Electric Vehicle Infrastructure Push Brings Cyber Concerns

By Andrea Vittorio | August 24, 2021 5:01AM ET

Electric car charging stations, potentially vulnerable to hacking, face heightened security concerns as shifts in the auto industry coincide with rising cyberthreats.

President Joe Biden in early August set a goal for electric vehicles to represent half of all new vehicles sold in the U.S. in 2030—a goal aimed at helping slow climate change by reducing fossil fuel use.

But shifting from gas-powered to battery-based cars brings with it new cybersecurity concerns, since vulnerability testing has shown that charging stations—by connecting to the internet and communicating with cars—are potential targets for hackers.

“Think about how disruptive it was with ransomware shutting down oil being delivered to gas stations,” said Brad Ree, chief technology officer for the ioXt Alliance, an industry-led security certification program for Internet of Things devices. In May, a ransomware attack against the Colonial Pipeline Co. forced nearly half of the East Coast’s fuel supply to shut down.

“Just imagine if all the gas stations connected to one common cloud point, what kind of target that would be,” Ree said.

He said that public chargers designed to be interoperable, so that EV drivers can charge and pay at different stations along their routes, could be vulnerable to a cyberattack that targets their connectedness, a typical way in for hackers to launch an attack that can quickly scale across a network.

Hackers could use chargers to gain entry to a home or business network, depending on where a charging station is installed, testing by cyber consulting company Pen Test Partners suggests.

User accounts for public charging stations are also at risk, creating the potential for a car charge to be billed to the wrong account, Pen Test Partners found.

There’s even a bigger fear that as more chargers are installed, hacking into many stations at once—then intentionally switching them on and off—could stress the electrical grid and cause a blackout, according to research funded in part by the National Science Foundation.

No Standards

In the rush to set up EV charging infrastructure, some manufacturers haven’t thought enough about security, according to Ken Munro, an electric vehicle owner and cyber consultant at Pen Test Partners who tested six chargers for vulnerabilities.

The situation is complicated by a lack of standards for safeguarding charging stations or certifying their security.

The National Institute of Standards and Technology, or NIST, could write cybersecurity standards for EV chargers, potentially echoing standards for IoT devices that federal agencies buy, the ioXt Alliance's Ree said. Enforcement of such standards would fall to a federal agency, he added. A likely enforcer could be the Transportation Security Administration, which recently imposed new cybersecurity mandates on oil, fuel, and natural gas pipelines.

"Regulation is a good idea in this space," Munro said. "It's the only way to stop manufacturers from rushing products to market."

State and local governments would need to consider charger cybersecurity if they want to tap into a $7.5 billion fund included as part of the Senate's $550 billion bipartisan infrastructure package. It's one of several provisions seeking to shore up the security of the electrical grid and devices connected to it amid a rise in cyberthreats.

The Senate-passed bill's prospects in the House are unclear, but if the cybersecurity provisions make it into law, it would mark the first time the federal government invests in EV charging stations.

Applicants for federal EV infrastructure funds would need to describe how they worked with stakeholders such as automakers, utilities, and charging providers to "protect personal privacy and ensure cybersecurity," among other factors, according to the bill's text.

Policy Directives

There are about 43,500 EV charging stations in the U.S., according to data from the Energy Department. That number doubled over just four years, from December 2015-19. Biden has called for building a national network of 500,000 EV chargers by 2030.

"Every charging station in the country could be an attack vector into the larger grid system," said Chris Carney, senior policy adviser at Nossaman LLP who was the U.S. representative for Pennsylvania's 10th District from 2007-10. Carney, a Democrat, served on the Transportation and Infrastructure and Homeland Security committees.

Although the Senate's language on charger cybersecurity in the infrastructure bill shows lawmakers are acknowledging potential risks, stronger policy directives are needed to make the EV industry move against the threat, Carney said.

The federal government should be clear about who bears the responsibility for a cyberattack on critical infrastructure and what steps must be taken to prevent or mitigate attacks, he said. With pipelines, the industry depended on a voluntary system of cyberdefenses—until the TSA imposed a security mandate after the Colonial Pipeline incident.

“The NIST can write all the cyber standards they want, but if there is not enforcement, either legislatively or in a strictly enforced agency mandate, any critical infrastructure system, including EV charging, would remain vulnerable,” Carney said in an email.

EV charging stations are designed with cybersecurity safeguards in mind, but there’s no standard for what the safeguards should be or how the systems should be certified, according to Sunil Chhaya, senior tech executive with the electric transportation group at the Electric Power Research Institute, or EPRI.

Chhaya said another challenge is that charging equipment is part of wider infrastructure that also includes electric vehicles themselves, cloud services, electric utilities, smart meters, and billing and payment systems.

EPRI is working with the Energy Department’s national labs, utilities, equipment providers, and third-party operators to develop a protocol for assessing cybersecurity risks that can be used for equipment and system certification.

Vulnerabilities Vary

Cyber risks can differ depending on how smart the charger is—for instance, whether it can be controlled remotely. Hacking risk also varies depending on whether a charger is installed at home or in a public location.

“For a compromised home charger, the whole home network could be at risk,” Chhaya said in an email. “In contrast, a compromised public charger has the potential for threat actors to intrude a larger network or systems since they are connected to different backends.”

So far, charging stations haven’t been installed on a scale that would pose a threat to grid stability if they were hacked, Chhaya said. But as higher-powered stations are more widely deployed, risk mitigation will need to be factored in, he said.

ChargePoint, a leading EV charging network in North America and Europe, secures its stations’ cloud connection so that if a hacker gains access to one station, they can’t take over other stations and draw excess power from a site.

The company’s software platform has built-in controls to thwart potential security breaches that could become safety issues, such as not allowing its mobile app to override certain settings. Those settings include the maximum output of the installed cable, which prevents adjustments that could cause damage to a vehicle or harm to the driver.

ChargePoint also safeguards EV drivers’ data, including their payment details, in a way that protects consumer privacy.

The company, based in Campbell, Calif., has a so-called bug bounty program that incentivizes people to test its systems for vulnerabilities, according to a recent blog post. Last March, ChargePoint brought in 50 security researchers from the cybersecurity company HackerOne to identify and close gaps in its website, apps, and infrastructure, the post said.

“Any device on a network becomes an attack vector,” said Eric Sidle, ChargePoint’s senior vice president of engineering. “We’re always learning about new attack vectors and closing them.”

To contact the reporter on this story: Andrea Vittorio in Washington at avittorio@bloomberglaw.com

To contact the editors responsible for this story: Melissa B. Robinson at mrobinson@bloomberglaw.com, Kibkabe Araya at karaya@bloombergindustry.com