National Good Practice Examples and Approaches in Addressing Cyber Threats to EVs and the Electricity Grid

Mahmut Esat YILDIRIM | Head of Department at TR-CERT / USOM

ULUSAL SİBER OLAYLARA MÜDAHALE MERKEZİ

Some Statistics

- At the end of 2022, there were 2.7 million public charging points worldwide.
- According to projections, there will be a total of 12.9 million publicly available EV charging stations by 2030
- By the end of 2022, EV sales are expected to reach 10.6 million in the world—almost 3 times more than in 2018
- The global EV charging station market is currently worth $18.22 billion, projecting that the market will be worth $115 billion in 2028.

Understanding the Threat Landscape

- **Unauthorized Access:** Attackers may attempt to gain unauthorized access to the charging station's control systems or user data. This could involve hacking into the station's network or exploiting vulnerabilities in the station's software.
- **Data Breaches:** Charging stations collect user data, such as payment information and charging history. Cybercriminals may target this sensitive information for financial gain or identity theft.
- **Malware and Ransomware:** Malicious software can infect charging station systems, leading to disruptions in service or data theft. Ransomware attacks can lock charging station operators out of their systems until a ransom is paid.
- **Denial of Service (DoS) Attacks:** Attackers may overload the charging station's network or systems with traffic, causing it to become unavailable for legitimate users. This can disrupt charging services and inconvenience EV owners.
- **Physical Attacks:** Physical damage to charging stations can also impact their operation. For example, vandals might damage charging equipment, leading to service interruptions.

Understanding the Threat Landscape

- **Phishing:** Cybercriminals may send phishing emails or messages to charging station operators or users, attempting to trick them into revealing sensitive information or clicking on malicious links.
- **Interception of Communication:** Man-in-the-middle attacks can intercept communication between charging stations and EVs, potentially allowing attackers to manipulate charging processes or steal data.
- **Firmware and Software Exploits:** Vulnerabilities in the firmware or software of charging stations can be exploited to gain unauthorized control over the equipment or manipulate charging processes.
- **Supply Chain Attacks:** Malicious actors might compromise the supply chain of charging station components, introducing compromised hardware or software into the stations during manufacturing or distribution.
- **Social Engineering:** Attackers may attempt to manipulate charging station staff or users into revealing sensitive information or assisting with unauthorized actions.

Key Challenges

- **Complex Ecosystem:** EV charging infrastructure involves a complex ecosystem of hardware, software, communication networks, and user interfaces. Securing all components and ensuring they work together without vulnerabilities is a challenge.
- **Interconnected Grid:** EV charging stations are often connected to the broader electricity grid. A breach in one part of the system can potentially impact grid operations, leading to cascading effects and potential power disruptions.
- **Diverse Stakeholders:** Multiple stakeholders, including charging station operators, EV manufacturers, utilities, and regulatory bodies, are involved in the deployment and operation of charging infrastructure. Coordinating cybersecurity efforts among these diverse parties can be challenging.
- **Rapid Growth:** The adoption of EVs is growing rapidly, leading to an increasing number of charging stations. As the infrastructure expands, so does the attack surface, making it harder to keep up with security measures.

Key Challenges

- **Legacy Infrastructure:** Many charging stations were deployed before cybersecurity was a significant concern. Retrofitting older infrastructure to meet modern security standards can be costly and complex.
- **Data Privacy:** Charging stations collect sensitive user data, including location information and payment details. Ensuring the privacy and security of this data is essential to build trust among users.
- **Firmware and Software Updates:** Charging stations rely on firmware and software updates to patch vulnerabilities and improve security. Ensuring that these updates are regularly applied across all stations can be challenging, especially for distributed networks.
- **Supply Chain Risks:** The global supply chain for charging station components can introduce vulnerabilities if not adequately monitored and secured. Compromised hardware or software components can be a significant risk.
- **Human Factors:** Insider threats and social engineering attacks can target employees, technicians, or contractors working with charging stations, making it essential to educate personnel about cybersecurity best practices.

Key Challenges

- **Regulatory Compliance:** Compliance with evolving cybersecurity regulations and standards can be complex, especially when dealing with international deployments.
- **Emerging Threats:** As technology evolves, new cybersecurity threats and attack vectors continue to emerge. Staying ahead of these threats and adapting security measures accordingly is a continuous challenge.
- **Limited Awareness:** Many stakeholders may not fully appreciate the cybersecurity risks associated with charging stations. Increasing awareness and understanding is crucial for driving cybersecurity improvements.

National Good Practice Examples

- **United States - DOE Guidelines:** The U.S. Department of Energy (DOE) has published guidelines for securing EV charging infrastructure. These guidelines provide recommendations for authentication, data protection, and network security to protect both the stations and user data.
- **Germany - ISO 15118 Standard:** Germany has been a pioneer in promoting the ISO 15118 standard, which defines a secure communication protocol for EVs and charging stations. This standard includes strong authentication, data encryption, and secure software updates.
- **United Kingdom - Regulation:** The UK government has introduced regulations that require EV charging infrastructure providers to meet cybersecurity standards. This includes ensuring secure access and data protection for users.
- **Netherlands - Public-Private Collaboration:** The Dutch government has worked closely with industry stakeholders to develop the "Cybersecurity and EV Charging Infrastructure" guide. It encourages public-private collaboration to address cybersecurity challenges effectively

National Good Practice Examples

- **Japan - Cross-Industry Collaboration:** Japan has encouraged collaboration between the automotive, energy, and IT industries to develop secure communication standards for EVs and charging stations. These standards include authentication and encryption mechanisms.
- **Australia - National Framework:** Australia's government has developed a national framework for EV charging infrastructure, which includes cybersecurity guidelines. The framework promotes secure data handling, network protection, and software security.
- **European Union - EMC Directive:** The EU has established the Electromagnetic Compatibility (EMC) Directive, which includes requirements for the electromagnetic compatibility of EV charging infrastructure. This indirectly addresses some cybersecurity aspects by ensuring interference-free operation.
- **South Korea - Smart Grid Standards:** South Korea has implemented cybersecurity standards for smart grids, which encompass EV charging infrastructure. These standards cover access control, data encryption, and incident response.
- **Canada - Public Awareness:** Canadian organizations, like Electric Mobility Canada, have been actively raising awareness about EV charging station cybersecurity among stakeholders, promoting best practices and standards adoption.

What to Do?

- Implementing the approaches and best practices
- Building a strong regulatory framework
- Following emerging Technologies and trends
- Setting cybersecurity standards.
- Improving public-private collaboration
- More and more public awareness

Thank you