Protecting Charging Stations Against Specific Threats

CSP008_S_E

PRESENTATION BY:
- **CRISTINA ALCARAZ**, UNIVERSITY OF MALAGA, SPAIN
- **ABDELKADER SHAABAN**, AIT, AUSTRIAN

Acknowledgement

- *Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or HADEA. Neither the European Union nor the granting authority can be held responsible for them.*
- *Project Agreement no. 101083594*

Protecting Charging Stations Against Specific Threats

Overview

- Topic-1: Introduction to the Energy Charging Infrastructures
- Topic-2: Security Challenges in Energy Charing Stations
- Topic-3: Cascading Effects and impact to other Critical Infrastructures
- Topic-4: Security Measures and Best Practices for Charging Stations

CSP008_S_E: Cristina Alcaraz (UMA)

Protecting Charging Stations Against Specific Threats

Overview

- Topic-1: Introduction to the Energy Charging Infrastructures
- **Topic-2: Security Challenges in Energy Charing Stations**
- Topic-3: Cascading Effects and impact to other Critical Infrastructures
- Topic-4: Security Measures and Best Practices for Charging Stations

CSP008_S_E: Cristina Alcaraz (UMA)

Security and privacy challenges in CSs

CSP008_S_E: Cristina Alcaraz (UMA)

Security and privacy challenges in CSs

- Since SCs and their control systems are "cyber-physical" systems by nature, we can examine the security and privacy weaknesses from four main perspectives:

Deployment

Cyber-physical nature

Communication

The role of the new paradigms

Security and privacy challenges in CSs

- Since SCs and their control systems are "cyber-physical" systems by nature, we can examine the security and privacy weaknesses from four main perspectives:

Deployment

Cyber-physical nature

Communication

The role of the new paradigms

Deployment challenges

- CSs are mostly deployed in **open environments**, accessible to the general public, such as:
  - Shopping malls
  - Parking
  - Gas stations
  - Parks
  - Highways
  - Tunnels
  - ...
- Some charging infrastructures can have support to enable **bidirectional power** transfer from EVs to the grid
  - Known as Vehicle-to-Grid (V2G) networks

And … which are the major security challenges?

Deployment challenges

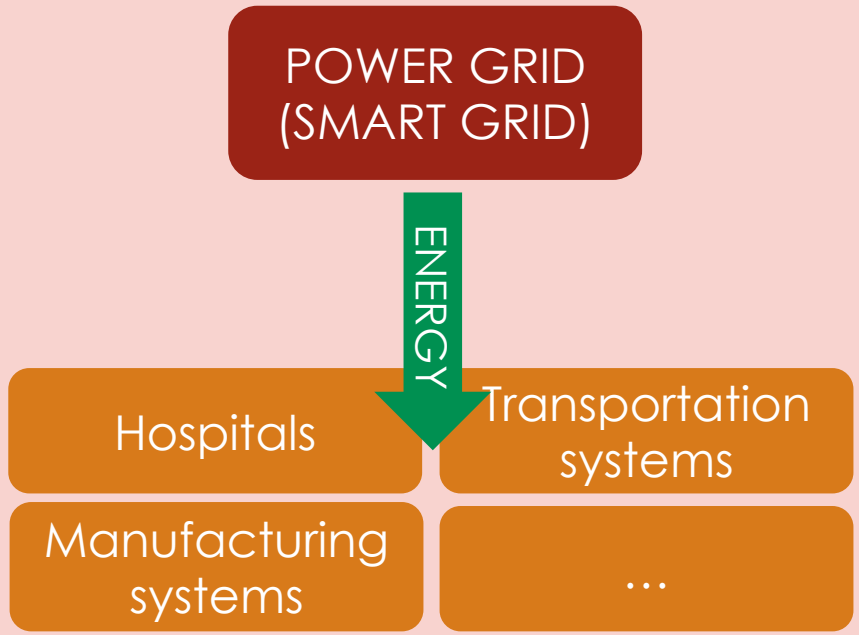
- CSs are mostly deployed in **open environments**, accessible to the general public, such as:
  - Shopping malls
  - Parking
  - Gas stations
  - Parks
  - Highways
  - Tunnels
  - ...
- Some charging infrastructures can have support to enable **bidirectional power** transfer from EVs to the grid
  - Known as Vehicle-to-Grid (V2G) networks

- CSs are exposed to **continuous change** due to their own deployment context
  - Variable contexts influenced by environmental or contextual changes (corrosion, floods, fire, …)
- There is freedom for **sabotage**, probably without permanent surveillance
  - Tampering issues: manipulation, reconfiguration, …
  - Theft issues: cables, hardware components, … power !!
  - Breakage: cables, hardware and software components, … power!!
- There is a **close connection and communication to the grid** and other energy components, such as EV batteries
  - which adds risks related to abuse, overheating and unexpected outages

Deployment challenges

- CSs are mostly deployed in **open environments**, accessible to the general public, such as:
  - Shopping malls
  - Parking
  - Gas stations
  - Parks
  - Highways
  - Tunnels
  - …
- Some charging infrastructures can have support to enable **bidirectional power** transfer from EVs to the grid
  - Known as Vehicle-to-Grid (V2G) networks

- Targeted DERs, microgrids and grid may address **unexpected cascading effects**
  - The interconnection of electricity grids and gas pipelines across Europe and beyond the EU can result in blackouts or supply shortages in other regions and countries if an outage occurs in one area



Deployment challenges

- CSs are mostly deployed in **open environments**, accessible to the general public, such as:
  - Shopping malls
  - Parking
  - Gas stations
  - Parks
  - Highways
  - Tunnels
  - ...
- Some charging infrastructures can have support to enable **bidirectional power** transfer from EVs to the grid
  - Known as Vehicle-to-Grid (V2G) networks

- CSs are exposed to **continuous change** due to their own deployment context
  - Variable contexts influenced by environmental or contextual changes(corrosion, floods, fire, …)
- There is freedom for **sabotage**, probably without permanent surveillance
  - Tampering issues
    - manipulation, reconfiguration, …
  - Theft issues
    - cables, hardware components, … power !!
  - Breakage
    - cables, hardware and software components, … power!!
- There is a **close connection and communication to the grid** and other energy components, such as EV batteries
  - which adds risks related to abuses and unexpected outages

Security and privacy challenges in CSs

- Since SCs and their control systems are "cyber-physical" systems by nature, we can examine the security and privacy weaknesses from four main perspectives:

Deployment	**Cyber-physical nature**	Communication
	The role of the new paradigms	

Cyber-physical challenges

- Both CSs and their CCs are mainly cyber-physical systems that accept the incorporation of multiples types of HW and SW components to the charging context
- In this case, we can find:
  - **"Traditional" IT devices** interacting with CSs
    - Personal devices (PCs, Tablets, Smartphones)
    - Server equipment, including virtualization support
  - **Industrial equipment** integrated as part of the CSs
    - Operations equipment (converters, connectors, …)
    - Process devices or controllers (PLC, RTU)
    - Field Devices (sensors, actuators, smart meters)
  - **Devices with limited capabilities** also integrated in CSs
    - Embedded devices (e.g., Arduino, …)
    - Small computers (e.g., Raspberry Pi, …)

And … which are the major security challenges?

Cyber-physical challenges

- Both CSs and their CCs are mainly cyber-physical systems that accept the incorporation of multiples types of HW and SW components to the charging context
- In this case, we can find:
  - **"Traditional" IT devices** interacting with CSs
    - Personal devices (PCs, Tablets, Smartphones)
    - Server equipment, including virtualization support
  - **Industrial equipment** integrated as part of the CSs
    - Operations equipment (converters, connectors, …)
    - Process devices or controllers (PLC, RTU)
    - Field Devices (sensors, actuators, smart meters)
  - **Devices with limited capabilities** also integrated in CSs
    - Embedded devices (e.g., Arduino, …)
    - Small computers (e.g., Raspberry Pi, …)

- Multiple connections and requests without discarding **inherited vulnerabilities**
- CSs/CCS and their Industrial equipment are designed to provide **safety**
  - Probably to ensure the stability of the whole system – remember that CSs are connected to DERs, the grid, …)
- It is seldom designed with **security** in mind
  - There is not native support for security mechanisms
  - Devices run outdated software and operative systems
- CSs/CCSs may still integrate "***legacy devices***"
  - Devices with support for only traditional industrial firmware and protocols, e.g. Modbus,
  - No direct interoperability with systems outside the industrial border
- CSs/CCSs are **exposed to (I)IoT devices**, some of them with HW/SW capabilities
  - And, therefore, with constraints to support basic security measures, such as cryptographic algorithm !! - <<10KB (RAM) and <<< 100KB (flash)

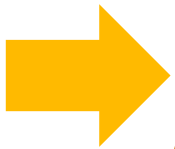
Security and privacy challenges in CSs

- Since SCs and their control systems are "cyber-physical" systems by nature, we can examine the security and privacy weaknesses from four main perspectives:

Deployment	Cyber-physical nature	**Communication**
	The role of the new paradigms	

Communication challenges

- Most charging infrastructures are based on several types of communication technologies that operate with multiple types of communication protocols
- In this case, we can find:
  - **Traditional communication technologies**
    - Wired (Ethernet) and Wireless (WiFi)
  - **Novel communication technologies**
    - Example: NB-IoT, Sigfox, LoRa… (Cellular IoT)
  - **Industrial-oriented protocols**
    - Example: OCPP, Modbus/TCP, OPC UA, …
  - **Internet-oriented protocols**
    - Lower layers: IP, TCP
    - Upper layers: RESTful frameworks, MQTT, CoAP, …



And … which are the major security challenges?

Communication challenges

- Most charging infrastructures are based on several types of communication technologies that operate with multiple types of communication protocols
- In this case, we can find:
  - **Traditional communication technologies**
    - Wired (Ethernet) and Wireless (WiFi)
  - **Novel communication technologies**
    - Example: NB-IoT, Sigfox, LoRa… (Cellular IoT)
  - **Industrial-oriented protocols**
    - Example: OCPP, Modbus/TCP, OPC UA, …
  - **Internet-oriented protocols**
    - Lower layers: IP, TCP
    - Upper layers: RESTful frameworks, MQTT, CoAP, …

- Increasingly **complex contexts**, which does not help its own maintenance
  - More technologies and more protocols is what prepares a Molotov cocktail
- Communications exposed to **interception**, especially if they are based on wireless communications
  - Consumption information must be transferred to the CCS to proceed with control tasks and billing - of great interest to attackers as well ☹
  - Again, most of the industrial protocols are of type "legacy", so preventive measures are likely to be basic or non-existent
- **Unexpected outages** due to actual consumption of limited devices
  - Traditional security protocols (e.g., TLS/DTLS, IPSec) on certain devices may severely penalise the real life-cycle of a limited device - e.g. smart meters
  - This limitations also adds the additional difficulty of incorporating other essential mechanisms such as sophisticated authentication and authorization mechanisms, logs, etc.

Communication challenges

- However, it is also important to note that there has been some progress in the security of some protocols, such as OCPP v2.0.1with respect to previous versions

Security	OCPP-v1.6	OCPP-v2.0.1
Encryption	SSL/TLS is not recommended	TLS is considered but it is **optional**
Certificate	NOT	YES
Logs	NOT	YES
ISO 15118 support (EV security)	NOT	YES
Secure upload firmware	Without verification	With verification (but **optional**)
Digital signatures	NOT	Only for meter values, **optional**
Secure data transfer	HTTP / HTTPS; FTP / FTPS	HTTP / HTTPS; FTP / FTPS

Security and privacy challenges in CSs

- Since SCs and their control systems are "cyber-physical" systems by nature, we can examine the security and privacy weaknesses from four main perspectives:

Deployment	Cyber-physical nature	Communication
	The role of the new paradigms	

IT-OT challenges

- Practically all the "smart" ecosystems, including smart cities and smart grids are today based on multiple information technologies to:
  - Ensure sustainability, controlling load according to actual demand
  - Improve quality for customers by simplifying the billing process and making it easier for them to control their own environment and resources
- In this case, we can find:
  - **New IoT** to book CSs and connect to charging space from anywhere, anytime and in any how
  - **Artificial intelligence and Big Data** to compute large volumes of data
  - **Cloud-edge computing** for processing data and applications
  - **Blockchain** for storing sensitive data
  - **etc.**

And … which are the major security challenges?

IT-OT challenges

- Practically all the "smart" ecosystems, including smart cities and smart grids are today based on multiple information technologies to:
  - Ensure sustainability, controlling load according to actual demand
  - Improve quality for customers by simplifying the billing process and making it easier for them to control their own environment and resources
- In this case, we can find:
  - **New IoT** to book CSs and connect to charging space from anywhere, anytime and in any how
  - **Artificial intelligence and Big Data** to compute large volumes of data
  - **Cloud-edge computing** for processing data and applications
  - **Blockchain** for storing sensitive data
  - **etc.**

- What is expected is just what everybody thinks, … an uncontrolled set of security risks and problems due to the fact that:

Pandora's box opens !

  - Increased complexity
  - Increased number of vulnerabilities
    - Probably of type zero-vulnerabilities
  - More susceptibility to more intelligent, sophisticated and persistent attacks
    - Increased range of threats and attack surface
  - More …
  - …

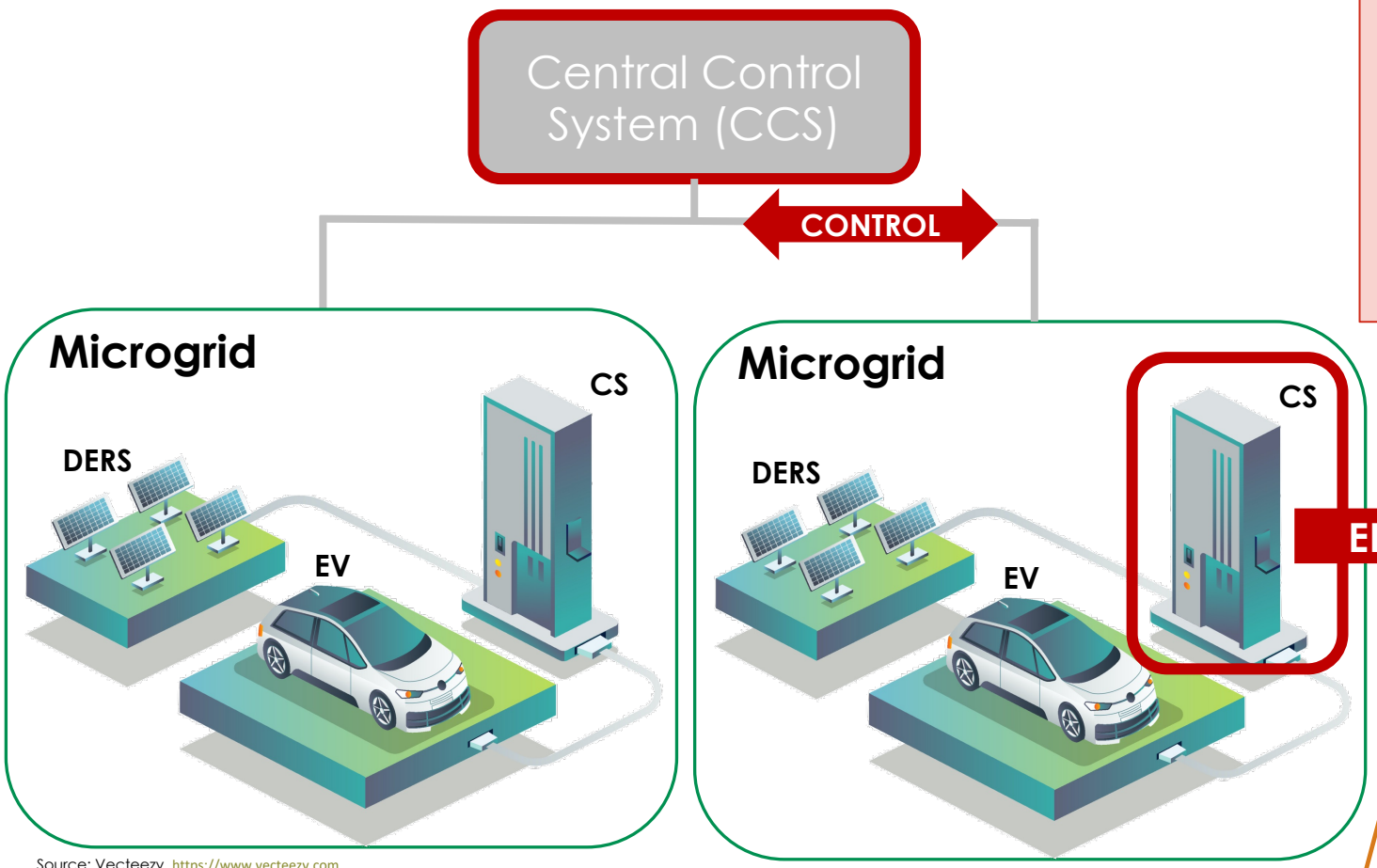
Summarizing: there is a growing cybersecurity risk in charging stations

- In fact, there is a remarkable increase in cybersecurity risks at charging stations, as also stated by U. Dorot:

Aspect	Details
Interactions	Communication among applications and with third-party payment services via APIs and JavaScript plugins
Data Handled	Processes sensitive personal driver information and vehicle details
Infrastructure Connection	Linked to sophisticated back-end systems for managing electricity distribution to charging stations
Security Vulnerabilities	Prone to various cybersecurity threats and targeted by malicious entities
Risk Exposure	Susceptible to data breaches, financial losses, and safety hazards
Market Challenges	Lacks sufficient awareness and regulatory measures for adequate protection
Common Threats	Vulnerable to account takeovers, location and identity spoofing, man-in-the-middle, supply chain attacks, API misuse, etc.
Endpoint Update Issues	Rarely updated, leading to outdated software and unaddressed vulnerabilities

Source: Uri Dorot, "EV Charging Station Applications – a Growing Cyber Security Risk", Radware Blog, 2023
URL: https://www.radware.com/blog/application-protection/2023/05/ev_charging_station_cyber_threats/

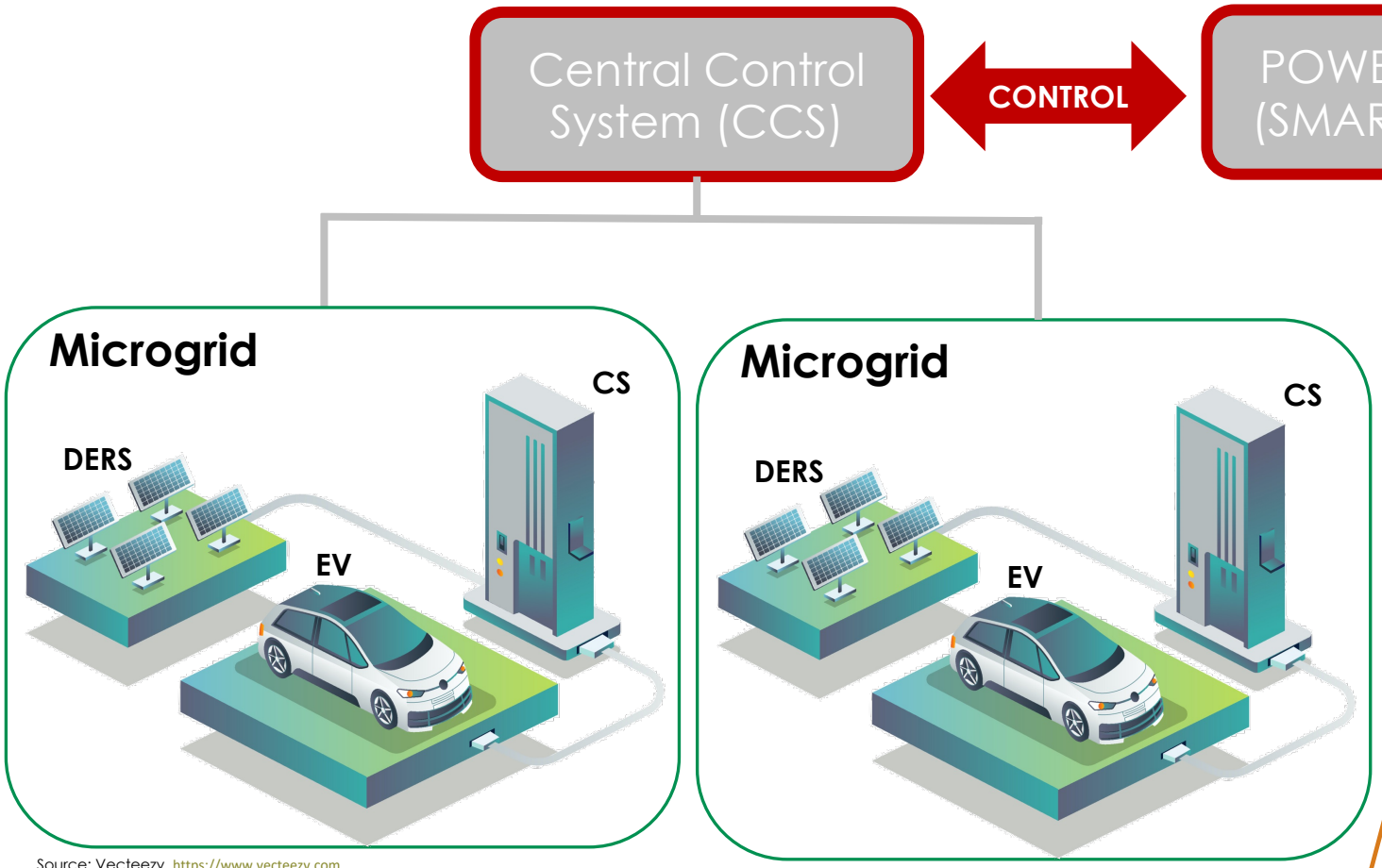
Two targets and multiple consequences (I)



Source: Vecteezy, https://www.vecteezy.com

- **Control and energy** are two of the main targets of attackers to sabotage the system, its main resources and customers
- **Cascading effects** may occur if the charging stations are severely affected

Two targets and multiple consequences (II)



Source: Vecteezy, https://www.vecteezy.com

- **Control and energy** are two of the main targets of attackers to sabotage the system, its main resources and customers
- **Cascading effects** may occur if the power grid is severely affected

Common CyberSecurity Risks To EV Charging Applications

CSP008_S_E: Abdelkader Shaaban (AIT), Cristina Alcaraz (UMA)

Cybersecurity Threats to EV Charging Applications: Risks and Implications

Threat Category	Description	Potential Impacts
Malware and Viruses	Introduced through third-party services, bot attacks, or compromised devices within the EV charging ecosystem.	Unauthorized access, data theft, and application damage.
Lack of Encryption	Absence of secure data transmission between applications and charging stations.	Data interception, user privacy compromise.
API Abuse	Inadequate security policies for API services leading to exploitations.	App APIs can leave the door open to various Bot attacks, code injections, and unauthorized access.
Insufficient Authentication	Weak mechanisms for user verification and access control.	Unauthorized access, misuse, data theft, or damage to the application.
Privacy Risks	Inadequate protection of sensitive user information collected by applications.	Privacy violations, identity theft, and financial fraud.
Supply Chain Risks	Complex networks of components and vendors not properly secured.	Vulnerabilities in applications and infrastructure.

EV Charging Station Applications – a Growing Cyber Security Risk – Radware Blog, accessed in March 2024

Vulnerability Analysis

CSP008_S_E: Abdelkader Shaaban (AIT), Cristina Alcaraz (UMA)

CSMS Case-Study

- Various vulnerabilities have been identified with only the focus on 13 significant vulnerability types in all the CSMS.
- They assessed multiple CSMS products to conduct the study.
- They categorized each vulnerability with its corresponding Common Weakness Enumeration (CWE) ID, providing a reference for further details on each weakness within the CWE database.

Category	Vendor/Developer	CSMS
Firmware	Schneider Electric	EVlink
	Eaton Corporation	xChargeIn
	Etrel	CSWI Etrel
	Smartfox	Smartfox
	Keba	Keba
Mobile	ChargePoint	ChargePoint
	Go Electric Stations	Go
	EV Connect	EV Connect
Web	Open Access to Sustainable Intermittent Sources	OASIS Portal
	Cornerstone Technologies Limited	BaSE EVMS
	Ensto	Ensto CSI
	Fuzhou Comprehensive Energy Inf. Service	FCEIS
	Bluesky Energy Technology	ICEMS
	Revolution Pi Project	PiControl
	Garo	Garo CSI
	Unicorn Systems	Lancelot

Nasr, Tony, et al. "Power jacking your station: In-depth security analysis of electric vehicle charging station management systems." *Computers & Security* 112 (2022): 102511.

Vulnerabilities found in the studied CSMS

		CWE-ID/Vulnerability												
		79	89	200	306	321	352	425	798	799	918	942	942	1236
	CSMS	Cross Site Scripting (XSS)	SQL Injection (SQLi)	Information Disclosure	Missing Authentication	Embedded Secrets	Cross-Site requite Forgery (CSRF)	Forced Browsing	Hard-Coded Credentials	Missing Rate Limit	Server-Side Request Forgery (SSRF)	CORS Misconfiguration	FCDP Misconfiguration	CSV Injection (CSVi)
Firmware	EVlink	X		X			X	X	X	X	X			X
	xChargeIn				X					X			X	
	CSWI Etrel	X			X				X		X		X	
	SmartFox								X	X				
	Keba				X							X		
Mobile	ChargePoint					X								
	Go					X				X				
	EV Connect					X				X				
Web	OASIS Portal	X					X							
	BaSE EVMS		X							X				
	Ensto CSI				X					X				
	FCEIS									X		X		
	ICEMS		X							X				
	PiControl	X					X		X	X	X	X		
	Garo CSI				X					X				
	Lancelot									X		X		

Nasr, Tony, et al. "Power jacking your station: In-depth security analysis of electric vehicle charging station management systems." *Computers & Security* 112 (2022): 102511.

Generic Taxonomy of threats in charging infrastructures

CSP008_S_E: Cristina Alcaraz (UMA), Abdelkader Shaaban (AIT)

Taxonomy of threats in charging infrastructures

- Thus, it is clear that CSs and their related components may become susceptible to multiples types of threats
- But:
  - **QUESTION 1**: Which ones ?
  - ANSWER: "*Basically, any threat against CPSs/IIoT*"
  - **QUESTION 2**: What are the main resources that may be affected by these threats?
  - ANSWER: "those resources in charge of managing the primary services in charging infrastructures such as: **control and energy**,
    - Control as an essential service to guarantee power
    - Power as an essential physical element for society

CONTROL

POWER

Taxonomy of threats in charging infrastructures

- Thus, it is clear that CSs and their related components may become susceptible to multiples types of threats
- But:
  - **QUESTION 1**: Which ones ?
  - ANSWER: "*Basically, any threat against CPSs/IIoT*"
  - **QUESTION 2**: What are the main resources that may be affected by these threats?
  - ANSWER: "those resources in charge of managing the primary services in charging infrastructures such as: **control and energy**,
    - Control as an essential service to guarantee power
    - Power as an essential physical element for society

Taxonomy of threats against control

- To classify the **threats against the control**, we will consider the typical category based on the ISO 7498-2 model:

Availability (data, resources)	Integrity (data, resources)	Confidentiality (data)

- but also the threat analysis performed in:
  - C. Alcaraz, J. Lopez, S. Wolthusen, "OCPP Protocol: Security Threats and Challenges", *IEEE Transactions on Smart Grid*, vol. 8, pp. 2452 – 2459, 2017, ISSN: 1949-3053

Threats against the control – CCS-CS

The **CCS** is the most affected asset

	IMPACT on			
	CCS	CS	EV	Power grid
MitM	■	■	■	■
Abuse of offline mode	■	■	■	■
On-path attack	■			
Render useless	■	■	■	■
Redirect traffic	■			
APTs	■	■	■	■
Web/TCP-IP attacks	■	■	■	■
DoS	■	■		■
Desynchronization	■	■		■
Physical attack / jamming	■	■	■	■

Availability

Integrity

Confidentiality

CSP008_S_E: Cristina Alcaraz (UMA), Abdelkader Shaaban (AIT)

Threats against the control - CCS-CS

The **CCS** is the most affected asset

	IMPACT on			
	CCS	CS	EV	Power grid
MitM	■	■	■	■
Impersonation	■	■	■	■
over-/undershooting				■
Data tampering	■	■	■	■
Fraud / energy theft	■		■	■
False injection	■	■	■	■
On-path attacks	■			
Redirect traffic	■			
APTs	■	■	■	■
Web/TCP-IP attacks	■	■	■	■
Desynchronization	■	■		■
Replacement	■	■	■	■

Availability

Integrity

Confidentiality

Threats against the control - CCS-CS

The **CCS** is the most affected asset

	IMPACT on			
	CCS	CS	EV	Power grid
MitM	■	■	■	■
Redirect traffic	■			
APTs	■	■	■	■
Covert/Side channels	■			
Passive analysis attack	■	■	■	
Deliberate exposures	■	■	■	■
Web/TCP-IP attacks	■	■	■	■

Availability

Integrity

Confidentiality

CSP008_S_E: Cristina Alcaraz (UMA), Abdelkader Shaaban (AIT)

Taxonomy of threats in charging infrastructures

- Thus, it is clear that CSs and their related components may become susceptible to multiples types of threats
- But:
  - **QUESTION 1**: Which ones ?
  - ANSWER: "*Basically, any threat against CPSs/IIoT*"
  - **QUESTION 2**: What are the main resources that may be affected by these threats?
  - ANSWER: "those resources in charge of managing the primary services in charging infrastructures such as: **control and energy**,
    - Control as an essential service to guarantee power
    - Power as an essential physical element for society, and

CONTROL

POWER

CSP008_S_E: Cristina Alcaraz (UMA), Abdelkader Shaaban (AIT)

Taxonomy of threats against energy

- If we consider the nature of the energy and "safety" restrictions, we can establish a correspondence with the previous classification but this time considering only the availability and integrity of the components and services, such as:

Disrupt services (availability)	Overloading (integrity, availability)	Energy theft (integrity)

- To do so, we also consider the work:
  - C. Alcaraz, J. Lopez, S. Wolthusen, "OCPP Protocol: Security Threats and Challenges", *IEEE Transactions on Smart Grid*, vol. 8, pp. 2452 – 2459, 2017, ISSN: 1949-3053

Threats against the energy

	IMPACT on			
Attacks	**CCS**	**CS**	**EV**	**Power grid**
MitM	■	■	■	■
Impersonation	■	■	■	■
Over-/undeershooting				■
Abuse of offline mode	■	■	■	■
Data tampering	■	■	■	■
False injection	■	■	■	■
On-path attacks	■			
Render unless	■	■	■	■
APTs	■	■	■	■
Web/TCP-IP attacks	■	■	■	■
DoS	■	■		■
DoES				■
Desynchronization	■	■		■
Physical attack and jamming	■	■	■	■
Replacement	■	■	■	■

The **power grid** is the most affected asset

Availability

Integrity

Threats against the energy

Availability

Integrity

	IMPACT on			
Attacks	**CCS**	**CS**	**EV**	**Power grid**
MitM	■	■	■	■
Impersonation	■	■	■	■
Over-/undershooting				■
Abuse of offline mode	■	■	■	■
Data tampering	■	■	■	■
Fraud / energy theft			■	■
False injection	■	■	■	■
APTs	■	■	■	■
Web/TCP-IP attacks	■	■	■	■
Replacement	■	■	■	■

The **power grid** is the most affected asset

Threats against the energy

Availability

Integrity

	IMPACT on			
Attacks	**CCS**	**CS**	**EV**	**Power grid**
MitM	■	■	■	■
Impersonation	■	■	■	■
Abuse of offline mode	■	■	■	■
Data tampering	■	■	■	■
Fraud / energy theft			■	■
False injection	■	■	■	■
APTs	■	■	■	■
Web/TCP-IP attacks	■	■	■	■
Replacement	■	■	■	■

The **power grid and EVs** are the most affected assets

More about: Specific Cyber Attacks in CSs

CSP008_S_E: Abdelkader Shaaban (AIT), Cristina Alcaraz (UMA)

Examples of EV Charging Application Cyber Attacks

Rogue EV Charging Stations: EV charging stations are vulnerable to hacking, enabling theft of user data or vehicle damage. Hackers achieve this by altering firmware or physically connecting a device to the station.

- **Consequences:** A rogue charging station, once connected, can launch more attacks.

Billing Fraud: Malicious actors exploit vulnerabilities in the billing process EV charging apps for fraud.

- **Consequences**: It involves using bots to create fake charging sessions or overcharge users.

Supply-Chain Attacks: Hackers exploit vulnerabilities in third-party JS services embedded in the EV charing app to execute Formjacking attacks to inject malicious code into the app's payment form.

- **Consequences:** Attackers can steal credit card and sensitive user data, leading to potential data leakage.

Location Spoofing: Location spoofing tricks the EV charging app into thinking the user is at another location.

- **Consequences:** It can bypass location-based pricing or access restricted charging stations.

Denial-of-Service (DoS) Attacks: The EV charging application becomes overwhelmed by network traffic in a DoS attack.

- **Consequences:** DoS attacks render the app unusable and disrupt charging infrastructure, and/or be used to extort money from the application provider.

EV Charging Station Applications – a Growing Cyber Security Risk – Radware Blog, accessed in March 2024

Examples of EV Charging Application Cyber Attacks

Injection Attacks: Malicious scripts are injected into user input fields or APIs in an injection attack.

- **Consequences**: Injection attacks manipulate databases and steal sensitive data. EV charging apps relying on databases for user data are vulnerable.

Cross-Site Scripting (XSS) Attacks: XSS attacks inject harmful scripts into EV charging app web pages, affecting other users.

- **Consequences:** EV charging apps with unvalidated input fields are prone to XSS attacks.

Cross-Site Request Forgery (CSRF) Attacks: CSRF attacks trick users into unknowingly executing actions for attackers, such as submitting forms or transferring funds.

- **Consequences:** EV charging apps using cookies or session tokens for authentication are vulnerable to CSRF attacks.

Server-Side Request Forgery (SSRF) Attacks: In a SSRF attack, the attacker tricks the charging app server to access an unauthorized resource on another server.

- **Consequences**: This enables the attacker to bypass authentication and acce sensitive data or control the charging station.

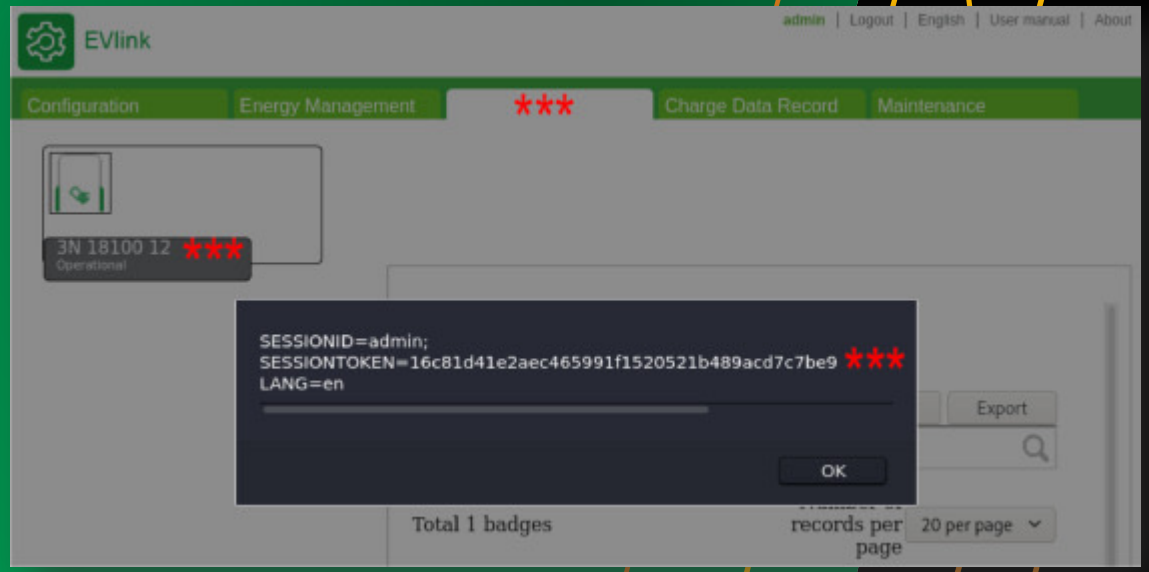
EV Charging Station Applications – a Growing Cyber Security Risk – Radware Blog, accessed in March 2024

Attacks Against the CS

- **Charging Process and Settings Manipulation**
- Attackers could manipulate the charging schedules and operations, such as initiating, delaying, or stopping charging processes.
- Lack of input sanitization led to XSS vulnerabilities, particularly in EVlink.
- Malicious JavaScript injection was possible due to inadequate cleansing and encoding of user input.
- Exploiting XSS vulnerabilities allowed attackers to hijack user sessions and gain control over the system.
  - Privileged accounts, like administrators, were particularly vulnerable.
  - A configuration initialization functionality within EVlink has been discovered that was vulnerable to Comma-Separated Values injection (CSVi), which can be exploited to embed an XSS payload that gets triggered and stored on the system database when the crafted CSV file is loaded.
  - This vulnerability leads to a stored XSS, which enables privilege escalation by hijacking the administrator's session tokens

Attacks Against the CS

- **Charging Process and Settings Manipulation**
- Attackers could manipulate the charging schedules and operations, such as initiating, delaying, or stopping charging processes.
- Lack of input sanitization led to XSS vulnerabilities, particularly in EVlink.
- Malicious JavaScript injection was possible due to inadequate cleansing and encoding of user input.
- Exploiting XSS vulnerabilities allowed attackers to hijack user sessions and gain control over the system.
  - Privileged accounts, like administrators, were particularly vulnerable.
  - A configuration initialization functionality within EVlink has been discovered that was vulnerable to Comma-Separated Values injection (CSVi), which can be exploited to embed an XSS payload that gets triggered and stored on the system database when the crafted CSV file is loaded.
  - This vulnerability leads to a stored XSS, which enables privilege escalation by hijacking the administrator's session tokens



Attacks Against the CS

- **Charging Process and Settings Manipulation**
- Found vulnerabilities in several CSMS related to CSRF weaknesses.
- Attackers exploit these weaknesses to manipulate CS settings by inducing users to perform unintentional actions.
- Attackers gain control over user accounts and access all CSMS data and functionalities, especially if the user has administrative privileges.
- For instance, a CSRF flaw in the OASIS administrator panel allows attackers to trigger a POST-based reflected XSS by exploiting the lack of a CSRF token.
- This XSS can hijack the user's account, as demonstrated by a crafted Proof-of-Concept form.
- PiControl-based CSMS also have POST-based CSRF weaknesses, allowing modification of control panel settings.
- Additionally, a GET-based CSRF vulnerability in EVlink enables attackers to take over user accounts by changing the password value through a vulnerable GET parameter.

Nasr, Tony, et al. "Power jacking your station: In-depth security analysis of electric vehicle charging station management systems." *Computers & Security* 112 (2022): 102511.

Attacks Against the CS

- **Denial of Service (DoS)**
- Attackers can gain control over CSMS to lock CS or disable features, denying legitimate access.
- Needs initial control over CSMS, possibly through XSS or CSRF, to perform DoS attacks on CS.
- Found CSRF flaws in EVlink and OASIS, enabling adversaries to force-restart CS, causing disruption in charging schedules.
- CSRF vulnerability in EVlink can cause CS to restart every 30 seconds due to the absence of randomized token validation.
- Attackers can flood CSMS with requests, preventing legitimate access, as several CSMS lack rate limiting mechanisms.
- Some CSMS lack rate limiting mechanisms (e.g., authentication), like xChargeIn, CSWI Etrel, Keba.
- Allows adversaries to crash CSMS and conduct dictionary attacks on login forms.
- Adversaries can brute-force CSMS web paths to find hidden endpoints and resources.

Nasr, Tony, et al. "Power jacking your station: In-depth security analysis of electric vehicle charging station management systems." *Computers & Security* 112 (2022): 102511.

Attacks Against the CS

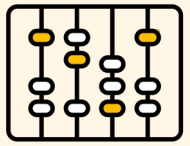
- **Denial of Service (DoS)**
- Attackers can gain control over CSMS to lock CS or disable features, denying legitimate access.
- Needs initial control over MS, possibly through XSS or CSRF, to perform DoS attacks on CS.
- Found CSRF flaws in EVlink and OASIS, enabling adversaries to force-restart CS, causing disruption in charging schedules.
- CSRF vulnerability in EVlink can cause CS to restart every 30 seconds due to the absence of randomized token validation.
- Attacker can flood CSMS with requests, preventing legitimate access, as several CSMS lack rate limiting mechanisms.
- Some CSMS lack rate limiting mechanisms (e.g., authentication), like xChargeIn, CSWI Etrel, Keba.
- Allows adversaries to crash CSMS and conduct dictionary attacks on login forms.
- Adversaries can brute-force CSMS web paths to find hidden endpoints and resources.

Nasr, Tony, et al. "Power jacking your station: In-depth security analysis of electric vehicle charging station management systems." *Computers & Security* 112 (2022): 102511.

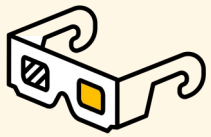
Attacks Against the CS

Other cyber attacks

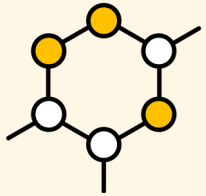
Firmware Manipulation



Billing Manipulation



Bot Recruitment and Network Proxy



Nasr, Tony, et al. "Power jacking your station: In-depth security analysis of electric vehicle charging station management systems." *Computers & Security* 112 (2022): 102511.

Attacks Against the User

- **Charging Data/Record Theft**
  - CSRF and SQLi let attackers pose as real users and access user data and resources.
  - Resources include charging data records and vehicle-specific log data.
  - This data can reveal user behaviors and charging activities.
  - Attackers can exploit this information for malicious purposes (e.g., surveillance, espionage, property heist, etc.).

Nasr, Tony, et al. "Power jacking your station: In-depth security analysis of electric vehicle charging station management systems." *Computers & Security* 112 (2022): 102511.

Attacks Against the User

Charge number	Charging station	Socket ID	Transaction ID	UID	Type of charge	Start time	End time	Energy (kWh)	Socket Type	Duration
464	EVB1A22P2RI3N18153120030045069 1E5	1	871860		AC_THREE_PHASE	2020-10-27 05:45	2020-10-27 10:00	36,782	TYPE2	04:00:31
463	EVB1A22P2RI3N18153120030045069 1E5	1	868892		AC_THREE_PHASE	2020-10-25 16:10	2020-10-25 16:29	2,929	TYPE2	00:18:52
462	EVB1A22P2RI3N18153120030045069 1E5	1	868872		AC_THREE_PHASE	2020-10-25 16:04	2020-10-25 16:07	0,310	TYPE2	00:02:57
461	EVB1A22P2RI3N18153120030045069 1E5	1	865974		AC_THREE_PHASE	2020-10-23 18:37	2020-10-24 09:31	37,929	TYPE2	04:07:31
460	EVB1A22P2RI3N18153120030045069 1E5	1	864465		AC_THREE_PHASE	2020-10-22 13:50	2020-10-22 17:11	12,666	TYPE2	01:22:24
459	EVB1A22P2RI3N18153120030045069 1E5	1	860798		AC_THREE_PHASE	2020-10-20 16:52	2020-10-22 06:48	48,797	TYPE2	05:17:54
458	EVB1A22P2RI3N18153120030045069 1E5	1	855163		AC_THREE_PHASE	2020-10-18 05:16	2020-10-18 16:19	53,112	TYPE2	05:45:29

- **Charging Data/Record Theft**
  - CSRF and SQLi let attackers pose as real users and access user data and resources.
  - Resources include charging data records and vehicle-specific log data.
  - This data can reveal user behaviors and charging activities.
  - Attackers can exploit this information for malicious purposes (e.g., surveillance, espionage, property heist, etc.).

Nasr, Tony, et al. "Power jacking your station: In-depth security analysis of electric vehicle charging station management systems." *Computers & Security* 112 (2022): 102511.

Attacks Against the User

- **Payment Fraud**
  - Most public CSMS support online payments for charging bills.
  - SQLi vulnerabilities can be exploited to extract payment records from the CSMS database.
  - Attackers can covertly steal payment information using techniques like stored XSS.
  - Stolen financial data can be used for payment fraud or sold to other malicious third-parties.
  - Several CSMS products are vulnerable to these attacks via SQLi and stored XSS.

Nasr, Tony, et al. "Power jacking your station: In-depth security analysis of electric vehicle charging station management systems." *Computers & Security* 112 (2022): 102511.

Attacks Against the Power Grid

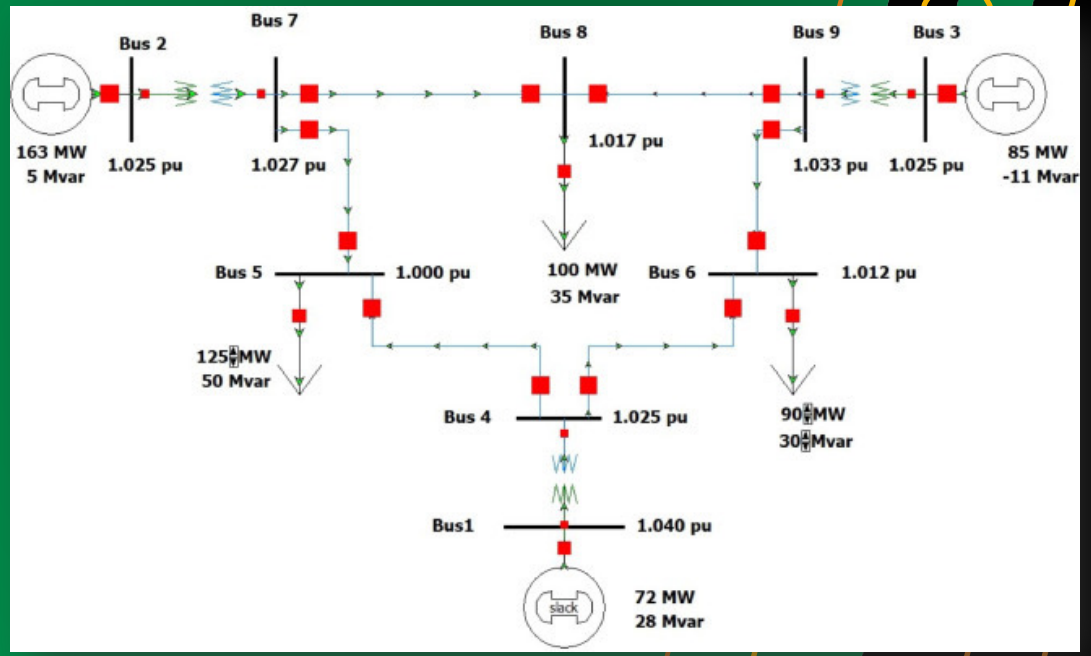
- **Increase in Charging Demand.**
  - Adversary uses compromised CS to launch synchronized charging operations.
  - Objective is to destabilize the grid by sudden increase in charging demands.

Nasr, Tony, et al. "Power jacking your station: In-depth security analysis of electric vehicle charging station management systems." *Computers & Security* 112 (2022): 102511.

Attacks Against the Power Grid

- **Increase in Charging Demand.**
  - Adversary uses compromised CS to launch synchronized charging operations.
  - Objective is to destabilize the grid by sudden increase in charging demands.

Western System Coordinating Council (WSCC) with 9 buses/lines and a demand equal to 315MW



- Benchmark setup for power systems transient stability analysis.
- Small size system, commonly used for this purpose.
- Buses 5, 6, and 8 are load buses.
- Generators at buses 2 and 3 have inertia, while the generator at slack bus 1 has variable generation.
- Generators 2 and 3 are set to IEEE type-2 speed-governing model (IEEE-G2) for testing.
- Adversary compromises CS (levels 1, 2, and 3) scattered across buses 5, 6, and 8.

Nasr, Tony, et al. "Power jacking your station: In-depth security analysis of electric vehicle charging station management systems." *Computers & Security* 112 (2022): 102511.

Attacks Against the Power Grid

- **Increase in Discharging Supply**
  - The adversary aims to reverse the flow of electricity into the grid by making numerous EVs discharge power using compromised CS with bidirectional power flow capability.
  - This capability is facilitated by Vehicle-to-Grid (V2G) technology, enabling the transfer of energy stored in EV batteries back to the power grid.
  - While V2G is designed to assist the grid during high-demand periods, attackers can exploit it to disrupt the grid by injecting excess power.
  - The goal is to coordinate large-scale discharging activities to destabilize the power grid, causing a sudden surge in electricity supply and disrupting the balance between power demand and supply.

Nasr, Tony, et al. "Power jacking your station: In-depth security analysis of electric vehicle charging station management systems." *Computers & Security* 112 (2022): 102511.

Attacks Against the Power Grid

- **Switching Attack.**
  - Adversary combines previous attack capabilities for switching attack.
  - Aims to synchronize large-scale charging and discharging among compromised CS and EVs.
  - Causing sudden and switching frequency disturbances, that throw off the stability of the power grid.
  - By forcing EV charging, the attacker decreases system frequency, prompting an increase in generation to restore it to normal levels.
  - The attacker will take advantage of the system's response to perform the opposite attack (increase in supply by forcing EVs to discharge), by removing the load they added and instead injecting power to the grid, by leveraging the Vehicle-to-Grid (V2G) feature of CS.
  - This would cause the system to have more generation than load, overshooting the frequency to the critical region. Consequently, the system will attempt to recover by reducing its own generation, to which the attacker will respond by increasing the load, causing a drop in frequency, and so on. Thus, the attacker does not allow the system to restore its frequency back to normal.

Nasr, Tony, et al. "Power jacking your station: In-depth security analysis of electric vehicle charging station management systems." *Computers & Security* 112 (2022): 102511.

References and sources

1. IEA, Electric Vehicles, 2024
   URL: https://www.iea.org
2. Global Market Insigths (GMI), "Europe Electric Vehicle Charging Station Market Size", 2022
   URL: https://www.gminsights.com/industry-analysis/europe-electric-vehicle-charging-station-market
3. C. Alcaraz, J. Lopez, and S. Wolthunsen, "OCPP Protocol: Security Threats and Challenges", IEEE Transactions on Smart Grid, vol. 8, pp. 2452 - 2459, 2017
4. C. Alcaraz, J. Cumplido, A. Triviño, "OCPP in the spotlight: threats and countermeasures for electric vehicle charging infrastructures 4.0", International Journal of Information Security, 2023, ISSN: 1615-5262
5. Uri Dorot, "EV Charging Station Applications – a Growing Cyber Security Risk", Radware Blog, 2023
   URL: https://www.radware.com/blog/application-protection/2023/05/ev_charging_station_cyber_threats/
6. Figures attributed to Vecteezy, 2024
   URL: https://www.vecteezy.com
7. DeepL Translator for proofreading.
   URL: https://www.deepl.com/translator

Connect with CyberSecPro:
How to register and other practical information

1. Website: www.cybersecpro-project.eu
2. X (Twitter): https://twitter.com/CyberSecPro_eu
3. LinkedIn: https://www.linkedin.com/company/cybersecpro-euproject/

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or HADEA. Neither the European Union nor the granting authority can be held responsible for them.

Project Agreement no. 101083594

Thank you

If you have any questions, please do not hesitate to contact us:

- Cristina Alcaraz
  alcaraz@uma.es
- Abdelkader Shaaban
  abdelkader.shaaban@ait.ac.at