Recommended

Cybersecurity Practices

for

EV Charging Systems

CYBERSECURITY CONSIDERATIONS

- There is a dramatic increase in the quantity of electric vehicles (EVs) and EV supply equipment (EVSE). High power EV chargers are commonly being installed at workplaces and publicly-accessible locations.
- EVSE cybersecurity attacks may impact many critical infrastructure sectors (e.g., transportation systems, energy, emergency services, manufacturing).
- Combined use of smart-grid technologies, mobile applications,and back-end networking systems introduces several risks, including:
  - New attack vectors for the U.S. electric grid
  - Loss of customer data such as personally identifiable information and financial information
  - Control of the EVSE cyber-physical system through the Internet, potentially offering a foothold on internal enterprise networks

CYBERSECURITY IMPACTS

- EVSE providers, grid operators, vehicle manufacturers, and government agencies must understand cyber-attacks targeting EVSE chargers can create both localized and widespread impacts:

Local impacts

- Theft of PII and financial information
- Failure to charge vehicle
- Damage to batteries or other EV components
- Compromise of EVSE life-safety systems
- Loss of EVSE service availability

Large-scale impacts

- Harvesting of PII and financial information
- Shutdown of entire EVSE charging network
- Exposure of upstream and partner IT networks
- Misconfiguration of EVSE creating damaging or dangerous conditions
- Loss of consumer confidence in EVSE ecosystem
- Bulk power system impacts

PREVALENT WEAKNESSES IN ELECTRIC VEHICLE SUPPLY EQUIPMENT

Physical Access

- Failure to log or generate an alarm when internal compartments are accessed.
- Unencrypted storage allows attackers to steal credentials for use in accessing EVSE or partner systems, networks, and cloud services.
- Spacious internal compartments allow placement of malicious hardware to obtain PII or financial information.
- Attackers can modify or damage internal power electronics and safety systems.
- Insufficient physical measures to deter and identify intrusions.

System Hardening

- Unused, enabled network ports in use.
- Debugging ports are not removed prior to deployment.
- Default or system accounts, using common credentials, prevent accountability for malicious activities.
- The use of common credentials prevents system administrators from revoking access when personnel leave the organization or no longer require access.

Network Protection & Monitoring

- EVSE networks do not always support encryption across necessary data modalities, such as at rest or in transit.
- Intrusion Detection Systems (IDSs) are not installed at key network locations, e.g., IT/OT DMZs and cloud firewalls.
- Lack of proper network segmentation in enterprise systems and EVSE networks.
- Regular vulnerability scanning and patching of backend/cloud infrastructure is not performed by EVSE owners/operators.

Best Practices

BUSINESS NETWORK & OPERATIONS

- ☑ Implement secure coding practices including integrity checks of code repositories and version controlling.
- ☑ Use separation of privilege for all EVSE-related operations.
- ☑ Ensure cybersecurity best practices like the NIST Cybersecurity Framework are used for internal assessments, cyber hygiene, patching, supply chain and insider threat mitigations, etc.

EVSE SECURITY

- ☑ Implement tamper-detection sensors and alarms on EVSE enclosures.
- ☑ Prioritize alarms and ensure timely actions on critical log events.
- ☑ Encrypt all information storage devices within the EVSE.

EVSE NETWORK

- ☑ Use network segmentation and VLANs to isolate EVSE installations.
- ☑ Install firewalls and IDSs at key network locations.
- ☑ Encrypt all network traffic using a FIPS 140-2 compliant cryptographic module.
- ☑ Disable unnecessary services and ports.
- ☑ Ensure proper defense in depth by limiting external access to device to only authorized users and devices using access control technologies.

EVSE OPERATIONS

- ☑ Validate all network traffic and EV inputs before routing them into the EVSE OT network.
- ☑ Utilize secure trust principles such as HW/SW signing, secure boot, and secure firmware and software to update processes.
- ☑ Manufacturers and developers should follow secure software development practices.

PROTECTING TOMORROW:
SECURITY RECOMMENDATIONS BASED ON EVSE PENETRATION TESTS

RISK MANAGEMENT

- Establish methodology to prioritize cybersecurity improvements based on risk to EVSE operations.
- Maintain updated network architecture diagrams to identify critical assets, Internet connections, open ports and supported protocols.
- Establish a process for updating deployed EVSEs, including additional on-site maintenance activities for critical patches.

ASSET, CHANGE, AND CONFIGURATION MANAGEMENT

- Create formal process for uploading code to corporate repositories.
- Stage updates for deployment using approval processes that require multiple personnel and a separation-of-duties model.
- Use digital signatures for all update packages.
- Use a bootloader that supports secure boot operations and verifies digital signatures and firmware update integrity.
- Modify the access control system to require authentication when reconfiguring the EVSE.
- Properly secure and back up critical credentials, keys, or other "secret" items for protection in case of personnel departure or system failure.

IDENTITY AND ACCESS MANAGEMENT

- Require individual credentials to log into systems. Do not reuse credentials across different systems.
- Disallow storage of common credentials inside the EVSE enclosure itself.
- Limit the use of system/maintenance accounts. If required, the shared credentials should be limited to only authorized users.
- Employ access-control mechanisms on all systems that support them.
- Configure internal information systems with NIST-compliant passwords; if possible, use multi-factor authentication to prevent compromised credentials from giving an attacker access.

THREAT AND VULNERABILITY MANAGEMENT

- Establish a threat profile for the types of attacks that are common on EVSE networks and back-end systems to effectively respond.
- Use a Common Vulnerability Scoring System (CVSS) to evaluate potential vulnerability impacts and prioritize the response.
- Review EVSE scripts and applications to ensure permissions are set to prevent an unprivileged user from executing code as the root user.

SITUATIONAL AWARENESS

- Ensure physical security and access logging for test chargers, manufacturing areas, and office spaces.
- Monitor network events and traffic for malicious anomalies. Consider using network-based and host-based intrusion detection systems (IDSs).
- Protect and position EVSE door sensors to prevent an attacker from bypassing them; consider installing an additional sensor to detect other signs of entry. Improve lock mechanisms to prevent picking or other bypass techniques.
- Install and inspect tamper-evident seals on internal covers to detect unauthorized access and potential addition of malicious hardware such as a credit card skimmer.
- Include vulnerability and configuration scanning at regular intervals to ensure systems are updated and do not have unauthorized configuration changes. Scanning can include internet services (e.g., Shodan) to find unintentionally internet-connected EVSEs.

INFORMATION SHARING AND COMMUNICATIONS

- Encrypt all communications internal and external to the EVSE.
- For external networks, apply best practices including network segmentation and security systems such as IDS and firewalls.
- If possible, establish a separate VPN to the system server for each EVSE. This would then block direct communication between two EVSE systems.
- Facilitate information sharing programs for EVSE vendors and network operators to exchange pertinent cybersecurity information with the community.
- Ensure that secure protocols are enabled whenever supported.

EVENT AND INCIDENT RESPONSE, CONTINUITY OF OPERATIONS

- Ensure that "Door Open" alarms, system login notifications, and other critical events are prioritized and uploaded immediately to a centralized logging service.
- Take remediation steps immediately if/when logs show critical events.
- Create a Security Operations Center (SOC) that employs security information and event management (SIEM) and/or security orchestration, automation and response (SOAR) technologies.
- Establish business continuity, incident response, and disaster recovery plans and review the strategy regularly.

SUPPLY CHAIN AND EXTERNAL DEPENDENCIES MANAGEMENT

- Prepare EVSE for shipping via a formal process that includes specified paperwork to document the exact state of the EVSE when it leaves the facility.
- Perform quality assurance at each manufacturing step to ensure appropriate components are used and malicious hardware is not present.
- Disassemble, inspect, and inventory a sample of equipment arriving from external partners and locations.
- Add security mechanisms to protect cryptographic material during manufacture.
- Track all external libraries and software components for newly discovered vulnerabilities.
- Create and maintain golden images of software to check against tampering.

WORKFORCE MANAGEMENT

- Ensure critical roles have proper redundancy in personnel.
- Evaluate competence of personnel with social engineering (e.g., spear phishing) audits and other education-based campaigns.
- Identify any current or future training or recruitment gaps. Fill missing cybersecurity skills.
- Ensure clear roles, responsibilities, and separation of duties for the cybersecurity workforce.

CYBERSECURITY PROGRAM MANAGEMENT

- Establish culture of cybersecurity across the EVSE vendor and network operations enterprise including non-technical employees.
- Mature a cybersecurity program strategy with priorities and governance model.
- Maintain clear reporting lines to corporate leadership for addressing high-priority issues.
- Create and maintain the enterprise network architecture with clear isolation between any IT and OT systems.

Domain headings taken from Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2), Version 1.1, February 2014. Please refer to this document for explanation of the domains and further cybersecurity guidance.
This work was funded by the U.S. Department of Energy's Vehicle Technologies Office.