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
Possible Applications

• Better driver and owner experience
  – Mobile phone used to access vehicle (locks, status, position, alarm, …)
  – Platooning (car trains), Remote diagnostics, Remote software updates
  – Buy additional functionality when needed

• Services unique to the driver
  – Insurance based on driver and driver’s behavior
  – Automatically pay road tolls and parking fees
  – Vehicle’s functionality follows the driver (3rd party software, horse power, …)

• Traffic optimization:
  – Exchange of information about congestion, optimal speed, …

• Safety enhancing [v2v, v2i]
  – Traffic light conditions, stop signs, speed limits
  – Lane change support, detection of hidden vehicles, …
  – Road condition reports (anonymous reporting)

• Commercial third party applications

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)
Risks and Consequences

• Execution of arbitrary code
  – After successful impersonation of other entities or intrusion to vehicle
  – Update ECU with modified software
  – Any function can be affected, at any time

• Disclosure of information
  – Impersonation of vehicles, drivers, road-side objects, ...
  – Gain access to private data (location, driver style)

• Denial of service
  – Attacks against vehicles, road-side objects, repair shops, etc.
  – Cause software updates to fail, diagnostics to report incorrect values
  – Make a complete fleet of vehicles grounded

Internet tracking of (marine) traffic

![Internet tracking of (marine) traffic](image)
Internet tracking of (marine) traffic

Do we want to see this type of app for our cars?

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
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 and 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
- Real-time constraints
- Fault tolerance and dependability aspects
SECURING INTERNAL COMMUNICATIONS

The CAN network (1990-)

- Any node can send any type of message
- Messages visible to all nodes
- Message type select receiver(s) and priority
- Up to 1 Mbps, ISO standard 2003
- Security: password to reprogram ECUs
Spoofing commands on the CAN bus

<table>
<thead>
<tr>
<th>Time</th>
<th>Dno</th>
<th>ID</th>
<th>Name</th>
<th>Sendnode</th>
<th>Dx</th>
<th>DLC</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.000710</td>
<td>1</td>
<td>0</td>
<td>Central Locking System State</td>
<td>MUT</td>
<td>Tx</td>
<td>1</td>
<td>00</td>
</tr>
<tr>
<td>~ AntiTheftSystemActive</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>~ LockState Unlocked</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12.000844</td>
<td>1</td>
<td>32</td>
<td>Vehicle Motion</td>
<td>MUT_Driver</td>
<td>Tx</td>
<td>3</td>
<td>00 00 02</td>
</tr>
<tr>
<td>~ Engine Running</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>~ Crash Detected</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>~ Velocity</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12.000520</td>
<td>1</td>
<td>64</td>
<td>Windows State</td>
<td>MUT</td>
<td>Tx</td>
<td>2</td>
<td>00 00</td>
</tr>
<tr>
<td>~ Window Position</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>~ Window Not Moving</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12.000322</td>
<td>1</td>
<td>65</td>
<td>Window Control</td>
<td>MUT_Driver</td>
<td>Tx</td>
<td>1</td>
<td>00</td>
</tr>
<tr>
<td>~ Key Down</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>~ Key Up</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12.000406</td>
<td>1</td>
<td>1</td>
<td>Locking Diesel Control Request</td>
<td>MUT_Driver</td>
<td>Tx</td>
<td></td>
<td></td>
</tr>
<tr>
<td>~ Lock Request Request Unlock</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Threats to internal security

- Compromised ECUs send arbitrary messages
  - Both to other ECUs and to external services
- CAN opener
  - Access to the bus from the outside allows attackers to open doors, start engine, inject traffic, ...
- Sniffing internal network
  - Copy firmware for other models
  - Copy keys shared between ECUs to falsify messages
- Cryptographic key sharing
  - Like “card sharing” for cable/satellite TV
  - One owner pays for a service many share
Internal gateways separate traffic

http://www.evita-project.org

**AUTomotive Open System ARchitecture**

- **AUTOSAR**
  http://www.autosar.org

- An operating system
  – Hides hardware and communication details for applications

- Standard for future software development

- Complex
SECURING EXTERNAL COMMUNICATIONS
V2X communication protocols

- **IEEE 1609 (WAVE)** for short range communications
- **WSMP = Wave Short Message Protocol** for broadcasted V2X communications
- **IEEE 802.11p** for physical (PHY) and link (MAC) layers
  - Uses DSRC band (5.9 GHz)
  - 27 Mbps in 7 dedicated channels
  - No security (802.11a authentication too slow)
Proposed security mechanisms

• X509v3 Certificates expected to be used for authentication

• But CRLs are complicated
  – Lists very long (world wide?), many issuers, very short time to verify
  – In highly populated areas, traffic may be high, > 100 msgs/sec
  – Certificate delivery to all new nodes consumes bandwidth

• Anonymous certificates (pseudonyms) must be issued
  – Short lived, used to not reveal real identity to other vehicles
  – MAC addresses and IP addresses may reveal vehicle

• Hardware Security Modules (HSMs)
  – Store private keys, possibly also a random number generator and a clock
  – Contain functionality to sign and encrypt messages
  – Can distribute session keys to ECUs
  – Evita project: Three different levels of HSMs (full, medium, light)

• ITS (Intelligent Transport System) station functionality defined by ETSI
  – Reference architecture describes required functionality
  – Standardized node for all V2X communications, for hosts, gateways, routers, ...

Summary

• Complicated problem, many parties involved

• Many limitations when implementing security
  – Cost, power, processing capabilities, memory, real time requirements, fault tolerance, reliability

• Internal communications
  – Buses contain no security
  – Gateways may get FW functionality
  – HSMs may offer internal encryption and signing of messages

• External communications
  – Ad hoc communications with certificates
  – Requires CRLs, may be too long, takes time do download
  – Pseudonyms to preserve vehicle identity