

Vulnerability analysis of electric vehicle charging ecosystem

Roland Plaka, Mikael Asplund, Simin Nadjm-Tehrani
Linköping University, Real-Time Systems Lab

Abstract - The rapid deployment of charging stations has exacerbated the need for adequate security measures in the electric vehicle charging ecosystem (EVCE). Integrating IT services into the electric vehicle charging infrastructure exposes it to several attack surfaces. In this paper, we propose a vulnerability analysis method to discover the current security posture of the internet-connected EVCE components. Our method is based on penetration testing principles using open-source cybersecurity search engines. We were able to gather security-related information about eight charging station vendors. Additionally, from our vulnerability assessment approach, we detected ten vulnerable technologies containing fifty-three vulnerabilities in total. Based on the information provided by vulnerability databases, we apply the STRIDE threat modeling technique to analyze the impact of the vulnerabilities on the security properties violated. Finally, we show the vulnerabilities without any developed exploit yet and recommend mitigations for future threats in this domain. With our effort, we contribute to the security of the electric vehicle ecosystem.