National Highway Traffic Safety Administration

NHTSA
www.nhtsa.gov

# NHTSA and Automotive Cybersecurity

Briefing to the Information Security and Privacy Advisory Board

October 2015

# The Need for Cybersecurity Research

- 32,719 people died due to motor vehicle accidents in 2013; new safety features enabled by vehicle-to-vehicle communications and computer controlled electronic safety systems have the potential to dramatically improve highway safety.

- New safety features and customer convenience features will introduce new challenges and vulnerabilities as demonstrated by our research and that of others.

- While no real world incidents have occurred to critical safety systems, we have developed a research approach to help improve the safety posture of future vehicles.

# Use of Electronics in Cars

- Not new…
  - The first common use of automotive electronics dates back to 1970s (not including uses in radio)
  - By 2009, a typical automobile featured over 100 microprocessors, 50 electronic control units, five miles of wiring and **50-100 million lines of code**.

Examples of functions on a modern vehicle

- Active Suspension
- Active Vibration Control
- Adaptive Cruise Control
- Adaptive Front Lighting
- Airbag Deployment
- Anti-lock Braking
- Autonomous Emergency Braking
- Battery Management
- Blind Spot Detection
- Cabin Environment Controls
- Communication Systems
- Cylinder Deactivation
- Driver Alertness Monitoring
- Electronic Power Steering
- Electronic Seat Control
- Electronic Stability Control
- Electronic Throttle Control
- Electronic Toll Collection
- Electronic Valve Timing
- Engine Control
- Entertainment System
- Event Data Recorder
- Hill Hold Control
- Idle Stop-Start
- Instrument Cluster Control
- Intelligent Turn Signals
- Interior Lighting
- Lane Departure Warning
- Lane Keeping Assist
- Navigation
- On-Board Diagnostics
- Parental Controls
- Parking Systems
- Pre-crash Safety
- Rear-view Camera
- Regenerative Braking
- Remote Keyless Entry
- Security Systems
- Tire Pressure Monitoring
- Traffic Sign Recognition
- Transmission Control
- Windshield Wiper Control

# NHTSA's mission

National Highway Traffic Safety Administration's (NHTSA's) mission is:

to reduce fatalities, injuries and economic losses resulting from motor vehicle crashes.

# NHTSA’s safety role and tools

- ## Regulation:

  NHTSA **creates mandatory requirements** known as Federal Motor Vehicle Safety Standards (FMVSSs). Motor Vehicle Safety Act (49 U.S.C. §§ 30101 et. seq.) directs NHTSA to establish FMVSSs that are:

  - practicable, stated in objective terms, and meet the need for motor vehicle safety.

  FMVSSs are also performance-based, and appropriate for each vehicle type to which they apply. Manufacturers self-certify compliance.

- ## Enforcement:

  NHTSA **investigates possible safety defects**, ensures that products meet established safety standards and are not defective (through safety recalls if necessary), and tracks safety-related recalls.

  – The agency also enforces regulations on fuel economy, odometer fraud, and vehicle theft.

# NHTSA’s safety role and tools

5-Star Safety Ratings
More Stars. Safer Cars.

- **Consumer Information:**

  NHTSA creates incentives for manufacturers to offer new safety technologies by providing information about these technologies to consumers.

  New Car Assessment Program (**NCAP**) ( http://www.safercar.gov/ )

  – Comparatively rates the performance of vehicles on different aspects of safety.

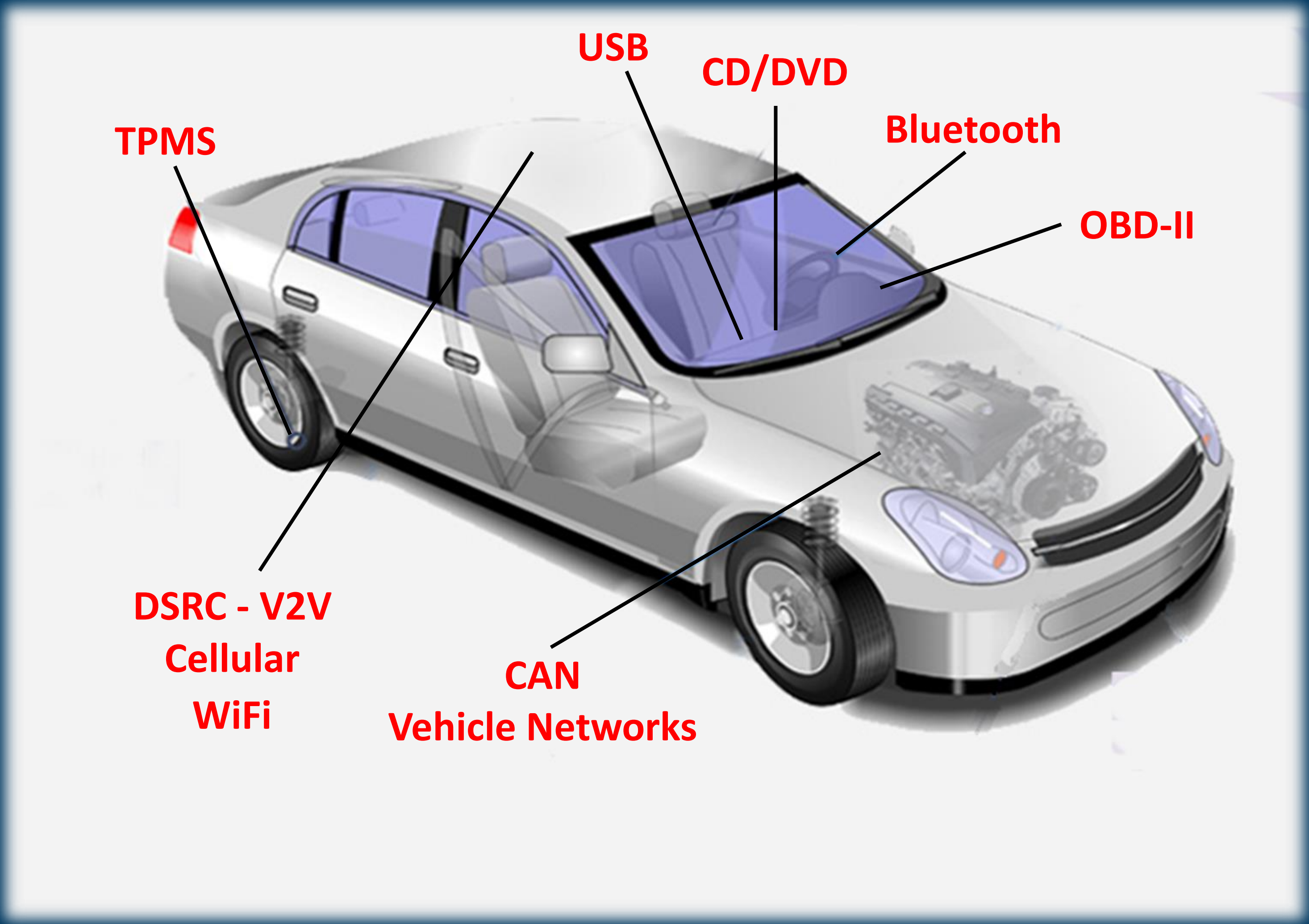
  – Some tests can be based on FMVSS, but at higher test speeds. Tests follow objective/performance-based style of an FMVSS. NHTSA does most of the testing.

- **Behavioral Programs:**

  NHTSA studies behaviors and attitudes in highway safety, focusing on drivers, passengers, pedestrians, bicyclists and motorcyclists. We, in collaboration with State programs and other partners,

  – identify and measure behaviors involved in crashes or associated with injuries, and develop and refine countermeasures to deter unsafe behaviors and promote safe alternatives.

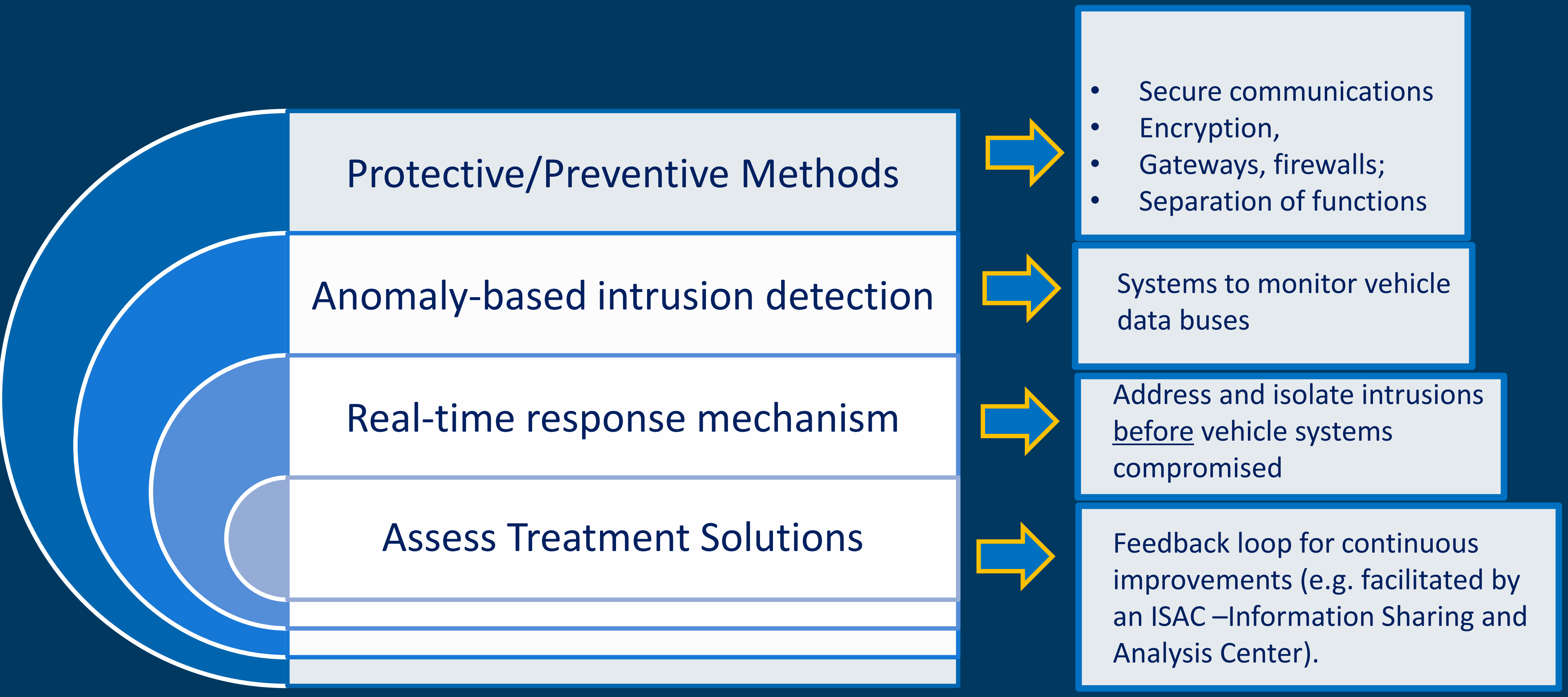
# Threat Vectors



# Threat Vectors Categories

- Physical and Remote access points into the vehicle:
    - Physical interfaces
        - On-board diagnostics port, CD/DVD Players, USB ports, direct ECU access
    - Short Range wireless interfaces
        - RF, Bluetooth, Wi-Fi, DSRC
    - Long range wireless interfaces
        - Cellular, satellite
    - *Aftermarket products can convert physical interfaces into wireless interfaces*
        - *E.g. Progressive insurance dongle for OBD-II*

# NHTSA Approach: Layers of Protection



Protective/Preventive Methods

- Secure communications
- Encryption,
- Gateways, firewalls;
- Separation of functions

Anomaly-based intrusion detection

Systems to monitor vehicle data buses

Real-time response mechanism

Address and isolate intrusions before vehicle systems compromised

Assess Treatment Solutions

Feedback loop for continuous improvements (e.g. facilitated by an ISAC –Information Sharing and Analysis Center).

# Organizational Changes to Address Challenges

- In 2012, NHTSA created a new office: Vehicle Crash Avoidance and Electronic Controls Research
  - Within the Office, Electronic Systems Safety Division responsible for performing research focusing on electronic control systems safety, including cybersecurity.
  - Office is also responsible for performing research on advanced driver assistance technologies and human factors

- In 2014, we also expanded our testing capabilities at our research center in Ohio

# NHTSA Completed Research

- Researched cybersecurity best practices in relation to automotive industry. Published four reports in 2014:
  - Assessment of the Information Sharing and Analysis Center Model;
  - A Summary of Cybersecurity Best Practices;
  - Characterization of Potential Security Threats in Modern Automobiles: A Composite Modeling Approach
  - National Institute of Standards and Technology Cybersecurity Risk Management Framework Applied to Modern Vehicles.

# Current NHTSA Research

- Researching and evaluating design processes and standards
  - Evaluating potential to adapt existing functional safety approaches
- Investigating Protective/Preventive solutions
  - Message authentication for communications Interfaces ( V2V project initiating)
  - Gateways, firewalls (project initiating)
- Researching Intrusion Detection Solutions
  - Vehicle bus monitoring for anomalous behavior; (project initiating)
- Assessing Treatment Solutions
  - Feedback loop for continuous improvements (Monitoring progress in standing up an Automotive ISAC ).
- Crosscutting Research:
  - Vulnerability Testing (Publish reports in 2016)
  - Software – including over the air updates
  - Evaluate Heavy Vehicle Cybersecurity
  - Collaboration/coordination with other Federal agencies (e.g. DHS, NIST, FAA)

# Additional Activities

- Report to Congress on the Need for Standards Sec 31402 of MAP-21, Electronic Systems Performance
    - NHTSA conducted a review on the need for standards for electronic systems, including cybersecurity
    - Published a Federal Register Notice in October 2014 to solicit stakeholder feedback
    - Prepared a draft report to Congress
    - Delivery to Congress expected early next year.

# FCA Recall

- Researchers demonstrated ability to intrude into the CAN bus via cellular/WiFi connection.
- Impacted up to 1.4 million Fiat-Chrysler (FCA) vehicles.
- Recall took place on July 23rd with two remedies:
  - Over the air via cellular service provider to close an open port
  - Manufacturer's update to firmware to address close proximity WiFi vulnerability
- Research results detailing how to perform the hack released on August 10
- Two Equipment Queries underway. One to the manufacturer and one to the supplier.

# NHTSA Path Forward

- Continue research at quickest reasonable pace;
- As research matures, consider rulemaking, recommended practices, and/or guidelines;
- Continue close working relationship with manufacturers and their organizations;
- Continue to encourage industry to expediently develop Automotive ISAC to ensure quick information exchange;
- Carefully review any reported incidents even if off-road;
- Use recall authority if needed;
- Continue to advocate for additional agency resources in budget and enactment of helpful legislation in Grow America.

# Other key Activities and Government Agencies

- SAE International
  - J3061: Cybersecurity Guidebook for Cyber-Physical Vehicle Systems
- Various worldwide activities
  - EVITA, PRESERVE, SCAAS, SESAMO, HEAVENS, MISRA SA, J-CSIP, JasPar, JARI
- Federal Entities
  - Department of Homeland Security / HSARPA / Science & Technology
  - Department of Defense / DARPA and TARDEC
  - NIST
  - Federal Trade Commission
  - Federal Communications Commission
  - National Science Foundation
  - Federal Aviation Agency
  - Food and Drug Administration
  - Etc.

# NIST involvement ?

- How can NIST help the automotive industry
  - Establishment of robust guidelines/best practices ?
  - Involvement and participation in worldwide automotive voluntary standards setting activities ?
  - Other forms of involvement ?
- Responsible Disclosure of Cyber vulnerabilities in automotive systems
  - Experience and knowledge in setting effective structures ?
    - ISO/IEC 29147:2014: IT-- Security techniques -- Vulnerability disclosure
    - ISO/IEC 30111:2013: IT -- Security techniques -- Vulnerability handling processes
  - Good examples of its uses in the cyber-physical systems domain ?