VTO Diagnostic Security Modules for Electric Vehicle to Building Integration

PI: Kenneth Rohde
Presenter: Barney Carlson

Cyber Security R&D Department
7 June 2016

Project ID VS184

This presentation does not contain any proprietary, confidential, or otherwise restricted information

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 PEV, EVSE, and connected buildings

Timeline

- Start Date: April 1, 2016
- End Date: September 31, 2018
- Percent Complete: 0%

Partners

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

Budget

- FY-16 = $500K (DOE)

Project Objectives

Overall Objective: Develop a Distributed 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
- The developed hardware, software, and monitoring algorithms will be shared with industry and standards committees to help ensure safe and secure energy delivery

Year One (FY-16) Objectives:

- Perform a complete Cyber Security assessment of a commercial Electric Vehicle Supply Equipment (EVSE) charging station
- Customize INL developed tools to operate in a laboratory owned Plug-in Electric Vehicle (PEV)
- Prototype communications hardware for security communications between EVSE, PEV, and a Building Energy Management System (BEMS)

Milestones

Date	Milestones and Go/No-Go Decisions	Status
October 2016	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.	In Process
October 2016	**Go/No-Go:** A CRADA or NDA agreement between INL and the University of Louisiana must be fully executed.	In Process
April 2017	Delivery of the Cyber Security Assessment performed on the ChargePoint EVSE	Queued
October 2017	Implementation of DSM nodes suitable for use in EVSE and PEV. Initial device and vehicle fingerprinting algorithms developed.	Queued
October 2017	**Go/No-Go:** DSM modules functioning in multiple PEV and EVSE units and coordinated by a BEMS operator.	Queued

Milestones

Date	Milestones and Go/No-Go Decisions	Status
April 2018	A complete BEMS-to-EVSE-to-PEV DSM framework implemented in the prototype environment at INL. A demonstration of the functionality of the system provided to all partners.	Queued
April 2018	**Go/No-Go:** DSM framework functioning in partner laboratory environment with multiple PEV and EVSE units.	Queued
October 2018	Deployment of the DSM framework in the partner laboratory building environment. A working demonstration of the DSM framework in the new integrated building environment. Cyber security testing (red team vs. blue team) of the building environment 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 (red team vs. blue team). Delivery of the DSM security protocol to the proposed industry standards. A detailed specification of the DSM protocol is provided.	Queued

Approach and Strategy

System Baseline

- Cyber Security Assessment of the EVSE to understand weaknesses and vulnerabilities
- Monitor the PEV to determine what normal communications are present

Algorithm Development

- Develop method for generating a valid system fingerprint for the PEV and EVSE
- Develop methods for determining if/why a system is functioning improperly

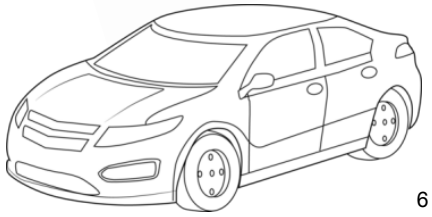
Prototype Environment

- DSM hardware identified and basic communications established
- DSM hardware installed in the EVSE and PEV in the INL lab space

Go/No-Go

- CRADA agreement with Lafayette

Phase 1 – FY-16



Approach and Strategy

Algorithm Analysis

- Further testing and development to determine if methods and algorithms are able to properly identify system problems in EVSE and PEV

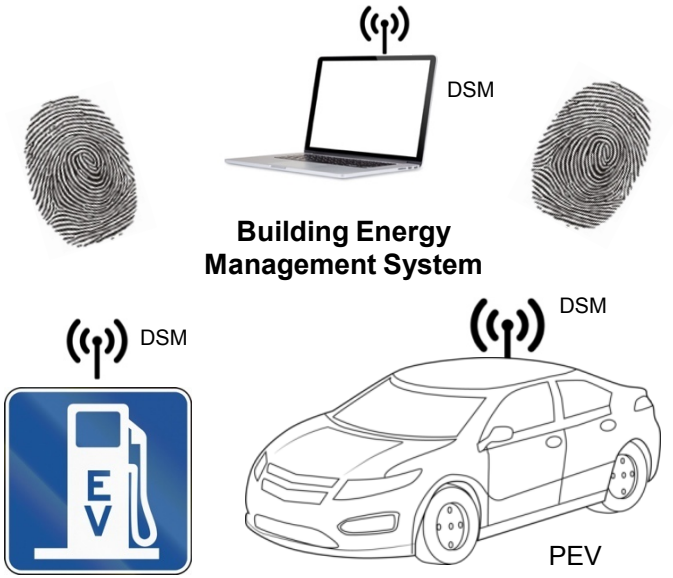
Laboratory Environment

- Integration of DSMs in the INL lab space with coordinated connectivity between the PEV, EVSE, and BEMS (security exchange protocol development)
- DSMs report suspicious or abnormal behavior to the BEMS
- BEMS operators are informed of problems so that they can take action
- Demonstration of functionality provided to VTO and partners

Go/No-Go

- DSMs functional in multiple PEV and EVSE units and are coordinated by a BEMS operator

Phase 2 – FY-17



Approach and Strategy

System Analysis

- Installation of DSM framework at partner laboratory
- DSM environment functioning with multiple EVSE and PEV
- Red vs. Blue (penetration) testing of DSM framework environment

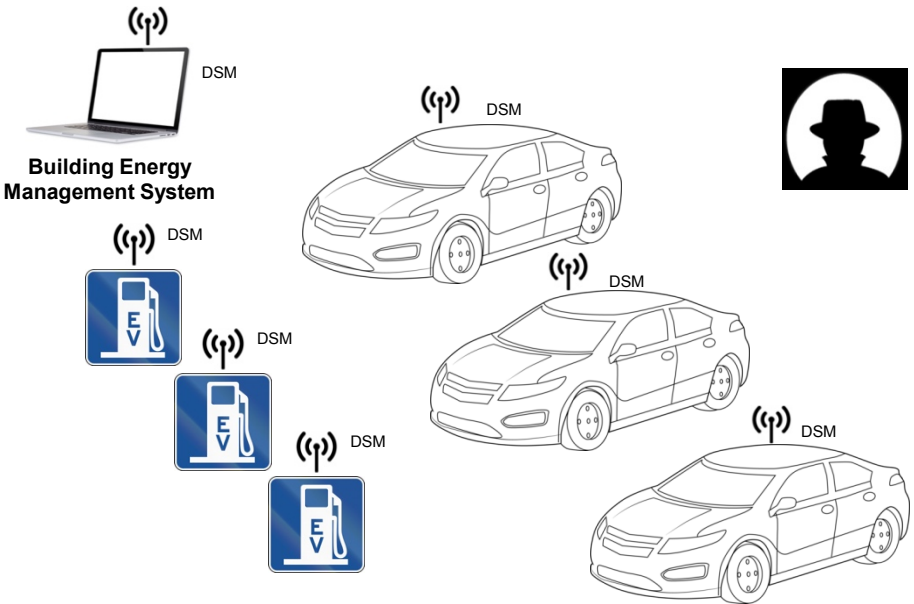
Industry Transfer

- Methods and algorithms for systems monitoring published
- Security exchange protocol published to standards bodies (e.g. SEP 2.0, SAE J2931/7)

Go/No-Go

- DSM framework functioning in partner laboratory environment with multiple PEV and EVSE units

Phase 3 – FY-18



Accomplishments

Contracts and Agreements

- ChargePoint NDA submitted
- Lafayette NDA, contract, and CRADA started

System Baseline

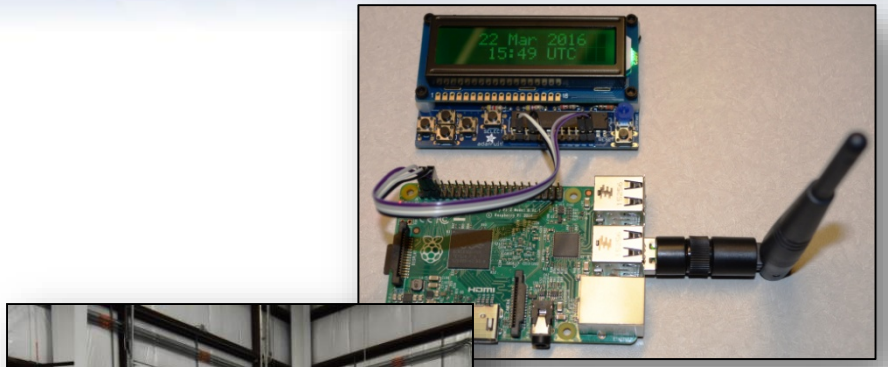
- ChargePoint EVSE procurement in process
  - Assessment starting soon
- PEV identified and allocated for project
  - Systems analysis on-going

Prototype Environment

- DSM hardware procured and development has started

Algorithm Development

- Lafayette identifying graduate students and starting analysis of EVSE



Response to Previous Year Reviewer's Comments

This project has just started the first 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

Future challenges and barriers are consistent with the initial work scope

Proposed Future Work

FY-16

- Procurement and setup of prototype laboratory and equipment
- Cybersecurity Assessment of selected EVSE(s) and PEV

FY-17

- Development of EVSE and PEV methods and algorithms for fingerprinting
- Deployment of DSMs in prototype laboratory environment

Summary

Relevance

- Developing a Distributed 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

Accomplishments

- Contracts and agreements with all partners started
- Prototype hardware identified and procurement process started
- Lab space and PEV EVSE equipment installed

Approach

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

Partnerships

- Industry and government partners to ensure research is applicable and effective
- Project being coordinated with other efforts funded by VTO
  - GM0085 – Systems
  - GM0062 – Vehicle to Building Integration Pathways