Securing Autonomous Vehicles

Tomas Olovsson
Computer Science and Engineering
Chalmers

Autonomous Driving – Safety Systems

Cooperative Vehicle Safety System or Cooperative Active Safety System

Virtual traffic lights

© Chalmers University of Technology
Modern Vehicles

- Contain **50-150 ECUs** (computers)
  - Internal networks: CAN, LIN, Most, FlexRay
  - 2 km cables
- 40 Antennas
- Depend heavily on **software**
  - 10 - 100 million lines of code
- Mercedes S-Class: 144 ECUs, 65M lines of code
- Networking can **enhance traffic safety**
  - New advanced functionality: ABS, ESP, drive by wire, platooning, ...
  - v2v and v2i connectivity for improved awareness
- It is a **safety-critical Real-time system**

---

How well can we test the software?

- **NASA Study on Flight Software Complexity**
  “Commissioned by the NASA Office of Chief Engineer, Technical Excellence Program, May 2009”
The vehicular network is complex

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

100-200 ECUs
>50M lines of code

2 errors per 1,000 lines of code = 100,000 remaining bugs

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** may 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
Vehicles have many interfaces to the outside

Researchers use exploit to disable Audi airbags

Researcher Hacks Self-driving Car Sensors

October 23, 2015

By Mark Harris
Posted 4 Sep 2015 19:00 GMT

Tracking & Hacking:
Security & Privacy Gaps Put American Drivers at Risk

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

Hacker Disables More Than 100 Cars Remotely

July 24, 2015

By KEVIN FOULSEN 01:20 | 1:52 PM | PERMALINK

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

PCWorld
BMW cars found vulnerable in Connected Drive hack

Jan 30, 2015

These are the cars most vulnerable to hacking. Is your car one of these? Sept 2015
How hackable is your car?

<table>
<thead>
<tr>
<th>Year</th>
<th>Attack Surface</th>
<th>Network Architecture</th>
<th>Cyber Physical</th>
</tr>
</thead>
<tbody>
<tr>
<td>2014</td>
<td>++</td>
<td>++</td>
<td>++</td>
</tr>
<tr>
<td>2015</td>
<td>++</td>
<td>++</td>
<td>++</td>
</tr>
<tr>
<td>2016</td>
<td>++</td>
<td>++</td>
<td>++</td>
</tr>
<tr>
<td>2017</td>
<td>++</td>
<td>++</td>
<td>++</td>
</tr>
</tbody>
</table>
- **Attack surface** = number of interfaces, features, etc.

- **Network Architecture** = if network access offers access to critical functions

- **Cyber physical** = how much “self-driving” the car is

- more hackable
- less hackable

Miller and Valasek 2014

What is required?

- Special tools?
- Extreme skill?
- Lots of resources?
- Plenty of time?
- How hard is it to find a security problem?
Conclusion

We have to design vehicles for security:

• Secure internal communications with robustness against failing/compromised components

• Ability to deal with malicious external network traffic