Engineers hack electric vehicle charging to demonstrate cybersecurity vulnerabilities

November 9 2020

Credit: Unsplash/CC0 Public Domain

Engineers at Southwest Research Institute were able to interfere with the charging process of an electric vehicle (EV) by simulating a malicious attack as part of an automotive cybersecurity research initiative.

The SwRI team reverse-engineered the signals and circuits on an EV and a J1772 charger, the most common interface for managing EV charging in North America. They successfully disrupted vehicle charging with a spoofing device developed in a laboratory using low-cost hardware and software.

"This was an initiative designed to identify potential threats in common charging hardware as we prepare for widespread adoption of electric vehicles in the coming decade," said Austin Dodson, the SwRI engineer who led the research.

SwRI performed three manipulations: limiting the rate of charging, blocking battery charging and overcharging. An SwRI-developed "man-in-the-middle" (MITM) device spoofed signals between charger and vehicle. Researchers also drained the battery and generated signals to simulate J1772 charging rates.

When overcharging, the vehicle's battery management system detected a power level that was too high and automatically disconnected from charging. To limit charging, the MITM device requested the smallest charge allowed (6 amps) to dramatically reduce the charging rate. To block battery charging, a proximity detection signal barred charging and displayed the warning: "Not Able to Charge."

"The project effectively tricked the test vehicle into thinking it was fully charged and also blocked it from taking a full charge," Dodson said. "This type of malicious attack can cause more disruption at scale."

The research focused on J1772 Level 2 chargers, but SwRI is evaluating future testing of Level 3 chargers and penetration of other devices used on fleet vehicles and electric scooters.

As automotive consumer and manufacturing trends move toward

widespread vehicle electrification, market share of EVs is expected to grow to 30% by 2030, according to the International Energy Agency (IEA). The cybersecurity-related issues of charging infrastructure will become increasingly important as demand for EVs grows.

"Discovering vulnerabilities in the charging process demonstrates opportunities for testing standards for electric vehicles and charging infrastructure," said Victor Murray, an SwRI engineer and team lead in the Critical Systems Department.

SwRI is leading several automotive cybersecurity initiatives for automated and connected vehicles, intelligent transportation systems and internet of things (IoT) networking devices.

Provided by Southwest Research Institute