CAN Bus Security Across Multi-Sector Platforms

Jonathan Chugg
Kenneth Rohde

www.inl.gov

Idaho National Laboratory

STIMS: INL/MIS-15-36290

Internal Research Efforts

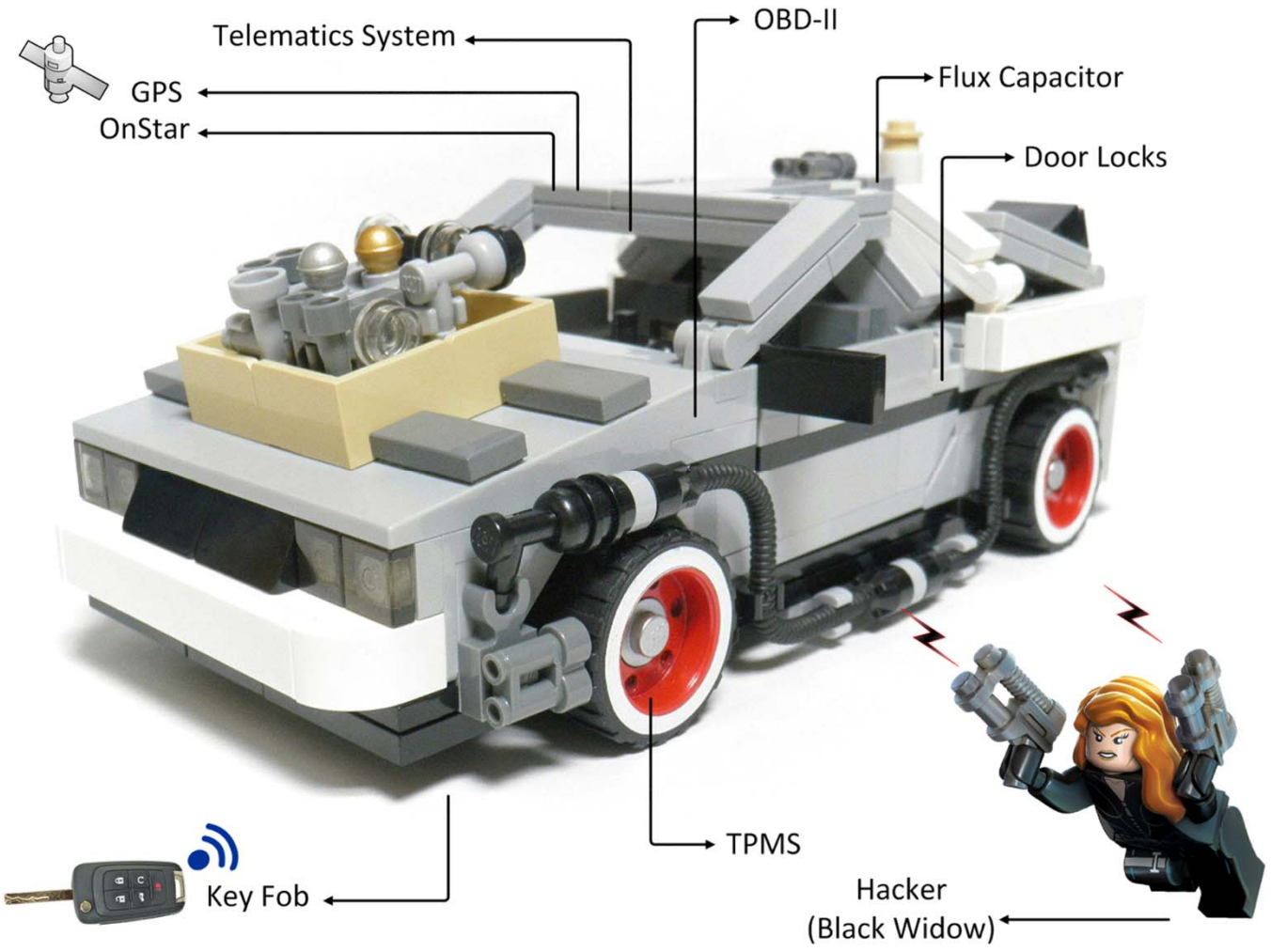
Modern CAN bus

- The CAN protocol has grown and now supports many different protocols which are used in a wide variety of areas:
  - Automotive
  - Road & Rail Transport
  - Industrial Automation
  - Power Generation
  - Maritime
  - Aviation
  - Military
  - Medical Devices
- CAN bus specification does not provide low-level security features
  - Each manufacturer may provide their own security mechanisms.
- Systems that use CAN bus are often constrained on resources and security mechanisms are weak and easy to defeat.

Project Goals

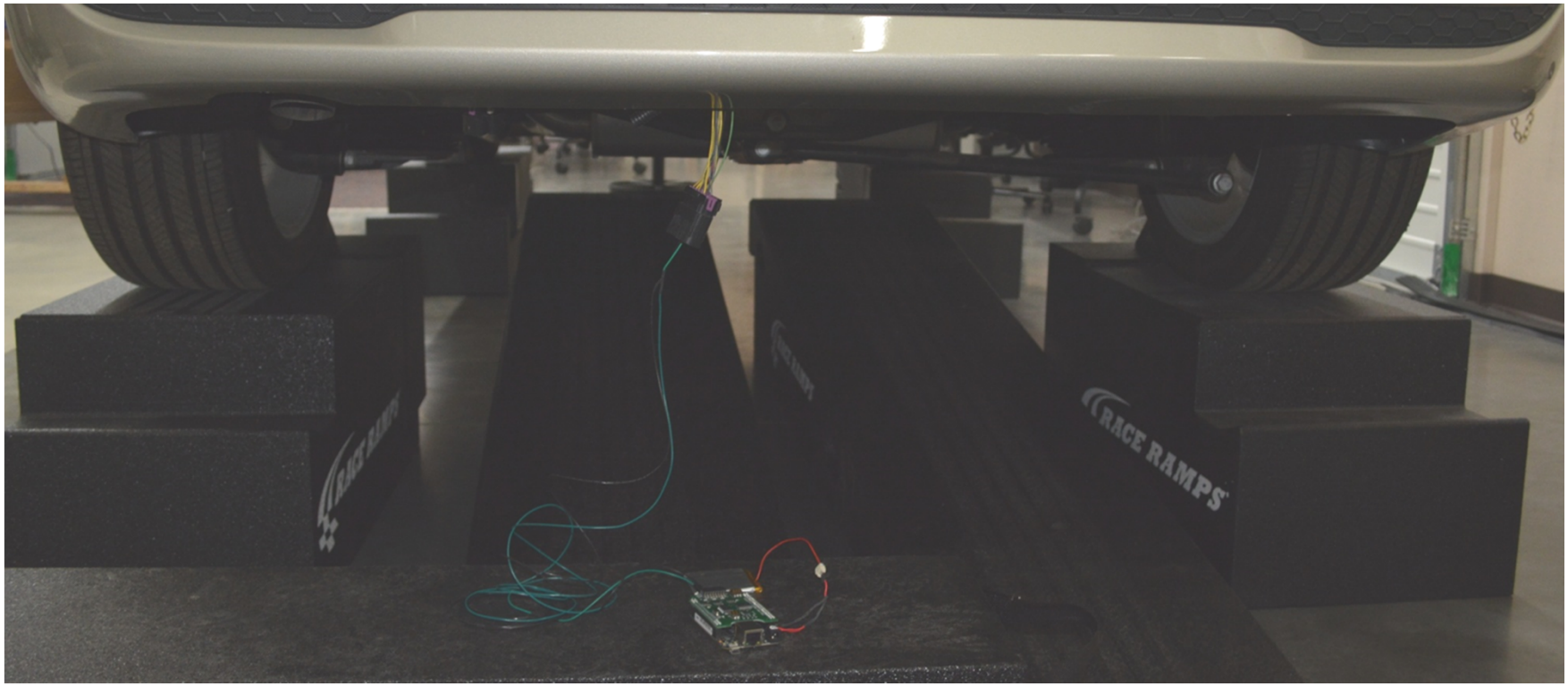
- Limited access to full CAN network?
  - Identify the possibility of circumventing CAN gateways and migrate from one CAN network to another.
  - Identify and asses vulnerabilities that can be exploited remotely to gain control of CAN.
- What are the outside effects of a compromised vehicle?
  - Identify effects on traffic, traffic control systems, and electric grid (V2V, V2I, DC Fast Charging).
  - Identify and asses vulnerabilities that can be exploited to gain control of external entities to CAN, or vise-versa.
- Other sectors vulnerable?
  - Fuse current INL critical infrastructure research into vulnerability assessment methodologies with research to determine vulnerability exposure for other sectors
- Identify and develop tools, products, or methodologies for mitigation

Modern Vehicle Attack Targets



CAN Bus Direct Network Access

- Discovered, as theorized, that to have control over devices on CAN network, 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 and opening the trunk.



Electric Vehicles

- Potential for overcharging the large lithium ion batteries since the car is communicating with the charger
  - Demands a variable charging rate
  - When to stop
- This communication is done over CAN bus
- What are the implications for Critical Infrastructure?

- Procured an ABB Terra DC Fast Charger with a CHAdeMO and SAE J1772-Combo plug charging interfaces
- Working with EES&T to do additional testing between vehicle, charger, and micro-grid

Vehicle-to-Infrastructure

- Acquired an all electric vehicle
  - Supports CHAdeMO
- Research will focus on the cyber security of the interconnectivity between vehicles, charging stations, and the Energy Grid
- Lots of potential research and findings

Vehicle-to-Infrastructure & Electric Vehicles

- Since control of the charging station is managed by the car, potential attacks could occur, including physical damage and propagation of malware (i.e. vehicle and charging station worms)

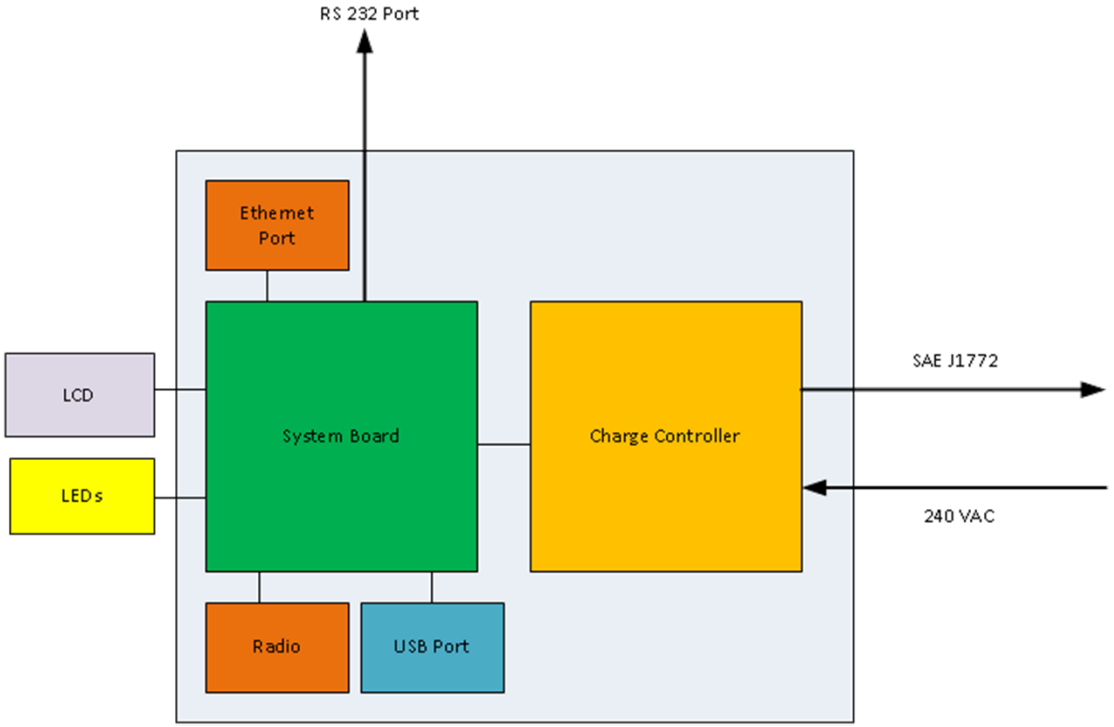
Smart Grid EVSE Assessments

Background

- The INL was selected to perform the Cyber Security Assessment of four EVSE Level 2 charging stations produced in response to a DOE NETL FOA.
- The units were required to implement remote management features suitable for the Smart Grid.
- The units were first tested by INL EES&T for energy efficiency and functionality.
- The units delivered were designed to be used in either a residential or commercial setting.
- These prototype chargers were designed and implemented by:
  - Siemens Corporate Research
  - General Electric
  - Eaton
  - Delta

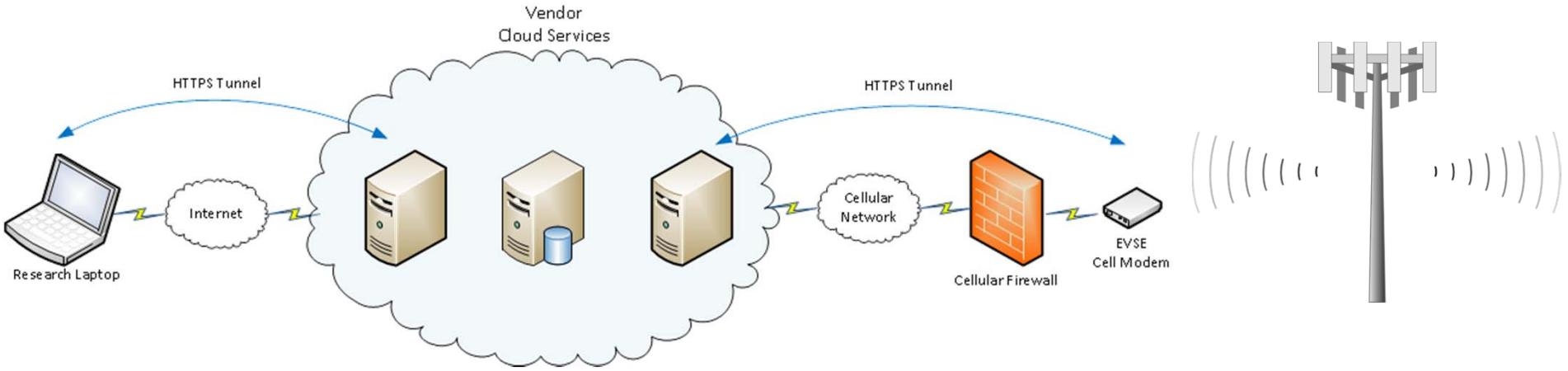
Basic Design

- Provide functionality for scheduling, curtailment, and authorization
- Each unit used existing hardware for the vehicle to charger interface
- An additional board was added to the system to provide remote management
  - All of the systems used an embedded Linux platform running on ARM



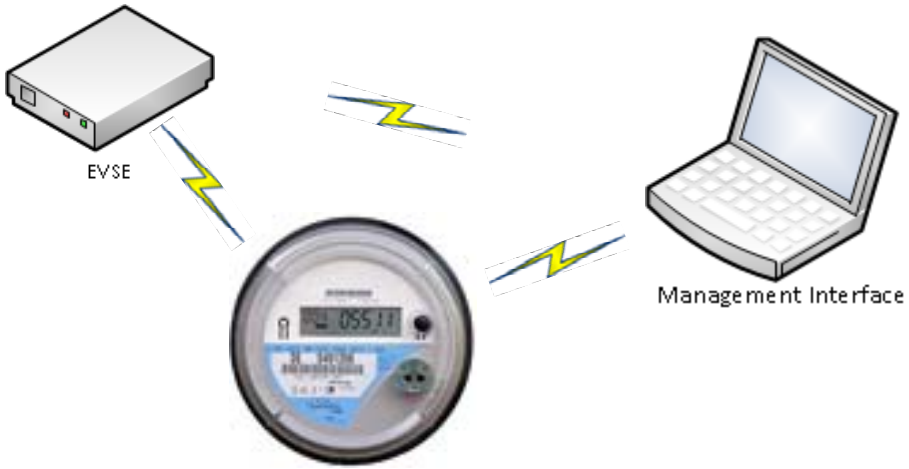
Remote Management (Commercial)

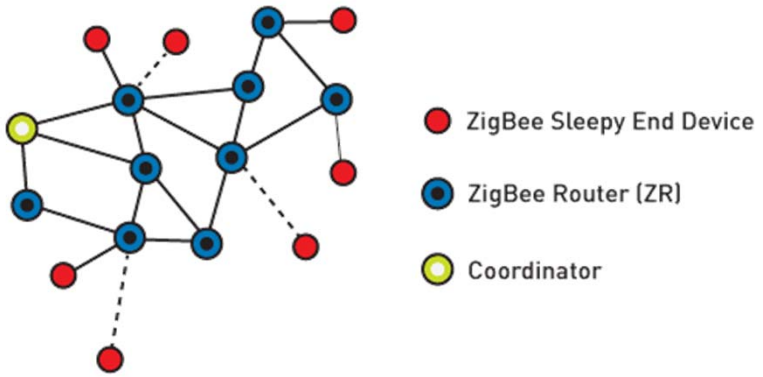
- Two chargers used a cellular network
- Both units utilized cloud servers as the management interface
- The communication protocols were secure
- The management applications were weak



Remote Management (Residential)

- One charger was connected directly to a wired Ethernet network
  - This unit communicated using the Modbus protocol (not secure)
- The second charger was designed to use a residential ZigBee mesh network
  - The ZigBee network was properly secure
  - This unit communicated using a proprietary protocol (not secure)
- Both units used a custom (proprietary) application for remote administration





Findings

- Nothing has changed in 15 years
  - Developers are still making the same silly mistakes
- Implementation of “complex” code on a small embedded device leads to poor decision making
  - Hardware constraints lead to the use of methods that should have died long ago
- Sanity checking of remote input is always lacking
- Processes are executed with extensive privileges (i.e. root)
- Memory corruption vulnerabilities work as well on ARM as they do on x86
- Add the additional vulnerabilities of poor web application implementation
  - SQL injection
  - XSS
  - Input validation
  - Insecure credentials

Findings (Continued)

- Luckily each of the chargers had a separate system responsible for handling the vehicle communications and charge state
- The assessment team was only able to stop a charging event
  - We were not able to energize a cordset without it being plugged into a vehicle
- Billing and price information were manipulated
- Remote updating was very poorly implemented
  - Malicious firmware lead to full compromise of all units from one vendor

Questions…