Electric Vehicle Cyber Research

Kenneth Rohde
Idaho National Laboratory
August 16, 2017
Background
CAN Bus Security (2013)
CAN Bus Physical Access

- Discovered, as theorized, to send valid CAN messages, attackers DO NOT have to be connected via OBD-II interface
- Control over devices was proven by accessing a wiring harness under the rear bumper and unlocking the doors, opening the trunk, and starting the engine
Gateway Devices

- Devices responsible for moving or rebroadcasting traffic from one CAN to another were fairly easy to identify
  - Diagnostic messages helped identify the gateways and actual ECU locations
- Monitoring of the multiple networks during “aggressive driving” identified where some messages were actually generated
- Another very good location and scenario for fuzz testing, but this project’s time was too limited
<table>
<thead>
<tr>
<th>Test Vehicle</th>
<th>Number of CAN</th>
<th>Use of CAN</th>
<th>Other Buses</th>
</tr>
</thead>
<tbody>
<tr>
<td>2012 Domestic</td>
<td>2 High Speed 1 Low Speed</td>
<td>Command &amp; Control Status OBD II OEM Diagnostics &amp; Programming</td>
<td>LIN</td>
</tr>
<tr>
<td>2014 Domestic</td>
<td>2 High Speed 1 Low Speed</td>
<td>Command &amp; Control Status OBD II OEM Diagnostics &amp; Programming</td>
<td>LIN</td>
</tr>
<tr>
<td>2012 BEV</td>
<td>4 High Speed</td>
<td>Charge Control Status OEM Diagnostics &amp; Programming</td>
<td>None</td>
</tr>
<tr>
<td>2016 PHEV</td>
<td>8+ High Speed 2+ Low Speed</td>
<td>Command &amp; Control Status OBD II UDS OEM Diagnostics &amp; Programming</td>
<td>Ethernet FlexRay MOST LIN</td>
</tr>
</tbody>
</table>
Nomenclature

- **PEV** (plug-in electric vehicle) are defined as any vehicle that connects or plugs in to the grid to fully recharge the traction battery pack
  - **BEVs**: battery electric vehicle
    - no internal combustion engine (ICE)
    - no fuel tank
  - **EREVs**: extended range electric vehicles
    - operates on electricity first
    - when electric range has been exceeded, operates like a normal hybrid electric vehicle
  - **PHEVs**: plug-in hybrid electric vehicles
    - blended electric and ICE operations in various schemes
Nomenclature

- **Charging infrastructure**
  - **Level 1 EVSE:**
    - AC 110/120V electric vehicle supply equipment (up to 1.4 kW)
    - SAE J1772 standard
  - **Level 2 EVSE:**
    - AC 208/240V electric vehicle supply equipment (up to 19 kW)
    - SAE J1772 standard
  - **DCFC: DC fast chargers (50 kW)**
    - CHAdeMO
    - SAE Combo Connector (CCS)
Smart Grid EVSE Assessments (2014)

• Four prototype Electric Vehicle Supply Equipment (EVSE) stations tested in 24 months
  – Level 2 AC Units (208-220 VAC)
• These units were “smart grid” enabled
• Each was evaluated for cyber security issues
  – Remote compromise
  – Unauthorized access and control
  – Firmware modifications
  – Potential impact to the Energy Grid
• Issues were reported to the vendor to help secure the product before it is commercialized
Vehicle-to-Infrastructure (2015)

- Research focusing on the cyber security of the interconnectivity between vehicles, charging stations, and the Energy Grid
- Lots of potential for research, but very little technology available...
Electric Vehicle DC Fast Charging

• Potential for overcharging the large lithium batteries since the Plug-in Electric Vehicle (PEV) is negotiating with the charger
  – Demands a variable charging rate
  – Notifies when to stop

• This communication is done over CAN Bus or Power Line Carrier (PLC)

• What are the implications for Critical Infrastructure?

• Procured a DC Level-2 Fast Charger (DCFC) with both a CHAdeMO and a SAE J1772-Combo cordset
The Problem
Attack Pathway

- Compromised PEV infects DCFC and vice versa
Compromise Details

1. PEV Charge Module

2. DCFC Vehicle Controllers

3. DCFC Local Server
Problem Details

- This DCFC is 480 VAC 100 A (50 kW, 500 VDC, ~125 A)
  - Future fast charging standards will push up to 400 kW
- Who owns the EVSE? What network(s) is it connected to?
- Does the utility company consider EVSE as part of their electronic (network) perimeter?
  - What about the EVSE owner (e.g. campus network)?
- Is the utility company ready to deal with the increased load, harmonic distortion, and noise?
- Remember... any idiot can purchase and modify a PEV
Considerations

- A compromised PEV is not only a potential safety concern, but it is also a grid network access concern.
- The biggest potential problem is for a coordinated charging event that causes widespread disruption of the grid.
A Potential Solution
U.S. DOE - VTO
Electric Vehicle Infrastructure Laboratory

- Evaluate Conductive and Wireless Charging Systems
  - System Efficiency
  - EM-field emissions
  - Power quality
    - Total harmonic distortion
    - Power factor
    - Transient response
  - Cyber security assessment
    - Communications security
      - Wired and wireless
    - Software and firmware
- Wide range of input power
  - 120 VAC, 208 / 240 VAC, 480 VAC 3 phase
  - 400 kVA total capability
- Grid Emulator (60 kVA) enables the evaluation of charging infrastructure performance and response during transient grid events
Grid Modernization Laboratory Consortium

- DOE Vehicle Technology Office funded a 3 year effort to develop a framework for securing the integration of electric vehicles, charging stations, and a Building Energy Management System (BEMS)
  - Collaborative work with other DOE labs, universities, and industry

- Initial project scope includes a cyber security assessment of 2 commercial AC Level-2 EVSE units
  - The identified cyber security issues will be used later to demonstrate project functionality

- INL is developing a set of Diagnostic Security Modules (DSMs) that will be integrated with the PEVs, EVSEs, and the Building Energy Management System (BEMS)
  - This functionality will someday be implemented by OEMs and vendors

- The DSM framework will allow a BEMS operator to intelligently decide if a PEV or EVSE is allowed to operate in the building infrastructure by notifying the operator of any cyber security issues

- DSM will be tested in a large scale EV lab environment by a “red team”

1) DSM senses closest EVSE using Bluetooth Low Energy
2) DSM Associates with EVSE using WPA-2 Protected WiFi
3) DSM sends security snapshot to EVSE
4) EVSE forwards security snapshot to BEMS
5) BEMS (or operator) makes decision to allow/deny charging
6) EVSE allows or denies charging
Project Details

- Inspired by a paper published by IBM T.J. Watson Research Center
  - “Secure Coprocessor-based Intrusion Detection”
- This is not another 3rd party security product for people to procure
- All technical details and results will be published to industry
- Support and feedback to emerging standards
  - Smart Energy Profile (SEP) 2.0 (Message API)
  - SAE J2931/7 (Standard Telematics API)
Vehicle Monitoring DSM

- Monitoring the primary CAN Buses as well as other diagnostic interfaces (e.g. K-line)
  - Traffic patterns, OBD, UDS/KWP, J2534, etc.
- Monitoring key Electronic Control Units (ECUs) for modification
- Generating a vehicle wide fingerprint at a known good state
- Experimentation in attempt to determine physical failure vs. cyber event
Vehicle Monitoring Methods

- **Diagnostic “Active Test” Messages**
  - Messages used by OEM tools for physical manipulation and testing

- **Conflicting Message Injection**
  - Valid messages competing with current messages to cause behavior

- **Program Modifications**
  - Changes in firmware or configuration to cause behavior

- **Error Frame Injection**
  - Convince modules that reads or writes on the CAN Bus failed

- **Physical Bus Alteration**
  - Some idiot plugged something into my car
EVSE Monitoring DSM

- **“Secure Coprocessor-based Intrusion Detection”**
  - Integrated with EVSE via JTag, I2C, SPI, etc.

- Monitoring vehicle to EVSE communications
  - J1772 PWM signal
  - CHAdeMO CAN Bus
  - CCS PLC/TCP

- Monitoring network (cellular) utilization and traffic patterns
EVSE Monitoring Methods

Via JTag Access

- Protected Memory Pages
  - Kernel memory modifications

- CPU Load and Memory Utilization
  - Abnormal usage or new processes

- Network Bandwidth
  - Why is my EVSE using so much bandwidth?

Via Serial Access

- System Statistics
  - What is Linux lying about this time?

- Process Monitoring
  - Who might be hiding?
DSM Hardware

- **COTS hardware components**
  - Raspberry Pi 3
  - CAN interfaces
  - JTag controllers

- **Small, self-contained module easily located in vehicle or EVSE**

- **Low cost prototypes**
  - Vehicle DSM ~ $180
  - EVSE DSM ~ $100 + JTag controller
The Bigger Picture

- A lack of PEV cyber security can lead to widespread disruption of the electric grid
- Security analysis of this large and complex problem is necessary
- This requires coordinated and collaborative research
Closing Thoughts

• We are still a long way from a unified communication architecture
  - We can’t even decide on a charging plug

• If security is priority, the OEMs and vendors must work together

• Functionality similar to DSM must be incorporated in emerging products and standards

• With the increase of electric vehicle adoption comes the increased load and risk to the energy grid and an expansion of potential network entry points
Questions

Kenneth Rohde  
(208) 526-0672  
kenneth.rohde@inl.gov

More Information:  
https://energy.gov/oe/services/technology-development/cybersecurity-for-energy-delivery-systems  
https://informaticsinstitute.louisiana.edu/  
http://nsfcvdi.org/wordpress/  
http://www.inl.gov