David M. Nicol
Herman M. Dieckamp Endowed Chair in Engineering
Director, Information Trust Institute
University of Illinois at Urbana-Champaign

Cyber-security Issues in Electric Transportation

Executive Summary

Increased cyber-security and privacy risks come from an increased attack surface made possible by extended physical exposure

- Software-governed coupling with electric grid
- Risk to
  - electric transportation infrastructure
  - electric grid
  - vehicles themselves

Other cyber-systems have significant exposure (e.g., WiFi, credit-card sales) but these aren't so exposed physically, nor do they threaten life-dependent infrastructure

View some risks through lens of use cases

Use Case: Paying for Use

Consider charging: Different modes, different ways to charge and pay

- At home
- Pass through occasionally at public station, e.g., Telsa
- At rest public location (street, parking garage, office parking lot)

Cyber-security/privacy issues with paying for public charging

- Several infrastructures, vendors involved
- Increased burden on utilities of protecting location information
  - Consider the impact HIPAA has had on sharing medical information
  - Privacy laws r.e., geolocation, exist and vary by state.
    - E.g., General Data Protection Regulation requires consent for use
- Increased opportunity for fraud
  - E.g., “charge-to-vehicle” with spoofed electronically accessed vehicle identifier

Use Case: Vehicle to Charging Infrastructure

Johnson J, Berg T, Anderson B, Wright B. **Review of Electric Vehicle Charger Cybersecurity Vulnerabilities, Potential Impacts, and Defenses**. *Energies*. 2022; 15(11):3931.

1. EV-EVSE (Electric Vehicle Supply Equipment) connectors
   - Charge vehicles
   - Create load
2. Charge session authentication
   - Link EV operator (or vehicle) to EVSE
3. EVSE to Internet
   - Link to cloud-based applications for monitoring, billing, control, …, everything
4. Maintenance Terminals

Reported vulnerabilities to follow have been observed….

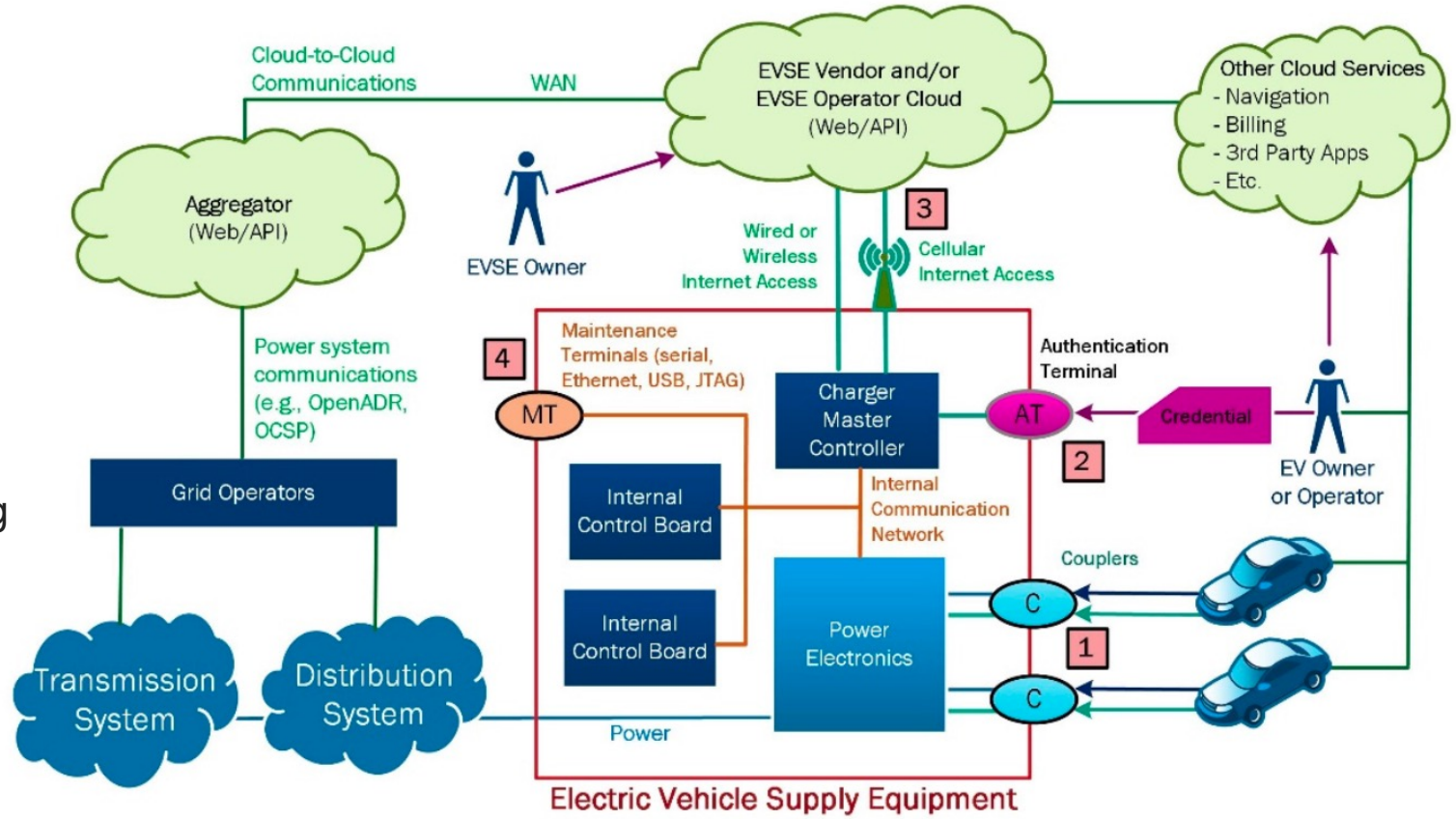


Figure 1. Electric vehicle communication ecosystem with EVSE components and external entities.

EV-EVSE Connectors

There are a variety of devices and protocols in use

Connection control exposed by physical devices used in coupling

- Communication protocols not typically protected

EV -> EVSE could convey

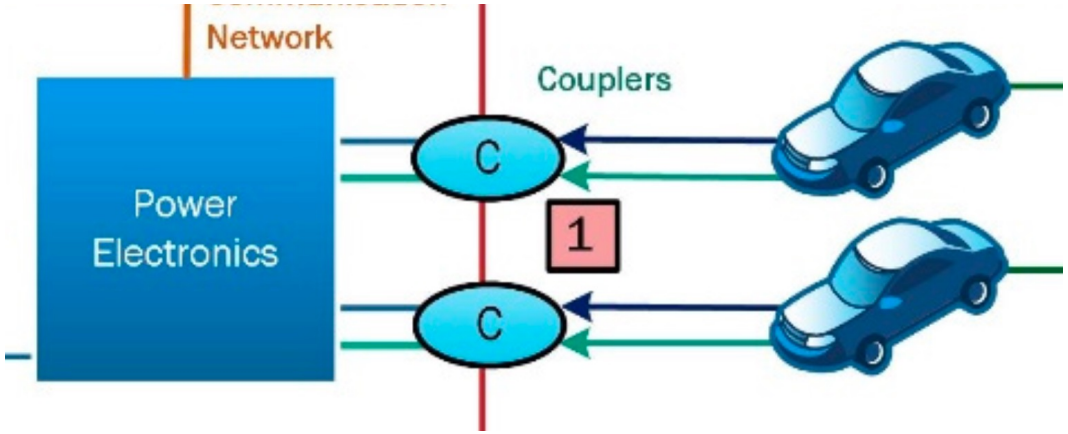
- falsified charging parameters
- Malware

Widespread coordinated EV infection

- System-side load manipulation

Compromised EVSE -> EV

- Overcome EV protections, damage EV



Authentication

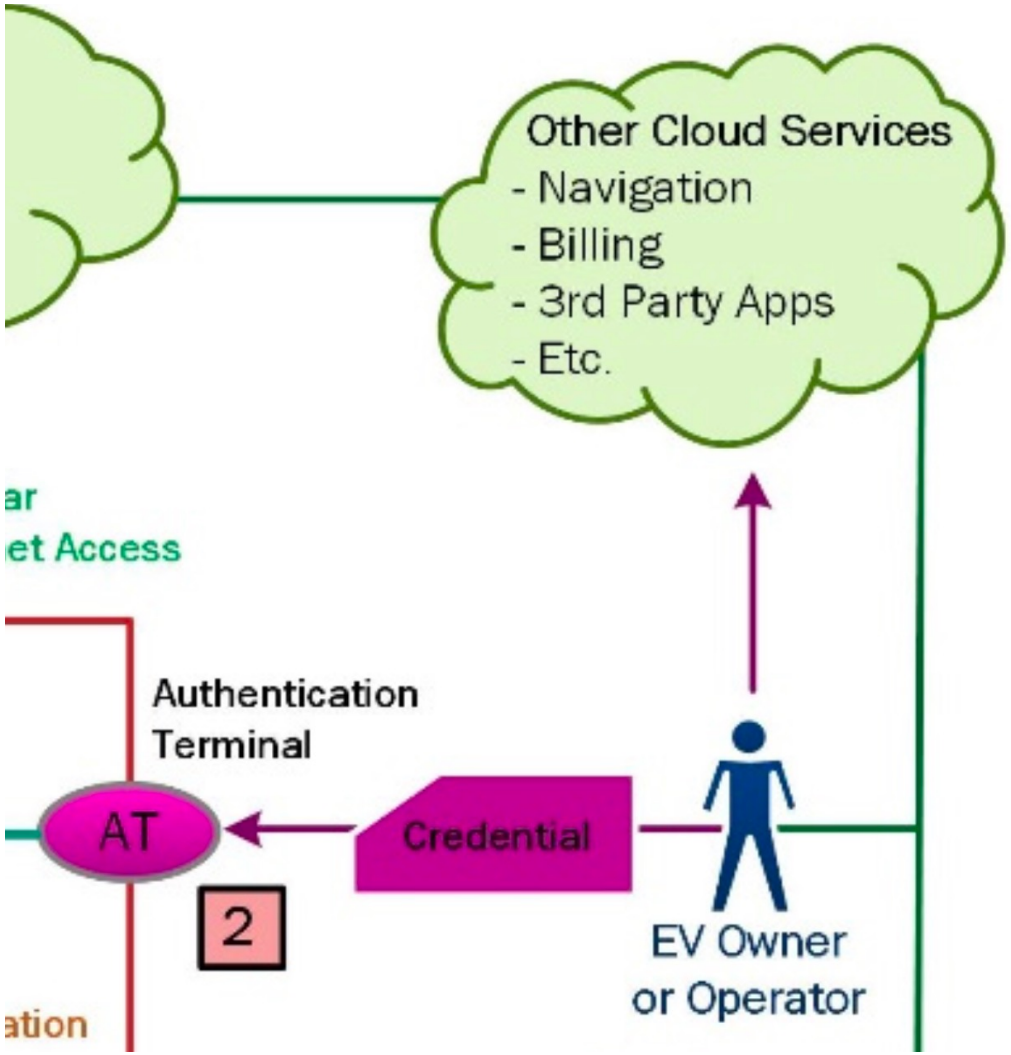
Authentication through RFID, NFA, credit card, terminal input

Plug-and-play authentication through cable itself

- Requires crypto-based authentication both sides, risks due to vulnerabilities of these
  - Intentional and unintentional

User interface a significant attack vector

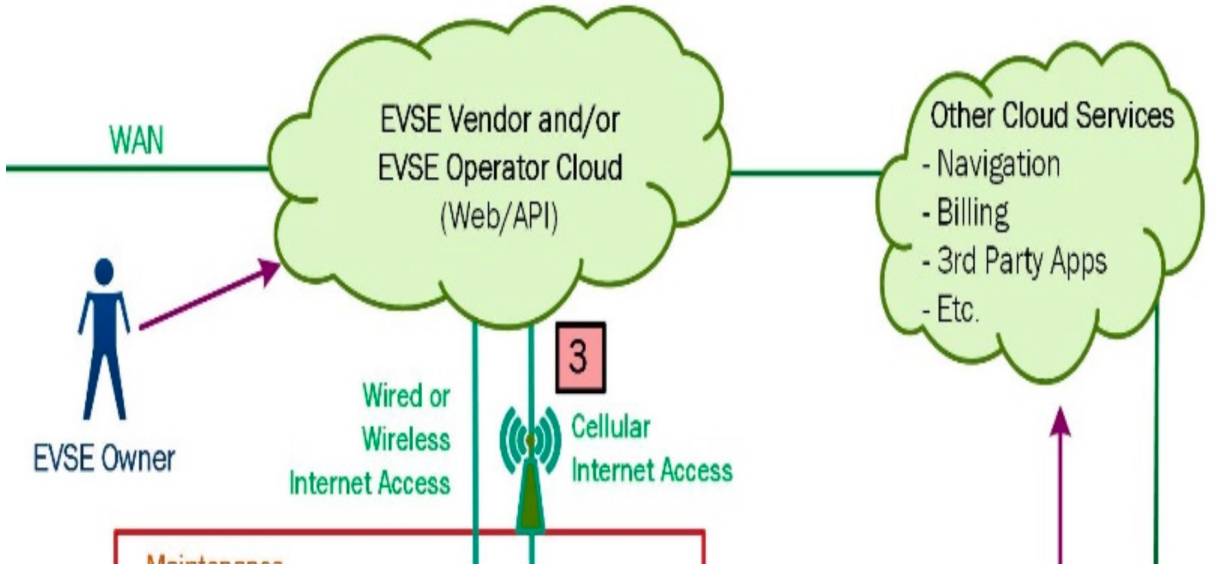
- Complex interfaces typically admit vulnerabilities, exploits may lead to
  - Deny access to selected customers
  - Bypass authentication altogether
  - Disable charging altogether
  - Change prices



EVSE Interface with Internet

Web-servers are used in EV charging infrastructure, and in cloud-based EV charging system applications

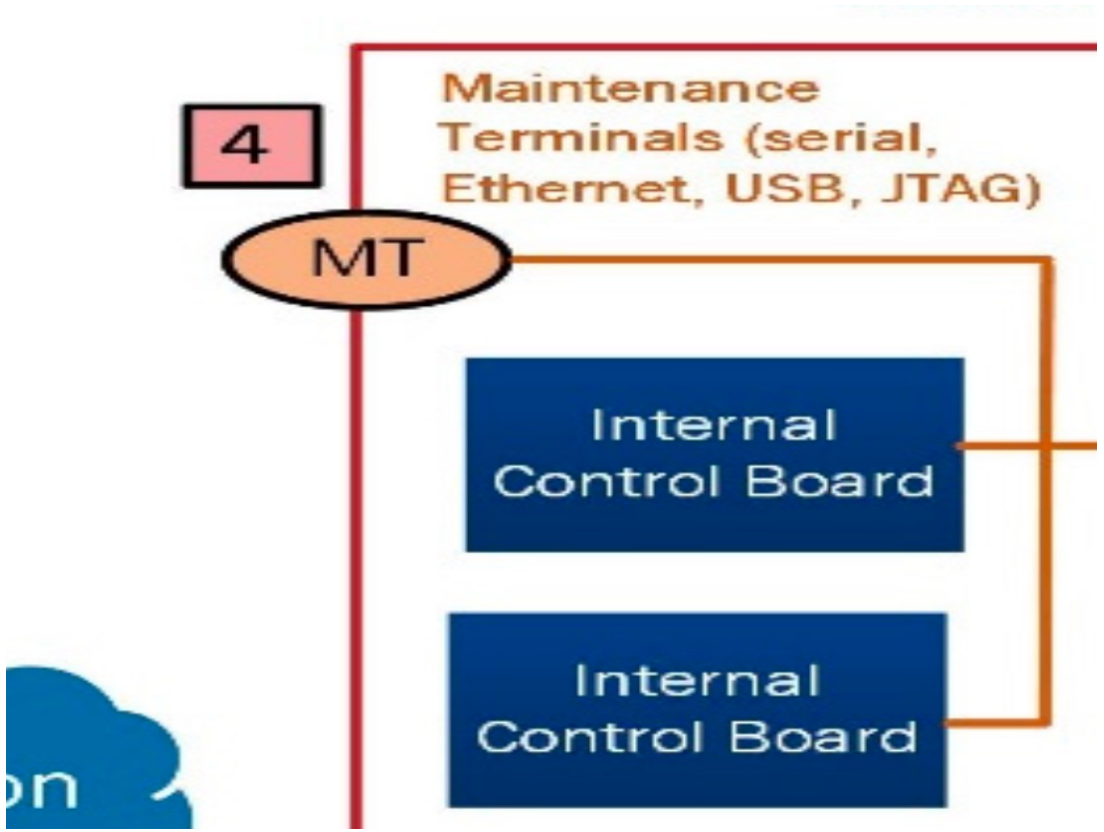
- Observed vulnerabilities in specific services
- Compromise may lead to
  - Manipulation of infrastructure from Internet
  - Attacker control of large collection of EVSE devices, capability to impact
    - Power grid
    - Transportation
    - Other critical infrastructures



EVSE Maintenance Interface

Modern EVSEs constructed with multiple circuit boards

- Communication using a variety of unsecured protocols
- Often connected through a switch, ensemble is accessible by connecting to a switch
- Connection points often left open in production systems
- Adversaries may monitor or disrupt operations



Use Case : Electric Highway

Variety of technologies being researched (based on rails, coils)

All depend exposed communication of some kind

Problems like ‘stationary’ EV charging infrastructure, with addition of

- Cyber-based systems for sensing, control, any billing, vehicle authentication

Image courtesy of Highways England

Summary/Conclusion

- Electrification increases societal dependence on complex cyber systems
- Electrification itself depends on other (vulnerable) systems which are dependent on cyber (e.g., authentication, billing)
- Electrification requires wide-spread physically unprotected exposure of infrastructure that is closely coupled to power grid
- Electrification infrastructure reduces impediments to potential wide-spread coordination interference through compromised vehicles and/or compromised EV charging infrastrastructure
- Electrification generates considerable personal data that legal frameworks may classify as requiring “protection”
- Policy may call for cyber-protected electrification, but responsibility and liability will be driven by incidents, and the courts