Security Concerns of a Plug-In Electric Vehicle

Theodore Bohn and Hina Chaudhry
Center for Transportation Research, Energy Systems Division
Argonne National Laboratory

Benefits and Advantages of an EV

- Use of Clean Energy or Electricity
- Will control growing pollution
- Cost effective in comparison to their gasoline brethren
- Major resource of Distributed Energy Resource
- Will be capable of V2G applications in the near future

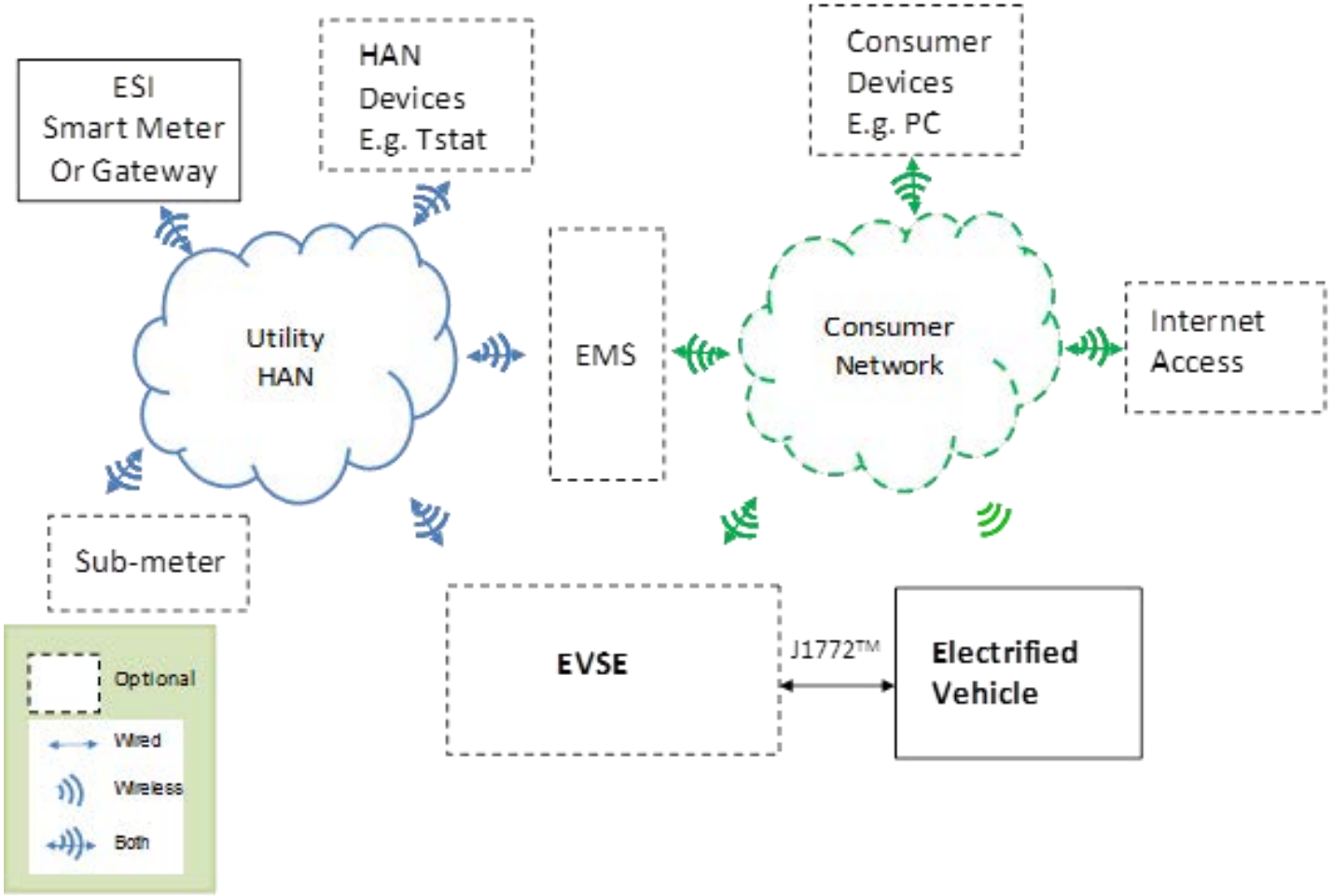
Related Research

- **Weimerskirch, Wollinger, & Wolf (2007)**
  - Described attacks on automotive hardware and software
  - Explained security objectives, technical & non technical constraints
- **Brooks, Sander, Deng & Joachim Taiber (2009)**
  - Security analysis of different vehicle systems like antitheft system, vehicular ad-hoc network, ECU flashing etc.
  - Used CERT taxonomy to analyze automotive attacks
- **Hoppe & Dittmann (2009)**
  - Sniffing & replay attacks on CAN bus, showcased security threats to CAN networks, provided some short term countermeasures
- **Kleberger, Olovsson, & Jonsson (2011)**
  - Emphasized problems in In-Vehicle Networks, misuse and poor implementation of CAN protocol, and information leakage.

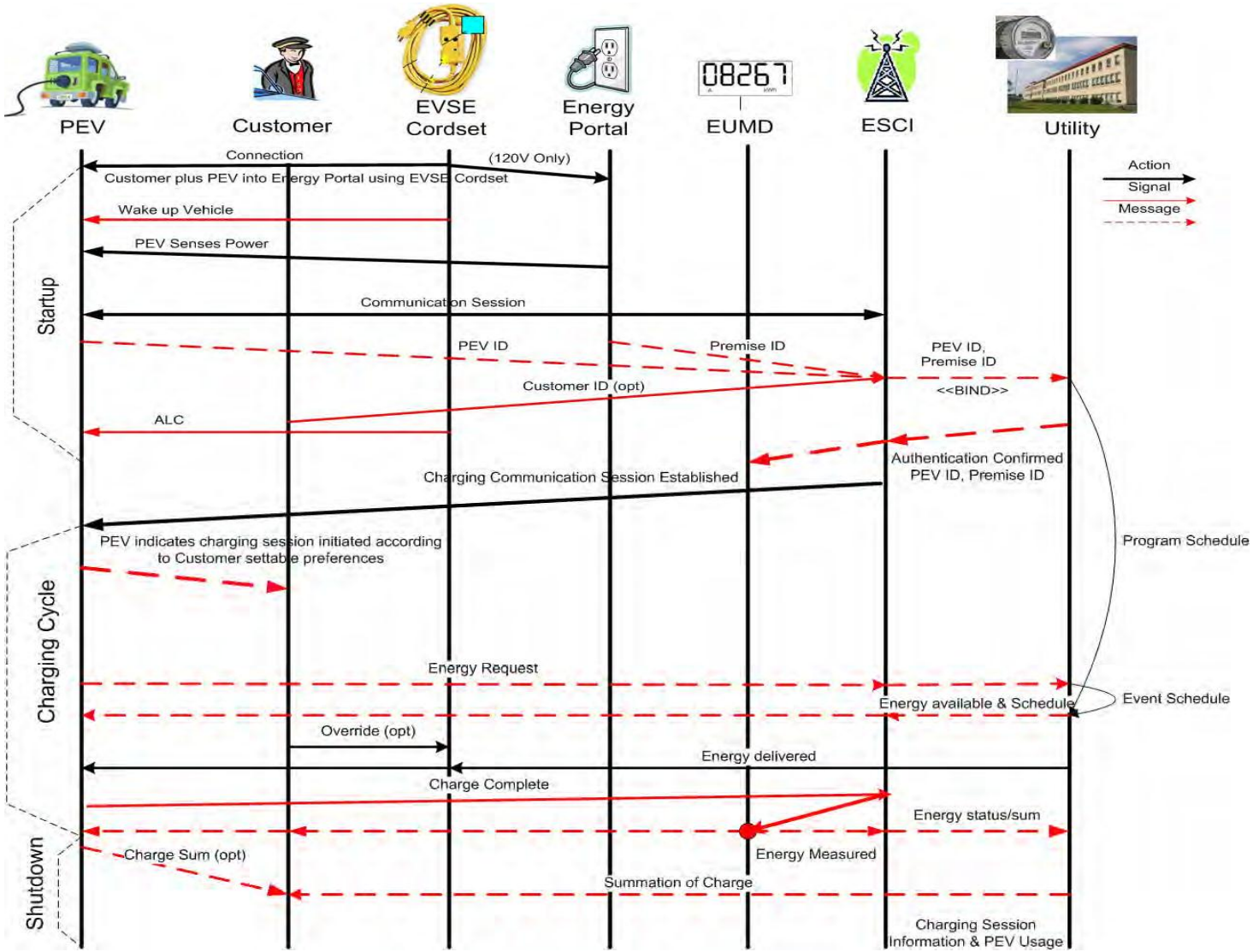
Need for external communication

- Charging
- Billing
- Demand Response
- Incentive Rates
- Ancillary Services
- Telematics

Electric Vehicle Infrastructure (SAE J2836/1)



A walkthrough of charging session (SAE J2836/1)



Security Concerns

- **Data**
  - Security Concerns
    - Data in Transit
    - Data at Rest
  - Possible Impacts
    - Unauthorized access/modification to customer information
    - Replay attacks (impersonation of identity)

Security Concerns

- **Communication Network**
  - Security Concerns
    - Communication Protocols
    - Disparate Networks
  - Possible Impacts
    - Sniffing
    - Replay Attacks
    - Manipulation of the data

Security Concerns

- **Infrastructure**
  - Security Concerns
    - Integrity of node/devices
  - Possible Impacts
    - Comprise of other devices in the PEV infrastructure
    - Possibility of infecting to substations/transformers with virus, malicious codes, spyware, etc. through infected EMS/ESCI
    - Break-downs and blackouts leading to catastrophic failures

Security Concerns

- **Firmware & Software**
  - Security Concerns
    - How to check the integrity of the software, updates?
    - How to stop vehicle owners, maintenance personnel from tampering the firmware?
  - Possible Impacts
    - With FOTA, sniffing can be performed, which can then lead to capturing and modification of the firmware.
    - Possibility of intrusion, thereby gaining access to critical systems like onboard diagnostic system and sending malicious diagnostic requests, causing harm and panic to the vehicle driver.
    - Comprised vehicle can further spread the infection to other entities (EUMD, EVSE, EMS, ESCI, etc.), which can spread upstream.

Possible Solutions for the existing systems

Verendel, Larson, Nilsson & Johnsson (2008)

- Use of honeypots in the in-vehicle networks to learn about attacker's preferences, techniques and weaknesses in the existing systems.

Oguma et al.(2008)

- Attestation based security architecture for the in-vehicle communication
- Use of PKI in a key pre-distribution system consisting of center (vehicle manufacturer) and multiple players (ECUs)

Possible Solutions for the existing systems

- **Nilsson & Larson (2009)**
  - Suggested protocol for data integrity, authentication and confidentiality
  - Creation of hash chain of the firmware, first packet signed by the trusted source for the authentication of the whole chain, packets themselves are encrypted
  - Also proposed the use of defense in depth strategy of prevention, detection, countermeasures and recovery
    - Authentication to prevent unauthorized access
    - Intrusion detection system (IDS) and logging for detection
    - Use of honeypots for information retrieval
    - Intrusion Prevention System (IPS) for countermeasure and traceability to perform recovery

Points to remember for the security of PEV & its infrastructure

- Proper authorization and authentication (correct billing, identity management, unauthorized charging/avoidance of payment)
- Privacy & Compliance (PCI- DSS standard compliance)
- Secure end to end communications (increased no. of entry points, protocols complexities, DoS, MITM attacks, least privilege violation, etc.)
- Secure financial transactions (stealing credit card details)
- Secure 3rd party applications (Malicious mobile apps, viruses, Trojans, etc.)
- Secure and hardened IT environments (Firewalls, encrypted communications, business continuity and resilient networks, unified threat management)
- User awareness and training (Gullible user can pass their credentials to untrusted source)

Challenges Ahead

- Number of PEVs will increase, and so will number of entry points or nodes for launching attacks
- Need for high security solutions to account for high safety requirements using very limited hardware, software and power resources
- Various mix of networks and hence different security requirements and issues
- Lack of standards

Thank You!