Protezione delle stazioni di ricarica da minacce specifiche

CSP008_S_E

PRESENTAZIONE DA PARTE DI:

- **CRISTINA ALCARAZ**, UNIVERSITÀ DI MALAGA, SPAGNA
- **ABDELKADER SHAABAN**, AIT, AUSTRIACO

Riconoscimento

- *Co-finanziato dall'Unione Europea. I punti di vista e le opinioni espresse sono tuttavia esclusivamente quelli dell'autore o degli autori e non riflettono necessariamente quelli dell'Unione Europea o di HADEA. Né l'Unione Europea né l'autorità che ha concesso il finanziamento possono essere ritenute responsabili.*
- *Accordo di progetto n. 101083594*

Protezione delle stazioni di ricarica contro Minacce specifiche

Panoramica

- Argomento-1: Introduzione alle infrastrutture di ricarica energetica
- Argomento-2: Sfide per la sicurezza nelle stazioni di rifornimento energetico
- Argomento-3: Effetti a cascata e impatto su altre infrastrutture critiche
- Argomento 4: Misure di sicurezza e migliori pratiche per le stazioni di ricarica

CSP008_S_E: Cristina Alcaraz (UMA)

Protezione delle stazioni di ricarica contro Minacce specifiche

Panoramica

- Argomento-1: Introduzione alle infrastrutture di ricarica energetica
- **Argomento-2: Sfide per la sicurezza nelle stazioni di rifornimento energetico**
- Argomento-3: Effetti a cascata e impatto su altre infrastrutture critiche
- Argomento 4: Misure di sicurezza e migliori pratiche per le stazioni di ricarica

CSP008_S_E: Cristina Alcaraz (UMA)

Sfide per la sicurezza e la privacy nelle CS

CSP008_S_E: Cristina Alcaraz (UMA)

Sfide per la sicurezza e la privacy nelle CS

- Poiché i CS e i loro sistemi di controllo sono sistemi "cyber-fisici" per natura, possiamo esaminare le debolezze della sicurezza e della privacy da quattro prospettive principali:

Distribuzione

Natura cyber-fisica

Comunicazione

Il ruolo nuovi paradigmi

Sfide per la sicurezza e la privacy nelle CS

- Poiché i CS e i loro sistemi di controllo sono sistemi "cyber-fisici" per natura, possiamo esaminare le debolezze della sicurezza e della privacy da quattro prospettive principali:

Distribuzione

Natura cyber-fisica

Comunicazione

Il ruolo nuovi paradigmi

Sfide di implementazione

- Le CS sono per lo più distribuite in **ambienti aperti**, accessibili al in generale, come esempio:
  - Centri commerciali
  - Parcheggio
  - Stazioni di servizio
  - Parchi
  - Autostrade
  - Gallerie
  - …

- Alcune infrastrutture di ricarica possono essere dotate di un supporto per consentire il trasferimento **bidirezionale** di **energia** dai veicoli alla rete.
  - Conosciute come reti Vehicle-to-Grid (V2G)

E… quali sono le principali sfide per la sicurezza?

Sfide di implementazione

- Le CS sono per lo più distribuite in **ambienti aperti**, accessibili al in generale, come esempio:
  - Centri commerciali
  - Parcheggio
  - Stazioni di servizio
  - Parchi
  - Autostrade
  - Gallerie
  - …

- Alcune infrastrutture di ricarica possono essere dotate di un supporto per consentire il trasferimento **bidirezionale** di **energia** dai veicoli alla rete.
  - Conosciute come reti Vehicle-to-Grid (V2G)

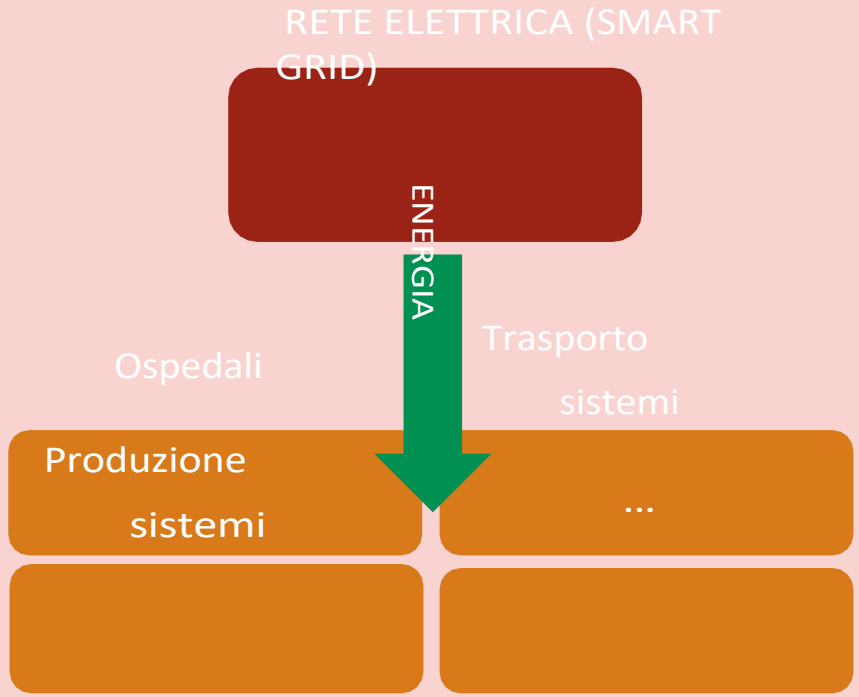
- Le CS sono esposte a **continui cambiamenti** a causa del proprio contesto di impiego
  - Contesti variabili influenzati da cambiamenti ambientali o contestuali (corrosione, alluvioni, incendi, ...)
- C'è libertà di **sabotaggio**, probabilmente senza sorveglianza permanente.
  - Problemi di manomissione: manipolazione, riconfigurazione, ...
  - Problemi di furto: cavi, componenti hardware, ... alimentazione !!!
  - Rottura: cavi, componenti hardware e software, ... potenza!!!
- Esiste **una stretta connessione e comunicazione con la rete** e con altri componenti energetici, come le batterie dei veicoli elettrici.
  - che aggiunge rischi legati ad abusi, surriscaldamento e interruzioni impreviste.

Sfide di implementazione

- Le CS sono per lo più distribuite in **ambienti aperti**, accessibili al in generale, come esempio:
  - Centri commerciali
  - Parcheggio
  - Stazioni di servizio
  - Parchi
  - Autostrade
  - Gallerie
  - …

- Alcune infrastrutture di ricarica possono essere dotate di un supporto per consentire il trasferimento **bidirezionale** di **energia** dai veicoli alla rete.
  - Conosciute come reti Vehicle-to-Grid (V2G)

- I DER, le microgrid e la rete possono affrontare **effetti a cascata inaspettati.**
  - L'interconnessione delle reti elettriche e dei gasdotti in Europa e al di fuori dell'UE può provocare blackout o carenze di approvvigionamento in altre regioni e paesi se si verifica un'interruzione in un'area.



Sfide di implementazione

- Le CS sono per lo più distribuite in **ambienti aperti**, accessibili al in generale, come esempio:
  - Centri commerciali
  - Parcheggio
  - Stazioni di servizio
  - Parchi
  - Autostrade
  - Gallerie
  - …

- Alcune infrastrutture di ricarica possono essere dotate di un supporto per consentire il trasferimento **bidirezionale** di **energia** dai veicoli alla rete.
  - Conosciute come reti Vehicle-to-Grid (V2G)

- Le CS sono esposte a **continui cambiamenti** a causa del proprio contesto di impiego
  - Contesti variabili influenzati da cambiamenti ambientali o contestuali (corrosione, alluvioni, incendi, ...)
- C'è libertà di **sabotaggio**, probabilmente senza sorveglianza permanente.
  - Problemi di manomissione
    - manipolazione, riconfigurazione, …
  - Problemi di furto
    - cavi, componenti hardware, ... alimentazione !!!
  - Rottura
    - cavi, componenti hardware e software, ... potenza!!!
- Esiste **una stretta connessione e comunicazione con la rete** e con altri componenti energetici, come le batterie dei veicoli elettrici.
  - che aggiunge rischi legati ad abusi e interruzioni impreviste.

Sfide per la sicurezza e la privacy nelle CS

- Poiché i CS e i loro sistemi di controllo sono sistemi "cyber-fisici" per natura, possiamo esaminare le debolezze della sicurezza e della privacy da quattro prospettive principali:

Distribuzione

Natura cyber-fisica

Comunicazione

Il ruolo nuovi paradigmi

Sfide cyber-fisiche

- Sia i CS che i loro CC sono principalmente sistemi cyber-fisici che accettano l'incorporazione di molteplici tipi di componenti HW e SW nel contesto di ricarica.
- In questo , possiamo trovare:
  - **Dispositivi informatici "tradizionali"** che interagiscono con le CS
    - Dispositivi personali (PC, tablet, smartphone)
    - Apparecchiature server, compreso il supporto per la virtualizzazione
  - **Attrezzature industriali** integrate nei CS
    - Attrezzature operative (convertitori, connettori, ...)
    - Dispositivi o controllori di processo (PLC, RTU)
    - Dispositivi di campo (sensori, attuatori, contatori intelligenti)
  - **Dispositivi con capacità limitate** integrati anche nei CS
    - Dispositivi embedded ad es. Arduino, ...)
    - Piccoli computer (ad esempio, Raspberry Pi, ...)

E... quali sono le principali sfide per la sicurezza?

Sfide cyber-fisiche

- Sia i CS che i loro CC sono principalmente sistemi cyber-fisici che accettano l'incorporazione di molteplici tipi di componenti HW e SW nel contesto di ricarica.
- In questo , possiamo trovare:
  - **Dispositivi informatici "tradizionali"** che interagiscono con le CS
    - Dispositivi personali (PC, tablet, smartphone)
    - Apparecchiature server, compreso il supporto per la virtualizzazione
  - **Attrezzature industriali** integrate nei CS
    - Attrezzature operative (convertitori, connettori, ...)
    - Dispositivi o controllori di processo (PLC, RTU)
    - Dispositivi di campo (sensori, attuatori, contatori intelligenti)
  - **Dispositivi con capacità limitate** integrati anche nei CS
    - Dispositivi embedded ad es. Arduino, ...)
    - Piccoli computer (ad esempio, Raspberry Pi, ...)

- Connessioni e richieste multiple senza scartare le **vulnerabilità ereditate**
- I CS/CCS e le loro attrezzature industriali sono progettati per garantire la **sicurezza**
  - Probabilmente per garantire la stabilità dell'intero sistema - ricordiamo che i CS sono collegati ai DER, alla rete, ...)
- Raramente è progettata tenendo conto della **sicurezza.**
  - Non esiste un supporto nativo per i meccanismi di sicurezza
  - I dispositivi eseguono software e sistemi operativi obsoleti
- I CS/CCS possono ancora integrare i "***dispositivi legacy***".
  - Dispositivi con supporto solo per firmware e protocolli industriali tradizionali, ad esempio Modbus,
  - Nessuna interoperabilità diretta con i sistemi al di fuori del confine industriale
- Le CS/CCS sono **esposte a dispositivi (I)IoT**, alcuni dei quali con funzionalità HW/SW
  - E, quindi, con vincoli per supportare misure di sicurezza di base, come l'algoritmo crittografico !!! - <<10KB (RAM) e <<< 100KB (flash)

Sfide per la sicurezza e la privacy nelle CS

- Poiché i CS e i loro sistemi di controllo sono sistemi "cyber-fisici" per natura, possiamo esaminare le debolezze della sicurezza e della privacy da quattro prospettive principali:

Distribuzione

Natura cyber-fisica

Comunicazione

Il ruolo nuovi paradigmi

Sfide di comunicazione

- La maggior parte delle infrastrutture di ricarica si basa su diversi tipi di tecnologie di comunicazione che operano con diversi tipi di protocolli di comunicazione.
- In questo , possiamo trovare:
  - **Tecnologie di comunicazione tradizionali**
    - Con cavo (Ethernet) e senza fili (WiFi)
  - **Nuove tecnologie di comunicazione**
    - Esempio: NB-IoT, Sigfox, LoRa... (IoT cellulare)
  - **Protocolli orientati all'industria**
    - Esempio: OCPP, Modbus/TCP, OPC UA, …
  - **Protocolli orientati a Internet**
    - Livelli inferiori: IP, TCP
    - Livelli superiori: Quadri RESTful, MQTT, CoAP, …

E... quali sono le principali sfide per la sicurezza?

Sfide di comunicazione

- La maggior parte delle infrastrutture di ricarica si basa su diversi tipi di tecnologie di comunicazione che operano con diversi tipi di protocolli di comunicazione.
- In questo , possiamo trovare:
  - **Tecnologie di comunicazione tradizionali**
    - Con cavo (Ethernet) e senza fili (WiFi)
  - **Nuove tecnologie di comunicazione**
    - Esempio: NB-IoT, Sigfox, LoRa... (IoT cellulare)
  - **Protocolli orientati all'industria**
    - Esempio: OCPP, Modbus/TCP, OPC UA, …
  - **Protocolli orientati a Internet**
    - Livelli inferiori: IP, TCP
    - Livelli superiori: Quadri RESTful, MQTT, CoAP, …

- **Contesti** sempre più **complessi**, che non aiutano la propria manutenzione
  - Più tecnologie e più protocolli sono ciò che prepara una molotov.
- Comunicazioni esposte all'**intercettazione**, soprattutto se basate su comunicazioni wireless.
  - Le informazioni sul consumo devono essere trasferite al CCS per procedere con le attività di controllo e la fatturazione.
    - di grande interesse per gli aggressori ☹
  - Anche in questo caso, la maggior parte dei protocolli industriali è di tipo "legacy", quindi le misure preventive sono probabilmente elementari o inesistenti.
- **Interruzioni impreviste** dovute al consumo effettivo di dispositivi limitati
  - I protocolli di sicurezza tradizionali (ad esempio, TLS/DTLS, IPSec) su alcuni dispositivi possono penalizzare fortemente il ciclo di vita reale di un dispositivo limitato, ad esempio i contatori intelligenti.
  - Queste limitazioni aggiungono anche l'ulteriore difficoltà di incorporare altri meccanismi essenziali come sofisticati meccanismi di autenticazione e autorizzazione, registri, ecc.

Sfide di comunicazione

- Tuttavia, è anche importante notare che ci sono stati alcuni progressi nella sicurezza di alcuni protocolli, come OCPP v2.0.1 rispetto alle versioni precedenti.

Sicurezza	OCPP-v1.6	OCPP-v2.0.1
Crittografia	SSL/TLS non è raccomandato	Il TLS è preso in considerazione ma è **facoltativo**
Certificato	NON	SÌ
Registri	NON	SÌ
Supporto ISO 15118 (sicurezza EV)	NON	SÌ
Caricamento sicuro del firmware	Senza verifica	Con verifica (ma **facoltativo**)
Firme digitali	NON	Solo per i valori del contatore, **opzionale**
Trasferimento sicuro dei dati	HTTP / HTTPS; FTP / FTPS	HTTP / HTTPS; FTP / FTPS

Sfide per la sicurezza e la privacy nelle CS

- Poiché i CS e i loro sistemi di controllo sono sistemi "cyber-fisici" per natura, possiamo esaminare le debolezze della sicurezza e della privacy da quattro prospettive principali:

Distribuzione

Natura cyber-fisica

Comunicazione

Il ruolo dei nuovi paradigmi

Sfide IT-OT

- Praticamente tutti gli ecosistemi "intelligenti", comprese le smart cities e le smart grids, si basano oggi su molteplici tecnologie informatiche:
  - Garantire la sostenibilità, controllando il carico in base alla domanda effettiva.
  - Migliorare la qualità per i clienti semplificando il processo di fatturazione e facilitando il controllo del proprio ambiente e delle proprie risorse.
- In questo , possiamo trovare:
  - **New IoT** per prenotare CS e connettersi allo spazio di ricarica da qualsiasi luogo, in qualsiasi momento e in qualsiasi modo
  - **Intelligenza artificiale e Big Data** per calcolare grandi volumi di dati
  - **Cloud-edge computing** per l'elaborazione di dati e applicazioni
  - **Blockchain** per l'archiviazione di dati sensibili
  - **ecc.**

E... quali sono le principali sfide per la sicurezza?

Sfide IT-OT

- Praticamente tutti gli ecosistemi "intelligenti", comprese le smart cities e le smart grids, si basano oggi su molteplici tecnologie informatiche:
  - Garantire la sostenibilità, controllando il carico in base alla domanda effettiva.
  - Migliorare la qualità per i clienti semplificando il processo di fatturazione e facilitando il controllo del proprio ambiente e delle proprie risorse.
- In questo , possiamo trovare:

- **New IoT** per prenotare CS e connettersi allo spazio di ricarica da qualsiasi luogo, in qualsiasi momento e in qualsiasi modo
- **Intelligenza artificiale e Big Data** per calcolare grandi volumi di dati
- **Cloud-edge computing** per l'elaborazione di dati e applicazioni
- **Blockchain** per l'archiviazione di dati sensibili
- **ecc.**

- Quello che ci si aspetta è proprio quello che tutti pensano, ... una serie incontrollata di rischi e problemi di sicurezza dovuti al fatto che:

Il vaso di Pandora apre !

- Aumento della complessità
- Aumento del numero di vulnerabilità
  - Probabilmente di tipo zero-vulnerabilità
- Maggiore suscettibilità ad attacchi più intelligenti, sofisticati e persistenti
  - Aumento della gamma di minacce e della superficie di attacco
- Altro ...
- ...

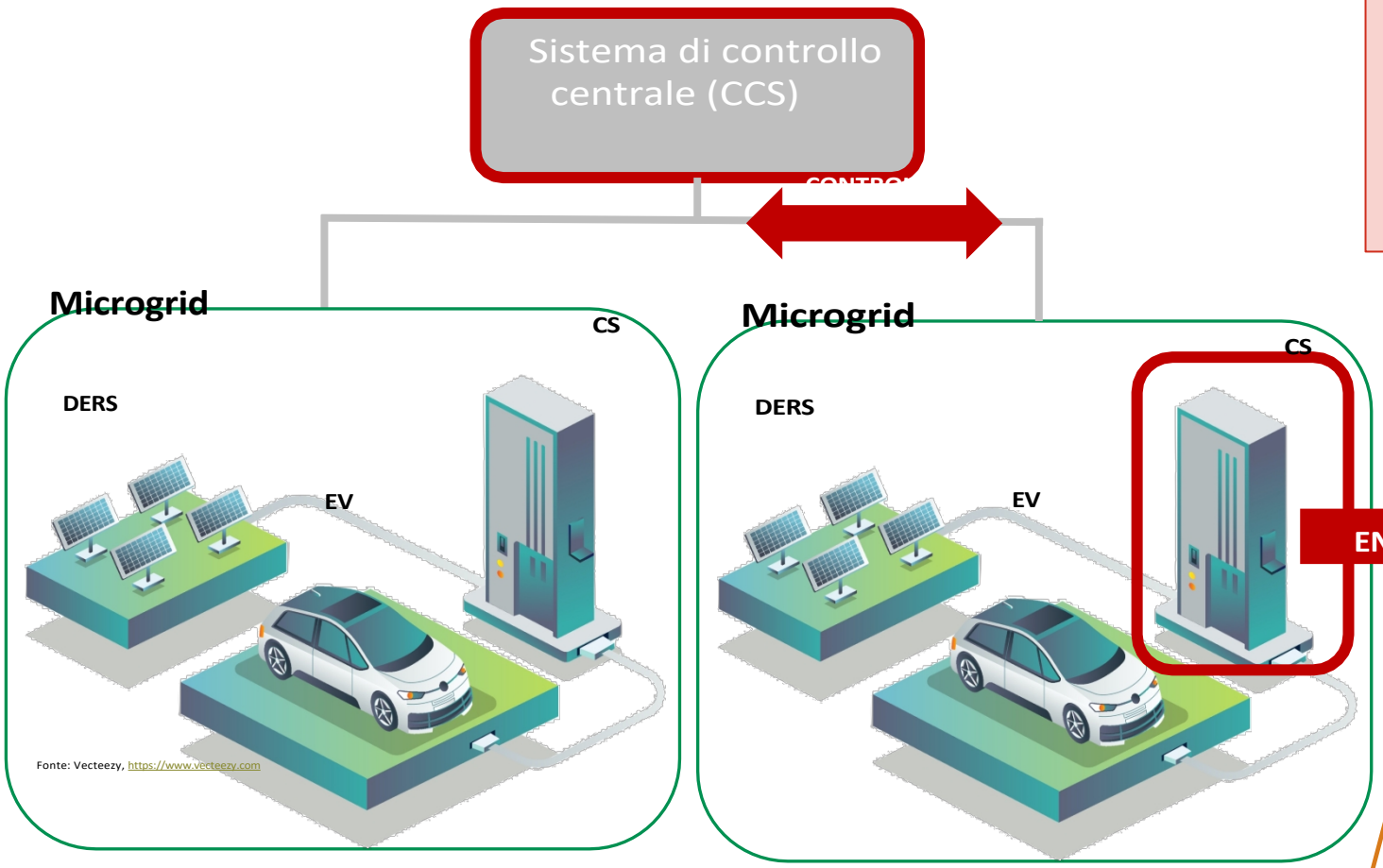
Riassumendo: c'è una crescente rischio di cybersecurity nelle stazioni di ricarica

- In effetti, si registra un notevole aumento dei rischi di cybersicurezza nelle stazioni di ricarica, come affermato anche da U. Dorot:

Aspetto	Dettagli
Interazioni	Comunicazione tra le applicazioni e con i servizi di pagamento di terze parti tramite API e plugin JavaScript
Dati gestiti	Elaborare le informazioni personali sensibili dei conducenti e i dettagli dei veicoli
Connessione all'infrastruttura	Collegati a sofisticati sistemi back-end per la gestione della distribuzione dell'elettricità alle stazioni di ricarica.
Vulnerabilità della sicurezza	Soggetto a varie minacce alla sicurezza informatica e preso di mira da entità malintenzionate.
Esposizione al rischio	Suscettibili di violazione dei dati, perdite finanziarie e rischi per la sicurezza.
Le sfide del mercato	Manca una sufficiente consapevolezza e misure normative per un'adeguata protezione
Minacce comuni	Vulnerabile all'acquisizione di account, allo spoofing della posizione e dell'identità, agli attacchi man-in-the-middle, alla catena di fornitura, all'uso improprio delle API, ecc.
Problemi di aggiornamento degli endpoint	Aggiornamenti rari, che portano a un software obsoleto e a vulnerabilità non affrontate.

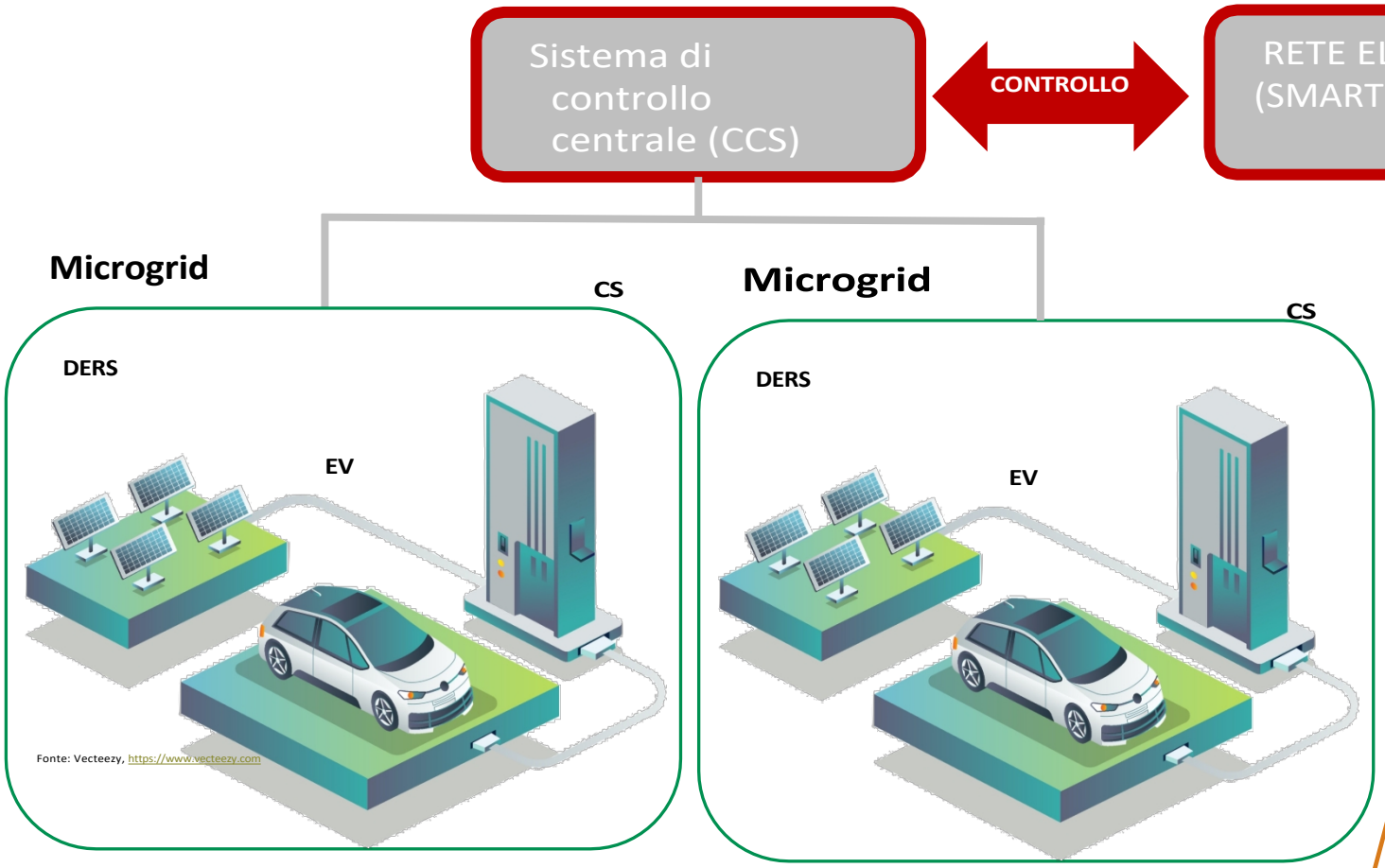
Fonte: Uri Dorot, "Le applicazioni delle stazioni di ricarica EV - un rischio crescente per la sicurezza informatica", Blog Radware, 2023 URL: https://www.radware.com/blog/application-protection/2023/05/ev_charging_station_cyber_threats/

Due obiettivi e molteplici conseguenze (I)



- **Il controllo e l'energia** sono due dei principali obiettivi degli aggressori per sabotare il sistema, le sue risorse principali e i clienti.
- **Gli effetti a cascata** possono verificarsi se le stazioni di ricarica sono gravemente compromesse

Due obiettivi e molteplici conseguenze (II)



- **Il controllo e l'energia** sono due dei principali obiettivi degli aggressori per sabotare il sistema, le sue risorse principali e i clienti.
- **Gli effetti a cascata** possono verificarsi se la rete elettrica viene colpita in modo grave.

Rischi comuni di sicurezza informatica per le applicazioni di ricarica dei veicoli elettrici

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

Minacce alla sicurezza informatica delle applicazioni di ricarica per veicoli elettrici: Rischi e implicazioni

Categoria di minaccia	Descrizione	Impatti potenziali
Malware e virus	Introdotto attraverso servizi di terze parti, attacchi bot o dispositivi compromessi all'interno dell'ecosistema di ricarica EV.	Accesso non autorizzato, furto di dati e danni alle applicazioni.
Mancanza di crittografia	Assenza di una trasmissione sicura dei dati tra le applicazioni e le stazioni di ricarica.	Dati intercettazione dei dati, compromissione della privacy degli utenti.
Abuso di API	Politiche di sicurezza inadeguate per i servizi API che portano a exploit.	Le API delle app possono lasciare la porta aperta a vari attacchi Bot, codice iniezioni di codice, e accesso non autorizzato.
Autenticazione insufficiente	Meccanismi deboli per la verifica degli utenti e il controllo degli accessi.	L'accesso non autorizzato, l'uso improprio, il furto di dati o il danneggiamento del sistema applicazione.
Rischi per la privacy	Protezione inadeguata delle informazioni sensibili dell'utente raccolte dalle applicazioni.	Privacy violazioni, furto di identità e frode finanziaria.
Rischi della catena di approvvigionamento	Reti complesse di componenti e fornitori non adeguatamente protette.	Vulnerabilità nelle applicazioni e nelle infrastrutture.

Applicazioni per stazioni di ricarica EV: un rischio crescente per la sicurezza informatica - Blog di Radware, accesso a marzo 2024

Analisi delle vulnerabilità

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

Studio di caso CSMS

- Sono state identificate diverse vulnerabilità, concentrandosi solo su 13 tipi di vulnerabilità significative in tutti i CSMS.
- Per condurre lo studio hanno valutato diversi prodotti CSMS.
- Hanno classificato ogni vulnerabilità con il corrispondente Common Weakness Enumeration (CWE) ID, fornendo un riferimento per ulteriori dettagli su ciascuna debolezza all'interno del database CWE.

Categoria	Fornitore/Sviluppatore	CSMS
Firmware	Schneider Electric	EVlink
	Eaton Corporation	xCaricaIn
	Etrel	CSWI Etrel
	Smartfox	Smartfox
	Keba	Keba
Mobile	Punto di ricarica	Punto di ricarica
	Stazioni elettriche Go	Vai
	Collegamento EV	Collegamento EV
Web	Accesso aperto alle fonti intermittenti sostenibili	Portale OASIS
	Cornerstone Technologies Limited	BaSE EVMS
	Ensto	Ensto CSI
	Fuzhou Comprehensive Energy Inf. Servizio	FCEIS
	Tecnologia energetica Bluesky	ICEMS
	Progetto Revolution Pi	PiControl
	Garo	Garo CSI
	Sistemi Unicorno	Lancillotto

Nasr, Tony, et al. "Power jacking your station: Analisi approfondita della sicurezza dei sistemi di gestione delle stazioni di ricarica dei veicoli elettrici". *Computers & Security* 112 (2022): 102511.

Vulnerabilità riscontrate nel CSMS studiato

		ID CWE/Vulnerabilità												
		79	89	200	306	321	352	425	798	799	918	942	942	1236
	CSMS	Cross Site Scripting (XSS)	Iniezione SQL (SQLi)	Divulgazione di informazioni	Autenticazione mancante	Segreti incorporati	Falsificazione di siti incrociati CSRF)	Navigazione forzata	Credenziali codificate in modo rigido	Limite di velocità mancante	Falsificazione delle richieste sul lato server (SSRF)	CORS Errata configurazione	FCDP Errata configurazione	Iniezione CSV (CSVi)
Firmware	EVlink	X		X			X	X	X	X	X			X
	xCaricaIn				X					X			X	
	CSWI Etrel	X			X				X		X		X	
	SmartFox								X	X				
	Keba				X							X		
Mobile	Punto di ricarica					X								
	Vai					X				X				
	Collegamento EV					X				X				
Web	Portale OASIS	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				
	Lancillotto									X		X		

Nasr, Tony, et al. "Power jacking your station: Analisi approfondita della sicurezza dei sistemi di gestione delle stazioni di ricarica dei veicoli elettrici". *Computers & Security* 112 (2022): 102511.

Tassonomia generica delle minacce alle infrastrutture di ricarica

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

Tassonomia delle minacce nelle infrastrutture di ricarica

- Pertanto, è chiaro che le CS e i relativi componenti possono essere soggetti a molteplici tipi di minacce.
- Ma:
  - **DOMANDA 1**: Quali?
  - RISPOSTA: "*Fondamentalmente, qualsiasi minaccia contro le CPS/IIoT*".
  - **DOMANDA 2**: Quali sono le principali risorse che possono essere colpite da queste minacce?
  - RISPOSTA: "quelle risorse incaricate di gestire i servizi primari nelle infrastrutture di ricarica quali: **controllo ed energia**",
    - Il controllo come servizio essenziale per garantire il potere
    - Il potere come elemento fisico essenziale per la società

CONTROLLO

POTENZA

Tassonomia delle minacce nelle infrastrutture di ricarica

- Pertanto, è chiaro che le CS e i relativi componenti possono essere soggetti a molteplici tipi di minacce.
- Ma:
  - **DOMANDA 1**: Quali?
  - RISPOSTA: "*Fondamentalmente, qualsiasi minaccia contro le CPS/IIoT*".
  - **DOMANDA 2**: Quali sono le principali risorse che possono essere colpite da queste minacce?
  - RISPOSTA: "quelle risorse incaricate di gestire i servizi primari nelle infrastrutture di ricarica quali: **controllo ed energia**",
    - Il controllo come servizio essenziale per garantire il potere
    - Il potere come elemento fisico essenziale per la società

CONTROLLO | POTENZA

Tassonomia delle minacce al controllo

- Per classificare le **minacce contro il controllo**, prenderemo in considerazione la categoria tipica basata sul modello ISO 7498-2:

Disponibilità (dati, risorse)	Integrità (dati, risorse)	Riservatezza (dati)

- ma anche l'analisi delle minacce eseguita 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

Minacce contro il controllo - CCS-CS

Il **CCS** è il sistema più attività interessata

	Impatto su			
	CCS	CS	EV	Rete elettrica
MitM	■	■	■	■
Abuso della modalità offline	■	■	■	■
Attacco on-path	■			
Rendere inutile	■	■	■	■
Reindirizzare il traffico	■			
APT	■	■	■	■
Attacchi Web/TCP-IP	■	■	■	■
DoS	■	■		■
Desincronizzazione	■	■		■
Attacco fisico / disturbo	■	■	■	■

Disponibilità

Integrità

Riservatezza

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

Minacce contro il controllo - CCS-CS

Il **CCS** è il sistema più attività interessata

	Impatto su			
	CCS	CS	EV	Rete elettrica
MitM	■	■	■	■
Impersonificazione	■	■	■	■
sovra/sotto tiro				■
Manomissione dei dati	■	■	■	■
Frode / furto di energia	■		■	■
Iniezione falsa	■	■	■	■
Attacchi on-path	■			
Reindirizzare il traffico	■			
APT	■	■	■	■
Attacchi Web/TCP-IP	■	■	■	■
Desincronizzazione	■	■		■
Sostituzione	■	■	■	■

Disponibilità

Integrità

Riservatezza

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

Minacce contro il controllo - CCS-CS

Il **CCS** è il sistema più attività interessata

	Impatto su			
	CCS	CS	EV	Rete elettrica
MitM	■	■	■	■
Reindirizzare il traffico	■			
APT	■	■	■	■
Canali secondari/di copertura	■			
Attacco di analisi passiva	■	■	■	
Esposizioni deliberate	■	■	■	■
Attacchi Web/TCP-IP	■	■	■	■

Disponibilità

Integrità

Riservatezza

Tassonomia delle minacce nelle infrastrutture di ricarica

- Pertanto, è chiaro che le CS e i relativi componenti possono essere soggetti a molteplici tipi di minacce.
- Ma:
  - **DOMANDA 1**: Quali?
  - RISPOSTA: "*Fondamentalmente, qualsiasi minaccia contro le CPS/IIoT*".
  - **DOMANDA 2**: Quali sono le principali risorse che possono essere colpite da queste minacce?
  - RISPOSTA: "quelle risorse incaricate di gestire i servizi primari nelle infrastrutture di ricarica quali: **controllo ed energia**",
    - Il controllo come servizio essenziale per garantire il potere
    - Il potere come elemento fisico essenziale per la società, e

CONTROLLO | **POTENZA**

Tassonomia delle minacce all'energia

- Se consideriamo la natura dei vincoli energetici e di "sicurezza", possiamo stabilire una corrispondenza con la classificazione precedente, ma questa volta considerando solo la disponibilità e l'integrità dei componenti e dei servizi, come esempio:

Interruzione dei servizi (disponibilità)	Sovraccarico (integrità, disponibilità)	Furto di energia (integrità)

- Per farlo, consideriamo anche il lavoro:
  - C. Alcaraz, J. Lopez, S. Wolthusen, "Il protocollo OCPP: Security Threats and Challenges", *IEEE Transactions on Smart Grid*, vol. 8, pp. 2452 - 2459, 2017, ISSN: 1949-3053

Minacce contro l'energia

Disponibilità

Integrità

Attacchi	CCS	CS	EV	Potenza griglia
MitM	■	■	■	■
Impersonificazione	■	■	■	■
Tiro eccessivo/scarso				■
Abuso della modalità offline	■	■	■	■
Manomissione dei dati	■	■	■	■
Iniezione falsa	■	■	■	■
Attacchi on-path	■			
Rendering a meno che	■	■	■	■
APT	■	■	■	■
Attacchi Web/TCP-IP	■	■	■	■
DoS	■	■		■
DoES				■
Desincronizzazione	■	■		■
Attacco fisico e disturbo	■	■	■	■
Sostituzione	■	■	■	■

La **rete elettrica** è l'asset più colpito

Minacce contro l'energia

Disponibilità

Integrità

	Impatto su			
Attacchi	CCS	CS	EV	Potenza griglia
MitM	■	■	■	■
Impersonificazione	■	■	■	■
Sovra/sovraccarico di tiro				■
Abuso della modalità offline	■	■	■	■
Manomissione dei dati	■	■	■	■
Frode / furto di energia			■	■
Iniezione falsa	■	■	■	■
APT	■	■	■	■
Attacchi Web/TCP-IP	■	■	■	■
Sostituzione	■	■	■	■

La **rete elettrica** è l'asset più colpito

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

Disponibilità

Integrità

Minacce contro l'energia

	Impatto su			
Attacchi	CCS	CS	EV	Potenza griglia
MitM	■	■	■	■
Impersonificazione	■	■	■	■
Abuso della modalità offline	■	■	■	■
Manomissione dei dati	■	■	■	■
Frode / furto di energia			■	■
Iniezione falsa	■	■	■	■
APT	■	■	■	■
Attacchi Web/TCP-IP	■	■	■	■
Sostituzione	■	■	■	■

e **reti elettriche e i veicoli elettrici** sono gli asset più colpiti

Per saperne più: Attacchi informatici specifici nelle CS

Esempi di attacchi informatici alle applicazioni di ricarica EV

Stazioni di ricarica EV non sicure: Le stazioni di ricarica EV sono vulnerabili all'hacking, consentendo il furto dei dati degli utenti o il danneggiamento dei veicoli. Gli hacker ottengono questo risultato alterando il firmware o collegando fisicamente un dispositivo alla stazione.

- **Conseguenze:** Una stazione di ricarica non autorizzata, una volta collegata, può sferrare altri attacchi.

Frodi di fatturazione: I malintenzionati sfruttano le vulnerabilità del processo di fatturazione delle app di ricarica EV a scopo di frode.

- **Conseguenze**: Si tratta dell'utilizzo di bot per creare false sessioni di ricarica o sovraccaricare gli utenti.

Attacchi alla catena di distribuzione: Gli hacker sfruttano le vulnerabilità nei servizi JS di terze parti integrati nell'app EV charing per eseguire attacchi di Formjacking e iniettare codice dannoso nel modulo di pagamento dell'app.

- **Conseguenze:** Gli aggressori possono rubare i dati delle carte di credito e i dati sensibili degli utenti, portando a potenziale perdita di dati.

Spoofing della posizione: Lo spoofing della posizione inganna l'app di ricarica EV facendo credere all'utente di trovarsi in un altro luogo.

- **Conseguenze:** Può aggirare la tariffazione basata sulla localizzazione o accedere a tariffe limitate. stazioni.

Attacchi Denial-of-Service (DoS): L'applicazione di ricarica EV viene sovraccaricata dal traffico di rete in un attacco DoS.

- **Conseguenze:** attacchi DoS rendono l'applicazione inutilizzabile e interrompono la tariffazione infrastruttura, e/o essere utilizzato per estorcere denaro al fornitore dell'applicazione.

Applicazioni per stazioni di ricarica EV: un rischio crescente per la sicurezza informatica - Blog di Radware, accesso a marzo 2024

Esempi di attacchi informatici alle applicazioni di ricarica EV

Attacchi di iniezione: Gli script dannosi vengono iniettati nei campi di input dell'utente o nelle API in un attacco di tipo injection.

- **Conseguenze**: Gli attacchi di iniezione manipolano i database e rubano i dati sensibili. Le applicazioni per la ricarica dei veicoli elettrici che si basano su database per i dati degli utenti sono vulnerabili.

Attacchi Cross-Site Scripting (XSS): Gli attacchi XSS iniettano script dannosi nelle pagine web delle app di ricarica EV, colpendo altri utenti.

- **Conseguenze:** Le app di ricarica per veicoli elettrici con campi di input non validati sono soggette ad attacchi XSS.

Attacchi Cross-Site Request Forgery (CSRF): Gli attacchi CSRF inducono gli utenti a eseguire inconsapevolmente azioni per gli aggressori, come l'invio di moduli o il trasferimento di fondi.

- **Conseguenze:** I VEICOLI ELETTRICI ricarica applicazioni utilizzando cookie o utenti sessione token per l'autenticazione sono vulnerabili agli attacchi e CSRF.

Attacchi di tipo Server-Side Request Forgery (SSRF): In un attacco SSRF, l'attaccante inganna il server dell'app di ricarica EV per accedere a una risorsa non autorizzata su un altro server.

- **Conseguenze**: Ciò consente all'aggressore di bypassare l'autenticazione e l'accesso. dati sensibili o controllare la stazione di ricarica.

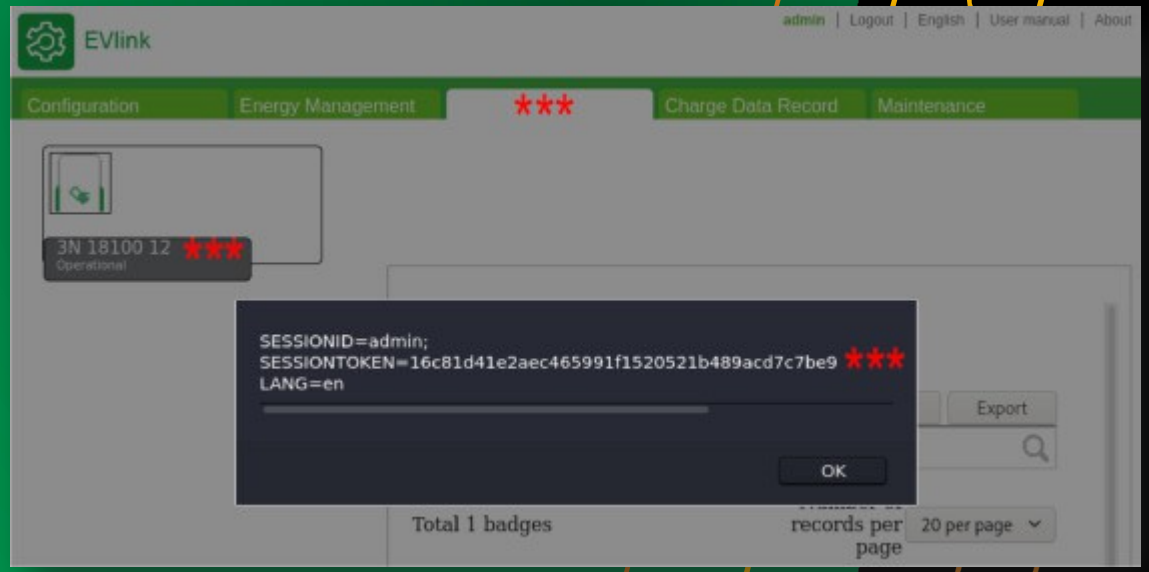
Applicazioni per stazioni di ricarica EV: un rischio crescente per la sicurezza informatica - Blog di Radware, accesso a marzo 2024

Attacchi contro la CS

- **Processo di carica e manipolazione delle impostazioni**
- Gli aggressori potrebbero manipolare i programmi e le operazioni di ricarica, ad esempio avviando, ritardando o interrompendo i processi di ricarica.
- La mancanza di sanitizzazione dell'input ha portato a vulnerabilità XSS, in particolare in EVlink.
- Maligno JavaScript malevolo era possibile a causa a causa di pulizia e codifica inadeguate dell'input dell'utente.
- Lo sfruttamento delle vulnerabilità XSS consentiva agli aggressori di dirottare le sessioni degli utenti e di ottenere il controllo del sistema.
  - Gli account privilegiati, come gli amministratori, erano particolarmente vulnerabili.
  - È stata scoperta una funzionalità di inizializzazione della configurazione all'interno di EVlink che era vulnerabile all'iniezione di valori separati da virgole (CSVi), che può essere sfruttata per incorporare un payload XSS che viene attivato e memorizzato nel database del sistema quando viene caricato il file CSV modificato.
  - Questa vulnerabilità porta a un XSS memorizzato, che consente l'escalation dei privilegi dirottando i token di sessione dell'amministratore.

Attacchi contro la CS

- **Processo di carica e manipolazione delle impostazioni**
- Gli aggressori potrebbero manipolare i programmi e le operazioni di ricarica, ad esempio avviando, ritardando o interrompendo i processi di ricarica.
- La mancanza di sanitizzazione dell'input ha portato a vulnerabilità XSS, in particolare in EVlink.
- Maligno JavaScript malevolo era possibile a causa a causa di pulizia e codifica inadeguate dell'input dell'utente.
- Lo sfruttamento delle vulnerabilità XSS consentiva agli aggressori di dirottare le sessioni degli utenti e di ottenere il controllo del sistema.
  - Gli account privilegiati, come gli amministratori, erano particolarmente vulnerabili.
  - È stata scoperta una funzionalità di inizializzazione della configurazione all'interno di EVlink che era vulnerabile all'iniezione di valori separati da virgole (CSVi), che può essere sfruttata per incorporare un payload XSS che viene attivato e memorizzato nel database del sistema quando viene caricato il file CSV modificato.
  - Questa vulnerabilità porta a un XSS memorizzato, che consente l'escalation dei privilegi dirottando i token di sessione dell'amministratore.



Attacchi contro la CS

- **Processo di carica e manipolazione delle impostazioni**
- Individuate vulnerabilità in diversi CSMS relative a debolezze CSRF.
- Gli aggressori sfruttano queste debolezze per manipolare le impostazioni del CS inducendo gli utenti a eseguire azioni non intenzionali.
- Gli aggressori ottengono il controllo degli account utente e accedono a tutti i dati e le funzionalità del CSMS, soprattutto se l'utente ha privilegi amministrativi.
- Ad esempio, una falla CSRF nel pannello di amministrazione di OASIS consente agli aggressori di attivare un XSS riflesso basato su POST sfruttando la mancanza di un token CSRF.
- Questo XSS può dirottare l'account dell'utente, come dimostrato da un modulo Proof-of-Concept modificato.
- I CSMS basati su PiControl presentano anche debolezze CSRF basate su POST, che consentono di modificare le impostazioni del pannello di controllo.
- Inoltre, una vulnerabilità CSRF basata su GET in EVlink consente agli aggressori di prendere il controllo degli account utente modificando il valore della password attraverso un parametro GET vulnerabile.

Nasr, Tony, et al. "Power jacking your station: Analisi approfondita della sicurezza dei sistemi di gestione delle stazioni di ricarica dei veicoli elettrici". *Computers & Security* 112 (2022): 102511.

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

Attacchi contro la CS

- **Negazione del servizio (DoS)**
- Gli aggressori possono ottenere il controllo del CSMS per bloccare il CS o disabilitare le funzioni, negando l'accesso legittimo.
- Necessita del controllo iniziale sul CSMS, eventualmente tramite XSS o CSRF, per eseguire attacchi DoS sul CS.
- Individuate falle CSRF in EVlink e OASIS, che consentono agli avversari di riavviare forzatamente i CS, causando interruzioni nei programmi di ricarica.
- La vulnerabilità CSRF in EVlink può causare il riavvio del CS ogni 30 secondi a causa dell'assenza di validazione randomizzata dei token.
- Gli aggressori possono inondare i CSMS di richieste, impedendo l'accesso legittimo, poiché molti CSMS non dispongono di meccanismi di limitazione della velocità.
- Alcuni CSMS non dispongono di meccanismi di limitazione della velocità (ad esempio, l'autenticazione), come xChargeIn, CSWI Etrel, Keba.
- Consente agli avversari di bloccare il CSMS e di condurre attacchi di dizionario sui moduli di accesso.
- Gli avversari possono forzare i percorsi web del CSMS per trovare endpoint e risorse nascoste.

Nasr, Tony, et al. "Power jacking your station: Analisi approfondita della sicurezza dei sistemi di gestione delle stazioni di ricarica dei veicoli elettrici". *Computers & Security* 112 (2022): 102511.

Attacchi contro la CS

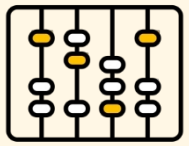
- **Negazione del servizio (DoS)**
- Gli aggressori possono ottenere il controllo del CSMS per bloccare il CS o disabilitare le funzioni, negando l'accesso legittimo.
- Ha bisogno di un controllo iniziale sul MS, eventualmente tramite XSS o CSRF, per eseguire attacchi DoS sul CS.
- Individuate falle CSRF in EVlink e OASIS, che consentono agli avversari di riavviare forzatamente i CS, causando interruzioni nei programmi di ricarica.
- La vulnerabilità CSRF in EVlink può causare il riavvio del CS ogni 30 secondi a causa dell'assenza di validazione randomizzata dei token.
- L'attaccante può inondare il CSMS di richieste, impedendo l'accesso legittimo, poiché diversi CSMS non dispongono di meccanismi di limitazione della velocità.
- Alcuni CSMS non dispongono di meccanismi di limitazione della velocità (ad esempio, l'autenticazione), come xChargeIn, CSWI Etrel, Keba.
- Consente agli avversari di bloccare il CSMS e di condurre attacchi di dizionario sui moduli di accesso.
- Gli avversari possono forzare i percorsi web del CSMS per trovare endpoint e risorse nascoste.

Nasr, Tony, et al. "Power jacking your station: Analisi approfondita della sicurezza dei sistemi di gestione delle stazioni di ricarica dei veicoli elettrici". *Computers & Security* 112 (2022): 102511.

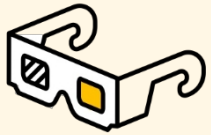
Attacchi contro la CS

Altri attacchi informatici

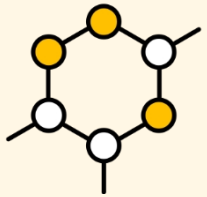
Manipolazione del firmware



Manipolazione della fatturazione



Reclutamento bot e proxy di rete



Nasr, Tony, et al. "Power jacking your station: Analisi approfondita della sicurezza dei sistemi di gestione delle stazioni di ricarica dei veicoli elettrici". *Computers & Security* 112 (2022): 102511.

Attacchi contro l'utente

- **Addebito Furto di dati/registrazioni**
  - CSRF e SQLi consentono agli aggressori di fingersi utenti reali e di accedere ai dati e alle risorse degli utenti.
  - Le risorse comprendono le registrazioni dei dati di ricarica e i dati di registro specifici del veicolo.
  - Questi dati possono rivelare i comportamenti degli utenti e le attività di ricarica.
  - Gli aggressori possono sfruttare queste informazioni per scopi malevoli (ad esempio, sorveglianza, spionaggio, furto di proprietà, ecc.)

Nasr, Tony, et al. "Power jacking your station: Analisi approfondita della sicurezza dei sistemi di gestione delle stazioni di ricarica dei veicoli elettrici". *Computers & Security* 112 (2022): 102511.

Attacchi contro l'utente

- **Addebito Furto di dati/registrazioni**
  - CSRF e SQLi consentono agli aggressori di fingersi utenti reali e di accedere ai dati e alle risorse degli utenti.
  - Le risorse comprendono le registrazioni dei dati di ricarica e i dati di registro specifici del veicolo.
  - Questi dati possono rivelare i comportamenti degli utenti e le attività di ricarica.
  - Gli aggressori possono sfruttare queste informazioni per scopi malevoli (ad esempio, sorveglianza, spionaggio, furto di proprietà, ecc.)

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

Nasr, Tony, et al. "Power jacking your station: Analisi approfondita della sicurezza dei sistemi di gestione delle stazioni di ricarica dei veicoli elettrici". *Computers & Security* 112 (2022): 102511.

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

Attacchi contro l'utente

- **Frodi di pagamento**
  - La maggior parte dei CSMS pubblici supporta i pagamenti online delle bollette.
  - Le vulnerabilità SQLi possono essere sfruttate per estrarre i record di pagamento dal database CSMS.
  - Gli aggressori possono rubare segretamente le informazioni di pagamento utilizzando tecniche come l'XSS memorizzato.
  - I dati finanziari rubati possono essere utilizzati per frodi di pagamento o venduti a terzi malintenzionati.
  - Diversi prodotti CSMS sono vulnerabili a questi attacchi tramite SQLi e stored XSS.

Nasr, Tony, et al. "Power jacking your station: Analisi approfondita della sicurezza dei sistemi di gestione delle stazioni di ricarica dei veicoli elettrici". *Computers & Security* 112 (2022): 102511.

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

Attacchi contro la rete elettrica

- **Aumento della domanda di ricarica.**
  - L'avversario utilizza il CS compromesso per lanciare sincronizzato operazioni di ricarica sincronizzate.
  - L'obiettivo è destabilizzare la rete con un aumento improvviso delle richieste di ricarica.

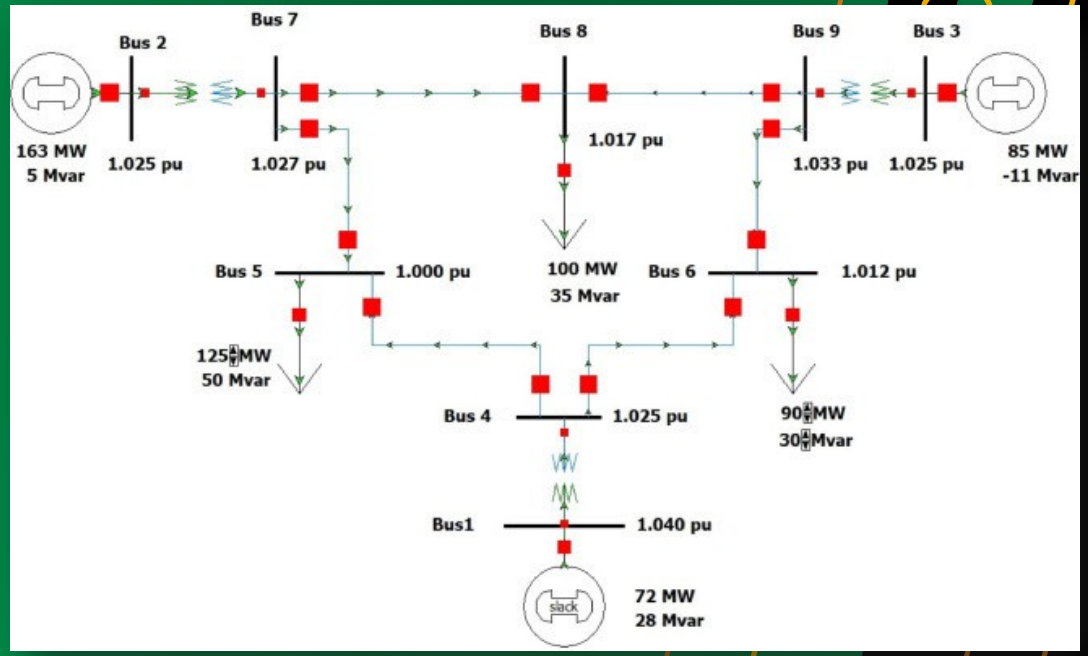
Nasr, Tony, et al. "Power jacking your station: Analisi approfondita della sicurezza dei sistemi di gestione delle stazioni di ricarica dei veicoli elettrici". *Computers & Security* 112 (2022): 102511.

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

Attacchi contro la rete elettrica

- **Aumento della domanda di ricarica.**
  - L'avversario utilizza il CS compromesso per lanciare sincronizzato operazioni di ricarica sincronizzate.
  - L'obiettivo è destabilizzare la rete con un aumento improvviso delle richieste di ricarica.

Western System Coordinating Council (WSCC) con 9 bus/linee e una domanda pari a 315MW



- Configurazione di benchmark per l'analisi della stabilità transitoria dei sistemi di potenza.
- Sistema di piccole dimensioni, comunemente utilizzato per questo .
- Gli autobus 5, 6 e 8 sono autobus di carico.
- I generatori dei bus 2 e 3 hanno un'inerzia, mentre il generatore del bus 1 ha una generazione variabile.
- I generatori 2 e 3 sono impostati sul modello di regolazione della velocità IEEE tipo 2 (IEEE-G2) per i test.
- L'avversario compromette CS (livelli 1, 2, e 3) sparsi per i bus 5, 6 e 8.

Nasr, Tony, et al. "Power jacking your station: Analisi approfondita della sicurezza dei sistemi di gestione delle stazioni di ricarica dei veicoli elettrici". *Computers & Security* 112 (2022): 102511.

Attacchi contro la rete elettrica

- **Aumento dell'offerta di scarico**
  - L'avversario mira a invertire il flusso di elettricità nella rete facendo scaricare energia a numerosi veicoli elettrici utilizzando un CS compromesso con capacità di flusso di energia bidirezionale.
  - Questa capacità è facilitata dalla tecnologia Vehicle-to-Grid (V2G), che consente il trasferimento dell'energia immagazzinata nelle batterie dei veicoli alla rete elettrica.
  - Sebbene il V2G sia progettato per assistere la rete durante i periodi di forte domanda, gli aggressori possono sfruttarlo per interrompere rete iniettando energia in eccesso.
  - L'obiettivo è quello di coordinare attività di scaricamento su larga scala per destabilizzare la rete elettrica, causando un'improvvisa impennata dell'offerta di elettricità e alterando l'equilibrio tra domanda e offerta di energia.

Nasr, Tony, et al. "Power jacking your station: Analisi approfondita della sicurezza dei sistemi di gestione delle stazioni di ricarica dei veicoli elettrici". *Computers & Security* 112 (2022): 102511.

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

Attacchi contro la rete elettrica

Attacco di commutazione.

- L'avversario combina le capacità di attacco precedenti per un attacco di commutazione.
- Mira a sincronizzare la ricarica e la scarica su larga scala tra CS e veicoli elettrici compromessi.
- Causando disturbi improvvisi e di frequenza di commutazione, che compromettono la stabilità della rete elettrica.
- Forzando la ricarica dei veicoli elettrici, l'aggressore riduce la frequenza del sistema, inducendo un aumento della generazione per riportarla a livelli normali.
- L'attaccante sfrutterà la risposta del sistema per eseguire l'attacco opposto (aumento dell'offerta costringendo i veicoli elettrici a scaricarsi), rimuovendo il carico aggiunto e iniettando invece energia nella rete, sfruttando la funzione Vehicle-to-Grid (V2G) del CS.
- In questo modo il sistema avrebbe una generazione superiore al carico, con un superamento della frequenza fino alla regione critica. Di conseguenza, il sistema cercherà di riprendersi riducendo la propria generazione, e l'aggressore risponderà aumentando il carico, causando un calo della frequenza, e così via. In questo modo, l'aggressore non consente al sistema di ripristinare la frequenza normale.

Nasr, Tony, et al. "Power jacking your station: Analisi approfondita della sicurezza dei sistemi di gestione delle stazioni di ricarica dei veicoli elettrici". *Computers & Security* 112 (2022): 102511.

Riferimenti e fonti

1. AIE, Veicoli elettrici, 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 e S. Wolthunsen, "Il protocollo OCPP: 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, "Le applicazioni delle stazioni di ricarica per veicoli elettrici - un rischio crescente per la sicurezza informatica", Radware Blog, 2023 URL: https://www.radware.com/blog/application- protection/2023/05/ev_charging_station_cyber_threats/
6. Cifre attribuite a Vecteezy, 2024 URL: https://www.vecteezy.com
7. DeepL Traduttore per la correzione di bozze.
   URL: https://www.deepl.com/translator

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

Connettersi con CyberSecPro: come registrarsi e altre informazioni pratiche

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

Grazie

Se avete domande, non esitate a contattarci:

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