Secure Product Design Lifecycle for Connected Vehicles

Lisa Boran
Vehicle Cybersecurity Manager, Ford Motor Company
SAE J3061 Chair
SAE/ISO Cybersecurity Engineering Chair
• Cybersecurity Standards Awareness
• Vehicle Complexity
• Holistic Cybersecurity Approach
• External Engagement
Automotive Cybersecurity Activity
(Not Exhaustive)

Widespread Interest In Automotive Cybersecurity Development
Past Vehicle Design Emphasis was on Engine Design, Comfort and Chassis and Security Primarily Revolved Around Vehicle Theft, Odo Tampering & Chip Tuning
Areas of Potential Cybersecurity Vulnerabilities

- Wireless Communications
- Onboard Diagnostic Interface
- Embedded Computers on Local Vehicle Network
- Roadside Networks
- Brought-In Device Communications
- Vehicle to Vehicle (V2V)
- Vehicle to Infrastructure (V2I)
- Vehicle to Grid
- Sensors/Cameras/Microphones

Security Measures In Place That Align With Industry Best Practices To Help Protect Current and Future Technologies
Connectivity and Complexity Explosion

3rd Party Connected Services

OEM Connected Services

- Built-in Connectivity
- Beamed-in Connectivity
- GNSS Antenna
- Mobile

Interconnectivity And Increased Hacker Capability Makes Vehicles Potential Targets for Attack
Importance of Designing Security Upfront

- Loss of function or denial of service impacts
  - Safety
  - Vehicle theft
  - Customer dissatisfaction

- Loss of privacy
  - Unauthorized personal information obtained
  - Unauthorized vehicle tracking

- Impact to reputation and integrity

- Financial loss
  - Warranty
  - Loss of sales
  - Unauthorized access to features/functions
  - Higher insurance costs to the customers
  - Fraudulent commercial transactions
  - Theft of intellectual property

Safety And Security Are Important To Our Customers
Secure Vehicle Design
(e.g. HW, SW, Data, Networks, Access Control Security)

Secure Vehicle Production
(e.g. Supply Chain Management, Service)

Secure Vehicle Operation
(e.g. Infrastructure Vehicle Assembly)

Assess ---- Test ---- Address

Monitor and Report
Secure Design

Proof of Security Due Diligence – Self Attestation
Risk Categories

Enterprise Impact (E.I.)

Functional Safety (F.S.)

Privacy (P.I.I.)

Connectivity/Access (C)

Helps Manage Priority And Resource Allocation
Security control needs to be a **Defense-in-Depth Layered Technique** involving a suite of controls. There are a number of potential tools in the security controls toolbox:

- Firewalls
- Authorization / Authentication mechanisms
- Gateways / Network separation
- Secure data storage / Secure hardware
- Intrusion Detection / Prevention
- Secure Data Transport
- Encryption
- Packaging / Tamper Proofing
- Access Control
- Memory Management
- Secure SW Coding / OS

No one is a complete answer, each potential tool has benefits and limitations.

Controls Are Applicable Within Context. Several Different Tools Are Required To Obtain The Appropriate Controls.
## Building A Cybersecurity Culture

### Secure Process and Planning

<table>
<thead>
<tr>
<th>Supply Chain Mgmt.</th>
<th>Auditing</th>
<th>Governance / Policy / Business</th>
<th>Comms / Reporting</th>
</tr>
</thead>
<tbody>
<tr>
<td>PII Policy</td>
<td>Vehicle Assessments</td>
<td>Security Governance</td>
<td>Escalation</td>
</tr>
<tr>
<td>Statement of Work</td>
<td>Insurance Witness Testing</td>
<td>Incident Management</td>
<td>Field Monitoring</td>
</tr>
<tr>
<td>Supplier Audits</td>
<td>Regulatory Witness Testing</td>
<td>Security Budget</td>
<td>Cyber Security Training</td>
</tr>
<tr>
<td>Technical Design Reviews</td>
<td>Security Attribute Meetings</td>
<td>Privacy Governance</td>
<td>Dealer Awareness Training</td>
</tr>
<tr>
<td>Compliance Tracking</td>
<td>Application/Infrastructure Code Reviews</td>
<td>Security Capability Study</td>
<td>Threat Intelligence</td>
</tr>
<tr>
<td>Product Development Process Integration</td>
<td>External Engagements</td>
<td>Public Disclosure Program</td>
<td>User Notification</td>
</tr>
<tr>
<td>Self-Attestation</td>
<td>NHTSA</td>
<td>Risk Management</td>
<td></td>
</tr>
<tr>
<td>Requirements/Specifications</td>
<td>Auto ISAC</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Red Team</td>
<td>Bug Bounty Program</td>
<td>Threat Modeling &amp; Analysis</td>
<td></td>
</tr>
<tr>
<td>Benchmarking</td>
<td>Static Code Analysis</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fuzz Testing</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Testing

- Secure Process and Planning
  - PII Policy
  - Statement of Work
  - Supplier Audits
  - Technical Design Reviews
  - Compliance Tracking
  - Product Development Process Integration
  - Self-Attestation
  - Requirements/Specifications
- Auditing
  - Vehicle Assessments
  - Insurance Witness Testing
  - Regulatory Witness Testing
  - Security Attribute Meetings
  - Application/Infrastructure Code Reviews
- Governance / Policy / Business
  - Security Governance
  - Incident Management
  - Security Budget
  - Security Capability Study
  - Public Disclosure Program
  - Regulatory Compliance
- Comms / Reporting
  - Escalation
  - Field Monitoring
  - Cyber Security Training
  - Dealer Awareness Training
  - Threat Intelligence
  - User Notification
Incident Management

- Field Monitoring
- Triage Inputs
- Determine Validity and Priority
- Product Team to Determine Impact, Containment, Recovery & Remediation
- Present to Appropriate Review Board
- Communication/Reporting

A Well Documented Incident Response Plan
External Engagement

- Industry Research Consortia
- Government Involvement
- Information Sharing

- Security Supply Base
- University Collaborations
- Standards Development
Questions?