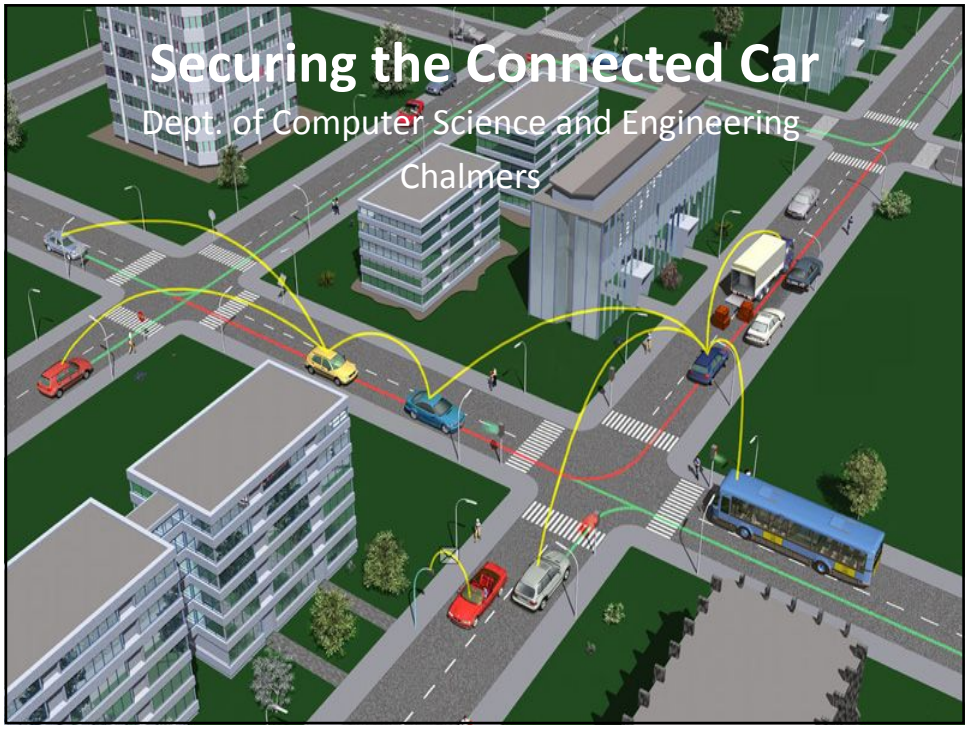
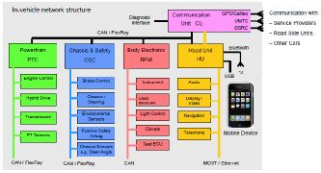


Modern Vehicles

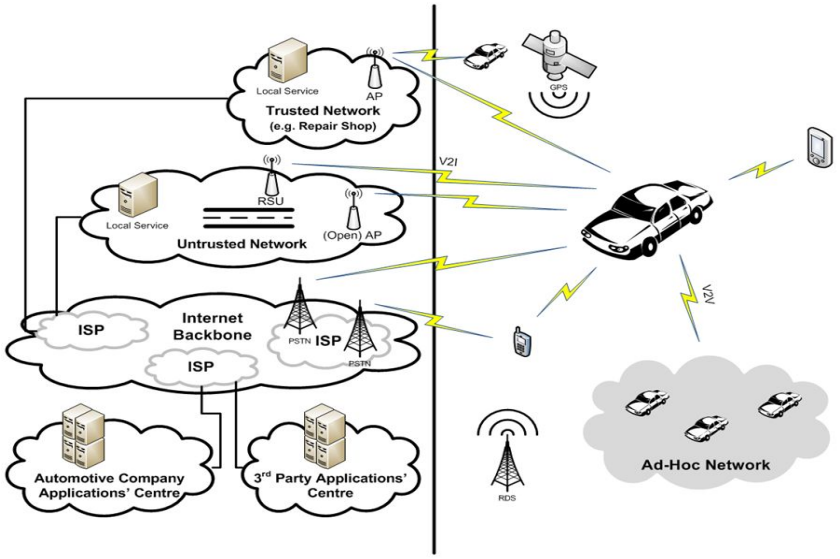
- Contain 50-100 computers, ECUs
  - Internal networks: CAN, LIN, Most, FlexRay
  - Network of the size of an office
- Depend heavily on software
  - 10 - 100 million lines of code
  - Real-time system with hard deadlines
- Networking makes it easy to…
  - add new advanced functionality: ABS, ESP, Drive by wire, platooning, …
  - offer v2v and v2i connectivity
  - develop an "Appstore" of applications
- It is a safety-critical system!
  - Failures of ECUs must be dealt with



EVITA Use Case Reference Architecture
(source: http://www.evita-project.org/)

CHALMERS

Vehicle communication is complex



CHALMERS

Securing the Connected Car

- Complex, networked, safety-critical real-time system
- One bug, in one application or ECU, may be enough
- Security problems can affect safety

Why care about security?

- Hackers
  - May manipulate vehicles and affect safety
  - Complete fleets grounded/disabled – because it is possible
- Theft of vehicles only using software
- Car owners and drivers may benefit from weak security
  - Lie about congestion, get green lights, …
  - Manipulate the mileage of vehicles, tachographs, …
  - Impersonation – for road tolls, parking fees, speed cameras, etc.
  - Card sharing for shared subscriptions
- Privacy issues
  - Software may enable vehicle tracing, driver behavior, …
- Reverse engineering of software
  - Car owners install free, possibly pirated, software
  - Third parties offer OEM functionality much cheaper
- **So far, just about every consumer device that's been desired to be hacked into, has.**

CHALMERS

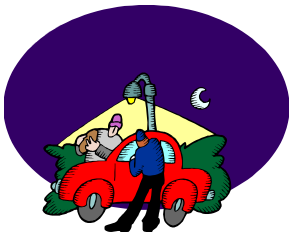
Hackers are not the only problem

- **Owners** may want to "upgrade" their own vehicles
  - Copy other vehicles software
  - Install third party devices (phones, navigators, …) that interface with the network
- **Driver** and owner may not fully trust each other
  - Owners track vehicles? Owners may limit functionality (horse power)
- Drivers do not trust each other
  - May send false messages to get improved functionality (e.g. lie about congestion)
- **Authorities** may require functionality
  - Road tolls: Driver 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

CHALMERS

Project

ATTACKS AGAINST, AND PROTECTION OF NETWORKED VEHICLES



CHALMERS

Demonstrated security threats

- The on-board diagnostics port (OBD-II)
  - Required by law
  - Gives (owner/hacker/…) full access to the internal network
  - Can be used to send arbitrary messages and connect new devices
- Compromised ECUs [Koscher et al.]
  - May fail by receiving malicious messages
  - Can send arbitrary messages. At any time…
- Media player attacks [Checkoway et al.]
  - Malicious music CD inserted by driver → Buffer overflow → can send arbitrary messages
- Tire pressure monitoring system (US) [Rouf et al.]
  - USENIX Security Symposium 2010
  - Can be remotely accessed (wireless)
  - Cause system failures (ECU must be replaced)
  - Trace vehicles with the ID (privacy problem)

Biltema €45

CHALMERS

Operating a vehicle from a laptop

FORBES 7/24/2013 @ 9:00m | 492 802 views

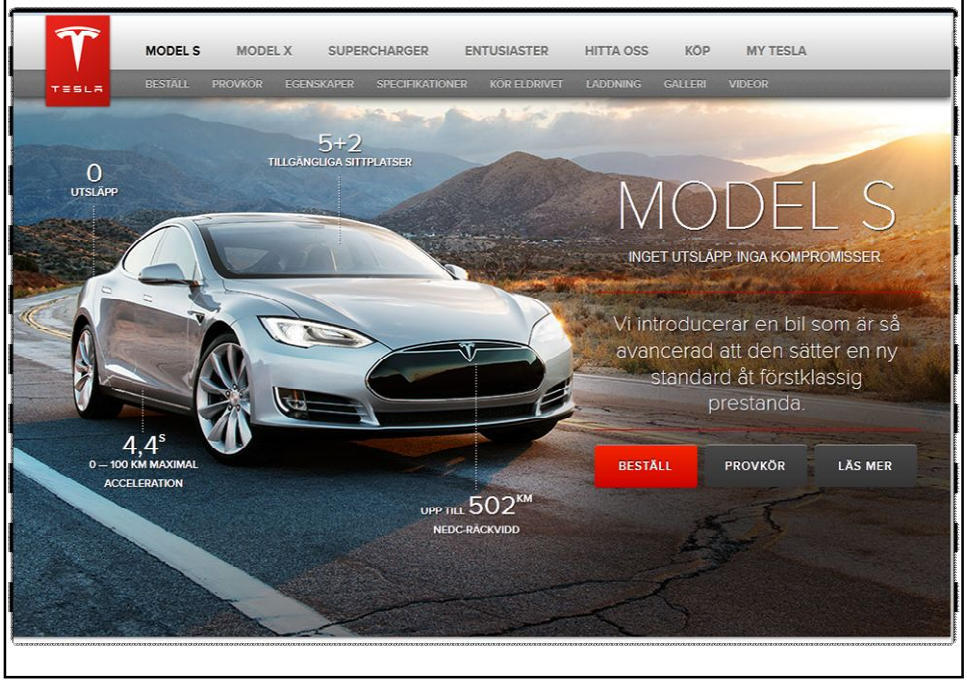
Hackers Reveal Nasty New Car Attacks--With Me Behind The Wheel (Video)

This story appears in the August 12, 2013 issue of Forbes.

Stomping on the brakes of a 3,500-pound Ford Escape that refuses to stop–or even slow down –produces a unique feeling of anxiety. In this case it also produces a deep groaning sound, like an angry water buffalo bellowing somewhere under the SUV's chassis. The more I pound the pedal, the louder the groan gets–along with the delighted cackling of the two hackers sitting behind me in the backseat.

http://www.forbes.com/sites/andygreenberg/2013/07/24/hackers-reveal-nasty-new-car-attacks-with-me-behind-the-wheel-video/

CHALMERS



Tesla Model S Ethernet Network Explored, Possible Jailbreak in the Future?

April 4th, 2014

Being the technical marvel that the Model S is with it's 17" multi-touch display, all digital dashboard, all electric 192.168.90.0 subnet, the center console, dashboard/nav screen and one more unknown device. Some ports and services that were open on the devices were:

- 22 (SSH)
- 23 (telnet)
- 53 (open domain)
- 80 (HTTP)
- 111 (rpcbind)
- 2049 (NFS)
- 6000 (X11)

Port 80 one one device was serving up a web page with the image or media of the current song being played. The operating system is modified version of Ubuntu using an ext3 filesystem.

http://www.dragtimes.com/blog/tesla-model-s-ethernet-network-explored-possible-jailbreak-in-the-future

CHALMERS

You should…

- Study and present different attack methods
  - Show what old attacks have been demonstrated
  - Show where weaknesses can be found in vehicular systems
- Investigate, invent(?) and discuss different protection mechanisms
- Evaluate the strength and weaknesses (pros and cons) of these solutions
- Your project can be either very wide or focus on a particular problem or type of problem

CHALMERS