DOT/DHS: Joint Agency Work on Automotive Cyber Security
March 16, 2017

Brendan Harris, Advanced Vehicle Technology Division

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

- DHS & DOT-Volpe Automotive Cybersecurity R&D Program Overview
- Telematics Cybersecurity
- Open Source Testing Tools
DOT’s Volpe National Transportation System Center

- Established in 1970
- Part of U.S. Department of Transportation (DOT) Office of Research and Technology
- Mission: To Improve the nation’s transportation system by serving as a center of excellence for informed decision making, anticipating emerging transportation issues, and advancing technical, operational, and institutional innovations
- Fee-for-service; no direct appropriations
- [www.volpe.dot.gov](http://www.volpe.dot.gov)
DHS Cybersecurity for Government Vehicles Program – Telematics Overview
Modern Vehicle Architecture

Angles of Attack

V2X (vehicle to everything)
embedded modems
Wi-Fi
TPMS

immobilizer
testing ports
OBD & OBD devices

Automotive Networks

CAN bus
Infotainment Networks

Key
- wired connections
- wireless connections
- direction of communication

telematics
embedded modems
Bluetooth
Wi-Fi cellular

broadcasts
USB
SD
smartphones

CDs
AUX
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
General Services Administration (GSA) Telematics Program

Telematics

• The term “Telematics” refers to a technology that combines telecommunications and information processing to send, receive, and store information related to remote objects, such as vehicles. (Source GAO 14-443, Federal Vehicle Fleets)

• **EO 13693: Sustainability into the Next Decade (March 2016) Requirements**
  - By 2017, all agencies should ensure that telematics collects the maximum vehicle diagnostics (**fuel consumption, emissions, maintenance, utilization, idling, speed, and location data**) at the asset level for acquisitions of new passenger, light duty and medium duty vehicles (where appropriate)

<table>
<thead>
<tr>
<th>Executive Order Reporting Requirement</th>
<th>GPS Tracking Only</th>
<th>GPS Tracking &amp; Vehicle Diagnostics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Speed</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Location data</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Idling</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Utilization</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Maintenance</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Fuel consumption</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Emissions (varies by year, manufacturer, make &amp; model)</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

Source: General Services Administration (GSA) Office of Fleet Management
Cybersecurity Assessment

- Potential risks associated with system
- Wanted to validate security concerns
- Partnered with Software Engineering Institute to do security testing

"It’s secure, we use encryption"

Vendor In 2016
SEI/CERT OBD-2 Device Testing Configuration

- Ettus Research Software-Defined Radio
- WiFi Access Point
- Power Supply
- Linux laptop with OpenBTS
- SIM cards
- Bus Pirate
- Device Under Test
- Android Phones
Software Engineering Institute (SEI) /CERT
OBD-2 Device Tests

- Development / un-configured device (Tested Q1 2016)
  - Accepted unauthenticated admin commands via SMS
  - Could load our own, trojan firmware
  - Unauthenticated service on Internet
  - No encryption in transit

- Production device (Tested Q1 2017)
  - SMS disabled
  - Can no longer force download of trojan firmware
  - Internet service appropriately firewalled
  - Remaining risks
    - Inherent cellular vulnerabilities
    - Still no encryption in transit (Man-in-the-middle)
SEI/CERT: OBD-2 Device Tests Methodology Report

- Explains **risks and potential impacts** of security problems in OBD-II devices

- Describes a **repeatable methodology** for testing the devices for the most common security problems and misconfigurations

- Technical appendices detail **how to perform some of the specialized testing** and what equipment is needed.
Cybersecurity Primer for Fleet Managers

- Fleet Management Solution is an Information System
  - All Federal Information Systems require Federal Information Security Management Act (FISMA) compliance
  - FISMA requires compliance with NIST standards

- Multiple components to the system

- Probability of multiple vendors working collaboratively to provide solution
  - Fleet managers need to remain aware of interactions between devices and and/or vendors
  - Fleet managers responsibility to ensure all devices and vendors comply with NIST guidelines

- Primary responsibility is to protect Government personnel, property, and data
Automotive Cybersecurity
R&D Showcase
Open Source Automotive Cybersecurity Research Tool Forum (October 19-20) – Many automotive cybersecurity Open Source Software (OSS) research tools are in development. Tools support areas: new hardware interfaces, discovery, injection, sniffing, reverse engineering, fuzzing, software defined radio (SDR) and simulation. Forum goals:

- Demonstrate the current state of the art in automotive cybersecurity tools on real automobiles
- Begin to foster researcher-to-researcher relationships
- Share knowledge about cybersecurity research issues and automation challenges
- Incentivize increased academic and security researcher interest in automotive cybersecurity
- Connect tool developers with collaborators, end users, and potential funding sources
Open Source Development Model

Goal: Active Community Development

Adapted from D. Wheeler: “Using an Open Source Software Approach for Cybersecurity Technology Transition”, November 2015
Why Use Open Source?

- Prevent duplication of effort
  - Easier to get started in a new space
  - Develop new rather than existing features

- Technology Transition
  - Fewer barriers to access the technology
  - Easy to continue where someone left off
  - Communication between developers and users

- Continuous Improvement
  - “User as Developer” model creates a positive feedback loop
  - More eyes on code, more bugs identified
Simulation Tool: UDS-SIM

- Created by Craig Smith (Open Garages/Rapid 7)
- Learn what modules are on a given CAN interface
- Simulates learned interfaces
- Useful for testing Diagnostic Tools
  - Dealership tools
  - Scan tools
- Useful for demonstrating attacks without a car and teaching students
- Integrated with open-source fuzzing tool “Peach Fuzzer”

*https://www.acsac.org/ (Annual Computer Security Applications Conference)
Hardware Tool: ChipWhisperer Power Analysis & Glitching Attacks

- Created by Colin O’Flynn (NewAE Technology Inc.)
- Combined hardware and software suite
- Make it easier to test for side channel vulnerabilities

- Power Analysis
  - Used to break encryption protocols such as AES

- Glitching
  - Used to bypass security completely, or cause unintended functions to occur
Information Gathering Tool: CANpy

- Developed by Francois Bernier’s team at Defense Research and Development Canada (DRDC)
- Multi-purpose tool written in Python
  - Data Logging
  - Interacting with CAN bus
  - ECU Discovery
  - Basic Visualization
- Can run on BeagleBone
Wireless Security Tools

- Briefed by Michael Ossmann (Great Scott Gadgets)
- Overview of wireless interfaces in the automotive industry
- Open source hardware interfaces and software suites for wireless security testing
Briefed by Uptane project

- University of Michigan Transportation Research Institute (UMTRI)
- Southwest Research Institute (SwRI)
- New York University (NYU)

- Method to deliver secure updates to automobiles
- Based on The Update Framework (TUF), an open source framework for delivering software updates
Hardware Interfaces

**CANtact**
- Developed by Eric Evenchick (Linklayer Labs)
- CAN to USB interface
- Supports custom scripting

**CanCAT**
- Developed by Matt Carpenter (Grimm SMFS)
- CAN Transceiver for providing low-level access to CAN bus
- Useful for Man-in-the-middle and reverse engineering functionality for a particular ECU
Light Detection and Ranging (LIDAR) Spoofing (brief)

- Briefing by Jon Petit (Security Innovation Inc.)
- One of the key sensors for Automated Vehicles
- Possible to create ‘fake’ objects and cause vehicle to treat them as real objects
Virtual workbenches are needed due to limited vehicle access
A growing proliferation of open source tools
Open source tools are getting more powerful and sophisticated
Open source software/hardware significantly lowers the entry barrier for researchers
“User as developer” model creates positive feedback loop
Open Source Automotive Cybersecurity Research Tool Forum – Next Steps

- Development of an Open Source OS Tools Portal for use by Government researchers, and academia

- Continuation of the Automotive Cybersecurity R&D Showcase type of event with more “hands on” activities (e.g. academia training classes)

- Continued outreach to the open source community
So what does this have to do with supply chain?

- **Tools and Methods are out there** –
  - **Acquisition Officers** - Use procurement language to ensure you are purchasing secure components
    - “We have encryption” promises aren’t enough
    - Ask for 3rd party validation & documentation
    - Ask about updates
  - **System Owners** - Do your own security testing to validate aftermarket products integrated in your system
    - Know what risks you are introducing to your system
    - If you are “not a cyber person” talk to one
  - **Vendors** – Security does not end at the sale, make sure you have a way to securely update your device
    - Get your products Pen Tested, have the documentation on hand & fix the bugs
    - Accept that bugs will be found, create a vulnerability disclosure policy
Contact Information

Brendan Harris
Advanced Vehicle Technology
USDOT Volpe Center
Email: Brendan.Harris@dot.gov
Phone: 617-494-2833