Cyber Security support to the HumanDrive Project

13\textsuperscript{th} Dec 2018

Luigi Bisbiglia
Business Development Manager

SBD Automotive Ltd
Using machine learning to develop natural, human like vehicle control

- ‘Grand Drive’ will be an end-to-end journey of around 200 miles including Motorway, A-Road and Country Road driving
- Using Machine Learning and AI to provide human-like control
- Research into human driving behaviour using physical vehicles and simulator
- Transport Systems Catapult and Horiba MIRA responsible for the Safety Work Package
- Cyber Security covered by a separate Work Package
SBD’s Cyber Support Package

- Analysis of public hacks
- New product and technology tracking
- New standards and guidelines
- Competitor activity
- Knowledge sharing

- Threat modelling for security requirements and design reviews
- Penetration testing
- Risk assessment (analysis of results, remediation and risk rating)

- Objective setting
- Design process improvement
- Cyber roadmap
- Incident response planning
- Training
- Supplier evaluation

Using machine learning to develop
natural, human like
vehicle control
SAE Definitions

1. NO AUTOMATION
2. DRIVER ASSISTANCE
3. PARTIAL AUTOMATION
4. CONDITIONAL AUTOMATION
5. HIGH AUTOMATION
6. FULL AUTOMATION

EXAMPLE
- Lane Departure Warning
- Adaptive Cruise Control
- Automatic Parking Assist
- Piloted Driving (Driver fall-back)
- Piloted Driving+ (System fall-back)
- Robot Taxi

Using machine learning to develop
natural, human like vehicle control
<table>
<thead>
<tr>
<th>SAE Levels</th>
<th>Key in-car architecture characteristics</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Level 0</strong></td>
<td></td>
</tr>
</tbody>
</table>
| “Legacy architecture”| • Piece meal implementation  
• Very few ADAS available, developed as a stand alone solution  
• No sensor fusion (sensor hardwired to ECU, not networked) and no actuators involved  
• Mainly CAN technology |
| **Level 1**          |                                                                                                         |
| “Carry-over architecture”| • Piece meal implementation  
• A few stand-alone ADAS  
• When there is actuation (e.g. braking), the ADAS ECU is usually on the same network as the actuator  
• Mainly CAN technology |
| **Level 2**          |                                                                                                         |
| “Primitive ADAS architecture”| • Dedicated ADAS network  
• Primitive / localised sensor fusion taking place (front sensing with rear facing). Some sensors are networked  
• FlexRay technology introduced  
• Ethernet used for 360 all round view  
• Some features communicate with key fob / smartphone |
| **Level 3**          |                                                                                                         |
| “Semi autonomous architecture”| • Dedicated ADAS domain to support sensor fusion on a much larger scale  
• Sensor fusion partitioned in domains  
• GPS / map data becomes a sensor that needs regular update  
• Communication with key fob / smartphone  
• FlexRay and Ethernet standard |
| **Level 4**          |                                                                                                         |
| “Full autonomous architecture”| • Dedicated ADAS domain to support full sensor fusion (Forward, Rear, All Around)  
• GPS / map data need near “real-time” update & high definition  
• Communicate with key fob / smartphone  
• OTA download and connected services (including Artificial intelligence)  
• FlexRay and Ethernet standard |
| **Level 5**          |                                                                                                         |
| “Driverless architecture”| • Same as for level 4 but with more sensors to accommodate all types of road, weather and lighting environment. |
Layer 3 and above layers architecture

Cloud layer

Sensors layer

Human Machine Interface layer

Vehicle Data layer

Actuators layer

Using machine learning to develop natural, human like vehicle control
Representative Electrical Architecture
STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service and Elevation of Privilege) is a threat modelling approach developed by Microsoft and it is currently considered the most applicable method for the automotive industry because it:

• Is a threat centric approach
• Provides a structured approach of categorising threats
• Enables direct mapping with system’s elements and security attributes

- **Spoofing**
  - Attempt to gain access to a system by using a false identity
  - Unauthorised modification of data

- **Tampering**
  - Ability of users to deny that they performed specific actions
  - Unwanted exposure of data

- **Repudiation**
  - Process of making a system unavailable to legitimate users
  - User with limited privileges gains access to restricted application

- **Information Disclosure**
  - User with limited privileges gains access to restricted application
  - Unauthorised modification of data

- **Denial of Service**
  - User with limited privileges gains access to restricted application
  - Ability of users to deny that they performed specific actions

- **Elevation of Privilege**
  - Process of making a system unavailable to legitimate users
  - Unauthorised modification of data
Reference: Who are the Hackers?

- Depending on hackers/hacker groups, targets can be different. Therefore attacking techniques and equipment are also different.

- Hactivists: Make Political Statements
- Cyber Criminal: Financial gain, Cyber Warfare
- Disgruntled ex-employees: Revenge
- State Hackers: Espionage
- Script Kiddies: Fun and Fame, Avoid paying
- Spy Hackers: Corporate Espionage
Defining the Actors Environment

Good Actors
Bad Actors
Actors that can be both good and bad

Using machine learning to develop
natural, human like
vehicle control
### Representative Abuse Stories

- User stories is a method for capturing high-level system functional requirements. The user stories are generated by the system stakeholders.

- User stories captured for malicious Actors can help in identifying potential system misuse or exploitation, at a high level.

- User stories written for intended Actors can help in identifying the functions that need protecting and the required interactions between the intended Actors.

<table>
<thead>
<tr>
<th>Case #</th>
<th>Actor</th>
<th>I Want</th>
<th>So That</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Bitcoin Miner</td>
<td>Use ability of ECUs</td>
<td>Get more bitcoin</td>
</tr>
<tr>
<td>2</td>
<td>Academic Researcher/Cyber Criminal</td>
<td>Spoof the system</td>
<td>Get private information from vehicle</td>
</tr>
<tr>
<td>3</td>
<td>Service Provider</td>
<td>Patch the vehicle but ignore some of them</td>
<td>Have this customer back and get more money</td>
</tr>
<tr>
<td>4</td>
<td>Vehicle Owner</td>
<td>Block the entrance parking</td>
<td>Annoy my neighbours</td>
</tr>
<tr>
<td>5</td>
<td>Vehicle Owner</td>
<td>Cheat after cars into giving ways</td>
<td>He can drive faster</td>
</tr>
<tr>
<td>6</td>
<td>Professional Hacker</td>
<td>Hack into the car</td>
<td>Ransom it to their owners</td>
</tr>
<tr>
<td>7</td>
<td>Competitor</td>
<td>Cause delays (jam) in some roads</td>
<td>Gain advantage/value</td>
</tr>
<tr>
<td>8</td>
<td>Criminal</td>
<td>Follow another vehicle</td>
<td>Do criminal activities</td>
</tr>
<tr>
<td>9</td>
<td>Criminal</td>
<td>Other CAV crash into my own</td>
<td>Get money</td>
</tr>
<tr>
<td>10</td>
<td>Criminal</td>
<td>Use Autonomous Car</td>
<td>Transport illicit goods</td>
</tr>
<tr>
<td>11</td>
<td>Terrorist</td>
<td>Use Autonomous Car</td>
<td>Damage traffic</td>
</tr>
<tr>
<td>12</td>
<td>Professional Hacker</td>
<td>Spoof signs</td>
<td>Change vehicle behaviour</td>
</tr>
<tr>
<td>13</td>
<td>OCA (Organise Crime Agent)</td>
<td>Data mining - sell products on web</td>
<td>Can get profit</td>
</tr>
<tr>
<td>14</td>
<td>OEM</td>
<td>Gather data to sell</td>
<td>Get money</td>
</tr>
<tr>
<td>15</td>
<td>Competitor</td>
<td>Develop new exciting products</td>
<td>Seize the market</td>
</tr>
<tr>
<td>16</td>
<td>Pranker</td>
<td>Direct traffic</td>
<td>Make giggles</td>
</tr>
<tr>
<td>17</td>
<td>OEM</td>
<td>Highlight deficiencies in system</td>
<td>Gan greater market sharing</td>
</tr>
<tr>
<td>18</td>
<td>Attacker/Terrorist</td>
<td>Remotely control cars</td>
<td>Commit a terrorist attack</td>
</tr>
<tr>
<td>19</td>
<td>Professional Hacker</td>
<td>Control the vehicle</td>
<td>Do the DDoS attack to others</td>
</tr>
</tbody>
</table>
Defence In Depth
Defence in Depth

1. Off-board Interfaces
   - Remote control app
   - Customer/dealer portal

2. On-board Interfaces
   - Wireless (cellular, Wi-Fi, BT, etc.)
   - Wired (OBD, USB, HDMI, etc.)

3. Inter-network
   - Secure gateway
   - Message filtering

4. Intra-network
   - ECU-ECU communications
   - Sensor – ECU communications

5. ECU level
   - Secure reprogramming
   - Secure boot

Most OEMs currently focused on levels 2 & 3

Leading OEMs starting to implement levels 4 & 5
HumanDrive Consortium

http://humandrive.co.uk

Richard.Hillman@ts.catapult.org.uk

Using machine learning to develop
natural, human like vehicle control