Car Connections
Dangerous Liaisons?

Johan Lukkien
Smart mobility, TU/e wide

Cooperative Driving (platooning), A270: Helmond-Eindhoven, 2011
(Mechanical Engineering/TNO)

Full electric: Lupo (ME)

Full Solar: Stella

Strategic Area Smart Mobility
Smart mobility, TU/e wide

- 4X Local controllers for steering, braking, suspension;
- Front and rear IVDC;
- 1X Global IVDC state estimation and supervisory control.

(Semi-)independent developed components by various partners!

Hybrid Innovations for Trucks (HIT) project

Safety-Critical Domain Certification

InMotion, Solar Team, “Cars in Context” TU/e projects

Functional safety methodology (PDEng projects)
Agenda

• Privacy, Safety and Security
• Intelligent Transport Systems overview
  – Communication ‘spheres’
    • within the vehicle
    • inter vehicle: short and long range
• Security in short range communication
  – applications, and architecture
    • US and EU schemes
  – safety, privacy
  – current viewpoints
• Security within the vehicle
• Conclusion and outlook
Video

https://www.youtube.com/watch?v=3jstaBeXgAs
What changed the game?

- *Internet connectivity*: you can reach a vehicle without leaving your chair
  – as opposed to reaching targeted vehicles physically

- *Wireless connectivity*: of many kinds and types

- *Networks in vehicles*: rather open

- *Automation*: computer does the work of breaking codes

- *Tooling*: advanced hacking tooling readily available as ‘condensed knowledge’

- *Sharing, similarity*: one break-in is enough for all similar vehicles

[https://www.youtube.com/watch?v=OobLb1McxnI](https://www.youtube.com/watch?v=OobLb1McxnI)
Privacy, Safety, and Security

• **Privacy**: control over personal information

• **Safety**: freedom from danger or risk on injury resulting from recognized but potentially hazardous events

• **Security**: regulating access to (electronic) assets according to some policy
  – *policy*: allowed and disallowed actions
  – *security mechanisms*: can be regarded as enforcing the policy

• Privacy and safety restrictions result in *security policies*
  – security for privacy and security for safety
Example requirements

• Safety:
  – safety violations by malicious external parties must be prevented (by a policy of forbidding certain actions)
  – safety must be maintained while executing regular functions (functional safety)

• Privacy:
  – personal data must remain under control of the owner

• Leads to *Common Criteria*, *classification of functions* and *development process* (ISO 26262), *certification*

• Sounds rather abstract, so, let’s look at some details....
Vehicles operate using networked ICT

Driver Control

In-car network

Local Control

Local Control

Local Control

Brake-by-wire
In-vehicle networks

- **Networks of ECUs**
  - 40-80 in a modern car
- Designed for
  - cooperative behavior
  - specialist (remote) management / diagnostics
- **Gateway support for isolation**

BMW 7 series infrastructure
Vehicles become parts of a larger whole
A conceptual view of ITS

- Example data flows:
  - (1) gather detailed driving data to determine
    • local weather
    • road condition
  - (2) accident prevention by direct intervention
  - (3),(4) informing driver about upcoming road conditions

- Example data flows:
  - Accident prevention
  - In-car network
  - Internet, V2I
  - V2V network
  - Congestion control
  - Road maintenance
  - Environment control
  - And whatever sensing you can think of...

- Example data flows:
  - Example: gather detailed driving data to determine
    • local weather
    • road condition
  - Example: accident prevention by direct intervention
  - Example: informing driver about upcoming road conditions

- Example data flows:
  - Example: gather detailed driving data to determine
    • local weather
    • road condition
  - Example: accident prevention by direct intervention
  - Example: informing driver about upcoming road conditions
A more detailed view on V2V/V2I
<table>
<thead>
<tr>
<th>Scenario and warning type</th>
<th>Scenario example</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Rear end collision scenarios</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Forward collision warning</strong>&lt;br&gt;Approaching a vehicle that is decelerating or stopped.</td>
<td><img src="image1" alt="Forward Collision Warning" /></td>
</tr>
<tr>
<td><strong>Emergency electronic brake light warning</strong>&lt;br&gt;Approaching a vehicle stopped in roadway but not visible due to obstructions.</td>
<td><img src="image2" alt="Emergency Electronic Brake Light Warning" /></td>
</tr>
<tr>
<td><strong>Lane change scenarios</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Blind spot warning</strong>&lt;br&gt;Beginning lane departure that could encroach on the travel lane of another vehicle traveling in the same direction; can detect vehicles not yet in blind spot.</td>
<td><img src="image3" alt="Blind Spot Warning" /></td>
</tr>
<tr>
<td><strong>Do not pass warning</strong>&lt;br&gt;Encroaching onto the travel lane of another vehicle traveling in opposite direction; can detect moving vehicles not yet in blind spot.</td>
<td><img src="image4" alt="Do Not Pass Warning" /></td>
</tr>
<tr>
<td><strong>Intersection scenarios</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Blind intersection warning</strong>&lt;br&gt;Encroaching onto the travel lane of another vehicle with whom driver is crossing paths at a blind intersection or an intersection without a traffic signal.</td>
<td><img src="image5" alt="Blind Intersection Warning" /></td>
</tr>
</tbody>
</table>

Source: GAO analysis of Crash Avoidance Metrics Partnership information.

from: Vehicle-to-Vehicle Communications: Readiness of V2V Technology for Applications, NHTSA, August 2014
How does this work?

• It is cooperative, dynamic and ad-hoc

• Two different approaches, same network technology (IEEE 802.11p)
  – **EU**: ETSI TC ITS standards, using Geo-networking

• Essentially: vehicles emit *periodically* or *event-driven* status information
  – called *Basic Safety Messages* (BSM, US)
  – and *Cooperative Awareness Messages* (CAM, EU)
Some application examples (BSM ~SAE J2735)

<table>
<thead>
<tr>
<th>Apps.</th>
<th>Comm.type</th>
<th>Freq.</th>
<th>Latency</th>
<th>Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lane Change Warning</td>
<td>V2V, periodic, P2M</td>
<td>10Hz</td>
<td>100ms</td>
<td>150m</td>
</tr>
<tr>
<td>Collision Warning</td>
<td>V2V, periodic, P2M</td>
<td>10Hz</td>
<td>100ms</td>
<td>150m</td>
</tr>
<tr>
<td>Emergency Brake Lights</td>
<td>V2V, event-driven, P2M</td>
<td>10Hz</td>
<td>100ms</td>
<td>300m</td>
</tr>
<tr>
<td>Pre-Crash Sensing</td>
<td>V2V, event-driven, P2P</td>
<td>50Hz</td>
<td>20ms</td>
<td>50m</td>
</tr>
<tr>
<td>Stop Sign Assists</td>
<td>I2V and V2I, periodic</td>
<td>10Hz</td>
<td>100ms</td>
<td>250m</td>
</tr>
<tr>
<td>Left Turn Assistance</td>
<td>I2V and V2I, periodic, P2M</td>
<td>10Hz</td>
<td>100ms</td>
<td>300m</td>
</tr>
<tr>
<td>Traffic Signal Violation</td>
<td>I2V, periodic, P2M</td>
<td>10Hz</td>
<td>100ms</td>
<td>250m</td>
</tr>
<tr>
<td>Curve Speed Warning</td>
<td>I2V, periodic, P2M</td>
<td>1Hz</td>
<td>1s</td>
<td>200m</td>
</tr>
</tbody>
</table>

Eight high priority vehicle safety applications as chosen by NHTSA and VSCC.

VSCC – Vehicle Safety Communication Consortium of CAMP (Crash Avoidance Metrics Partnership)

V2V = Vehicle to Vehicle
P2M = Point to Multipoint
I2V = Infra structure to Vehicle
(partial) Communication Stack: EU and US

Rate-adaptation Based Congestion Control for Vehicle Safety Communications, PhD thesis Tessa Tielert
Security to protect safety in BSM

• A vehicle could perform a (physical) action upon receiving certain messages. This response must be on good grounds, and safe.
  – authentication: does this message really come from
    • that particular car?
    • the car left behind me?
  – authorization: what is allowed
    • by this party?
    • by this message?
  – integrity: was this message not tampered with?

• Further concerns regarding safety:
  – are messages really delivered (and not lost or jammed)?
  – functional safety
    • maintain safe and responsive behavior while executing normal functions
Security to protect privacy in BSM

• Communication might reveal sensitive information
  – location of vehicle, one could track it
  – driver identity, number of passengers
  – driving behavior

• Security mechanisms might add to this
  – e.g. the *signing* of messages reveals the signature

• Hence:
  – policies for data handling, certification of those policies
    • e.g. collect only anonymous data, forbid vehicle tracking in mandatory services
  – requirements on security mechanisms
Requirements on security

• Interoperable
• Process-able in real-time and limited in size (bandwidth)
• Identity-free
• Non-repudiation (sender cannot deny having sent a message)

• Scalable
  – local: few hundreds of vehicles
  – global: millions of vehicles

• Extensible, towards other applications of V2x communication
Proposal (US)

- Use **Public Key Infrastructure** to *sign* messages
  - authentication, integrity & non-repudiation

- **Certificate** associates public and private key
  - decryption using the public key demonstrates:
    - that the sender knows the private key, which is associated with an identity by an authority
    - and that the message was not altered

- Complex extensions to deal with the specific concerns of these applications
  - intermittent connectivity, anonymity
  - small size keys and certificates: ECQVIC / ECDSA
    - though these require 10 times more processing power
System outline

- Security Credentials Management System
- Comparison: basic PKI / V2x design

from: Vehicle-to-Vehicle Communications: Readiness of V2V Technology for Applications, NHTSA, August 2014
Zooming in....

- Security concerns *within* the vehicle....
Hacker with access to internal systems

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

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

- Connecting notebook to CAN bus
- Funny or dangerous, but any harmful hack is possible ...
  - e.g. disabling the brakes
- ... since *any* malicious physical access is dangerous
When CAN access meets Internet...

https://www.youtube.com/watch?v=MK0SrxBBC1xs
Increasing wireless connections ... and vulnerabilities

- hacking *without* altering the electronics

https://www.youtube.com/watch?v=OobLb1McxnI
The drill...

- Attach a module to the CAN bus in order to send and receive control messages and connect to a wireless transceiver

  OR

  hack into the car via the Internet with the same effect

- Reverse engineer the messaging of this type of car

- Control the car via remote access
What to do about this?

- **Protect CAN bus**
  - access control for new CAN devices
  - CAN message signing and encryption
  - ... but who has the keys?

- **Physical separation** – make harmful influence from new components physically impossible

- **Policy separation**
  - implement policies that restrict behavior in certain modes
    - no remote access while driving
    - software update only under specific circumstances, e.g., in a car shop
    - (expose certain behavior while being examined)

- **Self monitoring** – intrusion detection
What about privacy?

- Policies about what to collect, communicate, store, e.g.,
  - collect only anonymous data
  - forbid vehicle tracking in mandatory services (e.g. road side)
  ... plus certification of these, access tracing, auditing

- A radically different approach to managing data
  - a personal data store where data about a person is stored under his control
    - no storage in private repositories of companies
Next Generation Vehicle OS...
Adjust design methods

- Attack model becomes more complex:
  - obtaining a virus during a repair
  - downloadable apps
  - all mentioned solutions introduce new vulnerabilities

- This has to become part of the systematic consideration of the safety of all (ICT) functions
  - ISO 26262
ISO 26262: functional safety

• Safety under performing normal functions
  – avoid excessive risk of normal functions
  – examine – and deal with – common failures [fault $\rightarrow$ error $\rightarrow$ failure]

• Explicit ‘safety life cycle’ for automotive products

• ‘Safety goals’ classified in risk classes, are determined for each ‘hazardous event’
  – risk class: ASIL, Automotive Safety Integrity Class
    • QM, ASIL A-D, order of magnitude of risk
    • combination of severity, exposure, controllability
      – e.g S3, E4, C3: life threatening, highly probable, difficult to control (ASIL D)

• Adherence to ISO 26262 expected to increase
Concluding remarks

• Security in ITS serves privacy and safety
• Security between vehicles is being designed in
• Security within the vehicle is lagging behind but catching up
  – the attack model is better understood
  – at least enforce the requirement of a per-vehicle physical contact
    (avoid Internet-style hacking of classes of vehicles)

• ITS is a required step towards fully automated driving
Literature

• Used in this presentation (a.o.):
  – Vehicle-to-Vehicle Communications: Readiness of V2V Technology for Applications, NHTSA, August 2014
  – Rate-Adaptation Based Congestion Control for Vehicle Safety Communications, PhD thesis Tessa Tielert

• Documentation from recent EU projects
  – e.g. Converge
  – DG Mobility and Transport