Cybersecurity And The Automotive Industry

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

2014 Global Symposium on Connected Vehicles & Infrastructure
April 21-23, 2014
Ann Arbor, Michigan
Agenda

• Delphi Overview
• 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
- $16.5B 2013 revenue
- 126 manufacturing sites
- 15 major global technical centers
- $1.7 B in Research & Development
- 160,000 people in 32 countries
Megatrends drive our technology portfolio

Safe
- Active Safety Systems
- Driver State Alerts
- Safety Electronics
- Battery Disconnects
- Human Machine Interface
- Occupant Classification Systems

Green
- Gasoline Direct Injection
- Diesel Fuel Injection Systems
- Fuel Economy & Performance Technologies
- Next Generation Energy Efficient AC
- Hybrid & Electric Vehicle Technologies

Connected
- Vehicle Infrastructure Interface (VII) & Vehicle-to-Vehicle Interface
- Telematics
- Digital Receivers
- Connected Vehicle
- Satellite, Audio, Video & Data Systems

Focused on solutions to customers’ problems
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
Why Cybersecurity Matters?

• About 40 million card accounts breached by Target credit card hack between Black Friday November 27 and December 15, 2013

• 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 cyberattack 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

• On April 7, 2014 the "Heartbleed" flaw in encryption protocol OpenSSL was made public:
  ▪ More than a Half-Million servers exposed to Heartbleed flaw
  ▪ Heartbleed makes 50 Million Android phones vulnerable, data shows

Sources:
http://www.markey.senate.gov/record.cfm?id=348146
http://www.markey.senate.gov/Markey_Letters_to_Car_Companies_on_Cyber_Security_Privacy.cfm
http://en.wikipedia.org/wiki/Heartbleed
Why Cybersecurity Matters?

• **Connected cars are becoming ubiquitous**
  - More than 60 percent of new cars worldwide will be connected directly to the Internet by 2017 (ABI Research, July 2012)
  - **Two primary manifestations**
    - Cars as “giant rolling smartphones” providing information, entertainment and communications
    - V2V/V2I communications enabling cars to talk to each other and transportation infrastructure to avoid accidents, speed commutes
  - **96 percent** of new cars and light trucks are equipped with “black boxes”

• **Customers are demanding that their cars be technologically sophisticated**
  - 39 percent of drivers surveyed said in-car technology was their primary consideration in choosing a new auto (Accenture, December 2013)
  - Compared with 14 percent who cite vehicle driving performance

Source: Bloomberg Government “Cybersecurity, Privacy and the Auto Sector” Presentation to the American Automotive Leasing Association – March 6, 2014 - Sanford Reback, Robert Litan
Why Cybersecurity Matters?

Technological Advances in the Auto Sector Bring Public Policy Concerns

• Cybersecurity
  ▪ Industry as a whole
    ▪ One of 16 designated critical-infrastructure sectors
  ▪ Individual vehicles
  ▪ Increased concern about car hacking
  ▪ Safety concerns, such as making vehicles crash
  ▪ Privacy concerns related to information transmitted

• Privacy
  ▪ “Infotainment” services produce a wealth of personal information in data streams
    ▪ Who owns the data?
    ▪ How will information be safeguarded?
  ▪ Black boxes record extensive information about driving habits
    ▪ How will law enforcement, insurance companies gain access to this data?

Source: Bloomberg Government “Cybersecurity, Privacy and the Auto Sector” Presentation to the American Automotive Leasing Association – March 6, 2014 - Sanford Reback, Robert Litan
Why Cybersecurity Matters?

• **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.
  - Integrity of emissions-control systems
  - Detection of counterfeit ECUs.

• **Heightened Threats**
  
  - Personal Device Integration,
  - Telematics,
  - Cloud Access,
  - V2X,
  - Automated Driving

Source: Delphi
What Needs To Be Addressed? Cybersecurity Policy

- 2013: A very busy year for cybersecurity
  - President Barack Obama’s February Executive Order 13636 kicked off several administration initiatives
  - The year started with a concerted U.S. focus on Chinese cyber hacking, but that was eclipsed by the National Security Agency surveillance controversy
  - The Target breach refocused attention on the impact on consumers
  - Congress made limited progress on legislation; the Cyber Intelligence Sharing and Protection Act stalled again
  - NIST was assigned to build the Cybersecurity Framework

- 2014: NIST Framework Version 1.0 released on February 12
  - The Framework gathers existing global standards and practices to help organizations understand, communicate, and manage their cyber risks.
  - Each of the Framework components (the Framework Core, Profiles, and Tiers) reinforces the connection between business drivers and cybersecurity activities. The Framework also offers guidance regarding privacy and civil liberties considerations that may result from cybersecurity activities.
    - The Framework Core is a set of cybersecurity activities and informative references that are common across critical infrastructure sectors. The cybersecurity activities are grouped by five functions -- Identify, Protect, Detect, Respond, Recover -- that provide a high-level view of an organization’s management of cyber risks.
    - The Profiles can help organizations align their cybersecurity activities with business requirements, risk tolerances, and resources. Companies can use the Profiles to understand their current cybersecurity state, support prioritization, and to measure progress towards a target state.
    - The Tiers provide a mechanism for organizations to view their approach and processes for managing cyber risk. The Tiers range from Partial (Tier 1) to Adaptive (Tier 4) and describe an increasing degree of rigor in risk management practices, the extent to which cybersecurity risk management is informed by business needs, and its integration into an organization’s overall risk management practices.

Source: http://www.whitehouse.gov/the-press-office/2014/02/12/launch-cybersecurity-framework
What Needs To Be Addressed?
Cybersecurity Policy

- NIST Framework Version 1.0

### Framework Core Structure

<table>
<thead>
<tr>
<th>Functions</th>
<th>Categories</th>
<th>Subcategories</th>
<th>Informative References</th>
</tr>
</thead>
<tbody>
<tr>
<td>IDENTIFY</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PROTECT</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DETECT</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RESPOND</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RECOVER</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Notional Information and Decision Flows

<table>
<thead>
<tr>
<th>Bill</th>
<th>Sponsor</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>S. 1193: Data Security and Breach Notification Act of 2013</td>
<td>Pat Tooney (R-Pa.)</td>
<td>Requires entities that collect and maintain personally identifiable information to provide notice to individuals in case of a security breach</td>
</tr>
<tr>
<td>S. 1353: Cybersecurity Act of 2013</td>
<td>Jay Rockefeller (D-W.Va.)</td>
<td>Codifies ongoing, voluntary public-private partnerships to improve cybersecurity and strengthen cybersecurity research and development, workforce development and education, and public awareness and preparedness</td>
</tr>
<tr>
<td>S. 1897: Personal Data Privacy and Security Act of 2014</td>
<td>Patrick Leahy (D-Vt.)</td>
<td>Prevents and mitigates identity theft; ensures privacy; provides notice of security breaches; and enhances criminal penalties, law enforcement assistance, etc. against security breaches, fraudulent access and misuse of personally identifiable information</td>
</tr>
<tr>
<td>S. 1927: Data Security Act of 2014</td>
<td>Tom Carper (D-Del.)</td>
<td>Protects consumer information and requires notice of security breaches</td>
</tr>
<tr>
<td>S. 1976: Data Security and Breach Notification Act</td>
<td>Jay Rockefeller (D-W.Va.)</td>
<td>Requires security policies and procedures to protect data containing personal information; provides for nationwide notice in the event of a breach of security</td>
</tr>
<tr>
<td>H.R. 624: Cyber Intelligence Sharing and Protection Act (CISPA)</td>
<td>Mike Rogers (R-Mich.)</td>
<td>Provides for the sharing of cyber threat intelligence information between the intelligence community and cybersecurity entities</td>
</tr>
<tr>
<td>H.R. 2952: Critical Infrastructure Research and Development Advancement Act of 2013 (CIRDA)</td>
<td>Patrick Meehan (R-Pa.)</td>
<td>Advances security technologies for critical infrastructure protection</td>
</tr>
<tr>
<td>H.R. 3107: Homeland Security Cybersecurity Boots-on-the-Ground Act</td>
<td>Yvette Clarke (D-N.Y.)</td>
<td>Establishes cybersecurity occupation classifications and requires a strategy to address identified gaps in the cybersecurity workforce</td>
</tr>
<tr>
<td>H.R. 3696: National Cybersecurity and Critical Infrastructure Protection Act of 2013</td>
<td>Michael McCaul (R-Texas)</td>
<td>Codifies existing national cybersecurity initiatives; enhances National Cybersecurity and Communications Integration Center; establishes partnership between private sector and Homeland Security Department to improve critical infrastructure protection and incident response</td>
</tr>
</tbody>
</table>

Source: Bloomberg Government “2014 Cybersecurity Policy Outlook” February 5, 2014 - Sanford Reback, Stacy O’Mara
What Needs To Be Addressed?
Broader Industry Initiatives

European EVITA (E-Safety Vehicle Intrusion Protected Applications)
• Co-funded by the European Commission and the automotive industry
  ▪ 6 Million €
  ▪ 4-year project (2008 – 2011)
• Objectives:
  ▪ To design, to verify, and to prototype an architecture for secure automotive on-board networks.
  ▪ To provide a basis for the secure deployment of electronic safety aids based on V2V and V2I
• Approach:
  ▪ Security Requirements Analysis
  ▪ Secure On-Board Architecture Design
    ▪ Development of Hardware Security Modules deployed with ECUs
    ▪ In-Car cryptographic protocols to secure ECU-to-ECU and sensor communications
    ▪ Software framework integrating authentication, encryption and access control
  ▪ Prototype-based Demonstration
  ▪ Dissemination of Results

Source: http://www.evita-project.org/EVITA_factsheet.pdf
What Needs To Be Addressed?
Broader Industry Initiatives

Japanese Information-technology Promotion Agency’s (IPA) guide

- Covers whole life-cycle of vehicle
- Three Categories of Functions
  - Basic Control Functions
  - Expanded Functions
  - General Functions

What Needs To Be Addressed? SAE Initiative

- 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
- Initial efforts will leverage the US Information Sharing and Analysis Centers (ISAC) model that is recognized by DHS and has been currently adopted by multiple industries

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.
What Needs To Be Addressed? Battelle’s Initiative

Battelle Cyberauto Challenge

- July 13-18, 2014 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
Cybersecurity And The Automotive Industry

• 2014 is the wake-up year for cybersecurity for all industry- and government-related activities:
  ▪ Target security breach,
  ▪ Heartbleed vulnerability,
  ▪ NHTSA’s rulemaking decision for V2V mandate

• Connected Vehicles technology heightens the cybersecurity challenges for the Automotive Industry
  ▪ Humongous tasks to be planned and executed!

• Solid foundations to build upon for turning the challenges into business opportunities for Safe and Secure Connected Vehicles
  ▪ NIST Cybersecurity Framework
  ▪ European EVITA
  ▪ Japanese IPA’s guidelines
  ▪ SAE’s Initiatives
  ▪ Battelle’s cyberauto challenge

Source: Delphi