Protezione delle stazioni di ricarica da minacce specifiche

CSP008_S_E

PRESENTAZIONE DA PARTE DI:
DR. ELIAS ATHANASOPOULOS UNIVERSITÀ DI CIPRO
DR. ABDELKADER SHAABAN
AIT ISTITUTO AUSTRIACO DI TECNOLOGIA

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 da minacce specifiche

Panoramica

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

AGENDA

1. Migliori pratiche

2. Contromisure

Migliori pratiche

Stazioni di ricarica

Si tratta essenzialmente di sistemi cyber-fisici con molti componenti.

I componenti hanno architetture diverse che interagiscono tra loro

- L'auto può funzionare con diversi microprocessori
- La stazione di ricarica può funzionare con software/hardware diversi I

componenti devono stabilire una comunicazione.

Misure di sicurezza a più livelli

Possiamo dividere una stazione di ricarica in diversi livelli

- Ad esempio, la parte di sistema dell'auto si trova su un livello diverso rispetto all'interfaccia che si collega alla stazione.

Possiamo quindi ipotizzare diversi **modelli di minaccia** per ogni livello

- Ogni modello di minaccia si rivolge a parti diverse del sistema cyber-fisico.
  sistema

Infine, per ogni modello di minaccia, si ricavano delle difese di sicurezza.

- Le difese di sicurezza non sono nuove, ma sono state adattate a questa configurazione.

Strati della stazione di ricarica

Sistema

Realizzato da codice di basso livello (C/C++) ed eseguito sul nucleo dei componenti

Applicazione

Realizzato su codice di alto livello (ad esempio, applicazione/servizio Web)

Comunicazione

Copre la comunicazione tra i sottosistemi

Livello di sistema

Il codice di sistema viene utilizzato per eseguire le operazioni di basso livello di un componente.

- Ad esempio, l'automobile è dotata di più microprocessori e di sistemi operativi.

Il codice di sistema è solitamente realizzato in linguaggi di programmazione non sicuri.
(C/C++)

La memoria è gestita dallo sviluppatore

Il problema principale del codice di sistema è la corruzione della memoria

Corruzione della memoria

Una vulnerabilità di corruzione della memoria si verifica quando uno sviluppatore gestisce la memoria in modo incauto

- Ad esempio, una copia in memoria inserisce nel buffer di destinazione una quantità di dati superiore a quella che può contenere e i dati in eccesso **corrompono la memoria**.
- La corruzione significa che la memoria verrà scritta con una nuova dati che di solito sono controllati dall'attaccante

Il codice di sistema, indipendentemente dall'applicazione, può soffrire di vulnerabilità di corruzione della memoria.

Corruzione della memoria nella stazione di ricarica

La corruzione della memoria viene sfruttata utilizzando input dannosi.

Nella stazione di ricarica sono presenti più aggressori che possono creare input dannosi.

- Se l'auto è vulnerabile, la stazione può attaccare l'auto.
- Se la stazione è vulnerabile, l'auto può attaccare la stazione.

In tutti i casi le difese esistenti sono simili

Difendere la corruzione della memoria

La difesa della corruzione della memoria è un problema aperto

Tuttavia, esistono tecniche di hardening che possono rendere più difficile lo sfruttamento.

L'hardening si basa su meccaniche di corruzione della memoria e di tentativi di disturbare parti di esso

L'hardening presuppone l'esistenza di una vulnerabilità e l'obiettivo di impedirne lo sfruttamento.

Difese esistenti

La maggior parte delle piattaforme, dei sistemi operativi e delle architetture supportano alcune difese standard.

- Pagine non eseguibili
- Canarini da pila
- Randomizzazione

Inoltre, ci sono alcune proposte di ricerca per la Tempra avanzata

- Alcune di esse (SafeStack, CFI) possono essere trovate come opzioni nei compilatori moderni (ad esempio, in clang)

Alcune architetture di CPU hanno difese programmate al livello h/w

- Intel incorpora gli shadow stack in alcune delle sue recenti CPU

Pagine non eseguibili

La corruzione della memoria può essere utilizzata per iniettare codice in un processo.

- Un utente malintenzionato può inserire del codice in un input dannoso e se il controllo i dati sono corrotti, allora il codice dell'aggressore può essere eseguito.

L'iniezione di codice si basa principalmente sull'esecuzione di dati (incorporati). in ingressi dannosi)

- Per contrastare l'iniezione di codice, le pagine di memoria possono essere eseguibili ma non scrivibili (pagine di codice) o scrivibili ma non eseguibili (stack, heap e altre pagine di dati).
- Purtroppo, gli aggressori possono utilizzare la programmazione orientata al ritorno (ROP) e il riutilizzo del codice.

Canarini da pila

La corruzione della memoria può essere facilmente utilizzata quando i buffer traboccano nello stack di un processo.

- Il modo più comune è quello di far traboccare un buffer e modificare il valore dell'indirizzo di ritorno

I canarini della pila sono valori casuali posizionati nella pila, tra i buffer e l'indirizzo di ritorno

- La modifica dell'indirizzo di ritorno attraverso un overflow lineare modificherà il valore del canary
- Il valore originale del canarino viene memorizzato in un registro h/w

I canarini di stack possono essere aggirati utilizzando le fughe di informazioni e le vulnerabilità nell'heap

Randomizzazione

Le iniezioni di codice possono essere evitate utilizzando pagine non eseguibili; tuttavia, lo sfruttamento è ancora possibile utilizzando la ROP.

- La ROP utilizza il codice esistente dellimmagine del processo che si assembla come una serie di gadget ROP.
- Il ROP si basa sulla conoscenza esatta del layout del codice
- Grazie alla randomizzazione dello spazio degli indirizzi, gli aggressori non sanno dove si trovano i gadget ROP.
- Le fughe di informazioni possono rendere inefficace la randomizzazione

Tempra avanzata

Sono state proposte diverse tecniche (ad esempio, CFI) per rendere più difficile lo sfruttamento della corruzione della memoria.

- L'integrità del flusso di controllo calcola staticamente il grafo del flusso di controllo di un programma e cerca di a tempo di esecuzione.
- Il CFG contiene tutti i trasferimenti di controllo legittimi di programma

CFI è presente in tutti i compilatori recenti come opzione

Corruzione della memoria - Sfide per le stazioni di ricarica

Le stazioni di Charing includono molti sistemi embedded

- È un sistema cyber-fisico che contiene molti "piccoli computer" (componenti).
- Di solito, i sistemi embedded eseguono codice di sistema realizzato in C/C++ e sono vulnerabili alla corruzione della memoria.

Le difese sono comuni nei sistemi più maturi

- Sistemi operativi completi
- Compilatori all'avanguardia
- CPU ricche di funzionalità ad esempio, Intel)

Livello applicazione

Il codice di sistema esegue il codice dell'applicazione, solitamente sviluppato in linguaggi di livello superiore.

Nella nostra impostazione, il Codice applicativo può essere un servizio Web

Le stazioni di ricarica possono offrire le loro funzionalità come servizio Web.

Attacco al codice web

Iniezioni di codice (XSS)

- Le applicazioni web possono soffrire di iniezioni di codice quando il codice viene mescolato ai dati.
- Per un'applicazione web, il codice è espresso in JavaScript che può essere inserito in una richiesta HTTP ed essere riflesso nel browser di un'altra vittima.

Falsificazione di richieste incrociate CSRF)

- I siti Web dannosi possono costringere un browser a eseguire richieste in altri siti Web in cui l'utente mantiene un account.

Difendere il Cross-Site Scripting (XSS)

Le iniezioni di codice possono essere mitigate filtrando il codice dai dati.

- Questo è un problema difficile

Un'altra soluzione consiste nel limitare i siti utilizzati per caricare il codice JavaScript.

- CSP proposto da Mozilla

Difesa contro le richieste di accesso incrociato (Cross-site Request Forgery)

Il CSRF può essere mitigato utilizzando token casuali CSRF.

- I moduli sensibili possono includere un token casuale che dovrebbe essere inviato con l'azione del modulo
- Il sito che ha bisogno di proteggere i propri utenti deve creare un maggior numero di stati per la generazione di codice lato server (ad esempio, abbinare token casuali all'invio di moduli).

Sono state proposte altre intestazioni (intestazione Origin)

Attacchi Web - Sfide per le stazioni di ricarica

Rispetto ai siti web tradizionali le stazioni di ricarica sono ambienti chiusi

- Possono incorporare applicazioni web, ma queste possono essere trattate in modo isolato rispetto al resto dell'ecosistema web.
- Considerate le applicazioni web a sito singolo

Contrastare XSS e CSRF potrebbe essere considerato più facile in questo contesto.

- Tuttavia, occorre attenzione (ad esempio, alle stazioni di ricarica dannose).

Livello di comunicazione

In una stazione di ricarica è prevista la comunicazione

La protezione delle comunicazioni dagli attacchi man-in-the-middle può essere ottenuta utilizzando la crittografia.

- Lo standard è TLS
- Oltre alla crittografia standard, TLS necessita di PKI

Sicurezza del livello di trasporto (TLS)

TLS è il protocollo di fatto per proteggere le comunicazioni utilizzando la crittografia.

- Offre protezione contro gli aggressori MitM passivi e attivi.

Basata sulla crittografia simmetrica, la crittografia asimmetrica
e funzioni di hash crittografico/MAC

Distribuito da molte applicazioni (web, e-mail, ecc.) Diversi attacchi

per TLS, ma è il migliore finora disponibile

Infrastruttura a chiave pubblica (PKI)

TLS, per la crittografia delle comunicazioni, necessita di un'infrastruttura PKI.

- Si tratta di un ecosistema per la creazione di un rapporto di fiducia tra soggetti remoti.

Nel corso di TLS due parti comunicanti devono stipulare una chiave simmetrica

- La creazione della chiave è realizzata con la crittografia a chiave pubblica.
- L'affidabilità di una chiave pubblica remota si ottiene attraverso i certificati

Ecosistema complesso, con molti problemi, soprattutto per la manutenzione

Comunicazioni: una sfida per le stazioni di ricarica

MitM la comunicazione con una stazione di ricarica è possibile

- Tuttavia, anche in questo caso il sistema può essere considerato *chiuso* rispetto all'intero Internet

D'altra parte, mantenere i certificati per tali sistemi chiusi
può essere considerato molto più difficile

Sintesi

Livello di sistema

Randomizzazione dei dati non eseguibili Hardening avanzato

Livello applicazione

CSP
Gettoni CSRF

Livello di comunicazione

TLS

Contromisure

Raccomandazioni prioritarie per le potenziali minacce in OCPP-v2.0.1

Panoramica delle mitigazioni raccomandate nell'ambito del CSMS analizzato.

Minacce	Mitigazione
DoS a CS	• TLSv1.3 sotto il profilo di sicurezza OPCC 3 o IPsec per evitare azioni MiTM • Funzioni di hash per verificare l'integrità dei componenti SW nelle CS • Firma digitale per ogni transazione OCPP o uso di funzioni di Message Authentication Message (MAC) • Aggiornamento periodico dell'elenco degli utenti autorizzati a cambiare energia nei CS • Meccanismi ridondanti (ad esempio, proxy, collegamenti di comunicazione) per prevenire gli attacchi on-path o l'autenticazione in modalità offline. • Manutenzione continua e certificazione dei componenti HW/SW • Meccanismi di reputazione per stimare i comportamenti anomali di utenti e dispositivi • Tracciabilità dei dati per individuare deviazioni occasionali o frequenti in una o più transazioni • Costruzioni di sorveglianza e antimanomissione • Sistemi di diagnostica, rilevamento e gestione dinamica degli eventi
Manipolazione dei CV OCPP	• TLSv1.3 con profilo di sicurezza OPCC 3 o IPSec per evitare azioni MitM • Crittografia dei dati sensibili (ad es. CV OCPP, ID) • Funzioni di hash per verificare l'integrità dei componenti SW e dei dati nei CS • Firma digitale per ogni transazione OCPP, o uso di funzioni MAC • Tracciabilità dei dati per individuare deviazioni occasionali o frequenti in una o più transazioni • Costruzioni di sorveglianza e antimanomissione

Alcaraz et al. "OCPP in the spotlight: threats and countermeasures for electric vehicle charging infrastructures 4.0". Rivista internazionale di sicurezza dell'informazione (2023) 22:1395-1421, maggio 2023.: link OCPP in the spotlight: threats and countermeasures for electric vehicle charging infrastructures 4.0 (springer.com)

Raccomandazioni prioritarie per potenziali minacce in OCPP-v2.0.1

Panoramica delle mitigazioni raccomandate nell'ambito del CSMS analizzato.

Minacce	Mitigazione
CS Spoofing	• Sistemi di diagnostica, rilevamento e gestione dinamica degli eventi • TLSv1.3 sotto il profilo di sicurezza OPCC 3 per evitare l'uso di CV di identificazione (Identity e BasicAuthPassword) e azioni di MitM, o IPSec • Gestione di ID univoci per ogni utente, dispositivo e transazione • Firma digitale per ogni transazione OCPP o utilizzo di funzioni MAC. • Sorveglianza e costruzioni antimanomissione • Sistemi di diagnostica, rilevamento e gestione dinamica degli eventi
Manipolazione delle DER e dei sistemi di accumulo	• Validare periodicamente i componenti di potenza per verificare la conformità ai quadri normativi e ai vincoli internazionali sui livelli di tensione e sulla frequenza operativa. • Manutenzione continua e certificazione dei componenti energetici • Tracciabilità dei dati per individuare deviazioni occasionali o frequenti nei componenti energetici e transazioni • Costruzioni di sorveglianza e antimanomissione • Diagnostica, rilevamento ed eventi dinamici • sistemi di gestione

Alcaraz et al. "OCPP in the spotlight: threats and countermeasures for electric vehicle charging infrastructures 4.0". Rivista internazionale di sicurezza dell'informazione (2023) 22:1395-1421, maggio 2023.: link OCPP in the spotlight: threats and countermeasures for electric vehicle charging infrastructures 4.0 (springer.com)

Raccomandazioni prioritarie per le potenziali minacce in OCPP-v2.0.1

Panoramica delle mitigazioni raccomandate nell'ambito del CSMS analizzato.

Minacce	Mitigazione
Spoofing di utenti, CSMS e EMS	• TLSv1.3 sotto il profilo di sicurezza 3 dell'OPCC per autenticare ogni parte (CSMS, EMS, CS) o IPSec • Gestione di ID univoci per ogni utente, dispositivo e transazione • Sensibilizzazione degli utenti finali sull'importanza di proteggere le loro credenziali e ID di sicurezza. • Sensibilizzazione degli operatori umani sull'importanza della tutela dell'ecosistema • Controllo dell'accesso al CS secondo i principi del minimo privilegio ed evitare l'escalation dei privilegi. • Firma digitale per ogni transazione OCPP, o utilizzo di funzioni MAC • Sistemi di diagnostica, rilevamento e gestione dinamica degli eventi
Informazioni divulgazione	• TLSv1.3 sotto il profilo di sicurezza OPCC 3 per autenticare ogni parte (CSMS, CS) o IPSec • Crittografia dei dati sensibili (ad es. CV OCPP, ID) • Principi di minimizzazione dei privilegi e segmentazione delle funzioni per evitare l'escalation di privilegio • Tecnologie e approcci a favore della privacy per il CSMS e l'EMS

Alcaraz et al. "OCPP in the spotlight: threats and countermeasures for electric vehicle charging infrastructures 4.0". Rivista internazionale di sicurezza dell'informazione (2023) 22:1395-1421, maggio 2023.: link OCPP in the spotlight: threats and countermeasures for electric vehicle charging infrastructures 4.0 (springer.com)

Raccomandazioni prioritarie per le potenziali minacce in OCPP-v2.0.1

Panoramica delle mitigazioni raccomandate nell'ambito del CSMS analizzato.

Minacce	Mitigazione
Autorizzazione e amministrazione degli utenti nel CSMS	• TLSv1.3 sotto il profilo di sicurezza OPCC 3 per autenticare ogni parte (CSMS, CS) o IPSec • Elenchi di autorizzazione locali validi composti da ID univoci associati a entità legittime e ricevuti da un CSMS valido. • Evitare il più possibile l'autenticazione in modalità offline e distribuire proxy che gestiscano il controllo degli accessi tramite il CSMS. • Principi di minimo privilegio e segmentazione delle funzioni per evitare l'escalation dei privilegi. • Firma digitale per ogni transazione OCPP o utilizzo di funzioni MAC. • Sistemi di diagnostica, rilevamento e gestione dinamica degli eventi

Alcaraz et al. "OCPP in the spotlight: threats and countermeasures for electric vehicle charging infrastructures 4.0". Rivista internazionale di sicurezza dell'informazione (2023) 22:1395-1421, maggio 2023.: link OCPP in the spotlight: threats and countermeasures for electric vehicle charging infrastructures 4.0 (springer.com)

Contromisure di mitigazione

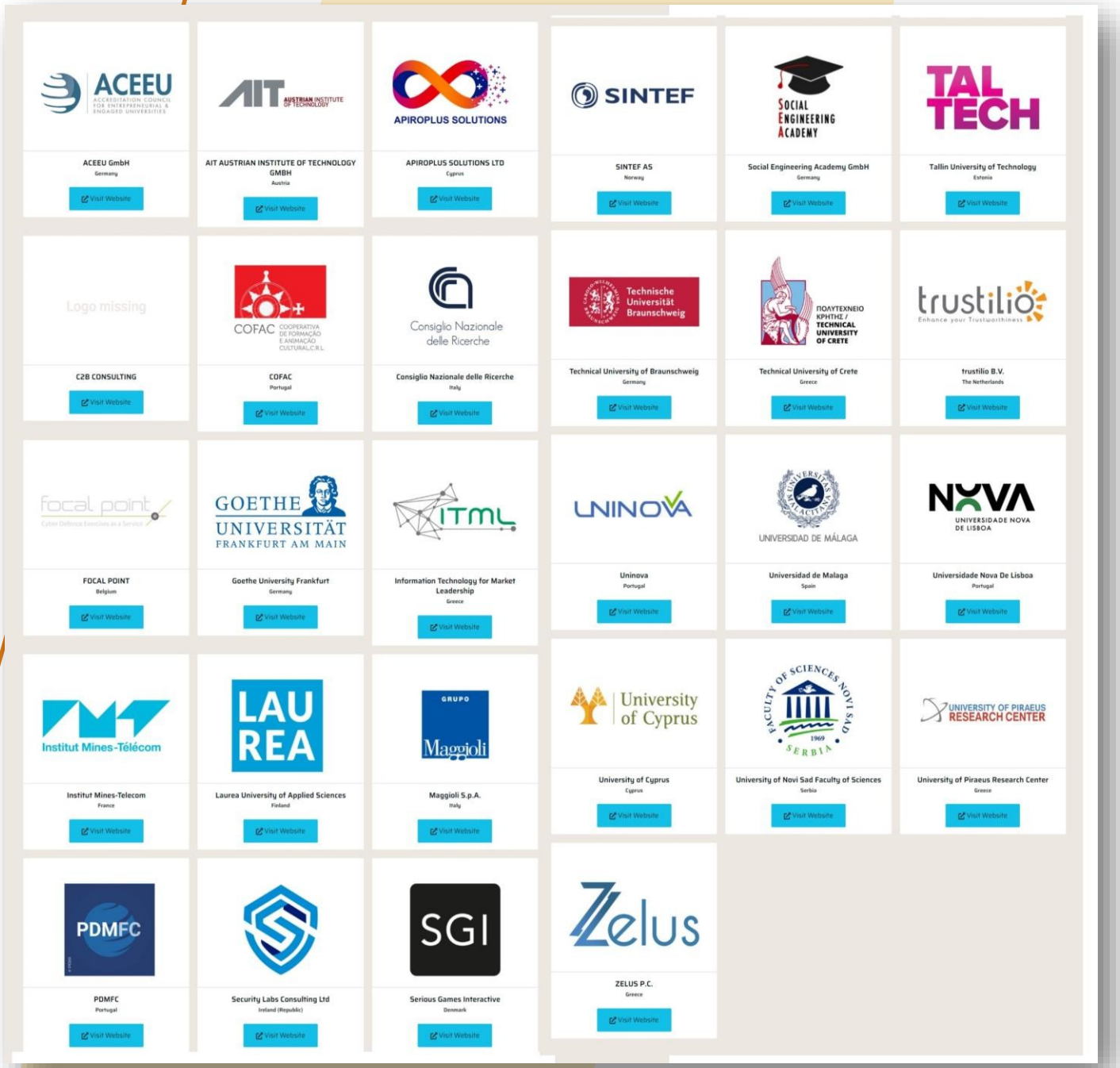
Panoramica delle mitigazioni raccomandate nell'ambito del CSMS analizzato.

ID CWE	Vulnerabilità	Mitigazione
79	XSS	Sanitizzare i dati di input controllabili dall'utente
89	SQLi	Utilizzare query parametrizzate
200	Divulgazione di informazioni	Applicare l'autenticazione a tutti gli endpoint
306	Autorizzazione mancante.	Applicare l'autenticazione a tutte le funzionalità
321	Segreti incorporati	Richiesta di chiavi crittografiche in fase di esecuzione
352	CSRF	Utilizzare token casuali per tutte le richieste
425	Navigazione forzata	Applicare migliori meccanismi di controllo degli accessi
798	Cred codificati in modo rigido	Applicare i criteri di aggiornamento delle credenziali
799	Limite di velocità mancante	Impedire richieste eccessive e veloci
918	SSRF	Sanificare gli indirizzi IP/URL sui parametri
942	Condivisione incrociata delle risorse (CORS) Configurazione errata	Applicare una politica più rigorosa per i domini incrociati
942	Errata configurazione di FCDP	Applicare una politica più rigorosa per i domini incrociati
1236	CSVi	Implementare l'analisi sicura dei file CSV

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.

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/



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

Grazie

Si prega di inviare tutte le domande a:
Dr. Elias Athanasopoulos athanasopoulos.elias@ucy.ac.cY

Dr. Abdelkader Shaaban,
abdelkader.Shaaban@ait.ac.at