EPRI Media Request, August 13, 2021

Safeguarding Electric Vehicle Charging Infrastructure Cybersecurity

By Sunil Chhaya
With contributions from Viswanath Ananth, John Halliwell, Galen Rasche, and Xavier Francia

Background: There is a significant spotlight on accelerating Electric Vehicle (EV) adoption, resulting in a renewed emphasis on large-scale EV charging infrastructure deployment. Since the customers, EVs, and the infrastructure ecosystem operate in a connected and networked environment, safeguarding cybersecurity of the communications backbone of the EV ecosystem is of paramount importance. This is further accentuated by recent reports of malicious actor activities on segments of the connected charging infrastructure. The following Q&As are a result of a recent media inquiry, that both highlight the issues and potential remediation measures, as well as how EPRI electric transportation and cybersecurity research is proactively addressing these.

Q: How vulnerable are EV chargers to cyberattacks?

EV charging stations are designed with the best available cybersecurity provisions and safeguards. However, the challenges today arise from the fact that:

(a) there is no uniform way to specify what these safeguards should be, or how these integrated systems should be certified, making cybersecurity assurance a best-effort implementation from the providers and is localized to their point within the system.

(b) the charging equipment is a part of an EV charging infrastructure ecosystem that involves the EVs, the charge stations, the cloud Electric Vehicle Service Providers, utility back office, advanced metering infrastructure, as well as billing and payment systems. Given that a chain is as strong as its weakest link, a cyber-intrusion from any weak link in this system has the potential to create reliability, safety, or economic risks.

EPRI is working to address this challenge. The latest project involves a broad cross-section of the charging infrastructure ecosystem including national labs, utilities, equipment providers, and third-party operators. The project defines system-wide methodologies, assesses risks and vulnerabilities, identifies threats and attack surfaces, and

proposes mitigation mechanisms. The end goal is to release widely available tools for practitioners to apply to create more robust EV charging infrastructure components and systems.

Further, EPRI intends to work with appropriate collaborators to create a cybersecurity risk assessment profile that can serve as the basis for equipment and system certification for enhancing the security and lowering the risks of the entire ecosystem and providing the technology procurement organizations a basis for comparing competing implementations.

Q: If a charger is hacked, what could that mean for an at-home charger vs. a public charging station? I've heard the charging device could be used to gain access to a network.

This is one of the scenarios we are looking at to figure out exactly the modes of intrusion, how far could they reach within the system, and the risks they create within the system. Without knowing the specifics of a scenario, it is sufficient to say that in theory, if an intrusion were to occur, it could potentially reach other exposed parts of the 'information chain'.

Some types of popular at home, non-networked chargers, that have relatively low smarts, not remotely managed, and are isolated, may not provide access to a home network. For systems which are remotely managed, intrusion scenarios for at-home networked charger and a public charging station are applicable and similar, but the impacts are different. For a compromised home charger, the whole home network could be at risk. 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.

Q: I've also heard that if a bunch of EV chargers are hacked and turned on/off at once, it could threaten the stability of the electric grid. How much of a concern is that? And what can be done to address it?

At a macro level, if the sum total of the installed capacity for EV charging is added up, the charging load impact on the grid is minuscule. Even at a distribution system feeder level, a geospatially scattered set of charging stations pose less of a risk to the distribution system in terms of stability and reliability.

However, as the deployment of high-power or megawatt-scale charging stations proliferates, systems will need to be designed so that the distribution capacity is allocated and sized for the worst-case scenarios, and a multi-layer mitigation strategy will need to be designed in. This mitigation approach must encompass the vehicles, the charge stations, the local energy management systems, and the grid management systems, to prevent and/or localize and isolate any such issues faster than their effects are felt in broader parts of the system. In other words, there is an opportunity to create and implement timely design and test protocols that enhance overall system security, including cybersecurity. A cybersecurity assurance and certification element should be an integral part of any EV charging infrastructure plan.

Q: What are potential privacy concerns associated with EV battery recycling? Do batteries record information about their use?

This is very unlikely, to the best of our knowledge. The internal battery management system algorithms may use historical data for computational purposes, but these parameters related to energy use data do not need to be associated with privacy, as batteries themselves do not typically store or involve any personally identifiable information.

DISCLAIMER OF WARRANTIES AND LIMITATION OF LIABILITIES

NOTE

For further information about EPRI, call the EPRI Customer Assistance Center at 800.313.3774 or e-mail askepri@epri.com.

Export Control Restrictions

Access to and use of this EPRI product is granted with the specific understanding and requirement that responsibility for ensuring full compliance with all applicable U.S. and foreign export laws and regulations is being undertaken by you and your company. This includes an obligation to ensure that any individual receiving access hereunder who is not a U.S. citizen or U.S. permanent resident is permitted access under applicable U.S. and foreign export laws and regulations.

In the event you are uncertain whether you or your company may lawfully obtain access to this EPRI product, you acknowledge that it is your obligation to consult with your company's legal counsel to determine whether this access is lawful. Although EPRI may make available on a case by case basis an informal assessment of the applicable U.S. export classification for specific EPRI products, you and your company acknowledge that this assessment is solely for informational purposes and not for reliance purposes.

Your obligations regarding U.S. export control requirements apply during and after you and your company's engagement with EPRI. To be clear, the obligations continue after your retirement or other departure from your company, and include any knowledge retained after gaining access to EPRI products.

You and your company understand and acknowledge your obligations to make a prompt report to EPRI and the appropriate authorities regarding any access to or use of this EPRI product hereunder that may be in violation of applicable U.S. or foreign export laws or regulations.

The Electric Power Research Institute, Inc. (EPRI, www.epri.com) conducts research and development relating to the generation, delivery and use of electricity for the benefit of the public. An independent, nonprofit organization, EPRI brings together its scientists and engineers as well as experts from academia and industry to help address challenges in electricity, including reliability, efficiency, affordability, health, safety and the environment. EPRI also provides technology, policy and economic analyses to drive long-range research and development planning, and supports research in emerging technologies. EPRI members represent 90% of the electricity generated and delivered in the United States with international participation extending to nearly 40 countries. EPRI's principal offices and laboratories are located in Palo Alto, Calif.; Charlotte, N.C.; Knoxville, Tenn.; Dallas, Texas; Lenox, Mass.; and Washington, D.C.

Together…Shaping the Future of Energy™

3002022788

EPRI
3420 Hillview Avenue, Palo Alto, California 94304-1338 • PO Box 10412, Palo Alto, California 94303-0813 • USA
800.313.3774 • 650.855.2121 • askepri@epri.com • www.epri.com