CYBERSECURITY BEST PRACTICES FOR MODERN VEHICLES

Cem Hatipoglu, Ph.D.
Director, Office of Vehicle Crash Avoidance and Electronic Controls Research
Fatalities and Fatality Rate, by Year

Motor vehicle crashes cost nearly $836 billion
Continued Technological Innovations…

35,092 people lost their lives due to motor vehicle accidents in 2015

- Modern crash avoidance, vehicle-to-vehicle (V2V) communications, and automated vehicle technologies hold the promise to address most crash challenges.
However, these safety features introduce **new cybersecurity challenges and vulnerabilities** as demonstrated by our research and that of others.

Failure to tackle the cybersecurity challenge would threaten the **technology-driven safety transformation** we all want to achieve.
NHTSA finalized a historic agreement with 18 automakers in January 2016, on proactive safety principles. The signatories agreed to work together to develop a collaborative, data-driven, science-based process, consistent with the law, to advance safety objectives.

**Vehicle Cybersecurity Specific Objective:** Explore and employ ways to work collaboratively in order to mitigate those cyber threats that could present unreasonable safety risks.

- **Best practices** that reflect lessons learned within and outside of the auto industry to foster enhanced cyber resiliency and effective remediation. **Executive summary recently released.**
- **Support and evolve** the auto industry’s information sharing and analysis center (Auto-ISAC), **enhance** it over time and **expand** its membership.
January 2016 Event

▪ **Four Panels**
  • 35 Panelists with different affiliations
    − OEMs, Suppliers, Federal Agencies, Security Researchers, Associations, Advocates, Technology Companies…

▪ **Audience**
  • Over 300 in attendance
    − Over 200 unique orgs
    − 25 Federal Groups
    − 17 OEMs
    − 13 Associations
Cybersecurity Best Practices for Modern Vehicles

Released on October 24, 2016

Docket: NHTSA-2016-0104
Comment Period Closed on 11/28/2016
...all individuals and organizations manufacturing and designing vehicle systems and software.

...all classes of motor vehicles, including passenger cars, trucks and buses
Document Framework

- **General cybersecurity guidance**
- **Auto-industry specific guidance**
  - Processes
  - Fundamental Protections for Consideration
- **Other guidance**
  - Education, Aftermarket Devices, Serviceability
General Guidance

- Adopt a risk-based approach
- Follow NIST’s cybersecurity framework
  - Identify, Protect, Detect, Respond, Recover
  - Comprehensive and systematic approach to develop layered protections
- Review and consider IT security suite of standards
  - ISO 27000 series, CIS CSC
Industry Specific Guidance

- **Vehicle development process** with inherent and explicit cybersecurity considerations
- Top-down **leadership priority** on product cybersecurity
- Cybersecurity **information sharing**
- **Vulnerability reporting** policy
- Incident response **process**
- Self-auditing
Fundamental Vehicle Cybersecurity Protections

- Limit **Developer/Debugging Access** in Production Devices
- Control **Keys**
- Control Vehicle Maintenance **Diagnostic Access**
- Control **Access to Firmware**
- Limit Ability to **Modify Firmware**
- **Control Proliferation** of Network Ports, Protocols and Services
- Use Segmentation and Isolation Techniques in Vehicle Architecture Design
- Control Internal **Vehicle Communications**
- **Log Events**
- Control Communication **to Back-End Servers**
- Control **Wireless Interfaces**
Other topics

- **Education**
  - an *educated workforce* is crucial to improving the cybersecurity posture of motor vehicles

- **Aftermarket Devices**
  - devices are interfaced with cyber-physical systems and they could **impact safety-of-life**

- **Serviceability**
  - do not **unduly restrict access** by authorized alternative third-party repair services
Also...

- **Federal Automated Vehicles (FAV) Policy**
  - Released September 2016
  - [www.transportation.gov/av](http://www.transportation.gov/av)

- Cybersecurity is called out as one of 15 safety assessment areas

- Docket No. NHTSA-2016-0090 (Document No. 2016-22993)