Summary of Recent Vehicle Cybersecurity Attacks/Vulnerability Research and State-of-the-Art Mitigations Applicable to Government Vehicles

December 10. 2015

Volpe The National Transportation Systems Center

Advancing transportation innovation for the public good

U.S. Department of Transportation
Office of the Secretary of Transportation
John A. Volpe National Transportation Systems Center

Agenda

Topics	Speakers
Introduction	Kevin Harnett
A Vehicle Cybersecurity Primer	Graham Watson
Cyber Attacks	
Early Research	Graham Watson
OBD-II Dongle/Telematics Attack	Brendan Harris
Automotive Cybersecurity Mitigations	Brendan Harris
Conclusions and Recommendations	Brendan Harris

Modern Vehicles

- **Telematics**
  - Remote control (locks, start)
  - Remote diagnostics
  - Remote repair (updates)

- **Driver support**
  - Navigation
  - Collision warning/avoidance
  - Augmented vision

- **System automation**
  - Dynamic EV charging
  - Computer control of engine, brakes, etc.

- **Content and communication**
  - Voice and data
  - Information and entertainment

Joint Focus on Vehicle Cybersecurity

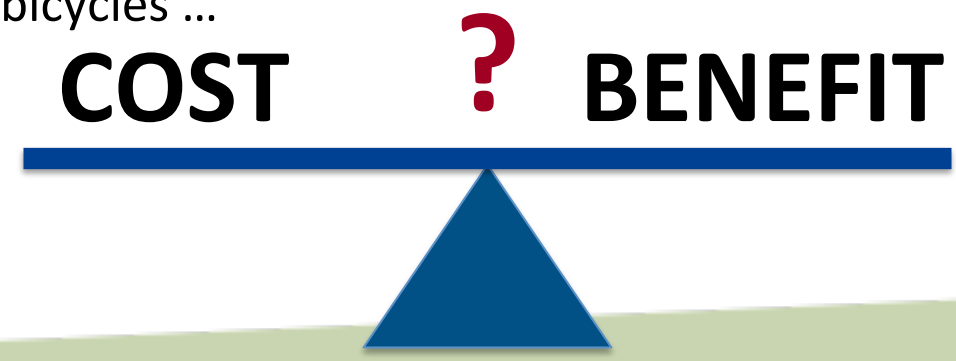
2014
2015

Major Automakers

- **Joint effort among DHS S&T, DOT Volpe Center, and SRI International**
- **Three primary focus areas:**
  - Promote/transition of the automotive cybersecurity best practices and guidelines in the private sector
  - Discussions with industry on key challenges and pre-competitive research and the development of an Automotive Cybersecurity Industry Consortium (ACIC)
  - **Cyber security needs for government vehicles**

Automotive Cybersecurity Context

- DHS S&T and DOT-Volpe are NOT regulatory agencies
  - Working with industry to find solutions to cybersecurity issues
- Goal is measured, balanced, and cost effective ways to mitigate cyber threats
  - Not telling everyone to give up cars and start riding bicycles …



Government Critical Mission Use

- **First responder and law enforcement vehicles** – fire, rescue, ambulance, police
  - Must be safe and reliable
- **Undercover vehicles** – mission critical
  - Must be safe and reliable
  - Blend in – not tracked or identified either by emanating too much or by not emanating at all
- **Government official / overseas embassy vehicles** (e.g., "Black SUV")
  - Must be safe and reliable but does not need to hide
- **Non-Tactical DoD Vehicles**
  - Commercial motor vehicles
- **General use government vehicles**
  - Vehicles that do not fall into above categories

"Unique" Government Risks

- Ease of attack (vulnerability)
  - Weakness in a particular make/model is capable of being multiplied across many hundreds of vehicles.
    - Remote hacking of telematics (e.g., Miller/Valasek, Kohno, Savage)
    - Insecure dongles used for fleet tracking (e.g., Progressive, Zubie)
    - Popularization of vehicle hacking tools, software and techniques
- Attractiveness of target
  - High profile type of target
  - Special badging and markings make them stand out
  - Critical missions
- Monetary or political gain
  - Ability to interfere with operation of a Government vehicle, for example:
    - Border control vehicle suddenly stops and cannot be restarted
    - Protection detail vehicles accelerates out of control
    - Surveillance vehicle starts blowing its horn
    - Eavesdropping on sensitive conversations via built-in hands-free microphone

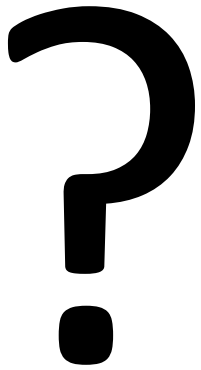
Resulting DHS and DOT-Volpe Government Project Tasks

Opportunity

Engage government fleet managers and GSA to provide automotive industry with target cybersecurity requirements

- Perform Vehicle RF Analysis and Fingerprint
- Initiate a Cybersecurity for Government Vehicle Steering Group
- Investigate and Assess Aftermarket Product Vulnerabilities
- Define Government Vehicle Cybersecurity Procurement Specification Requirements

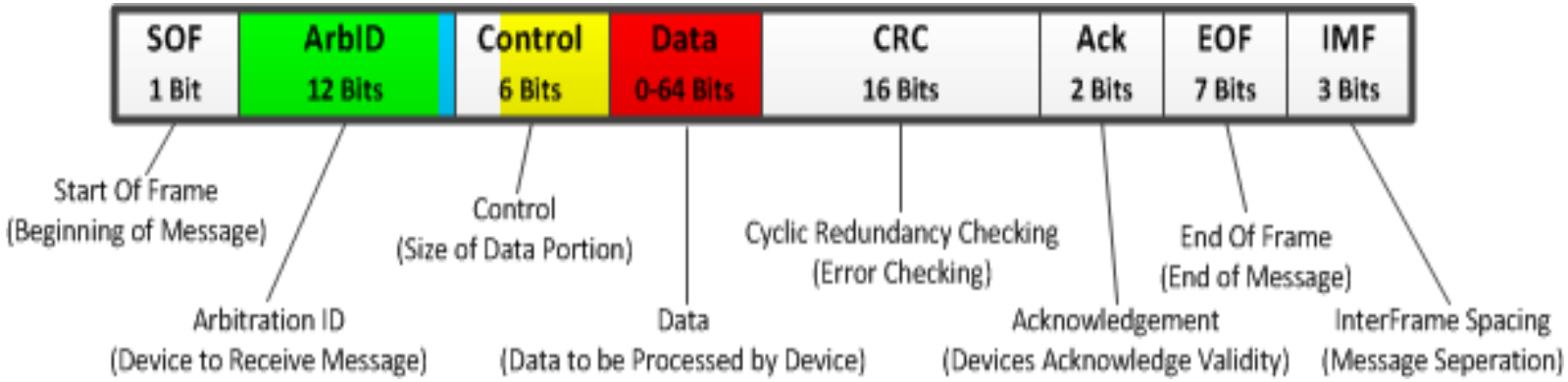
A Vehicle Cybersecurity Primer



Vehicle Networks

- There are many different types of vehicle networks
  - Controller Area Network (CAN)
  - Local Interconnect Network (LIN)
  - Media Oriented Systems Transport (MOST)
  - Flex-Ray
  - Etc.
- Most common network is the **CAN network**
- All CAN traffic to and from ECUs is carried **simultaneously over a single line**
- ECUs "listen" to all message traffic for messages addressed to that ECU

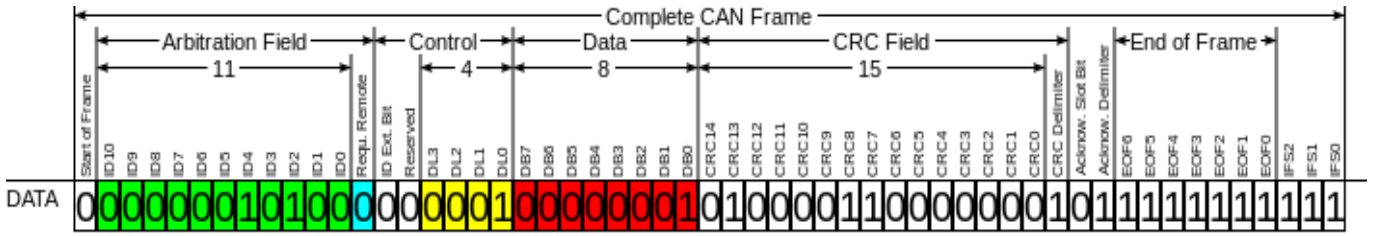
The CAN Message



- The CAN protocol is the common format all messages transmitted on the CAN network
- Constructed in this manner the message is referred to as a CAN packet
- Each of the sections within the packet is a field, that contains pertinent information
- The Arbitration ID (green) is the destination of the packet
- The Data Field (red)is the instruction it carries

The CAN Message

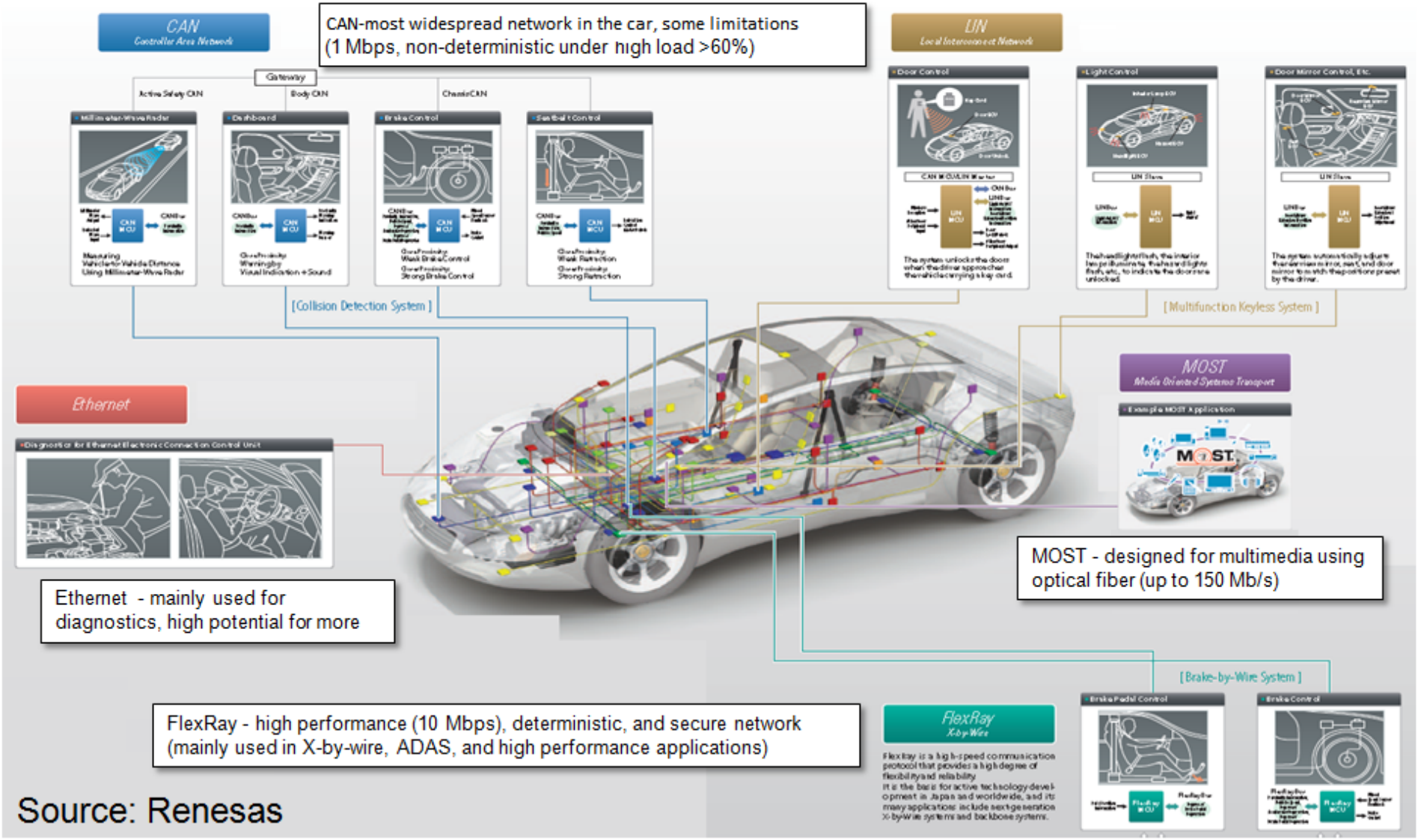
- The CAN protocol is the common format all messages transmitted on the CAN bus use
- Constructed in this manner the message is referred to as a CAN packet
- Each of the sections within the packet is a field, that contains pertinent information
- The Arbitration ID (green) is the destination of the packet
- The Data Field (red)is the instruction it carries



- The format for each of these fields is at the bit level which includes only 0 or 1, off or on

Intra-Vehicle Networking

LIN - low cost bus for body applications (19.2 Kbauds, UART interface)



Source: Renesas

Network External Interfaces

- In a modern vehicle there are a host of external interfaces

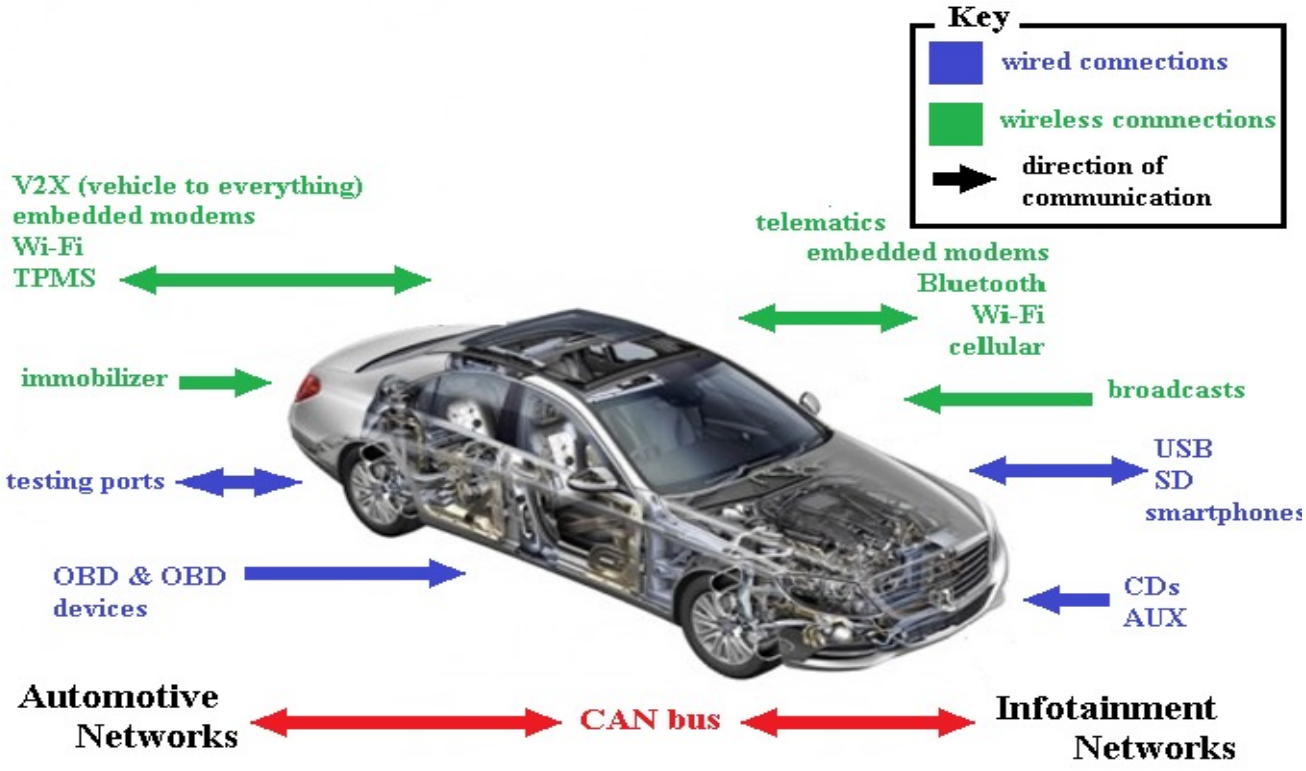


Photo Credit: IHS


CYBER
ATTACKS
AHEAD

Early Research

2010 - Experimental Security Analysis of a Modern Automobile

- 2010 University of Washington and the University of California, San Diego (UCSD) conducted **pioneering remote vehicle attacks**
- Attacks were wirelessly relayed to a computer attached to the OBD-II port
- Demonstrated it was possible to **read CAN network traffic and send commands to the vehicle**
- Many attacks that have been demonstrated to date can trace their roots back to this original work

Early Research

2011 - Comprehensive Experimental Analyses of Automotive Attack Surfaces

- University of Washington and UCSD performed a series of experimental attacks to gain access to a vehicle's network ***without*** using a physical connection
- A CD was created which while playing music also **sent data into the CAN network**
- **Bluetooth** was used as an attack surface, any paired device (i.e. smartphone) could be used to launch an attack
- Long-range attacks launched **utilizing the vehicle's telematics system (i.e., On-Star) via a cell interface**

Early Research

2011 - Privacy Vulnerabilities of In-Car Wireless Networks: A TPMS Case Study

- Tire Pressure Monitoring Systems (TPMS) have been mandated in vehicles sold in the US after 2007
- University of South Carolina conducted experiments to determine the security of the wireless TPMS network
- Sent **false messages (spoofing) to the TPMS unit** causing it to display inaccurate data to the driver
- Able to **track a vehicle by reading the TPMS ID** in one of the tires
- Able to greatly extend the read range of TPMS messages to 40 meters away

Recent Attacks

2015 - Miller/Valasek Remote FCA Jeep Attack

- Miller and Valasek using the internet and the Sprint cellular network were able to take control of an *unmodified* 2014 Jeep Cherokee Latitude edition

- "Hacker" located in Pittsburgh was able to perform "remote" attacks on the Jeep which was located in St. Louis

- Attack utilized an **open port on the Sprint Network** combined with a hardwire connection between the vehicle modem and a chip in the Infotainment unit which was connected to the CAN bus
- Miller and Valasek discovered the same type of vulnerabilities in other FCA vehicles

Results from the Jeep Hack

- Miller and Valasek contacted FCA (several months before the pubic attack) and Sprint and informed them of their findings
- **FCA issued a recall notice for 1.4 million vehicles** (first cybersecurity recall on record)
- A software patch needs to be installed either by the owner or at a dealership
- **Exploit was briefed at the 2015 Blackhat and DEFCON conferences** in August 2015 and the paper was posted on the Internet

Remote Exploitation of an Unaltered Passenger Vehicle

Dr. Charlie Miller (cmiller@openrce.org)
Chris Valasek (cvalasek@gmail.com)

August 10, 2015

Tools of the Trade

July 2015 - OwnStar

- Cyber researcher Samy Kamkar created "OwnStar", a device that allows a **hacker to track, unlock, remote start, and make full use of all features in the OnStar RemoteLink application on GM cars equipped with OnStar**
- Using "Man In The Middle" (MITM) exploit hacker inserts themselves in the communication chain
- Detects OnStar remote link application, listens to the user's phone making probe requests for a Wi-Fi hotspot, creates fake hotspot that matches probe request
- Once fake hotspot established, **attacker has access via the OnStar remote application**

Tools of the Trade (cont'd)

July 2015 - OwnStar

- Main exploit was **no check for valid secure socket layer (SSL)** certificates in the RemoteLink application
- On **July 31 2015, GM and OnStar issued mobile app update** for the iOS version
- Users encouraged to install the application update
- Blackberry, Android, and Windows phones **fixed via a back end patch** requiring no intervention on the users' part
- Inventor, Samy Kamkar, claims the same vulnerability exists in BMW Remote, Mercedes mbrace, and Chrysler's Uconnect

OwnStar

OwnStar and Remotelink App

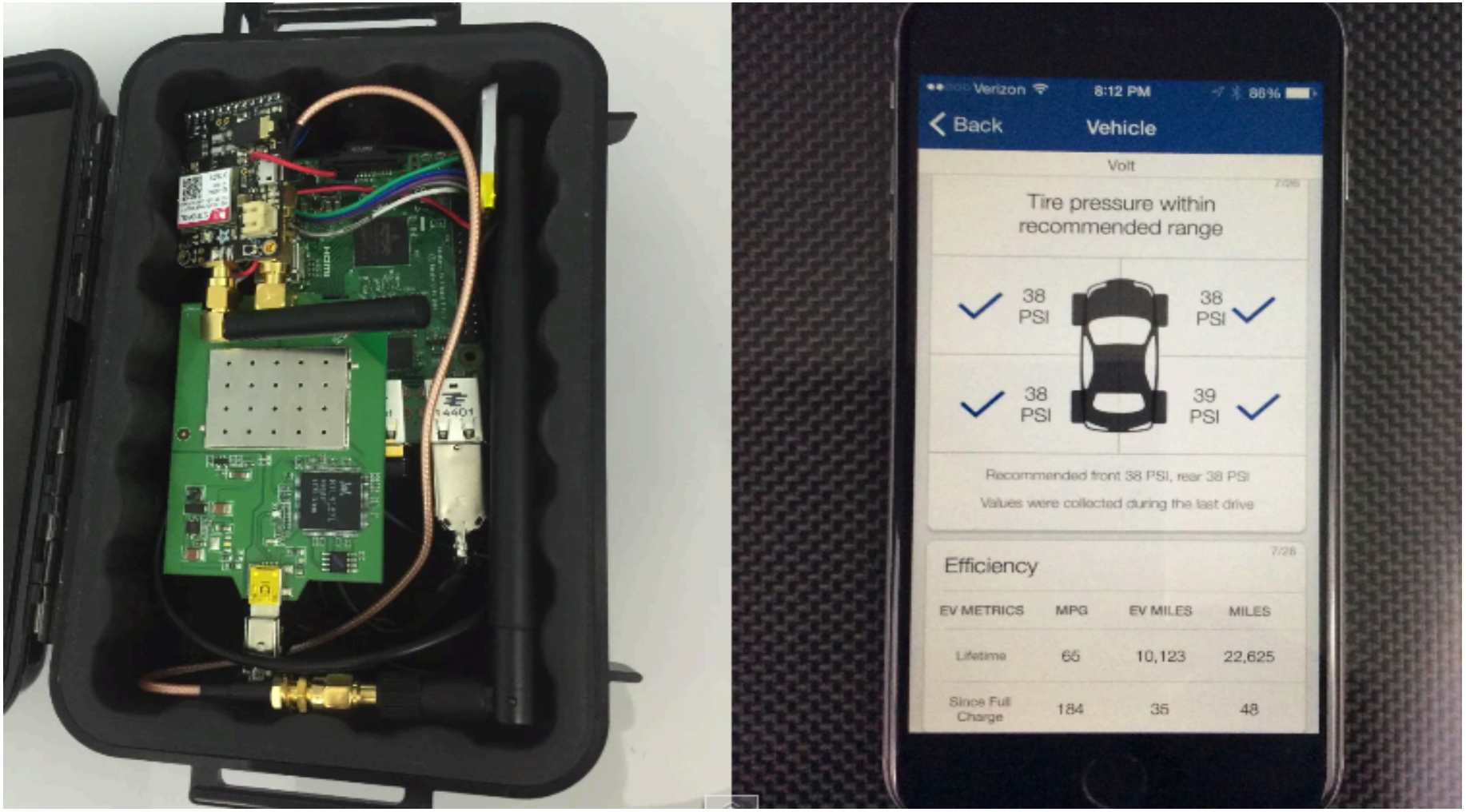


Photo Credit: Car and Driver

OBD-II Dongle/Telematics Attacks

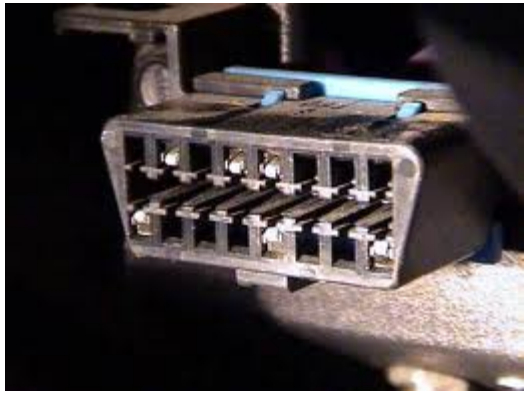
OBD-II Background

- In the 70's and early 80's OEMs started using electronic engine controls to meet EPA standards
- In 1988 the SAE set standards for the plug and diagnostic test signals
- All Cars built since January 1996 have an OBD-II port
- The OBD-II port was designed to provide a means to inspect that a car is performing to OEM standards for emissions purposes

The OBD-II Dongle

- OBD-II dongles interface with the vehicle's CAN network via the OBD-II port
- Typically dongles send queries into the CAN network and relay the responses to third party devices or systems
- Dongles typically connect to external devices/ networks via Bluetooth or cellular
- Size and complexity of dongles vary with feature sets

Sample OBD-II Dongles and OBD Port



2014 Zubie Aftermarket Dongle

- The Zubie OBD-II dongle allows drivers to track their driving habits, detect possible malfunctions in the vehicle, and share their location using a mobile application
  - It communicates with the CAN network of the vehicle and has a mobile modem that connects to the Zubie cloud
  - In 2014, Argus Automotive Cybersecurity released a joint press release with Zubie **disclosing a critical cybersecurity vulnerability, an attacker could remotely control all vehicle functionality and tracking using a "Man-in-the-middle (MITM)" exploit**
  - The device also accepted unsigned software updates, an **attacker could send malicious software updates to the device**

2014 Progressive Snapshot Dongle

- The Progressive Insurance Usage-Based Insurance (UBI) device allows customers to save on their insurance costs by sending information on their driving behavior to Progressive
  - In late 2014, security researchers at Digital Bonds Labs disclosed that the device was **completely lacking secure coding principles**
  - Digital Bonds exploited the device by **reverse engineering the dongle's firmware and executed a MITM cellular attack**
  - Digital Bonds noted "What we found with this device was that it **was designed with no security features** *…It wasn't even based on basic security coding practices. ... It's a house that has no doors, no windows and no fences, with valuables inside"*
  - This is not a case of researchers exploiting a weakness in the dongle's security; it was **simply that NO security existed**

BMW Telematics Attack and OTA Patch

- In 2015, the Allgemeiner Deutscher Automobil Club (ADAC), a German automobile association, exploited a vulnerability in the telematics system used by the BMW "ConnectedDrive" to gain access to the in vehicle CAN bus network
  - They took control of functions, such as locking and unlocking the doors by using a MITM attack that simulated a cellular base station
    - This attack is extremely **similar in the architecture and methodology that could be used to attack a fleet management/telematics system**
  - Also it was discovered the "ConnectedDrive"was using the same authentication for **all vehicles**
  - ADAC experts recorded the communications required to unlock the doors of one car, and replayed that communication against other BMWs **to successfully unlock their doors and manipulate other ECUs**
  - Once informed of the vulnerability BMW successfully transmitted an over-the-air (OTA) patch **to update telematics system across the entire range of models affected totally 2.2 million**

Automotive Cybersecurity Mitigations

Automotive Cybersecurity Vendors

DOT Volpe and DHS S&T recently interviewed a number of automotive cybersecurity vendors to learn about their risk mitigation capabilities

ARGUS CYBER SECURITY

cisco

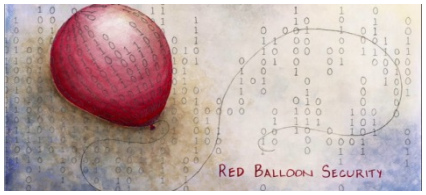
KAPRICA SECURITY

symantec™

TOWERSEC Automotive Cyber Security

Arilou Automotive Cyber Security

HARMAN



BOSCH

The following slides summarize the vendor automotive cybersecurity risk mitigation capabilities for legacy and new vehicles

What can I do today?

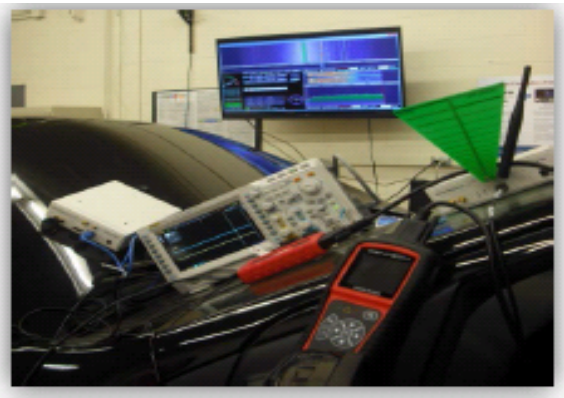
Short Term Mitigations

Traditional IT Security Mitigations

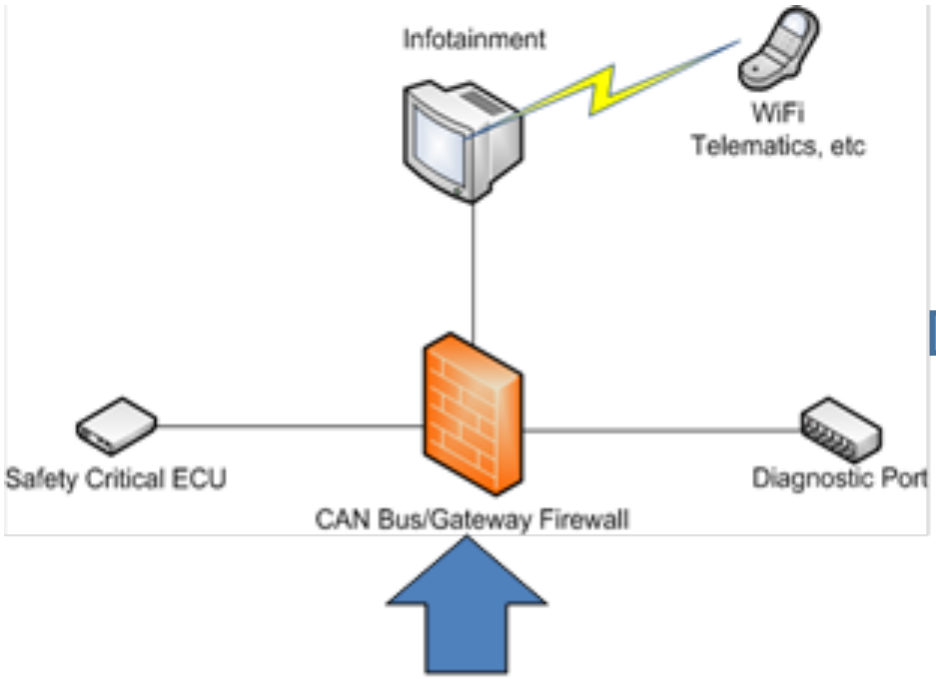
- Traditional IT mitigation methods are being leveraged and adapted to work within the automotive environment:
  - Firewalls
  - Gateways
  - IDS
  - IPS
  - Cryptography
- Traditional Mitigation Strategies such as a layered defense are also being incorporated

Short Term Mitigations

- Capable of being integrated into any vehicle with a CAN bus
- Require minimal installation
- Mitigate the highest risks
  - OBD-II port access
  - Telematics
  - Infotainment
- Examples include:
  - OBD-II firewall
  - Replacement ECUs with IPS or IDS protection

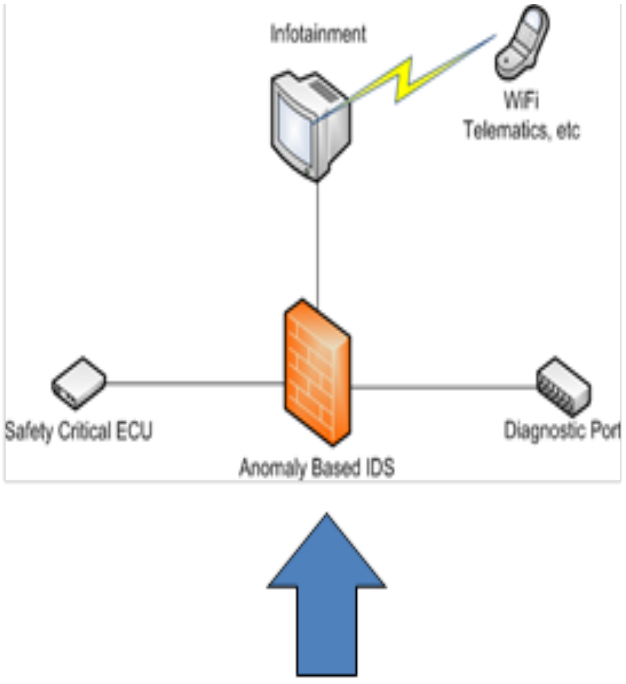


CAN Firewall Mitigation



- OBD-II gateway or CAN firewall creates a set of rules that ensure communication with the vehicle conforms to a certain policy
- A strong rule set will ensure that data traffic which does not conform to the gateway/ firewall security policy is blocked
- Enforces security through either a **whitelist of pre-approved acceptable commands, or a blacklist of known bad commands**
- Effective at stopping attackers after they have **breached the external interfaces to the CAN bus**
- Drawbacks are lists that the firewall depends on have to be extensive and be able to be updated remotely over-the-air
- May not detect an attack which uses properly formatted messages

IDS/IPS Mitigations

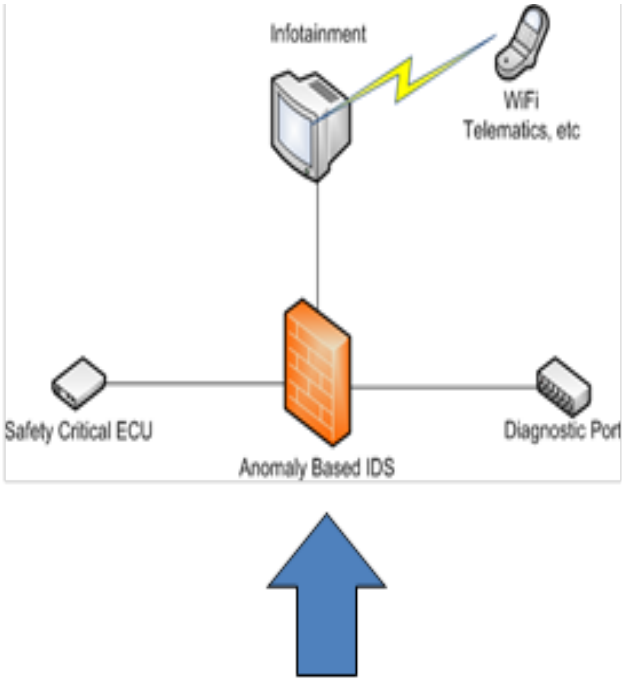


Enforcement via comparison to baseline

IDS Mitigation

- IDS systems monitor inbound and outbound network messages and compares CAN bus message traffic against a **"trained baseline"**
- Messages outside of the normal baseline, **trigger a security alert to the OEM, fleet manager, or driver**
- Automobiles are an **excellent candidate for an anomaly-based IDS solution** and the development of "learning algorithms"
- An IDS system does **NOT** prevent an attack from occurring

IDS/IPS Mitigations



Enforcement via comparison to baseline

IPS Mitigation

- Hybrid that combines the detection functionality of an IDS with the proactive protection of a firewall
- Will **detect and block CAN bus messages** that are against its policy
- Message anomalies are compared against a list of known attacks (similar to a firewall "blacklist"), **If the anomaly fits one of those attacks, the IPS takes action**
- Actions that the IPS can take (e.g., dropping the message, alerting the driver, sending an alert to a monitoring station) are developed by the IPS vendor often working in conjunction with the OEM
- **IPS's "blacklist" of known attacks must be kept current** so provisions for updating the blacklist must be included in the IPS

What can I do tomorrow?

Long Term Mitigations

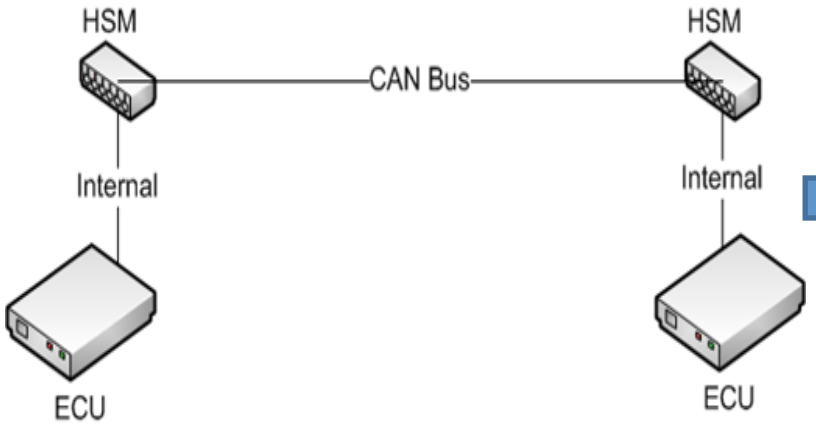
Future Mitigations

- **Integrated by OEMs and Tier 1 suppliers**
  - Close obvious flaws
  - Provide continuous support
- **Examples include:**
  - Secure over-the-air (SOTA) updates
  - Hardware Security Module (HSM)
  - Central Gateway which isolates critical systems
  - IDS/IPS integrated with ECUs, infotainment, and telematics

Secure Over-the-Air (SOTA) Updates

- Need to **quickly and securely apply updates, patches, and enhancements** (including cybersecurity patches) to the software and firmware in the vehicle
- Relying on owners to acquire and install patches has always met with incomplete success
- Currently, only a **few OEMs have the ability to provide OTA updates** for infotainment and telematics systems only (e.g. BMW "Connected Drive", Tesla Model S)
- Challenges facing SOTA updates are providing a **secure updating method across the entire chain of backend servers, wireless links, and the vehicle itself**
- Incorporating OTA capabilities in existing fleet vehicles, presents **major challenges for vehicles not equipped with OEM telematics capability**

Hardware Security Module (HSM) Architecture



- An HSM is a physical device that resides inside an ECU
- Safeguards and manages **digital keys used for authentication and cryptographic** processing
- Provides **secure boot, secure storage, secure software updates, tampering and counterfeit parts protection**
- Scalable depending on the level of security required by the HSM's operating environment
- Designed to be applied at the Tier 1 supplier level

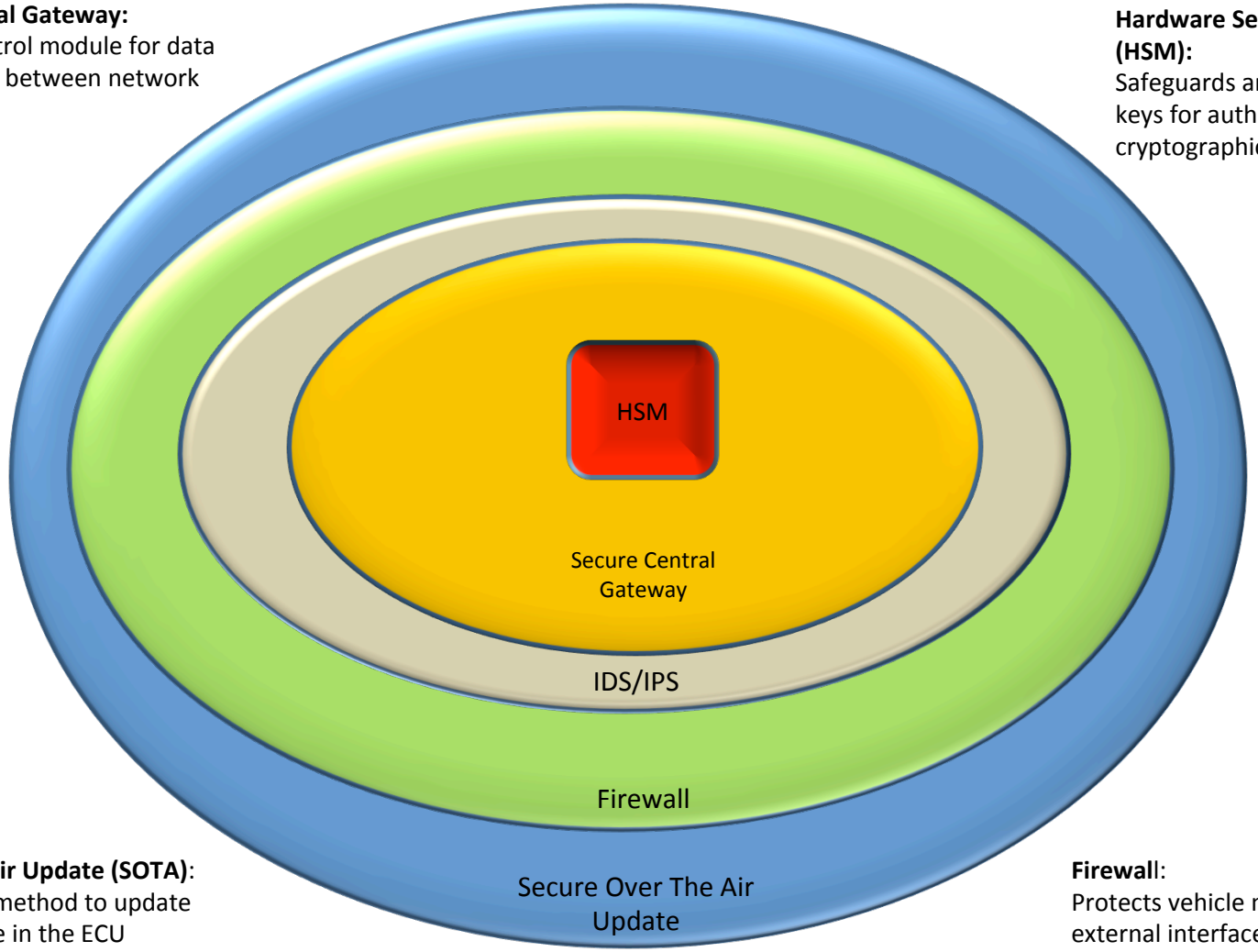
Central Gateway and Vehicle Functions Supported

- Acts as a control module for **data management between the various vehicle network domains** (i.e., engine, interior, body, infotainment, etc.)
- Ability to **process data from multiple vehicle networks**, as well as data from outward facing data sources such as telematics, OBD-II port, USB, Wi-Fi, etc.
- Directs data to a specific network segment based on addressing contained within the CAN packet
- Can be used as a **domain firewall** that does not permit critical ECUs to communicate with external interfaces

Layered Mitigations Example

Secure Central Gateway:
Acts as a control module for data management between network domains

Hardware Security Module (HSM):
Safeguards and manages digital keys for authentication and cryptographic processing



Secure Over The Air Update (SOTA):
Provides a secure method to update and verify software in the ECU

Firewall:
Protects vehicle network from attacks external interfaces

Intrusion Detection/Prevention System (IDS/IPS:
Detects anomalies ,sends alerts, and blocks attacks

Comparison of Mitigation Solutions for Legacy Vehicles

Vendor	HW / SW	Machine Learning	Detect Anomalies	Prevent Unknown Attacks	Prevent Known Attacks	Central Gateway / Network Segmentation	Possible to integrate at Gateway	Hardware Security Module (HSM)	OTA updates	OBD-II Protection	Telematics Protection
A	Both	Yes	Yes	OEM Dependent	Yes	No	Yes	No	OEM Dependent	Yes	Yes
C	SW	Yes	Yes	OEM Dependent	Yes	No	Yes	No	OEM Dependent	Yes	Yes
D	HW	No	Yes (Diagnostic)	No	Yes (Diagnostic)	No	No	No	No	Yes (Diagnostic)	Yes (Diagnostic)

Comparison of Mitigation Solutions for New Vehicles

Vendor	HW / SW	Machine Learning	Detect Anomalies	Prevent Unknown Attacks	Prevent Known Attacks	Central Gateway / Network Segmentation	Possible to integrate at Gateway	Hardware Security Module (HSM)	OTA updates	OBD-II Protection	Telematics Protection
A	Both	Yes	Yes	OEM Dependent	Yes	No	Yes	No	OEM Dependent	Yes	Yes
B	HW	No	Yes	Yes (whitelist)	Yes	No	Yes	No	OEM Dependent	Yes	Yes
C	SW	Yes	Yes	OEM Dependent	Yes	No	Yes	No	OEM Dependent	Yes	Yes
D	HW	No	Yes (Diagnostic)	No	Yes (Diagnostic)	No	No	No	No	Yes (Diagnostic)	Yes (Diagnostic)
E	SW	Yes	Yes	OEM Dependent	Yes	No	Yes	No	OEM Dependent	Yes	Yes
F	SW	Yes	Yes	OEM Dependent	Yes	No	Yes	No	OEM Dependent	Yes	Yes
G	HW	No	No	No	Yes	Yes	Yes (is gateway)	Yes	OEM Dependent	Yes	Yes
H	Both	No	No	Yes	Yes	Yes	Yes (is gateway)	Yes	OEM Dependent	No	Yes

Mitigations Summary

- Legacy Solutions are **here now**
  - Protect most vulnerable interfaces
  - Only 1 layer of defense
  - Most are specialized for a specific make/model, but scalable
  - Limited protection for undocumented "0-day" attacks
- Future solutions are **more robust**
  - Integrate security into vehicle architecture
  - Multi-layer solutions (IDS, IPS, Central Gateway, SOTA, and HSM)
  - Adaptable to new attacks via patching
  - Ultimately, much of the effort will be driven by OEMs and Tier1 Suppliers

Future Cyber Research Community Needs

- The Automotive sector continues to need research in the area of cybersecurity and as the vehicle becomes more connected, the need for cybersecurity "mitigations" become more important

Examples of Cyber Research Community Future Needs

Short-Term 1-3 Years

- Securing both legacy and new design vehicles
- SOTA Architectures
- OBD-II dongle protection (firewalls)
- Secure Infotainment and Telematics Systems (including BYOD protection)
- Automotive Hacker Motivational Database/ Threat Assessment
- Integrated Security Scanning Tools
- Establishment of an Independent testing facility for Government Vehicles
- Penetration Testing Best Practices/Toolsets

Examples of Cyber Research Community Future Needs

Short-Term 1-3 Years

- Securing both legacy and new design vehicles
- SOTA Architectures
- OBD-II dongle protection (firewalls)
- Secure Infotainment and Telematics Systems (including BYOD protection)
- Automotive Hacker Motivational Database/ Threat Assessment
- Integrated Security Scanning Tools
- Establishment of an Independent testing facility for Government Vehicles
- Penetration Testing Best Practices/Toolsets

Long-Term 4-7 Years

- Integrated and Layered Security Architecture
- SOTA Standards/Best Practices
- Real-time intrusion detection and prevention
- Incident Response Algorithms
- Trojan Car Support (e.g. banking, home networks, third parties, etc.)
- Securing ECUs through Binary Code Injection
- Remote On Board Platform Penetration Testing Tools
- Supply Chain/Software Assurance
- CAN Authentication
- Secure Electric Vehicles/Plug-In Vehicles
- Post Attack Forensic Data Recovery
- Cybersecurity And Privacy Curriculum For Academia

Conclusions and Recommendations

Conclusions

- Cybersecurity is a **critical component for vehicles**
- Risks and the potential consequences must be weighed against both economic and operational constraints,
- Automobiles are no longer purely mechanical systems, and must be treated accordingly **to secure vulnerable interfaces**
- Features which are only available on **high-end models will eventually transition into standard models** (e.g. Power windows)
- As **new features become common, attack surfaces expand** and the number of public vulnerabilities grow
- Continuing research in vehicle cybersecurity is needed

Recommendations and Best Practices

- No silver bullet to fix vehicle cybersecurity vulnerabilities until the OEM implements a secure architecture
- One-size fits all is not practical
- Implementation of cybersecurity solution set will be driven by the outcome of an assessment based on the risk to that particular fleet, etc.

- **Short-term (aftermarket) solutions that can be applied to legacy vehicles**
  - Intrusion Detection System (IDS)
  - Intrusion Prevention System (IPS)
  - Firewalls

Recommendations and Best Practices (cont'd)

Long term solutions:

- Most long-term solutions such as Integrated Hardware Security Modules (HSM), IDS, IPS, Firewalls, and secure software Over-the-Air (OTA) Patching will be accomplished at the OEM and Tier 1 Supplier level
- Continuous monitoring and timely reporting of cyber incidents will be vital in assisting to identify vulnerabilities within the fleets
- Timeliness is key to reporting cyber incidents as internet based communication allows for the possible rapid spread of a cyber attack