Protecting EV charging stations from cyberattacks

January 14 2022

Credit: Pixabay/CC0 Public Domain

As the number of electric cars on the road grows, so does the need for their electric vehicle (EV) charging stations and the Internet-based managing systems within those stations. However, these managing

systems face their own issues: cybersecurity attacks.

Elias Bou-Harb, director of the UTSA Cyber Center for Security and Analytics, and his colleagues—Claud Fachkha of the University of Dubai and Tony Nasr, Sadegh Torabi and Chadi Assim of Concordia University in Montreal—are shedding light on the vulnerabilities of these cyber systems. The researchers are also recommending measures that would protect them from harm.

The systems built into electric cars perform critical duties over the Internet, including remote monitoring and customer billing, as do a growing number of internet-enabled EV charging stations.

Bou-Harb and his fellow researchers wanted to explore the real-life implications of cyber-attacks against EV charging systems and how to utilize cybersecurity countermeasures to mitigate them. His team also assessed how exploited systems can attack critical infrastructure such as the power grid.

"Electrical vehicles are the norm nowadays. However, their management stations are susceptible to security exploitations," said Bou-Harb, who is an associate professor in the Carlos Alvarez College of Business' Department of Information Systems and Cyber Security. "In this work, we endeavored to uncover their related security weaknesses and understand their consequences on electrical vehicles and the smart grid while providing recommendations and sharing our findings with relevant industry for proactive security remediation."

The team identified 16 electrical vehicle charging managing systems, which they divided into separate categories such as firmware, mobile, and web apps. They performed an in-depth security analysis on each one.

"We devised a system lookup and collection approach to identify a large

number of electrical vehicle charging systems, then leveraged reverse engineering and white-/black-box web application penetration testing techniques to perform a thorough vulnerability analysis," Bou-Harb said.

The team discovered a range of vulnerabilities amongst the 16 systems and highlighted the 13 most severe vulnerabilities such as missing authentication and cross-site scripting. By exploiting these vulnerabilities, attackers can cause several issues, including manipulating the firmware or disguising themselves as actual users and accessing user data.

According to a recent white paper by the researchers, "While it is possible to conduct different attacks on various entities within the electrical vehicle ecosystem, in this work, we focus on investigating large-scale attacks that have severe impact on the compromised charging station, its user and the connected power grid."

During this project, the team developed several security measures, guidelines and best practices for developers to mitigate cyber-attacks. They also created countermeasures to patch each individual vulnerability they found.

To prevent a mass attack on the power grid, the researchers are recommending that the developers patch existing vulnerabilities but also incorporate initial security measures during the manufacturing of the charging stations.

"Many industry members have already acknowledged the vulnerabilities that we uncovered," Bou-Harb said. "This information will help immunize these charging stations to protect the public and provide recommendations for future security solutions in the context of EVs and the smart grid."

The researchers plan to continue analyzing more charging stations to further understand their security posture. They are also working with several industry partners to help shape new security products from the design phase and to develop security resiliency measures that protect vulnerable charging stations from exploitation.

The research was published in *Computers & Security*.

More information: Tony Nasr et al, Power jacking your station: In-depth security analysis of electric vehicle charging station management systems, *Computers & Security* (2021). DOI: 10.1016/j.cose.2021.102511

Provided by University of Texas at San Antonio