Engineers evaluate cybersecurity risks associated with EV fast-charging equipment

July 16 2024

SwRI research engineers, from left, FJ Olugbodi, Mark Johnson and Katherine Kozan demonstrate an adversary-in-the-middle device they developed to test the cyber resiliency of ISO 15118-compliant vehicle-to-grid charging systems. With the device, SwRI identified cybersecurity vulnerabilities with electric vehicles using direct current fast-charging systems. Credit: Southwest Research Institute

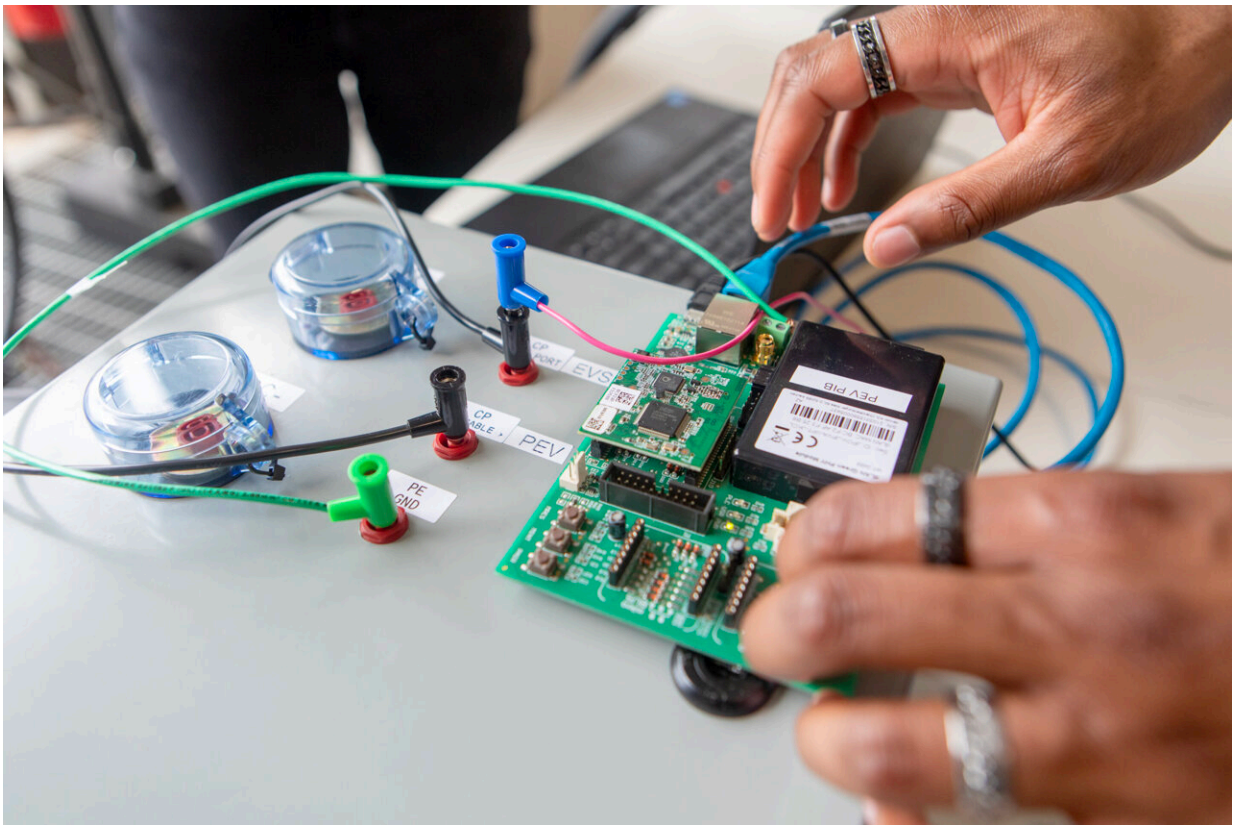
Engineers at Southwest Research Institute have identified cybersecurity vulnerabilities with electric vehicles (EVs) using direct current fast-charging systems, the quickest, commonly used way to charge electric vehicles. The high-voltage technology relies on power line communication (PLC) technology to transmit smart-grid data between vehicles and charging equipment.

In a laboratory, the SwRI team exploited vulnerabilities in the PLC layer, gaining access to network keys and digital addresses on both the charger and the vehicle.

"Through our penetration testing, we found that the PLC layer was poorly secured and lacked encryption between the vehicle and the chargers," said Katherine Kozan, an engineer who led the project for SwRI's High Reliability Systems Department. The team found unsecure key generation present on older chips when testing, which was confirmed through online research to be a known concern.

The research is part of SwRI's ongoing efforts to help the mobility sector and government improve automotive cybersecurity spanning embedded automotive computers and smart-grid infrastructure. It builds upon a 2020 project where SwRI hacked a J1772 charger, disrupting the charging process with a lab-built spoofing device.

In the latest project, SwRI explored vehicle-to-grid (V2G) charging technologies governed by ISO 15118 specifications for communications between EVs and electric vehicle supply equipment (EVSE) to support electric power transfer.



SwRI developed an adversary-in-the-middle device with a modified combined charging system to test the cyber resiliency of ISO 15118-compliant vehicle-to-grid, direct current fast charging systems. The high-voltage technology relies on power line communications (PLC) to transmit smart-grid data between vehicles and charging equipment. SwRI researchers exploited. Credit: Southwest Research Institute

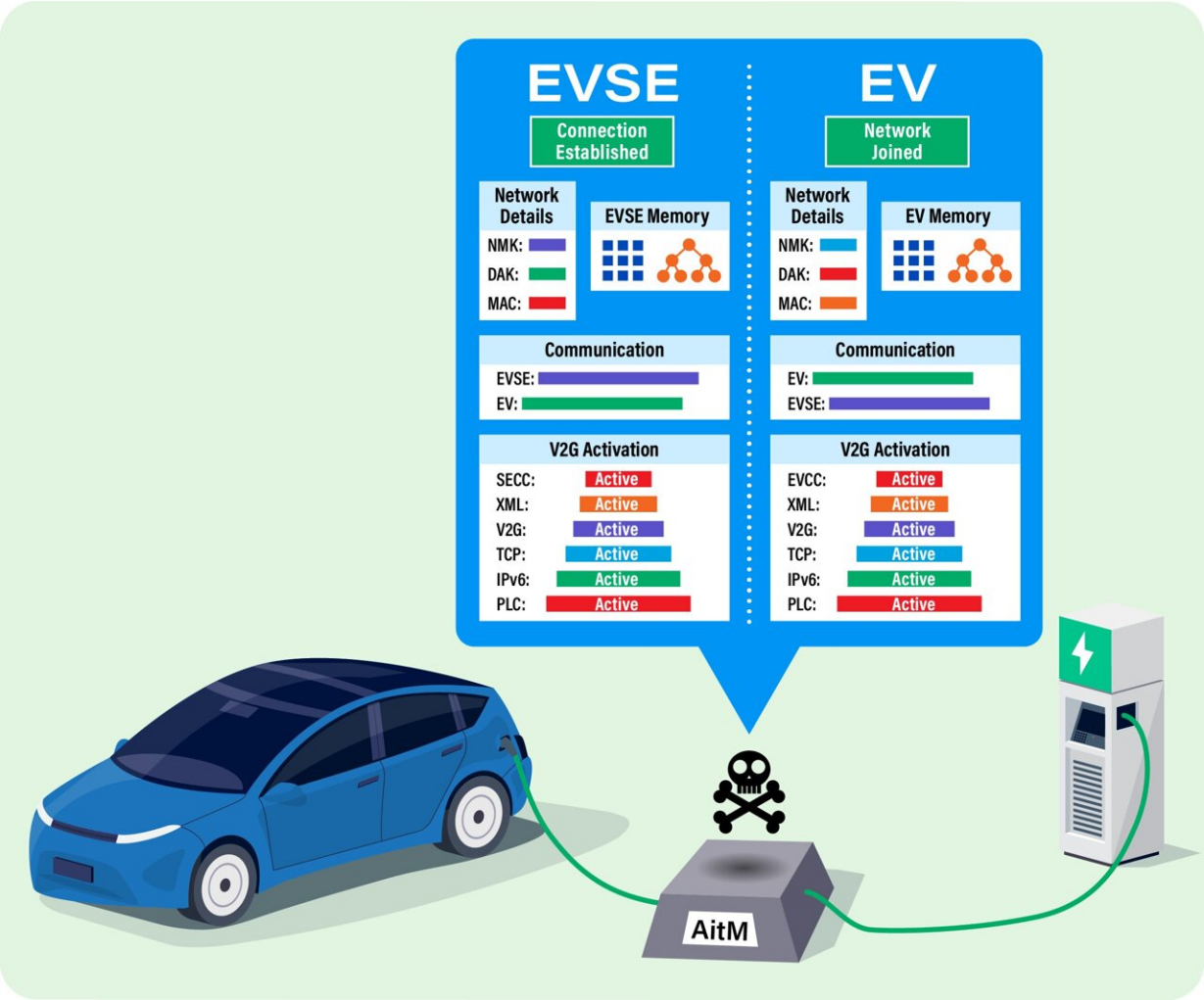
"As the grid evolves to take on more EVs, we need to defend our critical grid infrastructure against cyberattacks while also securing payments to charge EVs," said Vic Murray, assistant director of SwRI's High Reliability Systems Department. "Our research found room for improvements."

The SwRI team developed an adversary-in-the-middle (AitM) device

with specialized software and a modified combined charging system interface. The AitM allowed testers to eavesdrop on traffic between EVs and EVSE for data collection, analysis and potential attack. By ascertaining the media access control addresses of the EV and EVSE, the team identified the network membership key that allows devices to join a network and monitor traffic.

"Adding encryption to the network membership key would be an important first step in securing the V2G charging process," said FJ Olugbodi, an SwRI engineer who contributed to the project. "With network access granted by unsecured direct access keys, the nonvolatile memory regions on PLC-enabled devices could be easily retrieved and reprogrammed. This opens the door to destructive attacks such as firmware corruption."

However, encrypting embedded systems on vehicles poses several challenges. For instance, added layers of encryption and authentication could even become a safety hazard. A failure to authenticate or decrypt could interrupt a vehicle's functionality or performance.



This diagram demonstrates an SwRI-developed adversary-in-the-middle (AitM) attack and its capability to emulate both an electric vehicle and EV supply equipment (EVSE), as well as monitor their defined attributes. Credit: Southwest Research Institute

SwRI has developed a zero-trust architecture that can address these and other challenges. It connects several embedded systems using a single cybersecurity protocol. SwRI's future EV cybersecurity research will test zero-trust systems for PLC and other network layers.

"Automotive cybersecurity poses many layers of complexity, but we are excited about these new techniques to identify and address vulnerabilities," said Cameron Mott, an SwRI manager leading SwRI's automotive cybersecurity research.

Provided by Southwest Research Institute

Citation: Engineers evaluate cybersecurity risks associated with EV fast-charging equipment (2024, July 16) retrieved 16 July 2024 from https://techxplore.com/news/2024-07-cybersecurity-ev-fast-equipment.html