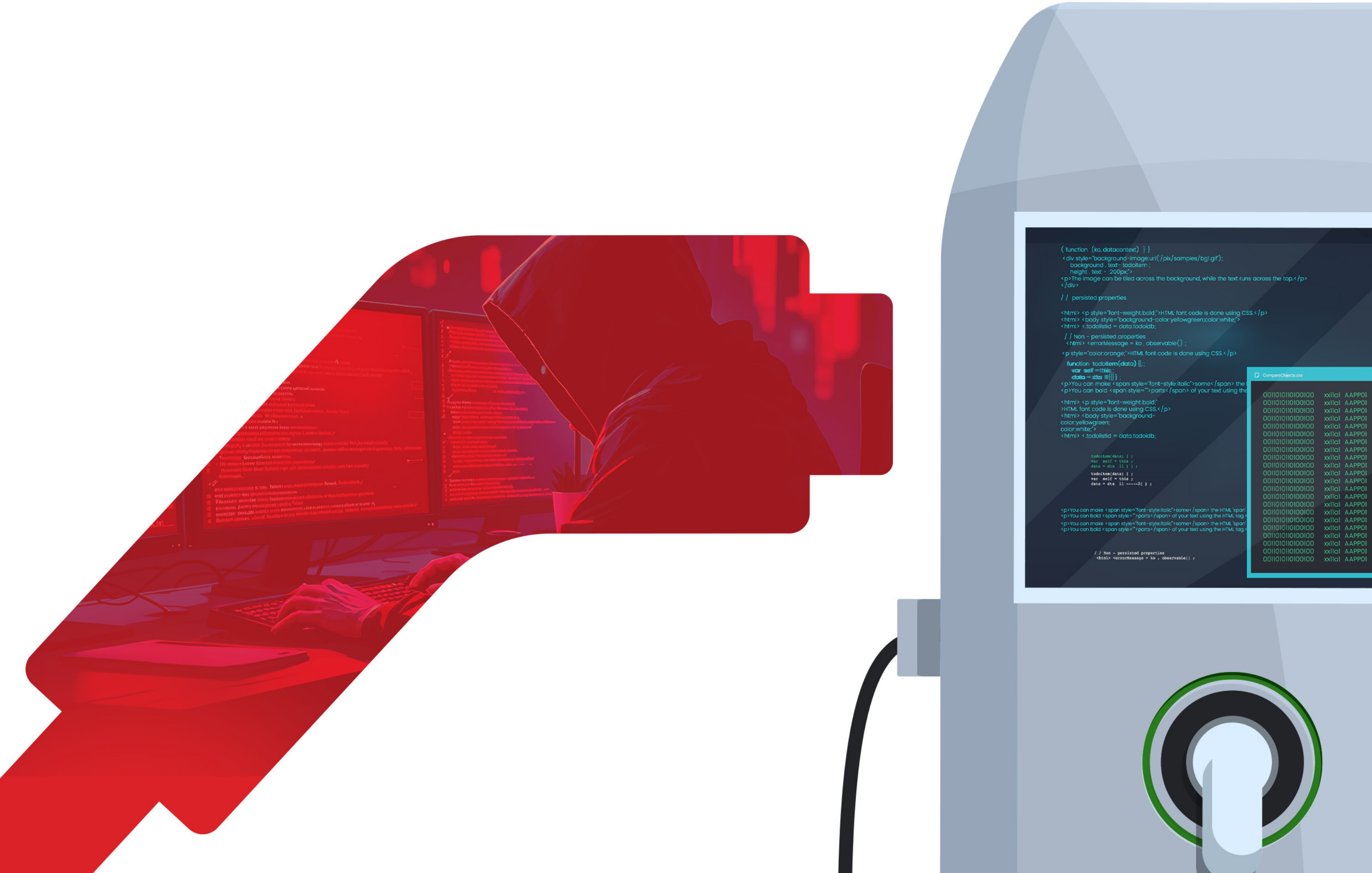
Payatu

SECURITY RISKS IN AN EV CHARGING STATION

LESSONS FROM A PEN TESTER



ABOUT THE AUTHOR

HEMANT SONKAR

Hemant Sonkar is a Senior Security Consultant at Payatu. He has demonstrated proficiency in delivering training sessions at prominent events such as NULLCON and NULL and various internal training programs. With an impressive four-year tenure in the field, he brings extensive expertise to the domain.

His professional portfolio includes the examination of a wide range of IoT devices, spanning medical devices, home automation tools, and electric vehicles. Throughout his hardware security research endeavors, he has cultivated invaluable skills in discerning attack surfaces and vulnerabilities within real-world IoT devices.

CONTENTS

Executive Summary...4

An Introduction to EV Chargers 5

Important Components You Should Know.. 6

Unlocking Vulnerabilities: Pentesting EV Charging Stations..................................9

Exploring Common Hardware Vulnerabilities in the Control Unit and Communication Moule..9

UART or Console Port

JTAG Access

Memory Reading or Firmware Extraction

Configuration Review

Exploring Vulnerabilities in the User Inteface...15

RFID

Display/Touchscreen:

Mobile Application

Exploring Vulnerabilities in the Communication Protocol..............................19

Introduction to OCPP

OCPP Working

OCPP Versions

Vulnerabilities in Ocpp

Conclusion.. 22

References 22

About Payatu 23

EXECUTIVE SUMMARY

With the growing demand for electric vehicles, the need for reliable EV charging stations is also skyrocketing. This growth brings security challenges that could be exploited to gain user data or tamper with the safety of the charging systems.

This ebook explores the security risks discovered while performing penetration testing of the charging station. It highlights critical vulnerabilities such as weak communication protocols, a poor user authentication mechanism, and hardware vulnerabilities that could lead to serious attacks.

The primary goal of this ebook is to raise awareness about the identified security issues and their impact and stress the importance of enhanced charging station security.

AN INTRODUCTION TO EV CHARGERS

An **EV (Electric Vehicle) charging station** is a complex device that supplies electric power to charge the batteries of electric vehicles. These stations can vary widely in terms of power output, charging speed, and technological features, and they are becoming increasingly common as the adoption of electric vehicles grows. There are three main types: Level 1, Level 2, and Level 3 chargers.

Level 1 chargers are the slowest. They use standard 120-volt AC power and provide up to 2.4 kilowatts (kW). These chargers are often used at home and take the longest to charge a vehicle.

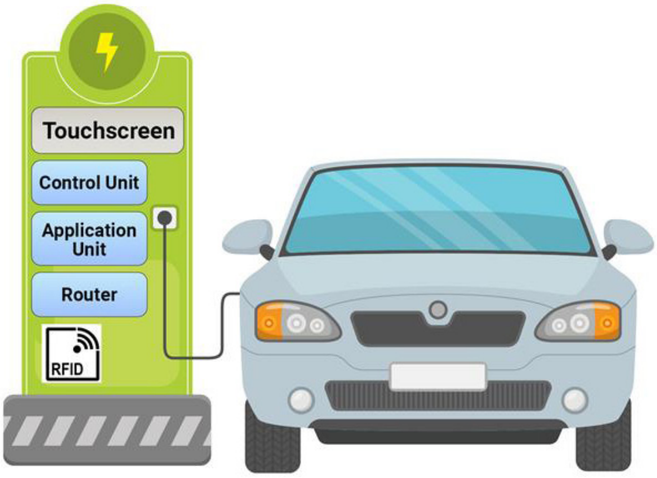
Level 2 chargers are faster, use 240-volt AC power, and offer up to 19 kW. They are commonly found at homes and public charging stations.

Level 3 chargers, also known as DC fast chargers, are the quickest. They provide up to 480 volts of DC power and can deliver as much as 350 kW, charging an EV in as little as 30 minutes. These are mostly used for commercial purposes.

This range of chargers offers flexibility depending on how fast a charge is needed.

The components and vulnerabilities discussed in this ebook primarily pertain to Level 2 and Level 3 EV charging stations.

COMPONENTS YOU SHOULD KNOW



Critical Components of EV Charging Station

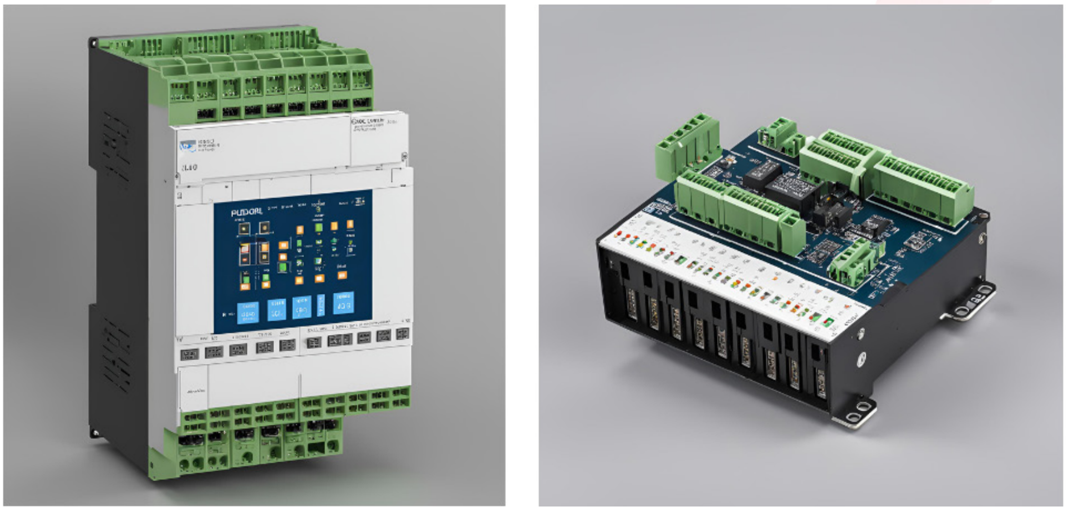
The internal circuitry of a typical EV charging station is quite complex. However, it is essential to understand the security issues associated with certain hardware that can be exploited upon physical access. These components include a microcontroller/SoC and flash chips to store the firmware of the hardware module. Below are the key elements/components within a typical EV charging station that are vulnerable to attacks:

I. CONTROL UNIT

The control unit in an EV charging station, which is often a PLC based device, plays an important role in managing the charging process. It ensures the EV gets the required amount of electricity safely and efficiently. It also maintains communication between vehicles and the charging system. Some of the main functions of control unit are:

- Managing the power required by the electric vehicle and supplying the required current.
- Communicating with electric vehicles to exchange information like charging status.

- The control unit interacts with the user interface, allowing the user to interact with the charging station to manage the charging process and get information like charging status or time left for charging to complete.



Typical PLC-Based Control Unit (AI-Generated)

2. COMMUNICATION OR APPLICATION

EV charging stations communicate with the backend server to manage authentication, billing, diagnostics, or remote management tasks. This happens using a specific hardware module, which can be termed a communication module. This module enables the EV charging station to exchange data with the backend server or the cloud platform.

This module could be a customized embedded board or any development board that typically runs Linux-based OS.

3. INTERNET CONNECTIVITY

The communication module inside the EV charging station requires internet connectivity to communicate with the backend server. There are multiple ways it can be used to communicate with the backend server:

Ethernet: A router can provide internet access via a wired ethernet connection to the communication module.

Cellular: This is typically used for remote stations where wired or Wi-Fi connections are not available. The communication module comes with a SIM card slot, which uses the cellular network for internet access.

Wi-Fi: Enables wireless connectivity in locations where ethernet connections are not practical.

4. USER INTERFACE

The user interface (UI) in an EV charging station is a component that allows the user to interact with the station to manage the charging process. The UI may vary depending on the type and complexity of the charging station. Here are some of the user interfaces that are typically found in charging stations.

Display Screen: Many modern EV charging stations have display screens that provide real-time information to the user. These screens can be either a simple LCD or an interactive touchscreen.

RFID Reader: Many EV charging stations use RFID to authenticate users and start charging. The charging station uses an RFID reader, where users tap the RFID tag to start the charging session.

Mobile App integration: Many charging stations come with the corresponding mobile application, where the user gets authenticated and makes payments to initiate the charging process.

UNLOCKING VULNERABILITIES: PENTESTING EV CHARGING STATIONS

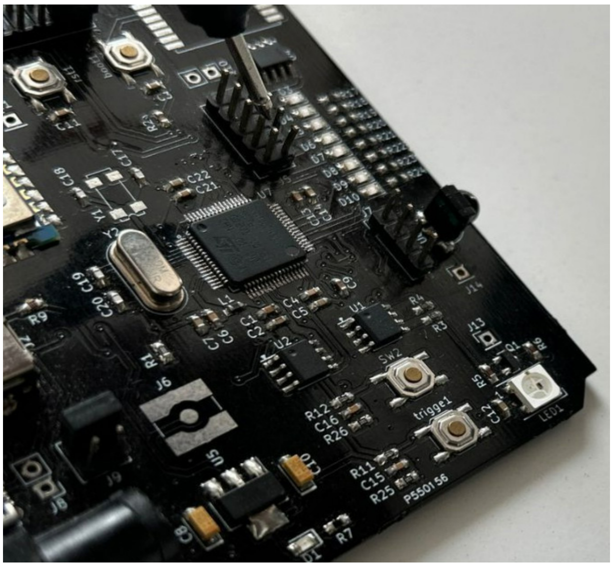
By now, we are familiar with certain hardware components that sit inside the EV charging station and are prone to hardware-based attacks. Although getting physical access to these components can be challenging, it is important to highlight their vulnerabilities. Identifying such risks is important to ensure the hardware-level security of the charging stations.

Beyond hardware attacks, EV charging stations also present vulnerabilities in the user interfaces and protocols they use to communicate with the backend server. A comprehensive penetration test should never miss the user interfaces and communication protocol assessment. Typically, EV charging stations use Open Charging Point Protocol (OCPP) to communicate with the backend server.

EXPLORING COMMON HARDWARE VULNERABILITIES IN THE CONTROL UNIT

These hardware modules contain a PCB with a microcontroller or SoC, which typically runs a Linux-based OS. Like any other embedded or IoT devices, these modules often include debug ports on the PCB that, when identified and accessed, may provide a debug shell. This access can escalate to a root shell or allow firmware extraction and modification. Therefore, understanding and mitigating the vulnerabilities related to these debug ports is essential for enhanced security.

UART OR CONSOLE PORT



Exposed Test Points on PCB

The microcontroller or SoC on the PCB often utilizes UART (Universal Asynchronous Receiver-Transmitter) for debugging purposes, such as accessing a debug shell or capturing boot logs. Exploiting a UART interface in these components is a common technique in hardware penetration testing. UART interfaces are typically used for debugging and communication between various components in embedded systems, and they may expose sensitive information or allow unauthorized access if not properly secured. Below is an overview of how an attacker might exploit UART in an EV charging station:

1. Accessing Debug Information

When connected, the UART interface mainly outputs debug logs, boot messages, or system status updates. These logs may reveal critical information such as:

- Details pertaining to the booting process.
- Details related to hardware and memory addressing.
- Version details of the software components like kernel and bootloader.
- Debugging information.

2. Stop the Autoboot

Typically, UART access allows the attacker to interrupt the boot sequence (e.g., via the U-Boot bootloader) and gain access to a shell or bootloader command line interface.

If the bootloader shell is accessible, vulnerable commands can be executed that allow for:

- **Memory inspection:** Viewing, analysing or dumping the contents of memory.
- **Firmware dumping:** Extracting and analysing the firmware further or reversing engineering to identify software-related vulnerabilities.
- **Modifying boot parameters or environment variables:** Altering the system's boot process to load malicious firmware or bypass security mechanisms.
- **Access to the root shell:** In some instances, the bootloader shell can escalate further to access the root shell. Gaining root access to the system may allow one to manipulate files, install malware, or turn off security features.

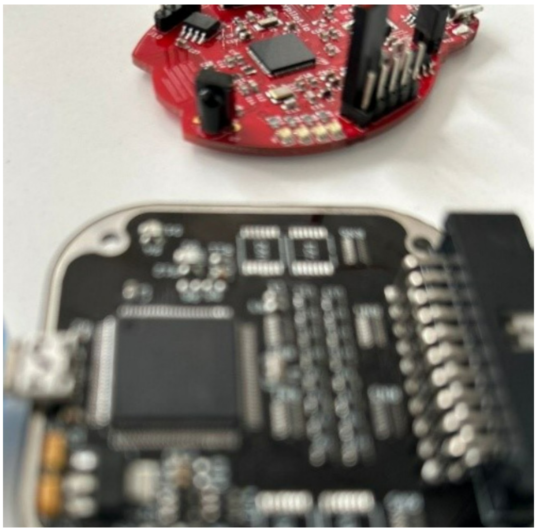
3. Gaining Unauthorized Access

Depending on how the charging station is configured, the UART interface may also allow direct access to a root shell or system command prompt after booting. If authentication is not implemented on the UART interface, the adversary could potentially gain full control of the device.

- Stealing sensitive information like user data, billing information, or authentication keys.
- Installing malware that could affect the functionality or bypass security features.

JTAG ACCESS

The JTAG port of the microcontroller/SoC is mostly exposed as a test point on the device's PCB, which makes it a potential attack surface. JTAG port, which was originally designed for debugging, testing and flashing programs in embedded systems, keeping it unprotected can be used maliciously to access the firmware running in the hardware module, bypass security measures, extract sensitive data, and take complete control of the hardware module.



Exposed Debug Test Points on PCB

An overview of how JTAG can be exploited, and its potential impacts are:

1. Debug access:

Through JTAG, an adversary can interact directly with the microcontroller or processor, allowing them to:

- Pause or halt the CPU
- Step through code execution
- Read and write to memory locations
- Access registers and peripheral components

2. Extracting Firmware:

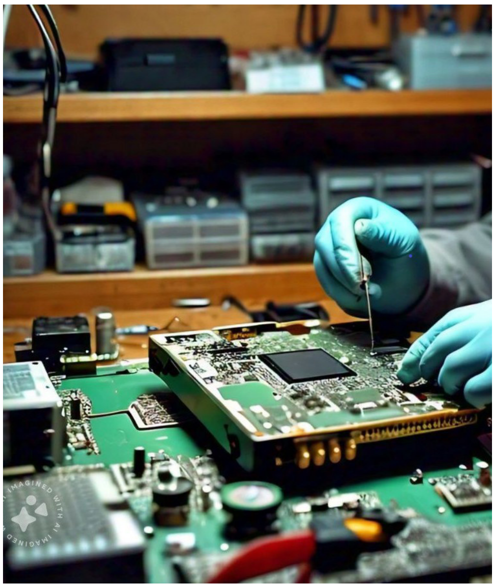
If accessed, JTAG may allow the microcontroller's internal or external flash memory to read. This can be used to:

- Dump the firmware from the module for reverse engineering to hunt software-level bugs, such as memory corruption vulnerabilities in the firmware binary or stealing the hardcoded sensitive information.
- Extract sensitive data such as encryption keys, credentials, or configuration files.

Firmware extraction allows attackers to analyse the software for vulnerabilities, hardcoded credentials, and proprietary algorithms that may be exploited further.

MEMORY READING OR FIRMWARE EXTRACTION

Hardware modules like the control unit and communication module typically run Linux-based OSs. These Linux-based OSs are mostly larger, and thus, external flash memory or eMMC is used for storing such firmware. These external memory components can be attacked to dump or patch modified firmware in the memory.



Invasive Attack on the External Memory (AI-Generated)

The vulnerability of firmware extraction from external flash memories in hardware modules presents significant hardware security risks. If these external flash memories or eMMC are not adequately secured, an adversary may gain physical access to dump the firmware from the memories and use it further for analysis. Addressing such vulnerabilities is important to safeguard the integrity and confidentiality of the firmware running in the hardware modules.

Firmware can be extracted from these external memories using hardware programmers or adapters. Once extracted, it can be reverse-engineered using tools like Ghidra to hunt for software-level vulnerabilities.

The attacker may look for vulnerabilities such as:

- Hardcoded credentials
- Encryption keys
- Firmware update mechanisms
- Memory corruption vulnerabilities
- Security flaws in the bootloader or application code

CONFIGURATION REVIEW

The control unit is typically a PLC-based device; thus, performing a configuration review of the PLC is an essential step for ensuring the security of this hardware module. An overview of how a comprehensive PLC configuration review might look like is as follows:

1. Access Control:

- Controller groups with privileged access
- Do not use default passwords or services
- Restricted remote access

2. Verify the configurations of the network

- Ensure that PLC is on a segmented network, separated from the EV charging infra network.
- Review and disable any unnecessary services and protocols that could expose the PLC to potential threats.

3. Logging and Monitoring

- Check if the event logging is enabled to log actions like configuration changes, user logins, and failed attempts to access the device.

4. Firmware and Software Updates

- Ensure the PLC has the latest firmware version, because updates usually include security fixes.

5. Protection Against Physical Access

- Check for physical security elements (locked enclosures, access controls, and surveillance) to deter unauthorized physical access to the PLC.

EXPLORING VULNERABILITIES IN THE USER INTERFACE

RFID

RFID (Radio Frequency Identification) technology plays a crucial role in EV charging stations, primarily for user authentication and access control. Many charging stations have RFID readers that allow users to initiate charging sessions using RFID cards or tags. While convenient, this technology introduces security challenges if not implemented securely. Below is an overview of how RFID functions in EV charging stations and the potential risks associated with its exploitation:

1. RFID in EV Charging Stations:

- **Authenticating Yourself:** EV users mostly use RFID tags to authenticate their identity or account to initiate the charging session. The charging station RFID reader reads the user information, such as credentials or a unique identifier, stored in the RFID tags.

- **Making Payments:** In some EV charging stations, RFID tags are used for contactless payments. These tags may store sensitive information, such as account details, balances, or transaction histories, enabling users to pay and initiate charging sessions seamlessly.

2. Unauthorized access by RFID cloning

Adversaries can use tools like Flipper Zero or RFID readers to extract data from RFID cards, capturing the unique identifier or authentication token stored in the RFID tags. If no or weak encryption like Crypto1 (Mifare Classic 1K) is used, this can be bypassed using tools like Flipper Zero. Bypassing the weak encryption and authentication allows any unauthorised user to make payments and start the charging session from the cloned RFID tags.

DISPLAY/TOUCHSCREEN:

User Interface of EV Charging Stations (AI-Generated)

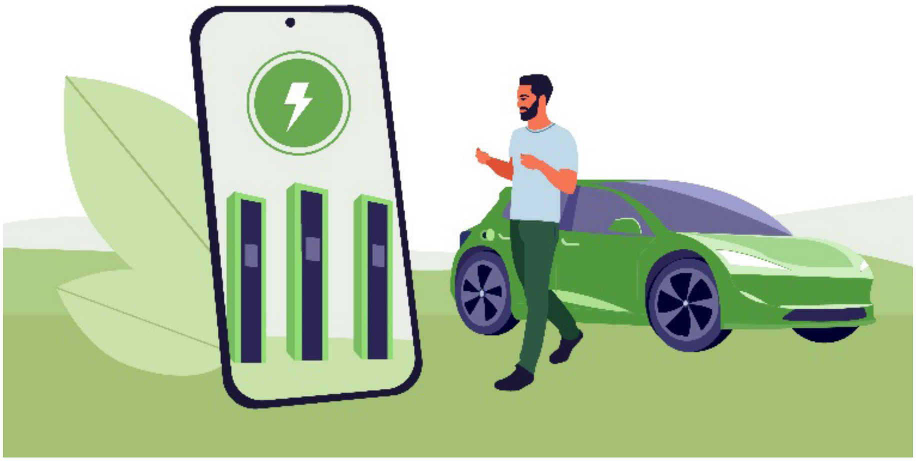
Touchscreens in EV charging stations allow users to interact with the device to perform tasks such as authenticating users, making payments or to fetch charging-related information. However, this user interface can be attacked if not adequately secured. Some of the attacks that can be performed are:

1. **Installing Malware via external ports/interfaces:** Most often these touchscreens use embedded OS which are susceptible to malware. Any malicious user with physical access may target external ports like USB to inject malware in the system which could lead to disruption or compromise of normal operation.

2. **Escaping the kiosk:** Some random touch at multiple screens may lead to escaping the kiosk, which gives access to the base OS running in the display system. Access to the base OS can be used to exploit the known vulnerabilities for that version of the OS, install malware, or tamper with the host application.

MOBILE APPLICATION

Another mode of managing vehicle charging status and connecting with charging stations is the mobile application provided by the vendor to its customers. This mobile app may allow users to find nearby charging stations, connect to specific stations, pay for the charging service, and get notifications about charging status (Paused, completed, not charged, etc.).



Mobile Application as the User Interface (AI-Generated)

Mobile applications associated with EV charging stations can be vulnerable to various security issues that could allow attackers to compromise user data, manipulate charging sessions, or disrupt the overall charging infrastructure. Here are some of the vulnerabilities that can affect these mobile apps:

1. Tampering API request:

When the mobile application connects with the EV server over the internet, it exchanges data via this connection. An adversary can intercept and tamper with the HTTP requests and responses between the app and the server. This tampering in the HTTP requests may allow the modification of the payment amount, bypassing charging time limits or exploiting vulnerabilities like SQL injection, remote code execution or SSRF to access sensitive data on the server.

2. Race condition attacks

The application is designed to let each user account connect to just one charging station at a time. However, an attacker can exploit a race condition in the mobile app to connect to multiple charging stations using the same account. In this attack, the attacker quickly sends multiple identical HTTP requests to the server. If the server doesn't handle these requests properly, some may slip through without being checked, bypassing the restriction and allowing multiple connections.

3. Identify attack surfaces by reversing the app

The backend servers and cloud systems managing charging stations, user data, and payments may have vulnerabilities in their APIs. If those APIs are exposed via mobile application, then the attacker can scan and identify weaknesses in cloud infra.

Many charging stations display QR codes on their screens for users to scan and start charging sessions, set time limits, or make payments. These systems often run in kiosk mode on Android or Windows to limit access to other features and enhance security. However, if an attacker bypasses kiosk mode, they could take complete control of the operating system. They might replace the legitimate QR code on the screen with a fake one. Users who scan this fake QR code could be redirected to a fraudulent website or app designed to steal personal information and payment details or even install malware.

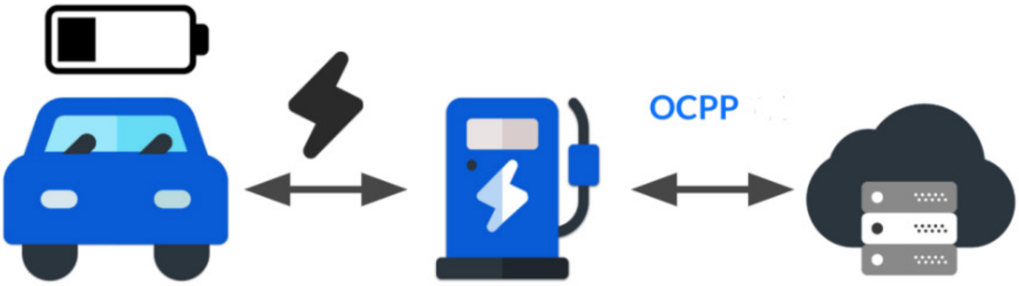
EXPLORING VULNERABILITIES IN THE COMMUNICATION PROTOCOL

INTRODUCTION TO OCPP

Open Charge Point Protocol (OCPP) is an application-layer protocol that allows communication between Electric Vehicle (EV) charging stations and their Central Management Systems (CMSs).

OCPP is an open-source protocol that enables interoperability between different charging stations and CMSs, regardless of the manufacturer or type of charging station. It's considered the de-facto standard for EV charging and typically used to:

- **Creates a universal language:** OCPP allows different charging technologies to communicate with each other.
- **Promotes competition:** OCPP offers a common platform and central management system, which encourages innovation and quality in the market.
- **Enables tech-agnostic operations:** OCPP allows charging providers to use a mix of technologies, which can lead to more efficient operations.



How OCPPP works

OCPP WORKING

Here is an overview of how OCPP allows EV chargers to communicate with the central management system.

1. The charging station and the management system establish a secure connection between each other for two-way communication.

2. Once this connection is established, messages are exchanged between the charger and the management system to communicate current status or requests. For examples:

   a. Status:
   (i) Whether a charger is available, in use, in need of maintenance, or in some other state
   (ii) Diagnostic information for charging stations

   b. Requests: When a charging session has been triggered to start or stop

OCPP VERSIONS

- OCPP 2.0.1 (Latest)
- OCPP 2.0
- OCPP 1.6
- OCPP 1.0

VULNERABILITIES IN OCPP

While OCPP provides many benefits, including interoperability and flexibility, it can also be susceptible to various security risks if not implemented properly. An overview of potential vulnerabilities and exploitation methods in OCPP are given below:

1. **Installing Malware via external ports/interfaces:** If OCPP communication is not secured with Transport Layer Security (TLS), an attacker could sniff and modify the data exchanged between the charging station and the central management system. By intercepting or injecting malicious commands into the traffic, an attacker could potentially alter charging commands, disrupt communication, or even alter billing data.

2. **Unauthorized Access to Charging Station:** Weak authentication mechanisms could allow attackers to impersonate the charging station or management server. This might allow them to bypass authorization to run admin commands. Thus, by connecting to OCPP endpoint with admin privileges, attackers could disable charging stations, tamper configurations or gain access to sensitive data.

2. **Firmware Update Manipulation:** OCPP allows for remote firmware updates, which may be insecure if not appropriately validated. If not secure, attackers may push malicious firmware on the EV charging station hardware modules.

2. **Denial of Service (DoS) Attacks:** OCPP networks can be susceptible to DoS attacks if proper rate-limiting and traffic filtering are not implemented. An attacker could flood the OCPP communication channel with requests, overwhelming the central system or individual charging stations, which may lead to service downtime and impact the availability of EV charging services.

CONCLUSION

In conclusion, this ebook highlights the security weaknesses identified during the pen testing of the EV charging station. Considering the constraints like time limitations and limited access imposed during the assessment, the vulnerabilities in the charging systems are not limited to the weaknesses discussed in this ebook.

This information serves as a starting point for individuals looking to understand and investigate the security landscape of EV charging stations. It can also guide organizations in identifying potential risks and implementing measures to strengthen the security of their charging infrastructure.

REFERENCES

- https://www.ampeco.com/guides/complete-ocpp-guide/
- https://sinoevse.com/what-is-ocpp/
- https://www.edrv.io/guide/ocpp-2-0-1-comprehensive-guide
- https://swtchenergy.com/open-charge-point-protocol-ocpp-explained-what-it-is-how-it-works-and-why-it-matters-for-ev-charging/#:~:text=How%20does%20OCPP%20work%3F,also%20called%20EV%20charging%20stations.

Payatu

About Payatu

Payatu is a Research-powered cybersecurity services and training company specialized in IoT, Embedded Web, Mobile, Cloud, & Infrastructure security assessments with a proven track record of securing software, hardware and infrastructure for customers across 20+ countries.

IoT Security Testing

IoT product security assessment is a complete security audit of embedded systems, network services, applications and firmware. Payatu uses its expertise in this domain to detect complex vulnerabilities & security loopholes to guard your IoT products against cyberattacks.

Mobile Security Testing

Detect complex vulnerabilities & security loopholes. Guard your mobile application and user's data against cyberattacks, by having Payatu test the security of your mobile application.

Cloud Security Assessment

As long as cloud servers live on, the need to protect them will not diminish. Both cloud providers and users have a shared responsibility to secure the information stored in their cloud Payatu's expertise in cloud protection helps you with the same. Its layered security review enables you to mitigate this by building scalable and secure applications & identifying potential vulnerabilities in your cloud environment.

Web Security Testing

Internet attackers are everywhere. Sometimes they are evident. Many times, they are undetectable. Their motive is to attack web applications every day, stealing personal information and user data. With Payatu, you can spot complex vulnerabilities that are easy to miss and guard your website and user's data against cyberattacks.

DevSecOps Consulting

DevSecOps is DevOps done the right way. With security compromises and data breaches happening left, right & center, making security an integral part of the development workflow is more important than ever. With Payatu, you get an insight to security measures that can be taken in integration with the CI/CD pipeline to increase the visibility of security threats.

Code Review

Payatu's Secure Code Review includes inspecting, scanning and evaluating source code for defects and weaknesses. It includes the best secure coding practices that apply security consideration and defend the software from attacks.

Red Team Assessment

Red Team Assessment is a goal-directed, multidimensional & malicious threat emulation. Payatu uses offensive tactics, techniques, and procedures to access an organization's crown jewels and test its readiness to detect and withstand a targeted attack.

Product Security

Save time while still delivering a secure end-product with Payatu. Make sure that each component maintains a uniform level of security so that all the components "fit" together in your mega-product.

Critical Infrastructure Assessment

There are various security threats focusing on Critical Infrastructures like Oil and Gas, Chemical Plants, Pharmaceuticals, Electrical Grids, Manufacturing Plants, Transportation systems etc. and can significantly impact your production operations. With Payatu's OT security expertise you can get a thorough ICS Maturity, Risk and Compliance Assessment done to protect your critical infrastructure.

Cyber Threat Intelligence

The area of expertise in the wide arena of cybersecurity that is focused on collecting and analyzing the existing and potential threats is known as Cyber Threat Intelligence or CTI. Clients can benefit from Payatu's CTI by getting – social media monitoring, repository monitoring, darkweb monitoring, mobile app monitoring, domain monitoring, and document sharing platform monitoring done for their brand.

More Services Offered

- AI/ML Security Audit
- Trainings

More Products Offered

- EXPLIoT
- EXPLIoT Academy

Payatu

Payatu Security Consulting Pvt. Ltd.

www.payatu.com

info@payatu.com

+91 20 47248026