WHAT'S THE RISK?
Vehicle charging stations are convenient and affordable for drivers. Many businesses now offer employees free hook ups for their EVs. However, researchers have found that these stations can be a target for cyberattack because they lack proper security measures—physical security, EV owner and maintenance work authentication, and backhaul encryption—which could allow an adversary to steal personal information, change vehicle or charger firmware, or control a fleet's charging rates. Any malware or ransomware could attack the computer systems of vehicles, rendering them inoperable and even allowing access to drivers' personal and financial information. The graphic below shows how vehicles communicate with charging systems and third-party applications, and grid operators.

FRAMEWORKS
Sandia—in partnership with Pacific Northwest National Laboratory, Argonne National Laboratory, the US Department of Transportation, BTCPower and National Motor Freight Traffic Association—is working to address electric vehicle supply equipment (EVSE) cybersecurity by creating a cybersecurity threat model, and performing risk assessments of existing EVSE, so that automotive, charging and utility stakeholders can better protect their customers, vehicles and power systems. The result of this project will provide stakeholders with a strong, technological basis for securing vehicle charging infrastructure from cyber threats.
EDUCATION IS KEY

It has been projected that globally, over the course of the next decade, the number of EVs will increase by tens of millions. This means that as the number of vehicles grows, so will the number of available charging stations these vehicles will need to use.

At this time, there is no comprehensive EV cybersecurity approach and the industry has only adopted limited best practices. One of the project’s main goals is to educate key industry leaders about the risks posed, and help them understand their role in providing grid security and resilience.

Sustained cybersecurity leadership and stakeholder commitment are necessary to continuously improve EV charging equipment and networks, build effective standards, and support government and commercial R&D efforts.

THREAT MODELING

To enumerate threats in a testing environment, researchers at the national laboratories used the STRIDE threat modeling methodology to determine potential vulnerabilities. This includes: communication and control interface with the EV’s battery management system, the controls that manage power flow to vehicle batteries, utility communications and grid operator control, and financial communications. This threat model was further informed by red team assessments of DC fast chargers and extreme fast chargers (xCFs).

The research team also investigated how the power system, vehicles and other services are impacted by coordinated cyberattacks on charging systems at the both the transmission and distribution levels. Based on these consequences, mitigations can be prioritized based on the potential risk to critical US infrastructure. The team expects that the results of the threat model will be the foundation for improvements to cybersecurity of EVs, EVSEs, and other support infrastructure.

CONTACT:

Jay Johnson
Principal Investigator
jjohns2@sandia.gov
(505) 284-9586

Figure: Distribution system voltage impact from coordinated EV charging and discharging with 2.25 MW EVSEs.