Intern develops technology to find EV charging vulnerabilities

July 18 2023

INL intern, Jake Guidry, is using the AcCCS system to interface with an electric vehicle through the CCS charge port to evaluate the cybersecurity posture of the charging communication protocols. Credit: Idaho National Laboratory

Idaho National Laboratory intern Jake Guidry has developed a

cybersecurity research tool that could improve the security of electric vehicle charging.

INL experts demonstrated the tool to colleagues from Sandia and Pacific Northwest national laboratories on June 7. The AcCCS tool provides access capabilities through CCS (combined charging system) communications protocol.

AcCCS (pronounced access) is a combination of hardware and software that emulates the electronic communications that occur between an electric vehicle and an extreme fast charger during the charging process. The tool gives researchers a new way to search for vulnerabilities in electric vehicles and charging stations.

The AcCCS hardware includes a charging port and a charging cable, both of which can be plugged into real-world equipment.

No charging power flows through the device. If you plug AcCCS into an electric vehicle, the vehicle's computer thinks the battery is receiving a charge. If you plug the tool into a 350-kilowatt fast charging station, the station thinks it is charging an electric vehicle.

"It's basically acting like one to trick the other," said Guidry, a master's degree student in mechanical engineering from the University of Louisiana at Lafayette. Guidry began an internship at INL last winter after being recruited by lab researchers at the 2022 SAE CyberAuto Challenge workshop. "With this technology, you can not only skew from normal operations, but also introduce cyberattacks."

INL intern, Jake Guidry, is using the AcCCS system to interface with an electric vehicle through the CCS charge port to evaluate the cybersecurity posture of the charging communication protocols. Credit: Idaho National Laboratory

"Currently, some commercial devices allow researchers to test EVs and charging equipment to make sure that they meet certain specifications, but AcCCS is less expensive and a lot more flexible," said Ken Rohde, a cybersecurity researcher at INL who serves as an advisor for Guidry's project. The tool further reduces costs by eliminating the need for real-world charging equipment or vehicles.

"It's a low-cost solution that allows us to test outside of the bounds," Rohde said. "It brings the barrier of entry to EV charging research way down."

During the June 7 meeting, researchers used AcCCS to hack a charging station and a vehicle. Researchers then demonstrated a mitigation to the cyberattacks. Future experiments will help researchers develop best practice recommendations for industry.

Guidry and his colleagues will next demonstrate the technology at this year's SAE CyberAuto Challenge. He plans to extend his internship to further test AcCCS.

"Immediate next steps are to see how much further I can go with it," Guidry said. "What is the extent of the things that we can do with this capability?"

More information: Conference: www.sae.org/attend/cyberauto

Provided by Idaho National Laboratory