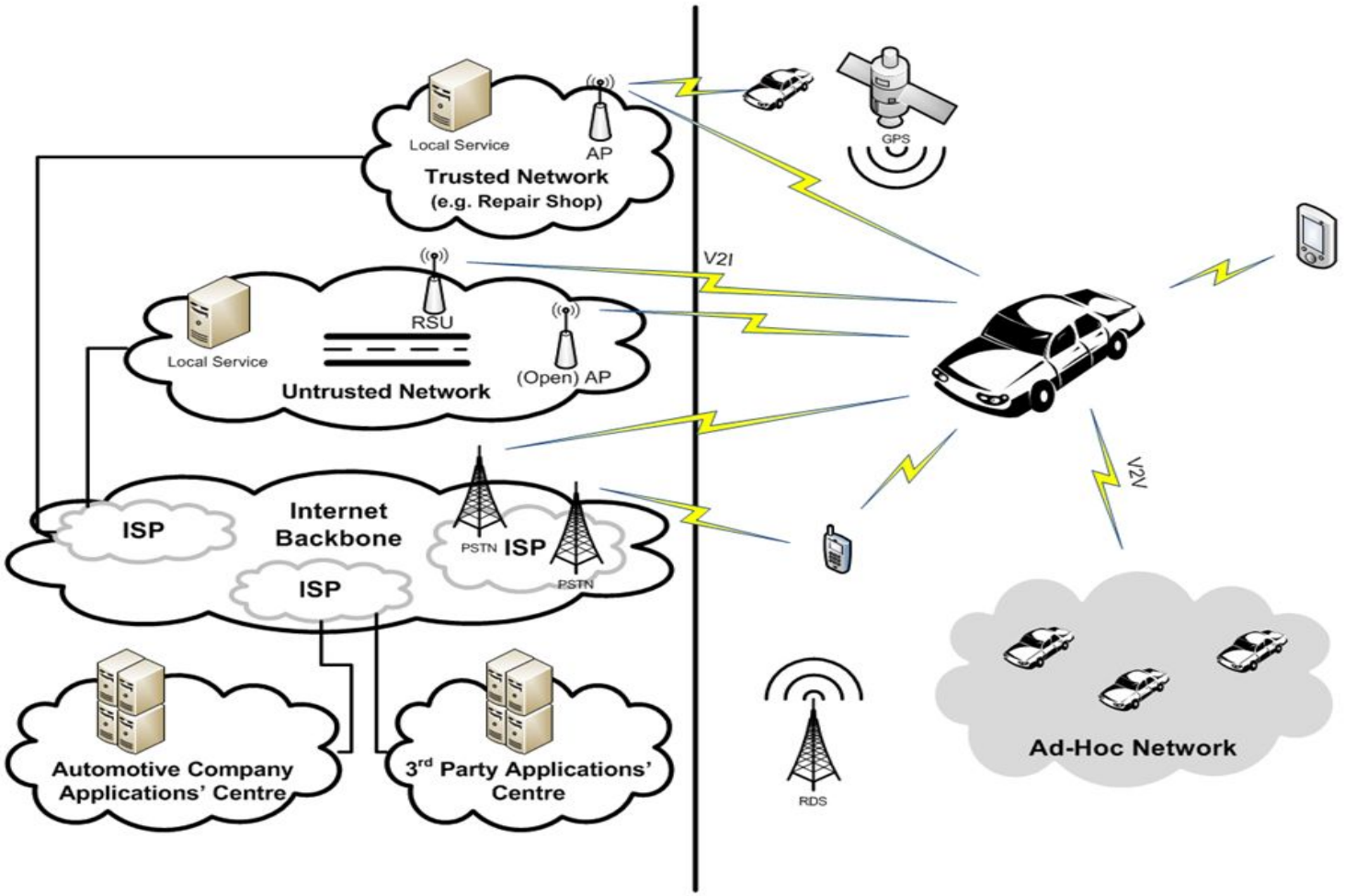
THE COMPLEX WORK WITH
SECURING AUTONOMOUS VEHICLES

Tomas Olovsson
Computer Science and Engineering
Chalmers University of Technology

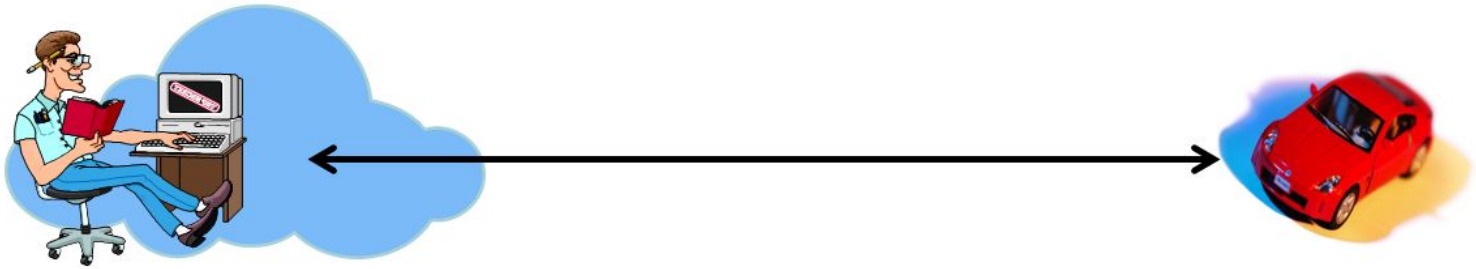
Communication increases



CHALMERS

Communication threats

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



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

What is required?

Special tools?

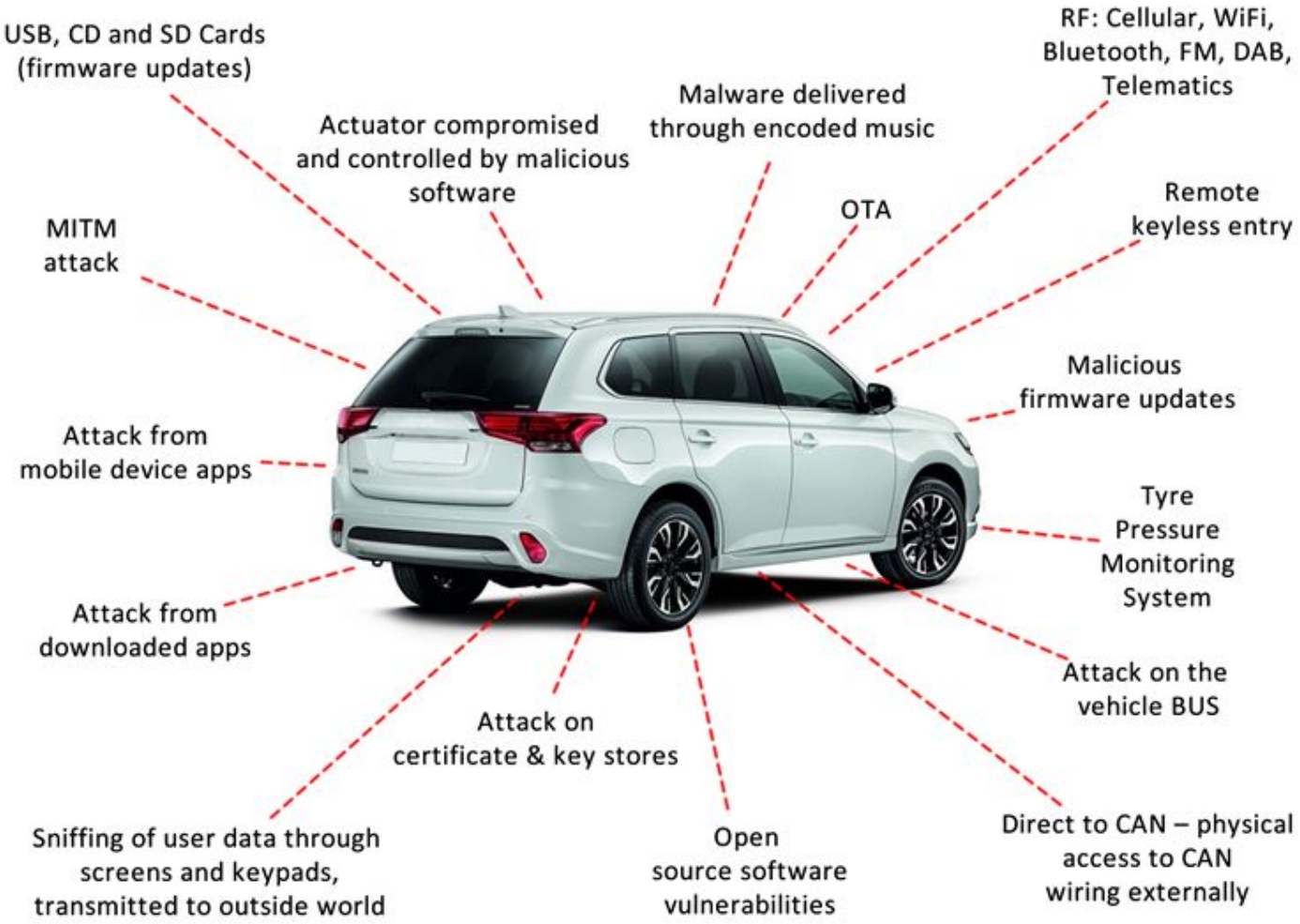
Extreme skill?

Lots of resources?

Plenty of time?

How hard is it to find a security problem?

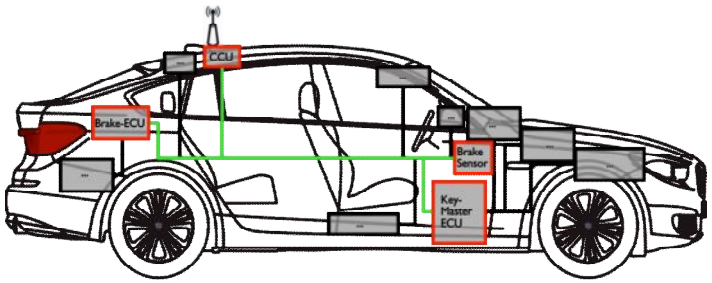
Attack Surfaces



Source: pentestpartners.com

The vehicular network is complex

Size of an ordinary
office network. But
without all its
protection mechanisms



100-200 ECUs
>50M lines of code

NASA: 2 errors per 1,000 lines of code
i.e. a vehicle has more than 100,000 remaining bugs
Some may affect security, the problem is to know which…

Applications can also be targets

- Yoshi Kohno at UW showed an attack with printed images stuck on road signs
- They confuse the cameras on which most self-driving vehicles rely upon
- 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/

Bugs…

What Is BlueBorne?

BlueBorne is an attack vector by which hackers can leverage Bluetooth connections to penetrate and take complete control over targeted devices. BlueBorne affects ordinary computers, mobile phones, and the expanding realm of IoT devices. The attack does not require the targeted device to be paired to the attacker's device, or even to be set on discoverable mode. Armis Labs has identified eight zero-day vulnerabilities so far, which indicate the existence and potential of the attack vector. Armis believes many more vulnerabilities await discovery in the various platforms using Bluetooth. These vulnerabilities are fully operational, and can be successfully exploited, as demonstrated in our research. The BlueBorne attack vector can be used to conduct a large range of offenses, including remote code execution as well as Man-in-The-Middle attacks.

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

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

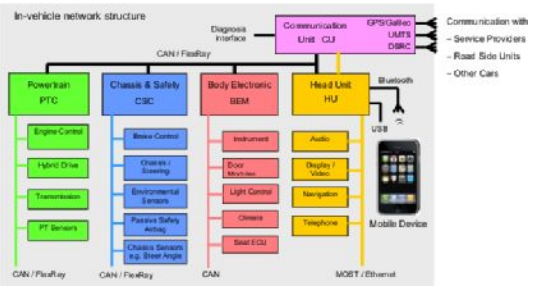
Third party developers want to offer functionality

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

CHALMERS

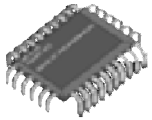
Some proposed security mechanisms

- Introduce security classifications (QA, Low, Medium, High, Critical)
- Isolation
  - Network domains for isolation
  - Separation of functions sharing the same ECU
- Verify authenticity in all communication (external, internal)
- Privacy: short-lived pseudonyms/certificates in V2X communication
- Software signing
- Hardware Security Modules, HSMs
  - Signs and encrypt messages
  - Can distribute session keys to ECUs
- Certification of critical modules
- Use of security protocols for important tasks
  - Secure remote software updates
  - Secure diagnostics



CHALMERS

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

Conclusions

- 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