Grid Modernization Laboratory Consortium: Diagnostic Security Modules for Electric Vehicle-to-Building Integration (163)

PI: Kenneth Rohde, INL

Cyber Security R&D
21 June 2018

Project ELT 196

INL/CON-18-45136

Overview

Barriers

- Energy Security: Support the Energy Independence and Security Act of 2007
- Vehicle Cyber Security: Addressing the emerging needs for integrated cyber security tools and methods in EV, EVSE, and connected buildings

Partners

- Project Lead: INL
- EDU: University of Louisiana at Lafayette
- Other Laboratories: ANL, NREL, PNNL
- Commercial: ChargePoint, Inc.

Timeline

- Start Date: May 1, 2016
- End Date: May 31, 2019
- Percent Complete: 66%

Budget

- FY-16 = $500K (DOE)
- FY-17 = $650K (DOE)
- FY-18 = $500K (DOE)

Project Objectives

Overall Objective: Develop a Diagnostic Security Module (DSM) Framework to provide secure communications between electric vehicles (EVs) and buildings

- Provide near real-time information regarding the security state of the monitored systems so that operators can make informed decisions and allow or deny EV charging
- Demonstrate a multi-vendor integrated environment running hardware, software, and monitoring algorithms that exchange security health information with a centralized server and operator
- Publish all findings and developed methods and algorithms to aid in the adoption of emerging security and protocol standards (SEP 2.0, SAE J2931/7, ISO 15118-1, DIN 70121, OCPP, etc.)

Previous Years Objectives:

- Perform a complete Cyber Security assessment of two commercial Electric Vehicle Supply Equipment (EVSE) charging stations
- Prototype communications hardware for security communications between EVSE, EV, and a Building Energy Management System (BEMS)
- Build and test selected DSM hardware and implement the initial framework communications network
- Initial development of monitoring algorithms for EV and EVSE and integration of DSM nodes with multiple systems

Project Objectives

Current Objectives:

- Add DSM hardware and software at the NREL vehicle laboratory. Perform functional testing of the combined NREL and INL vehicle labs.
- Complete a risk assessment of the DC Fast Charging (DCFC) station at INL to understand the extent of potential grid impacts (new scope).
- Develop DSM hardware and algorithms for monitoring DCFC and the connected EV (new scope).
- Complete a cyber security assessment of the vehicle labs to determine the effectiveness of the DSM framework.
- Publications of the DSM framework methods, algorithms, and protocol. Publication of an integration document for DSM to BEMS communications.
- Demonstration of a DSM enabled charging station at CyberAUTO 2019 (new scope).

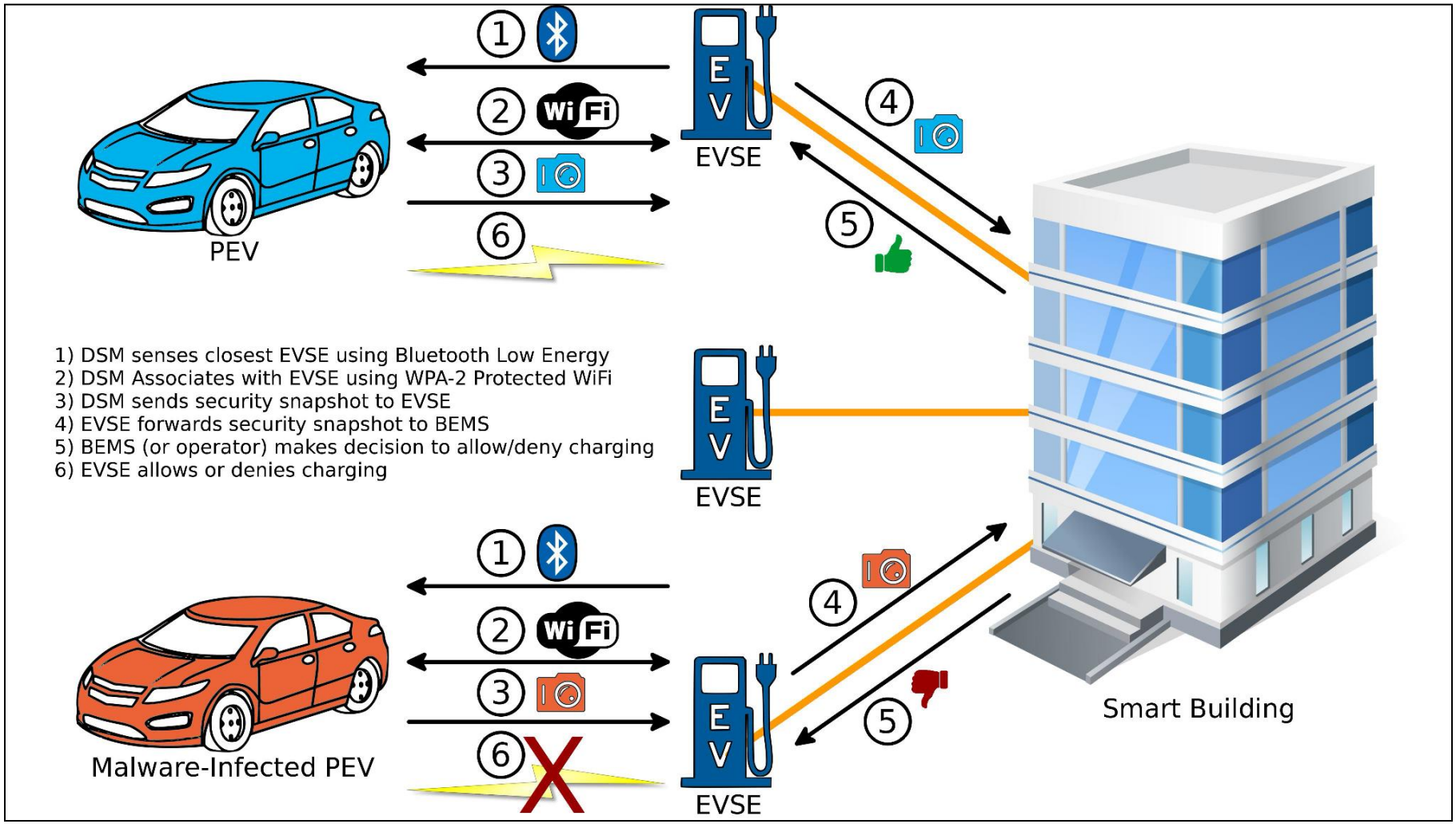
Year 1, 2 Milestones

Date	Semi-Annual and Annual Milestones	Status
October 2016 (6 Months)	Complete initial equipment setup in INL laboratory space and the initial development of the DSM framework and communications channels. Start the cyber security assessment of the ChargePoint EVSE.	Complete
April 2017 (Year 1)	Delivery of the Cyber Security Assessment performed on the ChargePoint EVSE.	Complete
October 2017 (Year 1.5)	Implementation of DSM nodes suitable for use in EVSE and EV. Initial device and vehicle fingerprinting algorithms developed.	Complete
April 2018 (Year 2)	A complete BEMS-to-EVSE-to-EV DSM framework implemented in the prototype environment at INL. A demonstration of the functionality of the system provided to all partners.	Complete

Year 3 Milestones

Date	Semi-Annual and Annual Milestones	Status
October 2018 (Year 2.5)	Deployment of the DSM framework in the partner vehicle laboratory environment. A working demonstration of the DSM framework in the integrated lab environment.	Coordination Started
April 2019 (Year 3)	A publication of the developed methods for monitoring DSM connected EV and EVSE. This includes the algorithms used for generating the system fingerprints and detecting anomalous behavior. A detailed specification of the protocols developed and used for exchanging the security information from EV and EVSE to the BEMS. Cyber security testing (red team vs. blue team) of the vehicle labs to examine the performance and functionality of the DSM framework. A final report detailing the effectiveness of DSM and the security framework during the cyber assessment.	Queued

Architecture Overview



Approach

Contracts and Agreements

- University of Louisiana at Lafayette
- ChargePoint

System Baseline

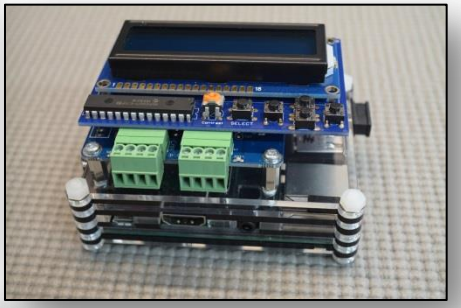
- ChargePoint EVSE assessment report delivered
- Nissan Leaf and Chevy Volt selected

Prototype Environment

- DSM hardware and software development is in beta testing

Framework Development

- Algorithms implemented and being tested
- Additional algorithms and authentication / authorization capabilities in development for DC Fast Charging



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
- BEMS integration available via JSON and BACnet/IP

Vehicle DSM

- Monitoring the primary CAN Bus(es) 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

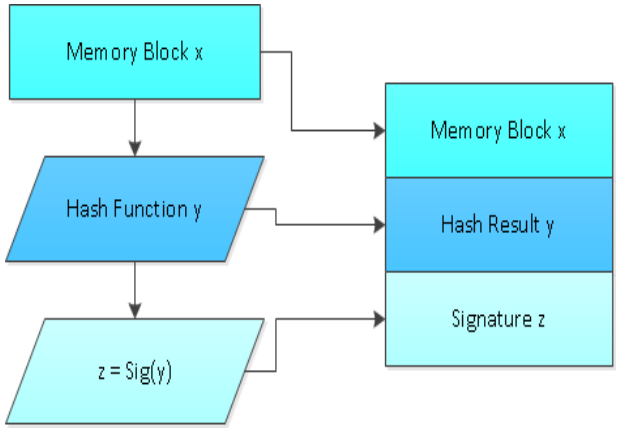
Diagnostic “Active Test” Messages
- Messages used by OEM tools for physical manipulation and testing

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



Level 2 AC EVSE DSM

- "*Secure Coprocessor-based Intrusion Detection*"
  - Integrated with EVSE via JTag, I2C, SPI, etc.
- Monitoring EV to EVSE communications
  - J1772 PWM signal
- Monitoring network (cellular) utilization and traffic patterns

Protected Memory Pages
- Kernel memory modifications

CPU Load and Memory Utilization
- Abnormal usage or new processes

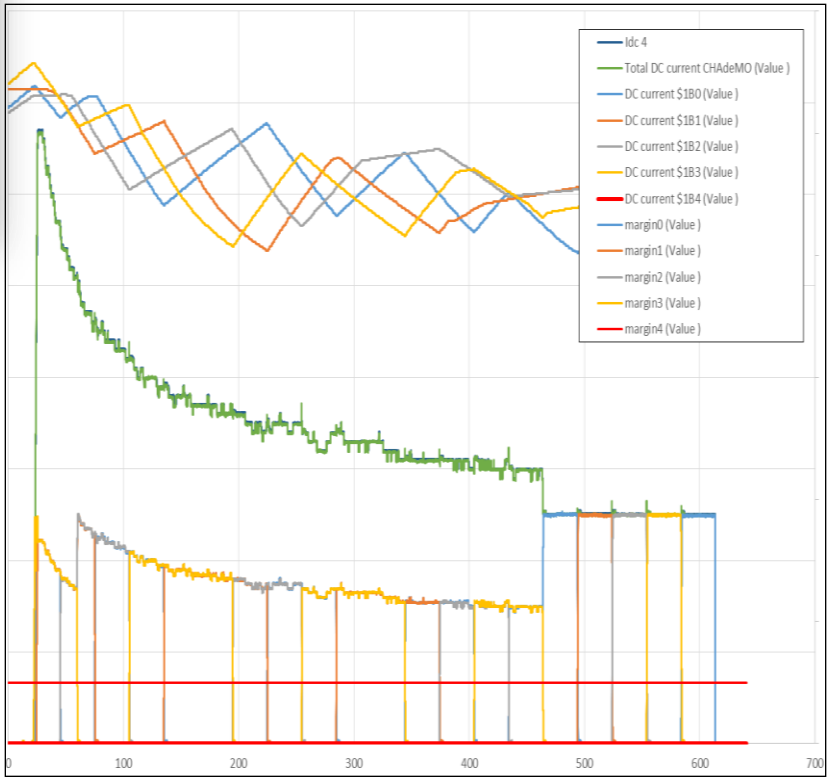
Network Bandwidth
- Why is my EVSE using so much bandwidth?

System Statistics
- What is Linux lying about this time?

Process Monitoring
- Who might be hiding?

DC Fast Charge DSM

- ABB Terra 53CJ Station
  - CHAdeMO
  - CCS
- 50 KW capacity
  - 5 x 10 KW modules



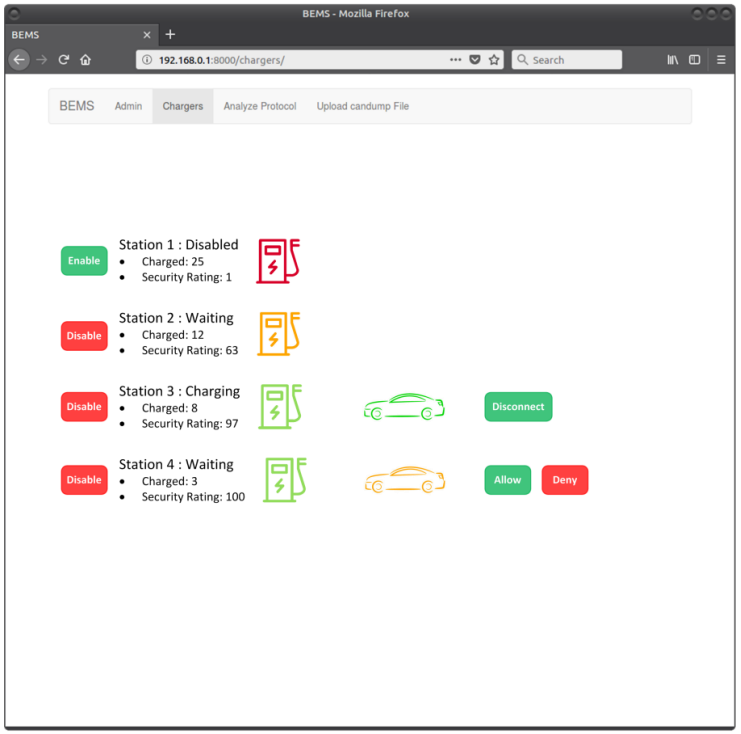
Internal control of power converters
- Is the module control typical?

Normal charge behavior
- CHAdeMO CAN Bus
- CCS PLC/TCP
- Deviations from baseline

Monitoring external connectivity
- Vendor control and logging

BEMS Integration

- Currently, status and requests are sent to a webserver
- Cyber security data is available as JSON objects and also published using BACnet/IP
- Operator takes appropriate action from the BEMS console
- Additional “open” data formats may be supported (e.g. LonWorks)



Response to Previous Year Reviewer's Comments

This project was not reviewed last year

Partners/Collaborators

ChargePoint, Inc.

- Providing the EVSE Application Program Interface (API) and technical support

University of Louisiana at Lafayette

- Utilizing resources available from the Informatics Research Institute
- Providing expertise in system information analysis

California Energy Commission

- Technical advisors for the project

ANL, PNNL, NREL

- Integrating DSMs into the vehicle building integration project
- Providing a system-level testing opportunity

Remaining Challenges and Barriers

- DC Fast Charging added as necessary scope
  - Public charging infrastructure is trending toward high power charging
  - Larger potential for grid impacts
- Baseline / fingerprint monitoring is not ideal
  - Vehicles, batteries, and EVSE change their properties with time
  - Monitoring needs to be implemented by the vendors and OEMs
- Physical failures vs. cyber attack
  - Determination of the source of an event is still very difficult

Proposed Future Work

Ongoing FY-18

- Add DSM hardware and software at the NREL vehicle laboratory. Perform functional testing of the combined NREL and INL vehicle labs.
- Complete a risk assessment of the DC Fast Charging (DCFC) station at INL to understand the extent of potential grid impacts.

FY-19

- Develop DSM hardware and algorithms for monitoring DCFC and the connected EV.
- Complete a cyber security assessment of the vehicle labs to determine the effectiveness of the DSM framework.
- Publications of the DSM framework methods, algorithms, and protocol. Publication of an integration document for DSM to BEMS communications.

Summary

Relevance

- Developing a Diagnostic Security Module (DSM) Framework to provide secure communications between electric vehicles and buildings
- Provide real-time information regarding the security state of the monitored systems so that operators can make informed decisions and allow or deny electric vehicle charging

Approach

- Cyber security assessment of the prototype environment to discover potential weaknesses and vulnerabilities
- Methods and algorithms developed to fingerprint a healthy EV and EVSE
- Small and inexpensive hardware monitor EVs and EVSEs and communicate with a BEMS

Accomplishments

- Assessments of 2 commercial EVSE complete
- DSM hardware identified and implemented in an alpha framework environment
- BEMS selected and integration with EVSE started
- DC Fast Charging risk assessment started

Partnerships

- Industry and government partners to ensure research is applicable and effective
- University of Louisiana at Lafayette provides informatics expertise and coordination with the state and local government
- Project being coordinated with other efforts funded by VTO
  - GM0085 – Systems