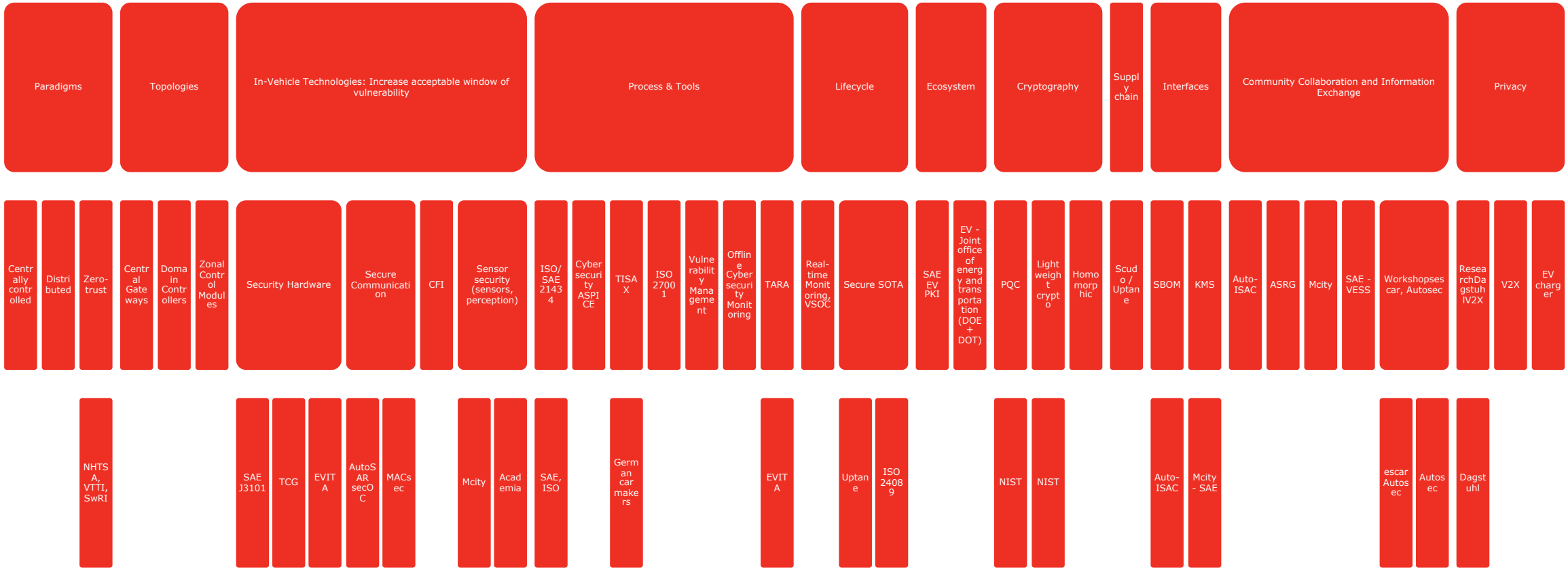
- Awkward situation where we have a hard time to justify cost due to lack of attacks but cost of a single successful serious attack could be quite costly to entire community.
- We need to make a reasonable guess where automotive cybersecurity goes
  - Financially driven
  - Attacks on vehicles might be starting point to attack 3rd party systems
- So far, no relevant attacks on vehicles except for car theft and manipulating infotainment
  - Latter is concerning since infotainment systems increasingly display safety-relevant information such as speed

➢ Stefan Savage, escar USA 2021

➢ Need more research in this area!



Map

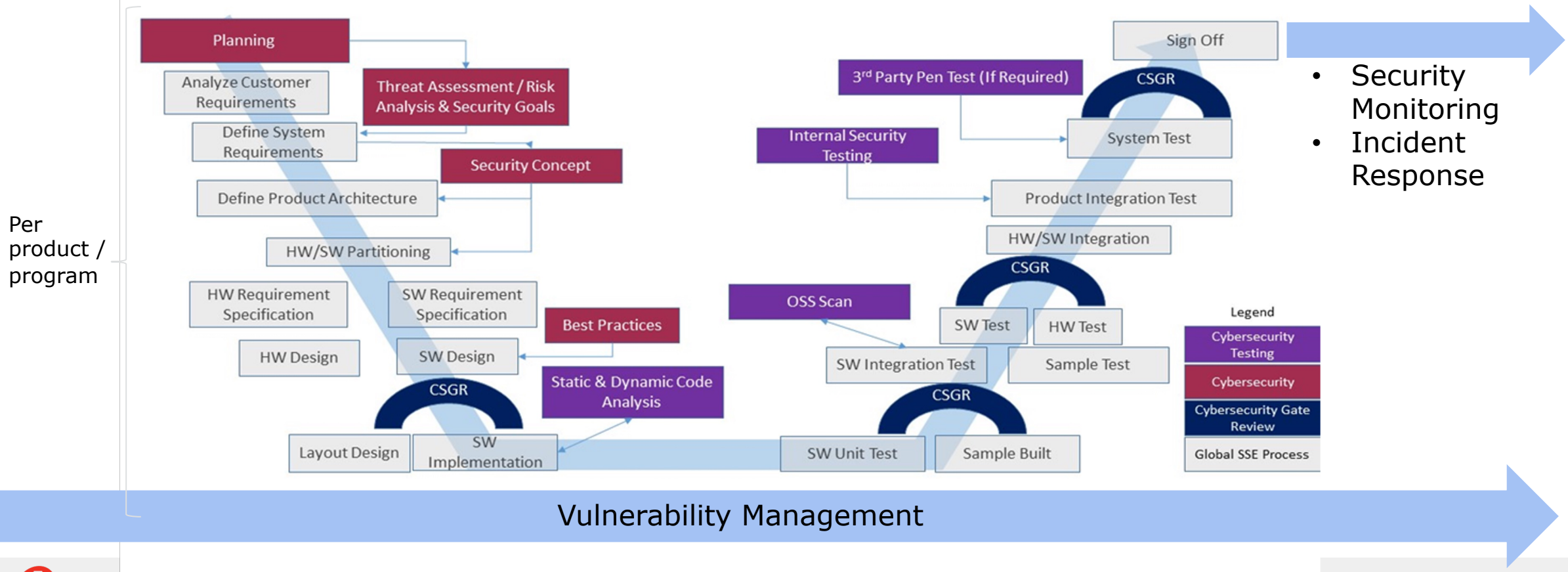


Process

- SAE/ISO 21434 was modeled after ISO 26262 (functional safety) and was published in 2022. The industry has worked on this standard since 2015.
- We don’t know how to measure the quality/level of security, hence we approximate by the quality of the process
- A good process does not prescribe any technologies, but the required technologies are derived during the process execution
- The lack of process adherence implies poor security on average – you still might be lucky and get it right occasionally
- Follow the process, continuously fix systemic issues and improve the process, and all is good!
- There are many more good processes and frameworks out there:
  - NIST Cybersecurity Framework
  - Common Criteria and FIPS 140
  - ISO 27001 and TISAX

Process Overview

- Security Process that is followed for each product development
- Efforts that apply for the organization: training, awareness, controls, escalation procedures, supplier risk management, vulnerability scanning, etc.



Process & Tools & Agile

- Following a process is painful, and it can feel frustrating to generate “paperwork” for process compliance
- The best process is invisible and is guided by automated tools
  - Very hard to utilize and change for large corporations
- ➢ Plenty of tools available to improve code hygiene, find CWEs, find CVEs, etc.
- ➢ We need more tools to automatically find security flaws and either fix them or propose fixes

- DevSecOps, automated tools, and Agile principles will enable efficient vulnerability management and quick security, safety and feature updates.
  - SAE/ISO 21434 vs. Agile: Bill Mazzara and Yuanbo Guo, “Cybersecurity by Agile Design”, 2023 SAE WCX
- The Future – (almost) fully automated development platform
  - Regular reports of vulnerabilities, with semi-automated risk assessment
  - Automated security fixing of vulnerabilities
  - Integration in next Agile Sprint, and quick release.
- ➢ Very little experience and research available around Agile, automotive security, and SAE/ISO 21434 compliance

Standards

Are mandatory standards good?

- Mandatory standards provide a target line and hence the minimum requirements to meet.
- Many use-cases do not need such minimum requirements but are challenged daily, e.g., car theft
- Individuals and corporations usually do a poor job to address risk that has extremely low likelihoods and extremely high negative impact
  - Fukushima singularity – we certainly need minimum requirements for those areas

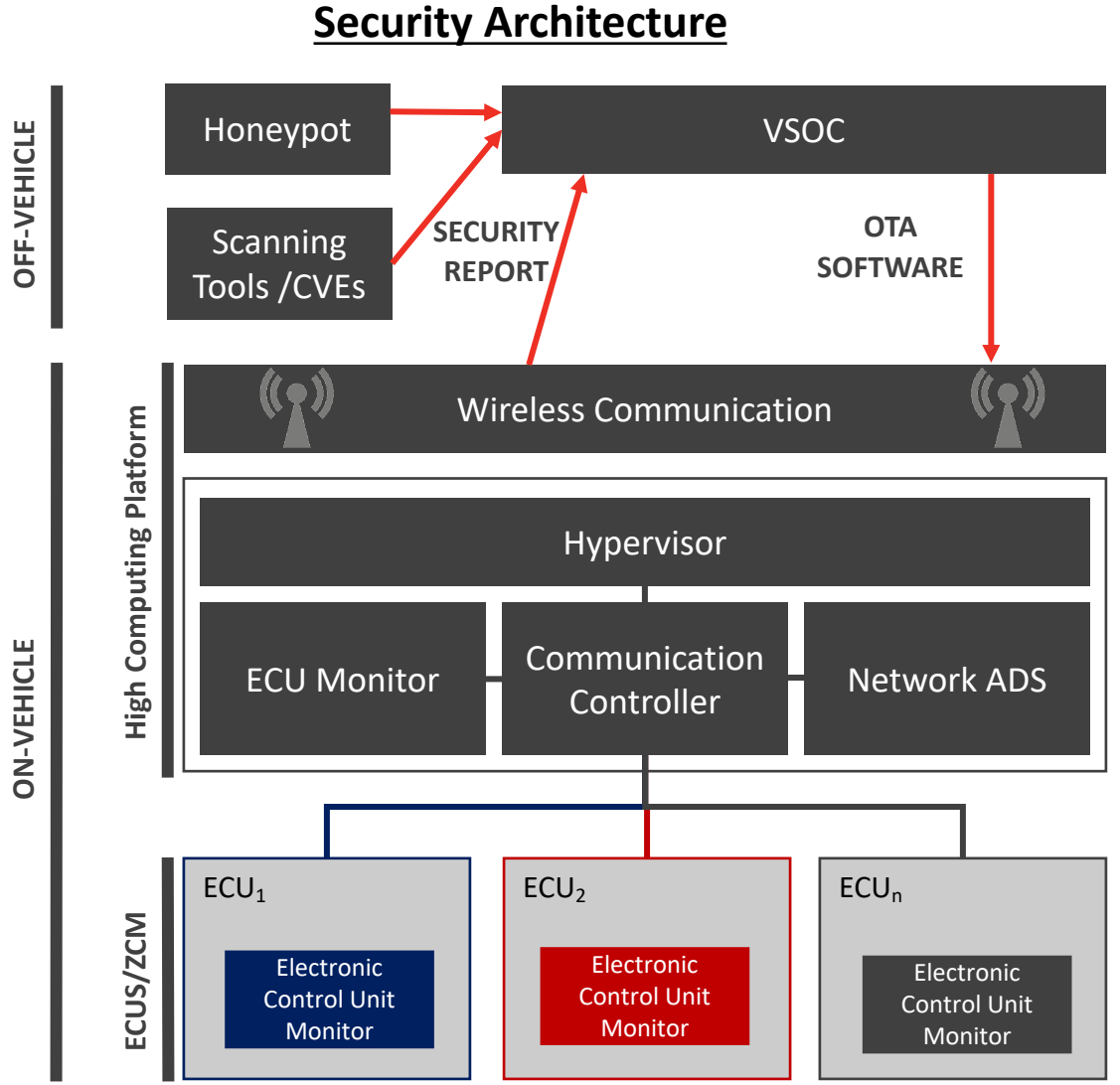
- There is no need to do more than the minimum mandatory requirements
  - Why would you design for more security than is useful?
- The concern is that we take shortcuts and do not include enough "buffers"
  - There will always be mistakes, flaws, etc., so we need additional security walls
- It is ok to do the minimum for low-security functions and focus effort on high-security functions.
  - ➢ It would be good to have a QM equivalent (default quality management) for security

➢ Yes, mandatory standards are necessary to ensure that we have proper security even in functions that are not challenged daily but that could open the door to concerning large-scale attacks.

IDS, VSOC, and SOTA

Background

- CAN-IDS has been in focus since a decade.
- Other IDS and monitors that detect anomalies on network traffic or computing platforms are available as well.
  - This can also include stack canaries, control flow integrity, meta data (such as CPU load), timing, etc.
- Prevention is only used for deterministic rules, but not for probabilistic ones
  - For instance, CAN-ID based filtering vs. cadence-based detection
- IDS start making it into vehicles on the road
- VSOCs start being deployed.
- We understand Secure SOTA: Uptane



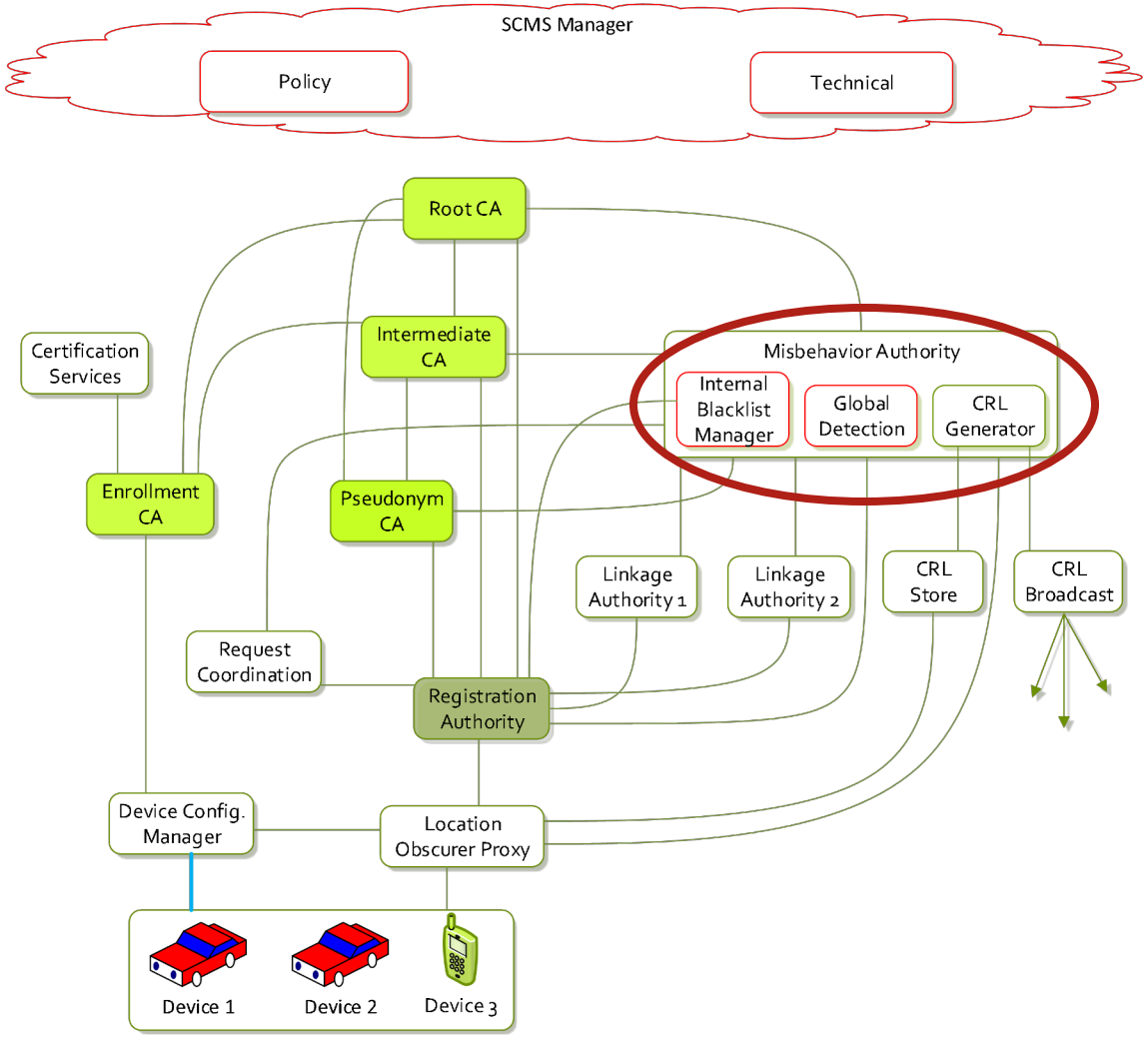
IDS, VSOC, and SOTA

Generic Anomaly Detection

- Plenty of good research available
  - IDS test criteria: NHTSA
  - Detecting physical automotive anomalies: Mcity
- Plenty of solutions around IDS and VSOC available from security vendors

- Anomaly detection also works for other areas:
  - V2X
  - Self driving vehicles
  - ➢ Generally, for all anomalies: car theft, use vehicle to hack into cloud, undermine business models, …

- ➢ More interesting research: PIVOT [http://pivot-auto.org]
  - NSF funded infrastructure and platform to collect vehicle data and utilize it in a secure and privacy protecting manner.



Privacy

- There are examples of comprehensive privacy solutions in the automotive space
  - V2X communication privacy
    - IEEE 1609.2 and IEEE 1609.2.1
  - EV Charging
    - [C. Höfer, J. Petit, R. K. Schmidt, F. Kargl, „POPCORN: privacy-preserving charging for eMobility“, CyCar 2013.]

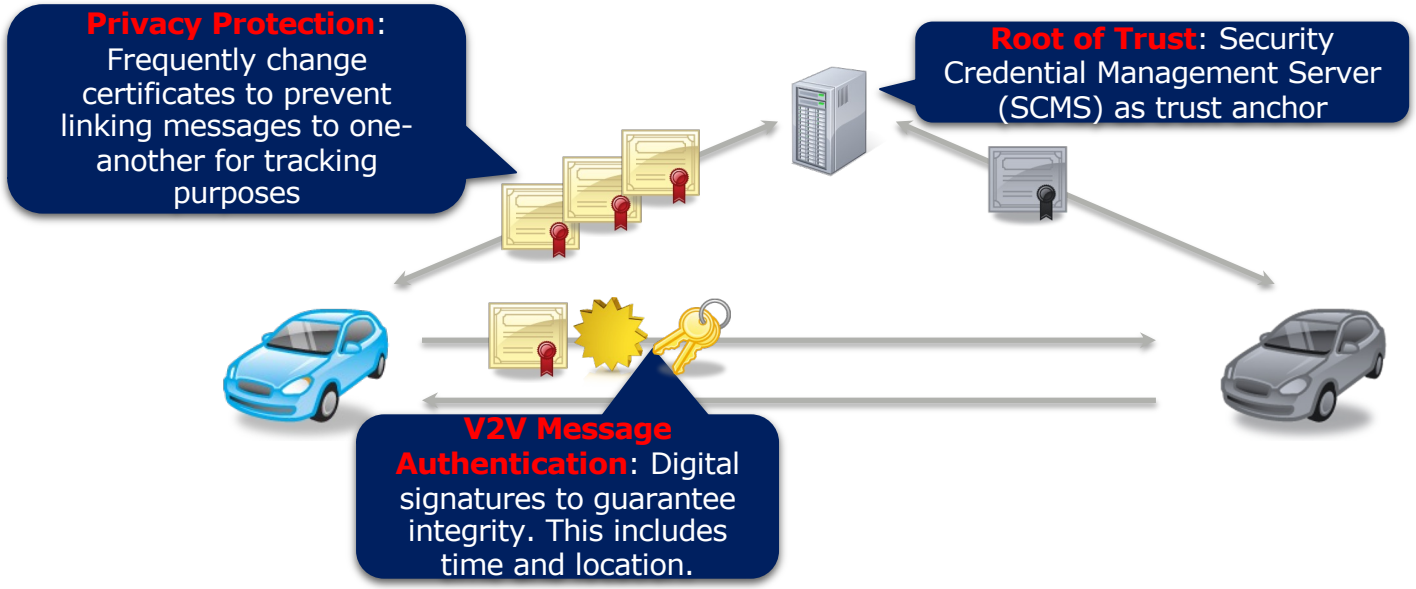
- Two Dagstuhl seminars explored privacy challenges and action items for self-driving vehicles
  - Commercial, ethical, legal, technical
  - [Dagstuhl Seminars 22042 and 23242]

➢ We need a process framework, similar to SAE/ISO 21434, for automotive privacy solutions, and tools that enable easy applications
  - Working out the privacy solution for V2X took almost a decade

➢ Should we even care about privacy?
  - Threat Landscape

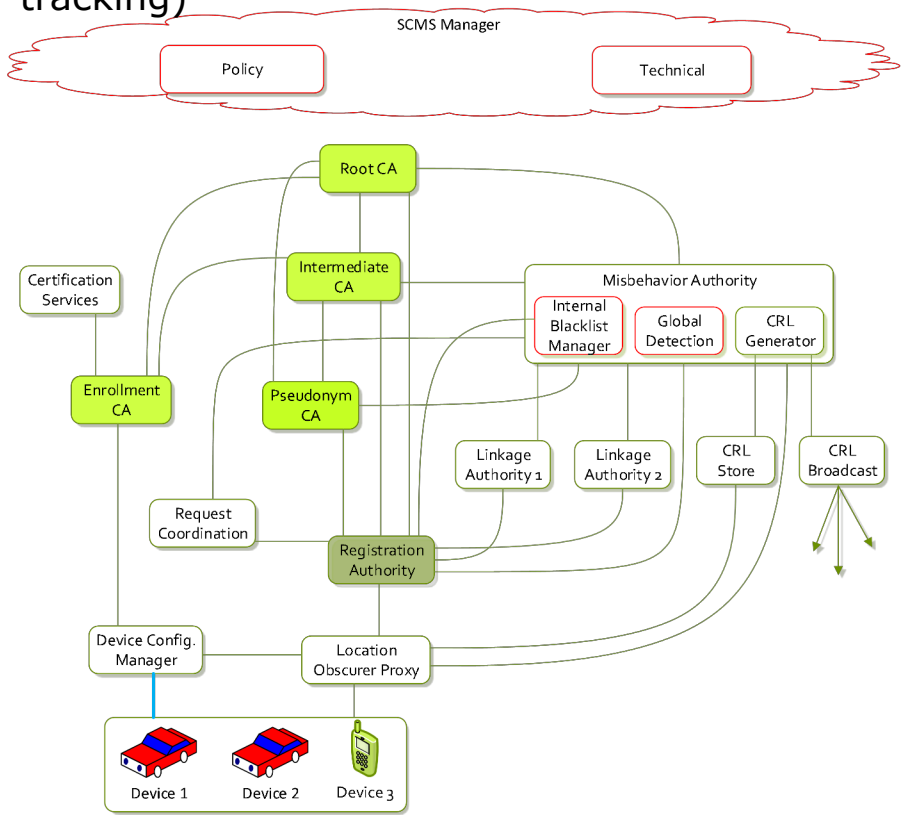
Privacy – V2X Example

- 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 (described later)
- To prevent tracking and linking of V2X messages to vehicles, we need to ensure privacy.



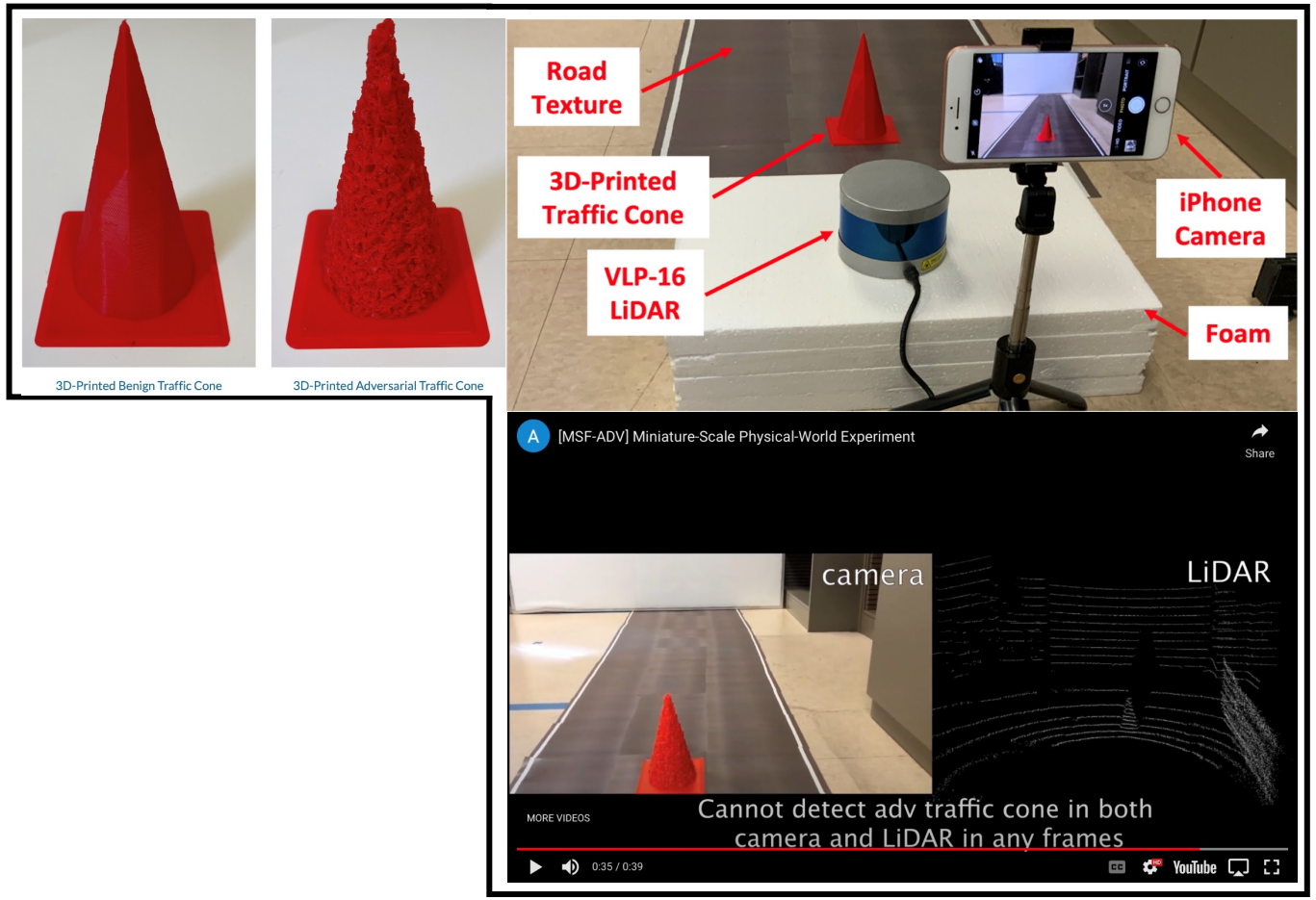
[Benedikt Brecht, Dean Therriault, André Weimerskirch, William Whyte, Virendra Kumar, Thorsten Hehn, and Roy Goudy, "A Security Credential Management System for V2X Communications"]

Separation of SCMS duties and information: a single SCMS component cannot link any two certificates to same device (no tracking)



The Future - Self Driving Vehicles

- Research performed on sensor security
  - Lidar
  - Radar
  - Sensor fusion
  - Perception algorithms
- Example: Hide Objects
- [Alfred Chen, Morley Mao, Mcity, AutoSEC]



Source: Qi Alfred Chen - https://sites.google.com/view/cav-sec

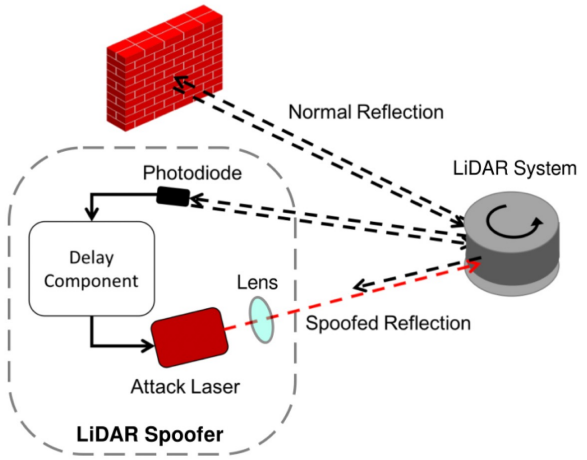
Self Driving Vehicles

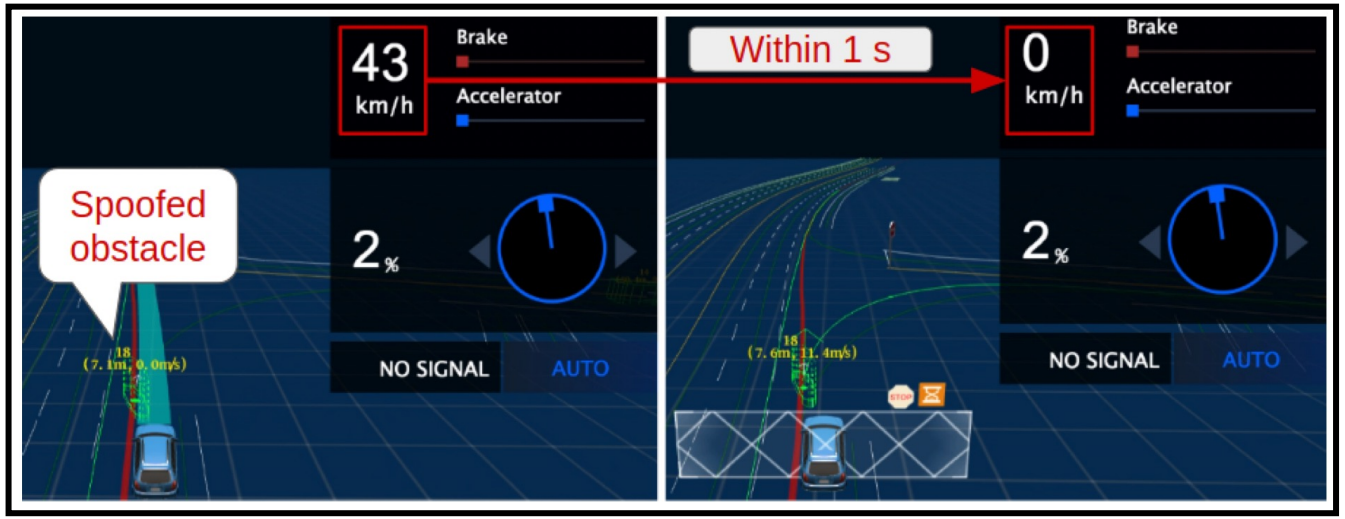
Manipulate objects

[Kevin Eykholt et al. – Robust Physical-World Attacks on Deep Learning Models https://arxiv.org/abs/1707.08945]

Spoof Objects

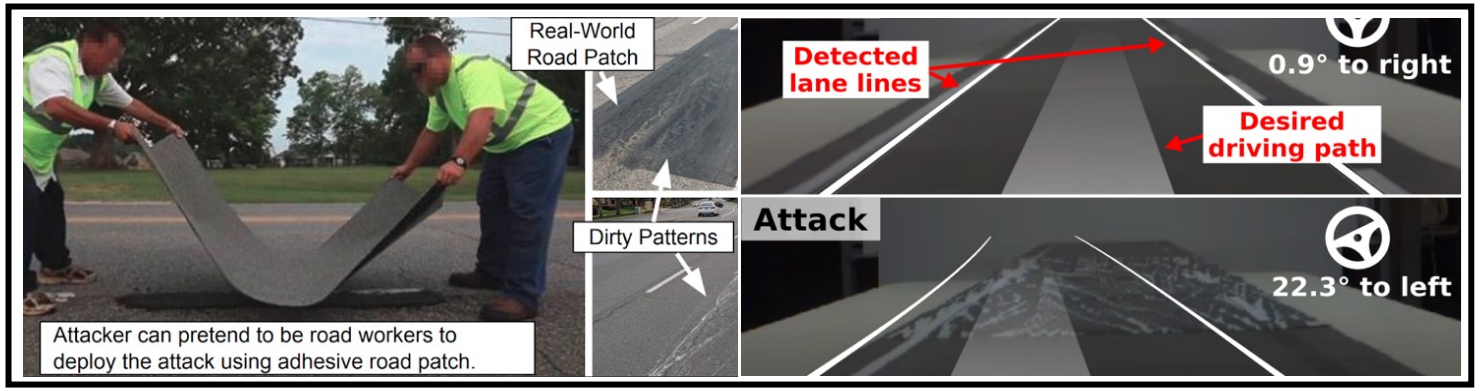
[Yulong Cao et al. – Adversarial Sensor Attack on LiDAR-based Perception in Autonomous Driving https://sites.google.com/view/cav-sec/adv-lidar-attack]





The Future - Self Driving Vehicles

Patching attacks



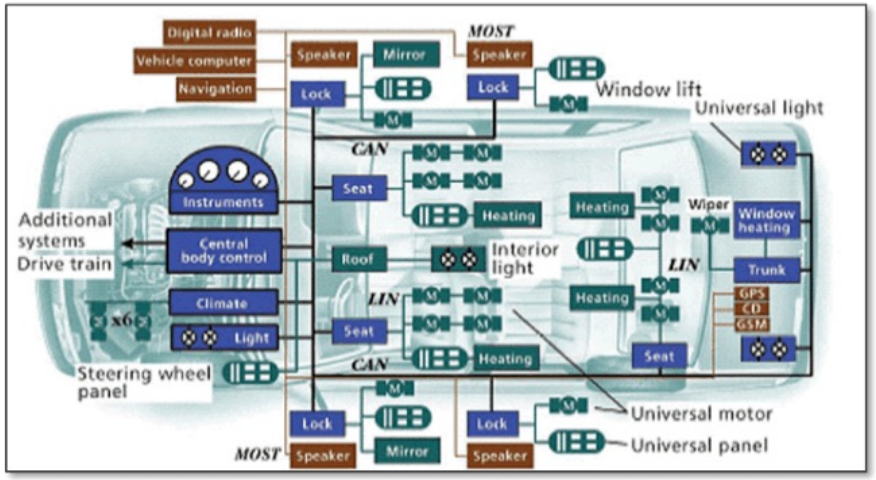
[Qi Alfred Chen - https://sites.google.com/view/cav-sec]

- Probably future area of cat-and-mouse game between researchers and security designers

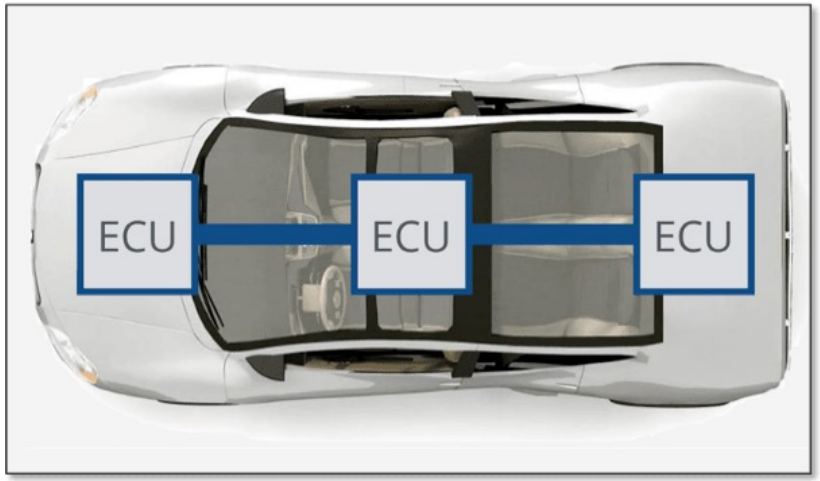
The Future - Vehicle Architectures

- From functional modules to service oriented modules
  - Similar to client/cloud/ Internet world
- Few powerful central nodes where virtual machines replace majority of ECUs
  - Think "replace 150 ECUs with 3 iPhones"
- Standard Internet technologies, such as Ethernet and IP

Conventional Architecture



Software Centric Approach



[https://www.autovision-news.com/hmi/vehicle-control/changes-vehicle-electrical-architecture/]

- Off-the-shelf solutions are required to handle complexity.
- Hackers will gain advantage because standard Internet tools can be applied.
- Defenders will gain advantage because standard Internet defense solutions can be applied, too ☺

The Future – Software Defined Vehicles (SDV)

- (Almost) fully automated development platform
  - Agile and DevSecOps
  - Automated vulnerability management and (semi-)automated security fixing
- Replaceable hardware: Vehicles will be available in many configurations, and trust models will have to be flexible – Zero Trust [Bob Kaster's idea]
  - DOT/NHTSA project: Virginia Tech Transportation Institute (VTTI) and Southwest Research Institute (SwRI)
- Supply chain integrity will become more important, since standard software will run on standard hardware with standard interfaces
  - Scudo
- Wide-spread standard software will be used, such as Linux
  - Or OSs that are tested in the field every day, such as iOS and Android

➢ SDV will come with a paradigm shift, and possibly have far more security implications and impact to our work than self-driving vehicles.

➢ SDV will require a new "kind" of automotive security engineer

The Unknown

- Walnut: Manipulate MEMS with acoustic signals

Bosch BMA222E Acoustic Resonance Interference

BOSCH-2016-0501

Advisory Information

- **Advisory ID:** BOSCH-2016-0501
- **Published:** 14 Mar 2017
- **Last Updated:** 14 Mar 2017
- **CVSSv3 Base Score:** 2.9

Summary

The BMA222E is a micro-electromechanical system (MEMS) accelerometer which senses tilt, motion, inactivity and shock vibration in cell phones, handhelds, computer peripherals, machine interfaces, virtual reality features, and game controllers.

Kevin Fu notified the Bosch PSIRT that an adversary, in close proximity to a device containing the BMA222E sensor, with the ability to generate acoustic resonance with a requisite frequency and a required amplitude (100-110 db Sound Pressure level), might be able to influence the accelerometer sensor readings of the device.

This is considered as an inherent property of MEMS accelerometers. The audible sound oscillates the surrounding components and material (e.g. housing, circuit board). Therefore a successful modification of sensor readings is rather dependent on several boundary conditions (such as positioning of the BMA222E on the circuit board or distance from other components on the circuit board).

A 'Handling, soldering & mounting instructions' document is provided for the BMA222E, which includes recommendations on minimizing the argued effects. As the vulnerability needs to be assessed on the system level (rather than on sensor level) we recommended to contact your end device manufacturer for advice. Per the datasheet, the use of the BMA222E is limited to consumer goods and it is not fit for use in life-sustaining or security sensitive systems.

[https://psirt.bosch.com/security-advisories/BOSCH-2016-0501.html]

Figure 13. **Smartphone Attacking its own Accelerometer to Control an RC Car.** An Android phone runs an application that controls an RC car based on the phones orientation, measured by its internal MEMS accelerometer. Simultaneously, a malicious audio file is playing over the phone's speaker, mounting an output control attack on the phone's accelerometer. The RC car is essentially piloted by the audio file.

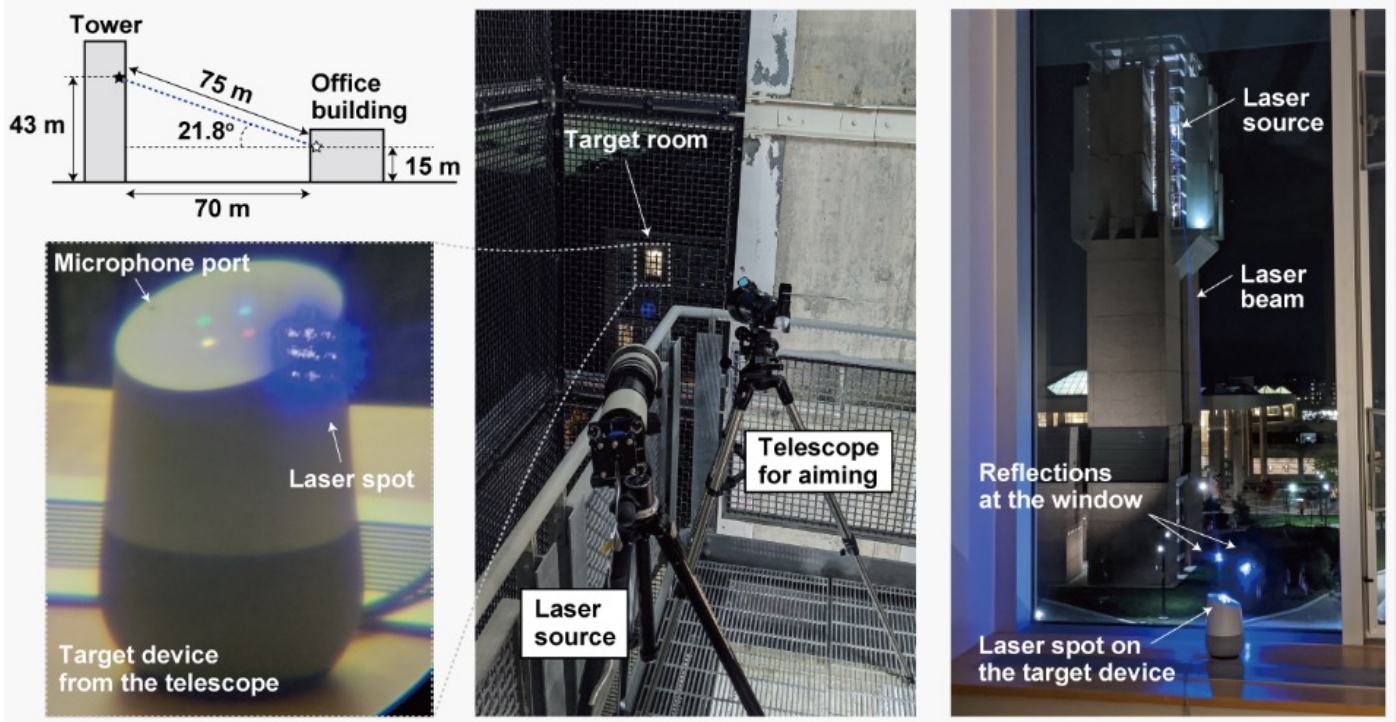
[T. Trippel, O. Weisse, W. Xu, P. Honeyman, K. Fu, WALNUT: Waging Doubt on the Integrity of MEMS Accelerometers with Acoustic Injection Attacks]

The Unknown

- Light Commands: Induce voice commands via laser

- How can we defend against The Unknown?
  - Security buffers
  - Secure SOTA for everything
  - Plans to (temporarily) turn-off features and interfaces
  - Agility?

➢ Do we need to better understand this?



[https://lightcommands.com]

Community

- There are many communities around
  - Auto-ISAC: industry - SBOM, threat modeling
  - ASRG: developers, researchers, security engineers, …
  - Mcity: research – sensor security, vehicle monitoring, key management, secure Ethernet, …
  - SAE: focus areas, guidance, standards – trust and authentication, key management, EV PKI, cybersecurity engineering, ISO/SAE 21434, CAL/TAF, secure hardware, secure SOTA, …
  - escar, AutoSEC: community
  - …
- Missing:
  - High quality collaboration on research, development as well as tools evaluation criteria and test methods between industry, academia, and developers

Opportunities

Development and Maintenance

- More software, more complexity, more OEM focus, strict regulations, cost pressure, shorter development cycles (1 year instead of 3), not enough talents
  - Anything that simplifies the security teams' jobs and enables SDV: automated TARA, vulnerability management, source code fixing, etc.

Technology

- It will take a while before we are able to update software in vehicles in a timely fashion, and updates will always require safety validation that lead to delays
  - Anything that extends the acceptable window of vulnerability: control flow integrity, buffer overflow protection, etc.

Threat Landscape

- Let's understand what the actual concerns are:
  - Should we really be concerned about safety relevant attacks?
  - Maybe much more about stealing data, tracking, using vehicles as attack path to the cloud, using vehicles to open garage doors, etc.

Collaboration

- Let's collaborate much better on technical projects

Thank you!

Dr. André Weimerskirch

VP Product Integrity and Technology

Lear Corporation
aweimerskirch@lear.com

Making every drive better™

Be Inclusive
Be Inventive
Get Results the Right Way

LEAR