Frost & Sullivan Cybersecurity Presentation

2015 will be the Year of Security, Prognostics & Evolution of OEM Vehicle Automation Strategies

Praveen Narayanan
Research Manager

Feb 2015
Key Trends Impacting the Infotainment Market to 2020
Trends ranging from OTA updates to level 3 automation to predictive analytics all require a very high level of in-car and back end security.

- Connectivity: Including Embedded LTE & Tethered
- Software & Analytics Capabilities: Major Tier 1 Threat
- CD & Navigation: Less Infotainment, Apple & Google Interfaces
- Mobility Offerings: Evolution of Connected Services
- Output and Input: HMI Innovations, Gestures & AR HUD
- Wireless OTA Updates: Software and Firmware Updates
- In-Car Security: Focus on preventing cyber attacks
- Influence of Connected Living: Infotainment will be Personalized
- Influence of Vehicle Automation: Content & Output
- High End Graphics: Changing Central and ICD Display
## OEM Activities in the Connected Space
Almost every OEM in the US has a connected telematics service – another key area that is currently the first point of attack for hackers

<table>
<thead>
<tr>
<th>OEM</th>
<th>Telematics Service</th>
<th>Connectivity</th>
<th>Free Trial Period</th>
<th>Features</th>
</tr>
</thead>
<tbody>
<tr>
<td>General Motors</td>
<td>OnStar</td>
<td>Embedded LTE – AT&amp;T</td>
<td>6-12 Months/5 Years</td>
<td>Safety, security, diagnostics, mileage-based insurance</td>
</tr>
<tr>
<td>Ford</td>
<td>SYNC</td>
<td>Tethered</td>
<td>3 Years</td>
<td>Vehicle health report, 911 Assist</td>
</tr>
<tr>
<td>Chrysler</td>
<td>UCONNECT Access</td>
<td>Embedded 3G – Sprint</td>
<td>6/12 Months</td>
<td>911 Assist, breakdown assistance, vehicle tracking, remote start/unlocking</td>
</tr>
<tr>
<td>Audi</td>
<td>Audi Connect</td>
<td>Embedded LTE – AT&amp;T</td>
<td>6 Months</td>
<td>Google connected services, smart parking (no telematics)</td>
</tr>
<tr>
<td>BMW</td>
<td>Assist</td>
<td>Embedded 3G</td>
<td>10 Years</td>
<td>ACN, 911 Assist, breakdown assistance, condition-based maintenance alerts</td>
</tr>
<tr>
<td>VW</td>
<td>Car-Net</td>
<td>Embedded 2G - VZ Telematics</td>
<td>6 Months</td>
<td>Safety, security, diagnostics, vehicle health reports, maintenance alerts</td>
</tr>
<tr>
<td>Hyundai</td>
<td>Bluelink</td>
<td>Verizon</td>
<td>3 Years</td>
<td>ACN, 911 Assist, breakdown assistance, vehicle tracking, recall alerts, critical fault notification, maintenance alerts, in-vehicle service scheduling, etc.</td>
</tr>
<tr>
<td>Kia</td>
<td>UVO</td>
<td>Tethered</td>
<td>Lifetime</td>
<td>Vehicle health reports, maintenance alerts, critical fault notifications</td>
</tr>
<tr>
<td>Mercedes</td>
<td>Mbrace 2</td>
<td>VZ Telematics</td>
<td>3-6 Months</td>
<td>Traditional safety and security services</td>
</tr>
<tr>
<td>Volvo</td>
<td>On Call</td>
<td>Embedded 3G – AT&amp;T</td>
<td>3 Years</td>
<td>Safety, security and remote link app</td>
</tr>
<tr>
<td>Nissan</td>
<td>Nissan Connect</td>
<td>Tethered</td>
<td>NA</td>
<td>Only connected apps such as a Pandora, etc.</td>
</tr>
<tr>
<td>Honda</td>
<td>HondaLink</td>
<td>Tethered</td>
<td>NA</td>
<td>911 Assist only</td>
</tr>
<tr>
<td>Tesla</td>
<td>NA</td>
<td>Embedded 3G- AT&amp;T</td>
<td>3-12 Months</td>
<td>No core telematics feature</td>
</tr>
</tbody>
</table>

Source: Frost & Sullivan.
ADAS Market Outlook to 2020 – Six Fold Growth

Growth in the market for ADAS by 2020 is backed largely by mass-market OEMs while innovation is expected to keep European OEMs ahead of the curve.

Note: All figures are rounded. The base year is 2012. Source: Frost & Sullivan
## Requirements for Various Levels of Vehicle Automation

The leap from semi- to highly-automated is fairly easy to accomplish as driver override exists; the leap to fully-automated driving requires artificial intelligence to replace the human driver.

<table>
<thead>
<tr>
<th>Level of Automation</th>
<th>Assistance</th>
<th>Semi-automated</th>
<th>Highly Automated</th>
<th>Fully Automated</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adaptive headlamp control</td>
<td>Optional</td>
<td>Optional</td>
<td>Imperative</td>
<td>Optional</td>
</tr>
<tr>
<td>Radar</td>
<td>Imperative</td>
<td>Imperative</td>
<td>Imperative</td>
<td>Imperative</td>
</tr>
<tr>
<td>Ultrasonic sensors</td>
<td>Optional</td>
<td>Imperative</td>
<td>Imperative</td>
<td>Imperative</td>
</tr>
<tr>
<td>Forward-looking camera</td>
<td>Imperative</td>
<td>Imperative</td>
<td>Imperative</td>
<td>Imperative</td>
</tr>
<tr>
<td>Rear-vision camera</td>
<td>Optional</td>
<td>Imperative</td>
<td>Imperative</td>
<td>Imperative</td>
</tr>
<tr>
<td>Surround-view camera</td>
<td>Optional</td>
<td>Imperative</td>
<td>Imperative</td>
<td>Imperative</td>
</tr>
<tr>
<td>Night vision</td>
<td>Optional</td>
<td>Optional</td>
<td>Imperative</td>
<td>Imperative</td>
</tr>
<tr>
<td>LIDAR</td>
<td>Optional</td>
<td>Optional</td>
<td>Imperative</td>
<td>Imperative</td>
</tr>
<tr>
<td>Map-supported ADAS</td>
<td>Optional</td>
<td>Optional</td>
<td>Imperative</td>
<td>Imperative</td>
</tr>
<tr>
<td>Steering and braking automation</td>
<td>Optional</td>
<td>Imperative</td>
<td>Imperative</td>
<td>Imperative</td>
</tr>
<tr>
<td>Artificial intelligence</td>
<td>Optional</td>
<td>Optional</td>
<td>Optional</td>
<td>Imperative</td>
</tr>
<tr>
<td>Multiple redundancies</td>
<td>Optional</td>
<td>Optional</td>
<td>Optional</td>
<td>Imperative</td>
</tr>
<tr>
<td>Self-Learning systems</td>
<td>Optional</td>
<td>Optional</td>
<td>Optional</td>
<td>Imperative</td>
</tr>
</tbody>
</table>

Source: Frost & Sullivan;
## Vehicle Design Changes due to Automation

Several of the factors that will change will require higher levels of security.

### 2003 VW Golf
- ~35 ECUs
- ~30 sensors
- <100 actuators

### 2013 Ford Fusion
- ~70 ECUs
- ~75 sensors
- ~150 actuators

### Automated car 2030
- ~120 ECUs
- >100 sensors
- ~200 actuators

<table>
<thead>
<tr>
<th>Present</th>
<th>Parameter</th>
<th>Future</th>
</tr>
</thead>
<tbody>
<tr>
<td>1-per safety-critical function</td>
<td>Redundancies</td>
<td>Several for each safety-critical function</td>
</tr>
<tr>
<td>Steering wheel, pedals, gearshift, etc.</td>
<td>Vehicle Controls</td>
<td>Buttons, navigation interface, touchscreens</td>
</tr>
<tr>
<td>Aesthetics, aerodynamics, ergonomics</td>
<td>Design Criteria</td>
<td>Aeodynamics, ergonomics</td>
</tr>
<tr>
<td>Primarily within the vehicle, with some</td>
<td>Data Exchange</td>
<td>High bandwidth data exchange for both inter-</td>
</tr>
<tr>
<td>telematics-based communication links</td>
<td></td>
<td>and intra-vehicular communication</td>
</tr>
<tr>
<td>All (or most) occupants face the road,</td>
<td>Seating</td>
<td>Seating can be swivelled, fully-reclined,</td>
</tr>
<tr>
<td>partially reclining, fixed seats</td>
<td></td>
<td>moved around to meet occupant’s desires</td>
</tr>
<tr>
<td>Limited infotainment</td>
<td>In-car experience</td>
<td>Purpose built full-fledged infotainment</td>
</tr>
</tbody>
</table>
Security the Big Picture
Over 50 vulnerable attack points exist in the modern day ECU driven smartphone on wheels and the concern is both in-car and back-end security

Remote Hacking
Short Range (e.g. RFID)
- Remote Lock/Unlock
- Manipulation
- Vehicle Theft

In-Car Hacking (e.g. USB)
- Firmware Manipulation
- Malware Injection
- Feature Activation/Disabling

Remote Hacking
Long Range (e.g. DSRC)
- Copyrights
- Valuable IP
- Licenses/Agreements
The Current Day Focus
Almost 16 clear attack points exist in the moderate connected/safe car today.
Personal Identifiable Information (PII)

PII practices are key topic of discussion in North America and Europe as they try to establish norms on protecting consumer personal data.

Data Privacy

Personal Data:
Information related to a person or data attached to unique identifiers which can be identified directly or indirectly

Anonymous data:
When no identity can be established by anyone with the right resources and correlation with other data sources

US GAO’s Recommended Practices

- Providing disclosure to consumers about data collection, use and sharing
- Obtaining consent and providing controls over location data
- Having data retention practices and safeguards
- Providing accountability for protecting consumers data

EU Data Protection Elements

- Definition of personal data and understandable explanation
- Predefined purposes, time and volume limitation
- Balance of legitimate interest, consent and legal obligation
- Protect confidentiality and integrity
- Right to review, correct and object

Source: Frost & Sullivan

Cybersecurity Market: Personal Identifiable Information, Europe and North America, 2014
How can Security be Improved
Most Important Action Item for OEMs currently is to create Virtualized Layers by which they can secure and stonewall mission critical vehicle systems

Ways to Secure

- Firewalls Separating Critical Components
- Secure/Hardened Operating System
- Virtualization HW Partition Layers
- Digital Certificates for Apps
- Data Retention Policies
- Data Ownership & Services for User
How is the Ecosystem Coordinated?
Specialist cybersecurity companies are working across the ecosystem to support security needs but the future might see a different scenario – e.g. Harman Acquiring Red Bend

Present
- Ford
- Toyota
- BMW
- Tesla
- Audi
- Volvo

Future
- Ford
- Toyota
- BMW
- Tesla
- Audi
- Volvo

• Currently OEMs piece together a cybersecurity solution as potential standards are yet to be established.
• Tier 1 suppliers who are also working with companies like IBM and Cisco will be one stop shop in the future.

Source: Frost & Sullivan
OEMs will be pushed towards Cybersecurity Solutions
Cybersecurity is a cost constraint to OEMs as it cannot be offered as a feature to the end consumer. OEMs today have to bare the cost of securing their cars.

3-5%

OEMs will be pushed towards Cybersecurity Solutions

Cybersecurity of the cost of electronics

- **Others (30%)**: Others include operational services, managing critical services, physically securing the solution and monitoring.
- **Integration (15%)**: Integration costs include implementation of business logic to a solution and integrating security critical operations and running the solution.
- **Software (15%)**: Software development module includes programming the device. OEMs can participate in the development and implementation of the software module.
- **Professional services (10%)**: Professional services cost includes initial planning, architecting designing the system.
- **Hardware (30%)**: Hardware cost includes the cost of backend, additional chipsets, crypto, key management or plug in controls.

Source: Frost & Sullivan
The Business Model of Connected car is like an “Iceberg” - The impact is significant, but the most important part is immersed!
Thank You

Praveen Narayanan
Research Manager, Connected Cars
Automotive & Transportation
P: 248.536.2008
M: 313.515.0614
cpraveen@frost.com