Overview of Automotive Security

Betty HC Cheng

Acknowledgements: Tito Mitra, Pieter Hartel
Automotive Security Concerns

http://youtu.be/MK0SrxBC1xs

http://youtu.be/MK0SrxBC1xs
Approach

• Key Cybersecurity Challenges:
  • Prevention
  • Detection
  • Mitigation

• Competing Concerns:
  • Safety
  • Information Access (e.g., “Internet of Things”)
  • Heterogeneity of Systems and Stakeholders

• Multidisciplinary Strategies:
  • Leverage enabling technologies from other disciplines (e.g., biology, AI, control theory, etc.)
  • Collaborate with other disciplines for a more holistic systems approach to address cybersecurity and safety

Risk Assessment

• Three questions to answer:
  – What am I trying to protect?
  – What do I need to protect against?
  – How much time, effort and money am I willing to expend to obtain adequate protection?

• Three key steps:
  – Identify assets
  – Identify threats
  – Calculate risks
Broad Categories of Threats

- **Interruption**
  - E.g., DOS attacks

- **Interception**
  - E.g., monitoring/copying of data

- **Modification**
  - E.g., virus, remove/change data

- **Fabrication**
  - E.g., generate fake data

Addressing Automotive cybercrime

- **Vehicle network architecture:**
  - Designed for safety rather than security.
  - Various target hardening implementation difficult (e.g., encryption)

- **Real time performance:**
  - Performance concerns impedes implementation of SCP-based strategies

- **Dynamic and situational nature of automotive domain:**
  - Vehicles are dynamic entities that pass through or are present in various environments/contexts
  - This pre-empts surveillance to a large extent.

- **Awareness issues:**
  - Threat to automotive entities is not yet widely understood/recognized by the general populace who are the primary user/potential target of the cyber threats.

- **Lack of non-repudiation:**
  - A major deterrence to crimes is exposure.
  - Automotive software lacks any effective logging or surveillance.
Challenges with Cybersecurity Solutions

- **Non-familiarity with incidents:**
  - Due to yet lack of voluminous data on perpetrated crimes, it is difficult to identify motives and subsequently put in place mechanisms to address them.

- **Research focus:**
  - Research to tackle automotive cybercrimes is still nascent.
  - Research towards prevention is still emerging

- **Standardization:**
  - Any progress on application of SCP would entail some amount of standardization of mechanism/equipment among OEM manufacturers.

- **Cost and adherence to standard practice:**
  - A major part of solutions prescribed may include a cost escalation
  - Adherence to some practice that may not be palatable to/strictly followed by end users.

### Threat Surfaces

<table>
<thead>
<tr>
<th>COMPONENT</th>
<th>SURFACE</th>
<th>THREAT TYPE</th>
</tr>
</thead>
</table>
| OBD-2 Port | • Direct Access  
• Access via pass-thru device | • Interception  
• Interruption  
• Modification  
• Fabrication |
| Key-Fob* | • Duplicate RFID chips | • Interception  
• Fabrication  
• Theft |
| Media Player & Auxiliary port (e.g. - audio jack or USB port) | • Connected media (e.g. Memory stick, iPods, CD etc) | • Interruption  
• Fabrication |
| Dealer Pass-thru device | • Connected service computer/device | • Interruption  
• Modification |
## Threat Surfaces (cont.)

<table>
<thead>
<tr>
<th>COMPONENT</th>
<th>SURFACE</th>
<th>THREAT TYPE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Telematics Unit</td>
<td>• Compromised software</td>
<td>• Interception</td>
</tr>
<tr>
<td></td>
<td>• Compromised connecting device</td>
<td>• Interruption</td>
</tr>
<tr>
<td></td>
<td>• Interception</td>
<td>• Modification</td>
</tr>
<tr>
<td>Vehicle Bluetooth Network</td>
<td>• Network PIN breakage by proximal device</td>
<td>• Interception</td>
</tr>
<tr>
<td></td>
<td>• Interruption</td>
<td></td>
</tr>
<tr>
<td>ECU*</td>
<td>• Duplicate/malicious non OEM component</td>
<td>• Modification</td>
</tr>
<tr>
<td></td>
<td>installation</td>
<td>• Interruption</td>
</tr>
<tr>
<td></td>
<td>• Fabrication</td>
<td></td>
</tr>
<tr>
<td>Tire Pressure Monitoring</td>
<td>• Intercept broadcast of readings to Dashboard</td>
<td>• Interruption</td>
</tr>
<tr>
<td>System</td>
<td>cluster</td>
<td>• Fabrication</td>
</tr>
<tr>
<td></td>
<td>• Interception</td>
<td></td>
</tr>
</tbody>
</table>

---

## Introduction to General Cybersecurity: Foundations and Pragmatics

Kira Chan