TRENDS IN AUTOMOTIVE SECURITY AND PRIVACY RESEARCH

Tomas Olovsson
Associate Professor
Computer Science and Engineering
Chalmers

Agenda

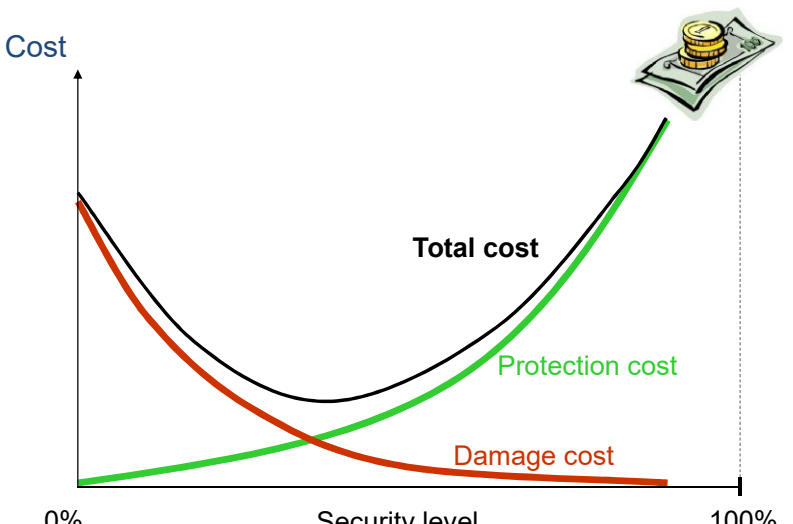
- Challenges in securing the next generations of the connected car
- Securing vehicle communication (V2X)
- Security architectures and promising mechanisms such as intrusion detection systems
- Overview of different research areas
- Privacy research and promising mechanisms such as Differential Privacy

Security = CIA

- **Confidentiality**
- **Integrity**
- **Availability**

- Privacy
- Reliability
- Safety
- …

100% security will never be reached!



The final bug will never be removed

Attacking Autonomous Vehicles

- Computer-security researcher Yoshi Kohno at UW described an attack algorithm that uses printed images stuck on road signs
- They confuse the cameras on which most self-driving vehicles rely
- Small stickers attached to a standard stop sign caused a vision system to misidentify it as a Speed Limit 45 sign!

http://blog.caranddriver.com/researchers-find-a-malicious-way-to-meddle-with-autonomous-cars/

October 23, 2015

Researchers use exploit to disable Audi airbags

Researcher Hacks Self-driving Car Sensors

By Mark Harris

Posted 4 Sep 2015 | 19:00 GMT

Tracking & Hacking:

Security & Privacy Gaps Put American Drivers at Risk

ANDY GREENBERG SECURITY 07.21.15 6:00 AM

HACKERS REMOTELY KILL A JEEP ON THE HIGHWAY—WITH ME IN IT

June 05, 2017

Subaru WRX STI hacked, eight vulnerabilities spotted

July 24, 2015

Zero-day in Fiat Chrysler feature allows remote control of vehicles

PCWorld

Jan 30, 2015

BMW cars found vulnerable in Connected Drive hack

IDG.se

These are the cars most vulnerable to hacking. Is your car one of these?

Sept 2015

Hackers are not the only problem

Owners may want to “upgrade” their own vehicles

- Copy other vehicles software
- Install third party devices (phones, navigators, …) that interface with the network

Drivers and owners may not fully trust each other

- Owners track vehicles and limit functionality (horse power)
- Drivers do not trust each other – may fake messages for improved service

Authorities may require functionality

- Post accident investigations
- Road tolls – drivers may lie about location

Repair shops not fully trusted by **car manufacturer** and car owner

- Third party repair shops
- Full access to vehicle networks – through laptops? Internal security?

Third party developers want to offer functionality

- Can they develop secure software?
- Creating shortcuts to “improve” products…

What is required?

Special tools?

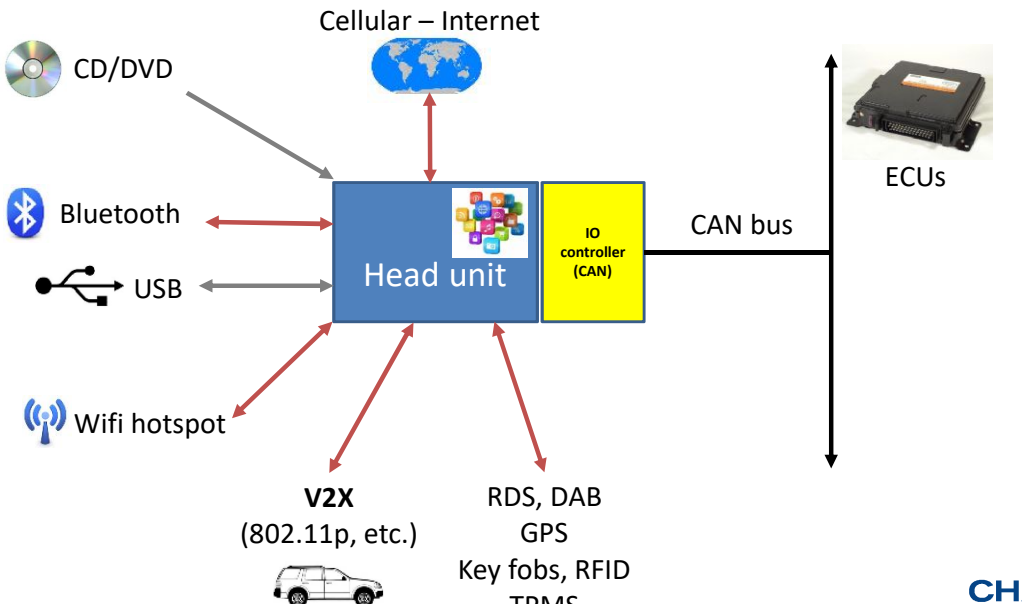
Extreme skill?

Lots of resources?

Plenty of time?

How hard is it to find a security problem?

Typical architecture – Attack surfaces

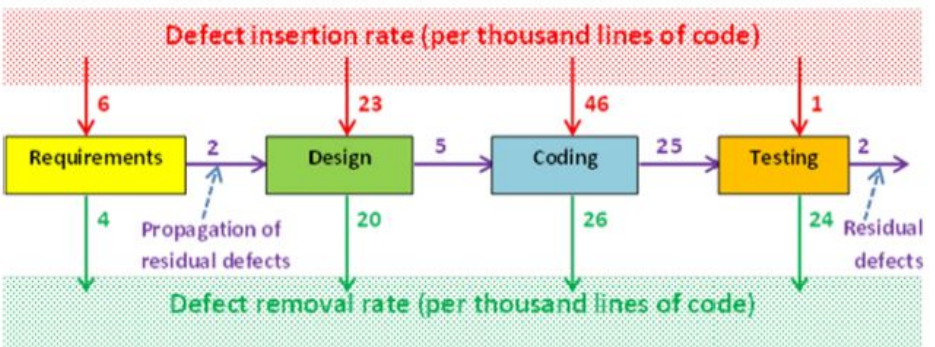


Communication threats

Eavesdrop, modify,
insert, delete,
delay, replay, flood,
impersonate, spoof origin, ...

NASA Study on Flight Software Complexity

"Commissioned by the NASA Office of Chief Engineer, Technical Excellence Program, May 2009"



65M lines of code ➔ 130,000 remaining defects

Critical with a good internal architecture

Why not use standard security tools?

- Non-standard protocols and buses

- Resource constraints in ECUs
  - Limited power consumption, processing power and memory

- Cost constraints
  - An increase of € 1 per ECU: 100 ECUs in 1,000,000 cars = €100 million in revenue loss

- Lifetime of the solution
  - Vehicles live 10-15 years
  - Add development time and overall life cycle can be as long as 20-25 years

- Performance
  - Real-time, latency and performance demands

- Off-line systems – e.g. during road-side assistance
- Reliability and safety requirements

Security must be part of the initial design

- Security mechanisms can not be designed in isolation
  - Must be designed and play well with safety and real-time requirements
- Safety – many tools and standards exist
  - ISO 26262, ASIL levels, …
- Security?
  - Main problem: the intelligence of the attacker – problems are not random but planned
  - If one attack works – all vehicles are vulnerable (it spreads)
  - The attack surface is very big
  - One bug/vulnerability enough

SC MAGAZINE
FOR IT SECURITY PROFESSIONALS
October 23, 2015

Researchers use exploit to disable Audi airbags

A trio of researchers disabled the airbags in an Audi TT using a zero-day exploit in third party software that is commonly used by mechanics.

Researchers András Szijj, Levente Buttyán of CrySyS Lab and Zsolt Szalay of Budapest University of Technology and Economics said the attack requires a mechanic's computer to be compromised or for a malicious USB drive to be plugged into the vehicle for the exploit to work, according to the Register.

A trio of researchers disabled the airbags in an Audi TT using a zero-day exploit in third party software that is commonly used by mechanics.

The attack takes control of the diagnostic system allowing items to be switched on or off without being noticed by the driver.

Buttyán told the Register that the exploit is not connected to Volkswagen (VW), Audi's parent company, but said the vulnerable software is compatible with cars sold by VW. Other researchers have also found the software used in repair shops and dealerships vulnerable.

February 03, 2015

BMW issues security patch for bug allowing attackers physical access into vehicles

BMW released a security patch on Friday to address a security flaw that could have affected 2.2 million Rolls-Royce, Mini and BMW vehicles.

The addressed vulnerability could have allowed hackers to unlock the doors and gain physical access to vehicles hooked up to the company's ConnectedDrive software, which relies on SIM cards to identify mobile device users, Reuters reported. ADAC, a German motorist association and consumer protection organization, discovered the bug this past year but waited until it was patched to release its findings, the company said in an emailed statement to SCMagazine.com.

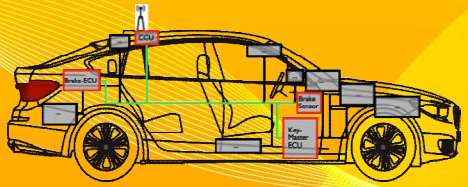
The German automobile maker issued a patch for a security issue that could have affected more than 2 million vehicles and allowed attackers to gain physical access to the cars.

Reuters reported that ADAC's researchers successfully exploited the bug by creating a fake phone network with which the vehicles attempted to connect. During this connection attempt, attackers could take over the SIM card ConnectDrive functions. More specifically, attackers could monitor the vehicle's current location and real-time traffic information. They could also obtain emails sent through BMW online.
In addition to the security update, BMW said it was removing the possibility of breaches by encrypting the cars' communications through HTTPS.

http://www.scmagazine.com/bmw-patches-sim-card-software-bug/article/395979

The Jeep Cherokee hack 2015

- Researchers have for long complained about (lack of) security
  - Demonstrated many problems on Ford Escape and Toyota Prius
  - Criticized from car manufacturers that physical access was needed…
- Two researchers, Miller & Valasek, picked one vehicle
- Toyota released a statement that said:
  "Our focus, and that of the entire auto industry, is to prevent hacking from a wireless device outside of the vehicle. We believe that systems are robust and secure."
- *Therefore "we" had to demonstrate remote attacks…*
- Selected Jeep Cherokee – many attack surfaces, simple architecture, many features
  - 1.4 Million cars recalled
  - No special skills needed – just the will to investigate
- The problems are not unique to Jeep Cherokee / Fiat-Chrysler

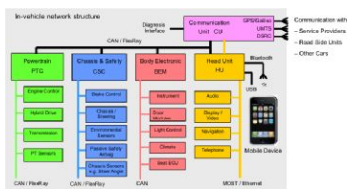


Many possible solutions exist

SECURE COMMUNICATION

Some proposed security mechanisms

- Introduce security classifications (QA, Low, Medium, High, Critical) [Heavens project]
- Isolation
  - Care with functions sharing ECUs
  - Isolate traffic in domains
- Verify authenticity in all communication (external, internal)
  - Short-lived anonymous certificates in V2X communication (i.e. pseudonyms)
- Software signing
- Hardware Security Modules (HSMs)
  - Stores private keys, possibly also a random number generator and a clock
  - Contain functionality to sign and encrypt messages
  - Can distribute session keys to ECUs
- Certification of critical modules
- Use of security protocols for important tasks [SIGYN projects]
  - Remote software updates
  - Secure diagnostics



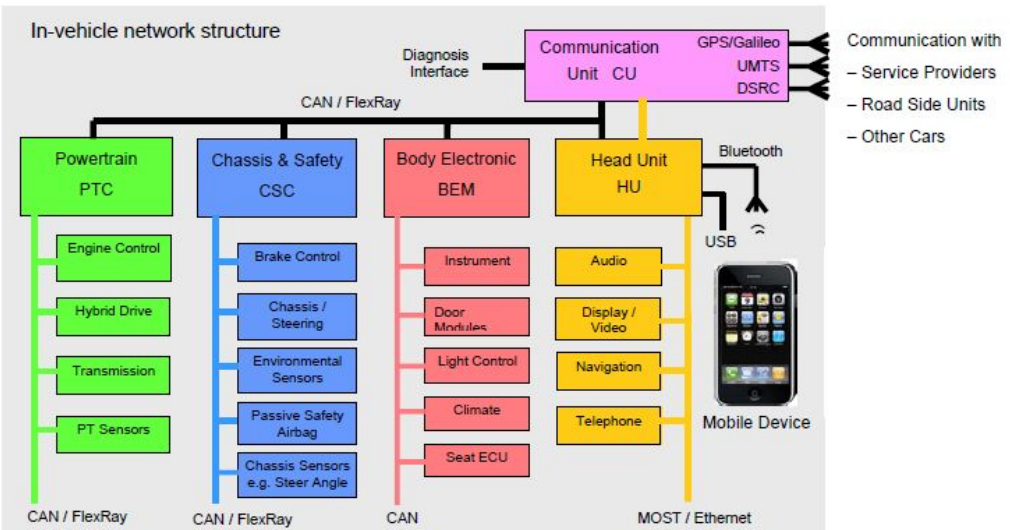
CHALMERS

Isolation and separation is essential

- Components communicating with external services and devices
  - Separation: Virtualization, Containers, Sandboxes, Memory protection, Firewalls, IDS systems [HOLISEC project]

- Third Party components
  - Demand secure design – i.e. security levels
  - The security level dictates design method, security mechanisms and testing [HOLISEC project]
  - Isolation/separation of software components
  - Isolation in network domains if h/w component, use gateway controllers (IDS)
  - Certification

Internal gateways separate traffic

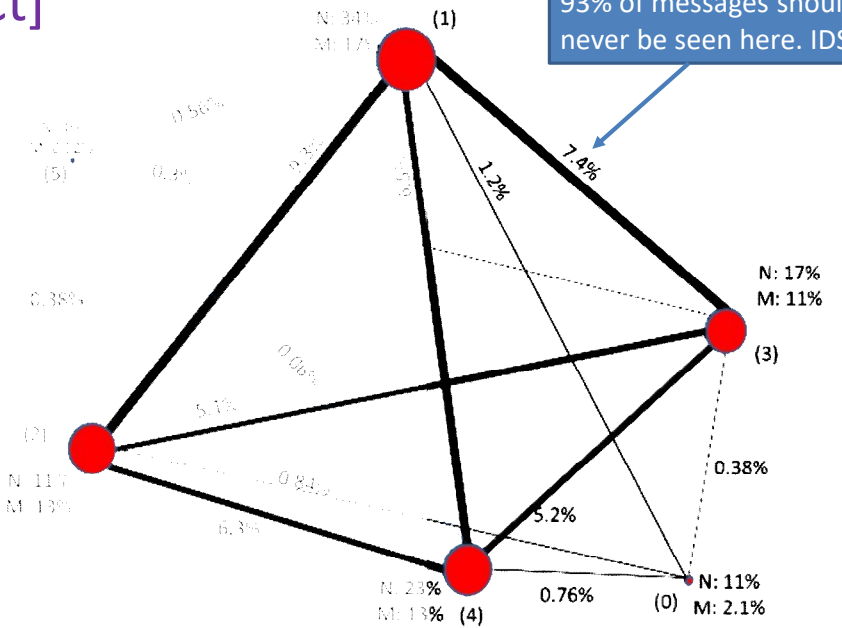


http://www.evita-project.org

[SeFram Project]

93% of messages should never be seen here. IDS system!

M = message types
N = ECUs

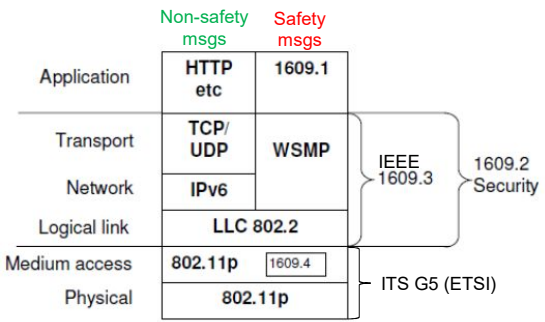


Can guide designers toward more secure architectures.
Now have an architecture to compare own designs with.

CHALMERS

V2X communication protocols

- ETSI and IEEE working in parallel with IEEE 802.11p – same physical (PHY) and link (MAC) layers
  - Based on DSRC/WAVE in the US, and
  - ETSI ITS G5 containing small European adoptions
- Derived from 802.11a (CSMA/CA)
  - No association or authentication to an AP to decreases delays
  - 7 channels, 6 Mbps typical transfer rate
- Higher level protocols (Network and above) differ
- IEEE 1609 in the US
  - WSMP – Wave Short Message Protocol for broadcast communication
- ETSI TS nnnn in Europe, e.g. safety messages:
  - CAM – Cooperative awareness messages ("I am here"), periodic transmissions
    ETSI TS 102 637-2
  - DENM: Decentralized Environmental Notification Messages (Hazards and warnings) ETSI TS 102 637-3



PRIVACY

European General Data Protection Regulation (GDPR)

- In action from May 25, 2018
  - Replaces “PUL”
  - Penalty of up to 4% of annual world-wide turnover or €20 million whichever is the greater
  - Applies to all types of personal data
- Personal data vs technical data? What is what?
  - OEM owns vehicular data
  - Drivers/owners own their data and can trade it (consent)
  - Owners may demand deletion of data
- Potential customers may not like the idea of consent

Privacy

The vehicle **knows**…

- Where you drive
- When you drive
- What type of driver you are
- When you break traffic laws

It **broadcasts** identity, speed, position, intention (v2x)

Third party apps, Remote diagnostics, Remote software updates, Wireless sensors, …

What data is personal? Or vehicular?

Fuel injection

GPS position

ESP system

ABS system

Speed

Chair positions

Passenger seat occupied

Turning lights

Wheel rotation

Music choice

Acceleration

Vehicle ID number

CHALMERS

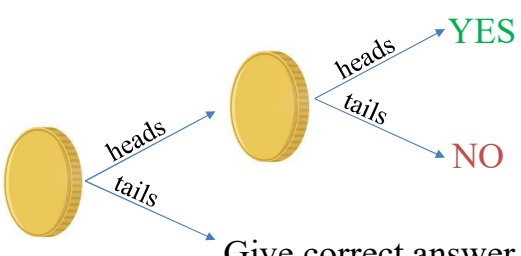
Privacy preserving models

- k-anonymity [2002]
  - Cannot distinguish between k individuals
  - Method: Modify data to fit property
  - Drawback: if k=2, we may know that user has either property X or Y
  - Methods patented in the US
- l-diversity
  - Extends k-anonymity to have at least l values for sensitive attributes
- t-closeness
  - Controls distance between sensitive attributes
  - Good for numerical properties
- Differential privacy
  - Same answer regardless of whether an individual is in the dataset or not
  - Adds Laplace noise to answers
  - Privacy budget

Differential Privacy promising solution

- Mathematically proven
- Adds noise to answers – all noise will average itself out
- Impossible to figure out individual answers
- Privacy budget governs amount of noise: low budget = more noise
- Example:

[BAUD Project]



Privacy as a marketing tool?

- Google RAPPOR [2014]
  - Differential Privacy
  - Learning about malicious software, open source
  - Sharing old statistics about

- Apple [2016]
  - Differential Privacy
  - Intelligent suggestions in iOS
  - https://www.youtube.com/watch?v=8qBfjx24YMU (starts at 14:00)

- Should we be here?

Summary

- All bugs cannot be found and removed
- Many examples of hacked vehicles
  - Hackers are not the only problem
- Privacy upcoming problem
- Security and privacy by design needed
  - Security classification of functions with strict design rules
  - Sound internal architecture with domains – separation and isolation
  - Message integrity through signatures, internal and external
- The new technology will make driving even safer ☺

CHALMERS