German OWASP Day 2016
CarIT Security: Facing Information Security Threats

Tobias Millauer
# Daimler – Business Units

<table>
<thead>
<tr>
<th>Business Unit</th>
<th>Revenues</th>
<th>Employees</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mercedes-Benz Cars</td>
<td>€ 83.8 bn</td>
<td>136,941</td>
</tr>
<tr>
<td>Daimler Trucks</td>
<td>€ 37.6 bn</td>
<td>86,391</td>
</tr>
<tr>
<td>Mercedes-Benz Vans</td>
<td>€ 11.5 bn</td>
<td>22,639</td>
</tr>
<tr>
<td>Daimler Buses</td>
<td>€ 4.1 bn</td>
<td>18,147</td>
</tr>
<tr>
<td>Daimler Financial Services</td>
<td>€ 19.0 bn</td>
<td>9,975</td>
</tr>
</tbody>
</table>

2015
Daimler – 284,000 employees worldwide

Status 31.12.2015

North America (incl. Mexico) 33,040
Europe 208,230
South- and Central America 14,450
Asia 21,740
Africa 5,500
Rest of Europe 37,770
Australia 1,060

Daimler AG
Daimler – IT: 24x7x365

- Present on 6 continents
- More than 500 sites cross linked
- IT services for 284,000 employees
- 9,136 locations in focus
  - 41 Daimler group branches,
  - 61 production locations,
  - 9,034 distribution locations
The Connected Car
The relationship of objects in a security chain

- **Threat**
  - Exploits (Risk scenario)
- **Security vulnerability**
  - Occurrence of
- **Security event**
  - Classified as
- **Security incident**

Exposes

Implications on security (and safety)

Asset
Self-improvement for security leaders

Self-improvement for security leaders: Enterprise security professionals need to communicate more effectively about the things that matter most.

- **Enablement, Risk**
- **Compliance, Cost**

Effectiveness of communicating

High

Strategic business value provided by information security

Low

Self-improvement imperative for enterprise security leaders

STRIDE Threat Model

S – Spoofing  Authentication
T – Tampering  Integrity
R – Repudiation  Non-Repudiation
I – Information disclosure  Confidentiality
D – Denial of service  Availability
E – Elevation of privilege  Authorization
HEAVENS Security Model

Security Attributes
- Confidentiality
- Integrity
- Availability
- Authenticity
- Authorization
- Non-repudiation
- Privacy
- Freshness

Security Objectives
- Operational
- Safety
- Privacy
- Financial
- Legislations

Impact

https://www.sp.se/en/index/research/dependable_systems/heavens/sidor/default.aspx
STRIDE Threat Model + HEAVENS Security Model

S – Spoofing
Authentication, *Freshness*

T – Tampering
Integrity

R – Repudiation
Non-Repudiation, *Freshness*

I – Information disclosure
Confidentiality, *Privacy*

D – Denial of service
Availability

E – Elevation of privilege
Authorization
Vehicle Cybersecurity

- **Protective/preventive measures and techniques**
  These measures, such as isolation of safety-critical control systems networks or encryption, implement hardware and software solutions that lower the likelihood of a successful hack and diminish the potential impact of a successful hack.

- **Real-time intrusion (hacking) detection measures**
  These measures continually monitor signatures of potential intrusions in the electronic system architecture.

- **Real-time response methods**
  These measures mitigate the potential adverse effects of a successful hack, preserving the driver's ability to control the vehicle.

- **Assessment of solutions**
  This involves methods such as information sharing and analysis of a hack by affected parties, development of a fix, and dissemination of the fix to all relevant stakeholders.
Cybersecurity Best Practices for Modern Vehicles

- Vehicle Development Process With Explicit Cybersecurity Considerations
- Vulnerability Reporting/Disclosure Policy
- Vulnerability / Exploit / Incident Response Process
- Self-Auditing (Risk Assessments, Penetration Tests, Organizational Decisions)
- Fundamental Vehicle Cybersecurity Protections (see Details)
- Leadership Priority on Product Cybersecurity
<table>
<thead>
<tr>
<th>Security threat severity class</th>
<th>Safety</th>
<th>Privacy</th>
<th>Financial</th>
<th>Operational</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>No injuries.</td>
<td>No authorized access to data.</td>
<td>No financial loss.</td>
<td>No impact on operational performance.</td>
</tr>
<tr>
<td>1</td>
<td>Light or moderate injuries.</td>
<td>Anonymous data only (no specific driver of vehicle data)</td>
<td>Low-level loss.</td>
<td>Impact not discernible to driver.</td>
</tr>
<tr>
<td>3</td>
<td>Life threatening or fatal injuries. / Serve injuries for multiple vehicles.</td>
<td>Driver or vehicle tracking. Identification of driver or vehicle, for multiple vehicles.</td>
<td>Heavy loss. / Moderate losses for multiple vehicles.</td>
<td>Significant impact on performance. / Noticeable impact for multiple vehicles.</td>
</tr>
<tr>
<td>4</td>
<td>Life threatening or fatal injuries for multiple vehicles.</td>
<td>Driver or vehicle tracking for multiple vehicles.</td>
<td>Heavy losses for multiple vehicles.</td>
<td>Significant impact for multiple vehicles.</td>
</tr>
</tbody>
</table>
Information Security Risk Management Treatment Strategy

https://www.owasp.org/images/9/96/ThreatMatrix_medium.png
"Doc, I'm gonna keep eating cheeseburgers until I have a heart attack. Then we'll deal with it." - Wendy Nather