Connected and Automated Vehicles and the Cybersecurity Threat

—How the Industry is Responding

Dr. Andrew Brown, Jr., PE, FESD, FSAE, NAE
Vice President & Chief Technologist

CAR Breakfast Briefing Series
February 17, 2015
Livonia, Michigan
Agenda

• Delphi Overview
• The Road Toward Automated Driving
• Why Cybersecurity Matters?
• What Needs To Be Addressed?
• Delphi’s Approach
Delphi’s Global Team – At the center of technology innovation

- 19,000 engineers and scientists
- 126 manufacturing sites
- 15 major global technical centers
- $17B 2014 revenue
- $1.7 B in Research & Development
- 160,000 people in 32 countries
Delphi – Changing the way transportation is delivered

In the next 10 years:

- 50% more vehicles on the road
- Stricter fuel economy regulations @ 54.5 MPG by 2025
- Automated driving reality

And, Delphi technologies are creating a world with:

- 50% fewer accidents
- 50% less emissions
- 100% better fuel economy
- 1000% more computational power in the vehicle
• Sensing technology and electronic controls have been in development for decades, forming the building blocks of autonomous driving
What’s next? Convergence of technologies

- **Today**
  - Assisted automation
  - Increasing personalization

- **2015**
  - Conditional automation
  - Increasing levels of active safety

- **2020**
  - Safety eco-system
  - Increasing levels of infotainment

- **2025**
  - Fully autonomous
  - Smartphone integration
  - Full cloud connectivity
  - Internet of everything
Malicious cyber activity could generate costs comparable to car crashes, piracy, pilferage, or drug trafficking.

### Putting Malicious Cyber Activity in Context

<table>
<thead>
<tr>
<th>CRIMINAL ACTION</th>
<th>ESTIMATED COST</th>
<th>PERCENT OF GDP</th>
<th>SOURCE</th>
</tr>
</thead>
<tbody>
<tr>
<td>GLOBAL</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Piracy</td>
<td>$1 billion to $16 billion</td>
<td>0.008% to 0.02%</td>
<td>IMB</td>
</tr>
<tr>
<td>Drug Trafficking</td>
<td>$600 billion</td>
<td>5%</td>
<td>UNODC</td>
</tr>
<tr>
<td>Global cyber activity</td>
<td>$300 billion to $1 trillion</td>
<td>0.4% to 1.4%</td>
<td>Various</td>
</tr>
<tr>
<td>US ONLY</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Car Crashes</td>
<td>$99 billion to $168 billion</td>
<td>0.7% to 1.2%</td>
<td>CDC, AAA</td>
</tr>
<tr>
<td>Pilferage</td>
<td>$70 billion to $280 billion</td>
<td>0.5% to 2%</td>
<td>NRF</td>
</tr>
<tr>
<td>US- cyber activity</td>
<td>$24 billion to $120 billion</td>
<td>0.2% to 0.8%</td>
<td>Various</td>
</tr>
</tbody>
</table>

Source: “The Economic Impact of Cybercrime and Cyber Espionage” Mc Afee Center for Strategic and International Studies July 2013
Why Cybersecurity Matters

• On December 2, 2013, Senator Edward J. Markey [D – MA] sent letters to 20 major automobile manufacturers requesting information about how consumers are protected from cyber attack or unwarranted violations of privacy
  ▪ Letters sent to Volvo, Volkswagen, Toyota, Tesla, Subaru, Porsche, Nissan, Mitsubishi, Mercedes Benz, Mazda, Lamborghini, Jaguar, Hyundai, Honda, GM, Ford, Chrysler, BMW, Audi, and Aston Martin

• 2014: Data security is the name of the game across all industries
  ▪ April: the "Heartbleed" flaw was made public (1/2-million servers exposed; 50 million Android phones vulnerable)
  ▪ June: AT&T confirmed insider data breach occurred in April
  ▪ July: JP Morgan revealed data breach affected 76 million households and 7 small businesses
  ▪ August: celebrity photo hack
  ▪ November: Sony Pictures Entertainment hack
  ▪ December: More than 4.6 million North American Snapchat users’ phone numbers and usernames leaked online

• 2015: Health insurer Anthem hit by hackers. Breach gets away with names, social security numbers of customers, employees.
Why Cybersecurity Matters?

- Even low-end cars have embedded more than 30-50 so-called Electronic Control Units (ECUs) that talk over Controller Area Networks (CANs).
- Modern high-end car features around 100 million lines of code, and this number is planned to grow to 200-300 millions in the near future with the advents of Connected Vehicle and Automated Driving.
- A F-22 fighter jet is less than 2 million, a Boeing 787 is around 14 million and even a cumbersome operating system such as Windows Vista is “only” 50 million.

Sources: (1) Information is Beautiful http://www.informationisbeautiful.net/visualizations/million-lines-of-code/
What Needs To Be Addressed?

- **Scope of Problem(s)**
  - Prevention of taking control of in-vehicle electronic systems via wireless or wired means.

- **Related Areas**
  - Security of mobile media information such as copyrighted video and audio being used in the car.
  - Security of in-vehicle parameters such as engine calibrations, odometer, etc.
  - Accuracy and validity of in-vehicle parameters such as vehicle speed. Will involve Functional Safety ISO 26262.
  - Integrity of emissions-control systems
  - Detection of counterfeit ECUs.

- **Heightened Threats**
  - Most of today’s vehicle networks were not intended to be secure
  - Personal Device Integration
  - Telematics
  - Cloud Access
  - V2X
  - Automated Driving

**Automotive Security – Different Scopes**

- Protect Individual ECU
  - ECU as secure part of the E/E-architecture
  - Security goal: protect integrity of ECU SW & data
  - HSM as trust anchor

- Protect in-vehicle network
  - Vehicle as network of components
  - Security goal: protect integrity of critical in-vehicle signals

- Protect connected vehicle
  - Connected vehicle as node in a larger scale network
  - Security goal: protect safety and integrity of vehicle and privacy of driver
What Needs To Be Addressed?

Automotive Initiatives

- Cyber security is a global concern and is a real and growing threat for the automotive industry
- Like other industries, the automotive industry would benefit from a concerted, industry-wide approach
- SAE is proposing a shared, secure and common platform for the automotive industry to communicate, analyze, exchange, and share information on imminent cyber security threats
- SAE International, through its Industry Technologies Consortia, is assembling a global consortia of major automotive manufacturers to define the need, scope and operational requirements
- The Alliance of Automobile Manufacturers and the Association of Global Automakers are spearheading the formation of an ISAC (Auto-ISAC) to help share information about cyber threats.

Delphi’s Approach

- Designs are secure
- Products are manufactured reliably
- Vehicles need to operate safely
- Integrity of the people in the system
- Delphi is developing standards for: Embedded controller (ECU), Cloud computing platforms, IT infrastructure, Network operations, Encryption, Device connection, Anomaly detection, Intrusion prevention
- We are working with a number of national and international organizations to ensure a coordinated approach.
- Internally, we have a dedicated team of engineers, IT professionals and attorneys to provide the necessary oversight in the area of cyber security and connected vehicles from supply to delivery and aftermarket


Delphi Confidential
Delphi Cybersecurity Organization

Cybersecurity Steering Committee

CTO
Executive Sponsor

Chief Technologist
Chief Information
Security Officer, Co-Chairs

Manufacturing Excellence TT
Information Technology
Legal Oversight & Patent Support
Engineering Task Team

Enterprise Risk Committee
Global Supplier Management
Independent Third Party

Vehicle Cybersecurity Steering Committee Charter
To enable a safe and secure vehicle experience through the identification and mitigation of cybersecurity risks.

Vehicle Cybersecurity Mission Statement
Enhance Delphi’s reputation as a leader in the development of safe and secure vehicle systems by providing awareness and training, adopting standards and implementing procedures. The team will engage with standards-setting bodies, government groups, academic institutions, and leading industry organizations.
Connected and Automated Vehicles and the Cybersecurity Threat

How Industry is Responding

- Data security is the name of the game across all industries
- The economic impact of cybercrime may reach $100 billion annually
- Connected and Automated Vehicles technology heightens the cybersecurity challenges for the Automotive Industry
  - Humongous tasks to be planned and executed!
  - Cross-industry collaboration
- Solid foundations to build upon for turning the challenges into business opportunities for Safe and Secure Connected Vehicles
  - SAE’s Initiative
  - Auto-ISAC
  - Battelle’s CyberAuto Challenge
What Needs To Be Addressed?

SAE International to Join Battelle CyberAuto Challenge

• July 13-17, 2015 at 5725 Delphi Drive, Troy, MI
• Practicum based challenge week
  - Real current model full-feature cars
  - Real equipment
  - Real communication protocols
  - Real industry/government experts
  - Ethical “White Hat” hackers
• Value Proposition:
  - Cooperative relationships building
  - Bottom-up learning
  - Interns/employees recruitment

Source: Battelle
Recommended Industry Approach

• Designs are secure
• Products are manufactured reliably
• Vehicles need to operate safely
• Integrity of the people in the system