Protecting Charging Stations Against Specific Threats

CSP008_S_E

PRESENTATION BY:

- CRISTINA ALCARAZ, UNIVERSITY OF MALAGA, SPAIN
- ABDELKADER SHAABAN, AIT, AUSTRIAN
- STEFAN SCHAUER, AIT, AUSTRIAN
- ELIAS ATHANASOPOULOS, UNIVERSITY OF CYPRUS, CYPRUS

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

01. Goals: Who-What-Why you need to take this training

02. Training logistics: When-Where-How

03. Learning outcomes

04. Training outlines

05. Exercises details

06. Practical information and requirements

07. Registration information and contacts

Goals: Who-What-Why you need to take this training

WHO

All those interested in learning about the cyber security of charging infrastructures, such as CISO, cybersecurity architect, researchers, and risk managers, among others

WHAT

Establishes the basis (though in an advanced level) for understanding the relevance of cybersecurity in a specific field of the energy sector

WHY

Equipping participants with the knowledge and skills necessary to make a strategy to protect critical systems, data and essential resources such as control and power

CSP Training Logistic: When-Where-How

WHEN

As the module is held several times, it is advisable to check the CyberSecPro DCM platform for updated information

4 hours in total
with a break
(appr. 30 min)

WHERE

Online, physical or both

All information on the connection mode will be published the DCM system

HOW

A seminar based on **synchronous classes** where each trainer will explain specific topics, and the end of the seminar various activities will be proposed, and an evaluation test will be carried out

Value Propositions

Benefits to Participants

- Exploration of a Specific, but very common, field of application within the Energy Sector
- Level of training module: Advance
- Cybersecurity professional training in the field of charging stations
- Hands-on and practical skills development
- Rooted with European cybersecurity skills frameworks
- Cutting-edge insights from industry-academic experts
- Helps with skills development and career advancement

WHO

Profile of Training Participants

- Managers and Leaders
- Energy sector employees (operators, engineers, administrators, etc.) and SMEs
- Cybersecurity architects and risks managers
- Cybersecurity researchers and educators
- Cybersecurity practitioners and enthusiasts

WHO

Profile of Trainer

- Cristina Alcaraz
  Associate Professor at University of Malaga
  PhD. in computer Science
- Abdelkader Shaaban
  Scientist Security & Communication Technologies
  Center for Digital Safety & Security
  PhD in Computer Science
- Stefan Schauer
  Thematic Coordinator
  Center for Digital Safety & Security
  PhD in Computer Science
- Elias Athanasopoulos
  Associate Professor at University of Cyprus
  PhD. in computer Science

WHAT

Training Topics

- Introduction to the Energy Charging Infrastructures
- Security Challenges in Energy Charing Stations
- Cascading of Energy and impact to other Critical Infrastructures
- Security Measures and Best Practices for Charging Stations

WHY

Learning Outcomes

- Understand the definition, scope, and importance of stations charging across the energy sector, and their impact to other critical infrastructures
- Grasp the unique security challenges and vulnerabilities specific to the charging stations
- Develop knowledge of cyber and physical threats, attack vectors, and potential consequences of security breaches in charging stations
- Understand the principles and methodologies to analyze cascading effects and evaluate security risks
- Gain knowledge of effective security measures, controls and best practices for protecting charging stations
- Stay informed about new threats and trends in the field of charging station security

WHY-2

Learning Outcomes

- Apply best practices for implementing physical and cyber security controls in charging infrastructures
- Identify and utilize specialised security tools and mechanisms
- Critical thinking and problem-solving in charging station security scenarios.
- Ability to analyse and interpret technical information and develop data-driven security solutions.
- Strong decision-making skills based on comprehensive understanding of risks and best practices

Trainers:

- Cristina Alcaraz
- Shaaban Abdelkader

Training Outline

Session-1 – appr. 1 hour

Topic-1: Introduction to the Energy Charging Infrastructures

Conceptualization of "charging infrastructures", their components and environment, as well as Stakeholders and interests

Overview of dependencies and impact

Topic-2: Security Challenges in Energy Charing Stations

Main security challenges in the context of charging stations

An overview of main threats in such a context

Specific attacks in charging stations – a further exploration of the issue

Trainer:

- Stefan Schauer

Training Outline

Session-2 – appr. 1 hour

Topic-3: Cascading of Energy and impact to other Critical Infrastructures

Introduce the dependences and interdependencies with respect to other critical infrastructures

Provide practical studies based on simulations and analysis of cascading effects

Trainer:

- Shaaban Abdelkader
- Elias Athanasopoulos

Training Outline

Session-3 – appr. 1 hour

Topic-4: Security Measures and Best Practices for Charging Stations

Introduce the dependences and interdependencies of the stations charging with respect to other critical infrastructures

Provide practical studies based on simulations and analysis of cascading effects

Topic-1: Introduction to the Energy Charging Infrastructures

We will cover these skills

- Introduction to the concept of "charging stations": This section will know the main systems conforming a charging infrastructure, as well as their main components, protocols and technologies
- Stakeholders and interests: This section will show the main stakeholders interested in using or managing the charging stations, either for consumption, management or maintenance purposes
- Relationships with other critical infrastructures: This section will show a simple overview of the direct relationship between charging stations and the main grid, with impact on other critical infrastructures

Topic-2: Security Challenges in Energy Charing Stations

We will cover these skills

- Main security challenges: This section will detail the main security challenges in many aspects related to the type of deployment, cyber-physical components and communications
- Security and privacy challenges in CSs: This section will address both the typical and specific attacks in charging stations, showing the susceptibility of the context to multiple attacks against control and power

Topic-3: Cascading of Energy and impact to other Critical Infrastructures

We will cover these skills

- Dependencies and interdependencies: This section will cover the study required to understand the cascading effect between critical infrastructures, such as healthcare and maritime sectors
- Cascading effect from a practical standpoint: This section will remark the relevance of preventing, and ultimately to mitigate, effects that may seriously impact other critical infrastructures

Topic-4: Security Measures and Best Practices for Charging Stations

We will cover these skills

- Best practices and recommendations: This section will cover a set of best practices and recommendations given by international organizations such as ENISA
- A more customized security countermeasures: This section will address specific measures both in terms of deployment, communication and components

Training Practical Exercises

Various activities will be offered throughout the entire module:

- **Analysis of case studies** focused on the energy sector – optional task
- **An evaluation test** – compulsory task

Evaluation method

Outline the evaluation elements and assessment process

Evaluation Element	How	Notes
Final report about a use case	Individual report submitted on time	Required analysis and discussion about a specific topic
Tests (REQUIRED)	Assessment test, which may integrate case studies where learners must show practical knowledge	In presence of the trainers (approx. 10-15 minutes)

Background Knowledge and Prerequisites

Background knowledge:

- Basic knowledge of cybersecurity fundamentals (related to CSP module 1)
- Basic understanding of computers and networking
- Experience with operating systems

Prerequisites:

- Basic knowledge of IT and cybersecurity essentials
- Experience with operating systems, network configurations and communication protocols

Technical Tools and Other Requirement

Technical Tools

- Computer with Internet access for connection
- Access to the DCM platform
- Office software for reports
- Technical Tools: None at the moment

Other Requirements

- **Willingness to learn and experiment**
- **Awareness of Internet security practices, and its caution**
- **Active Participation**

Resources: Books and Reference Materials

1. IEA, Electric Vehicles, https://www.iea.org
2. Global Market Insigths (GMI), "Europe Electric Vehicle Charging Station Market Size", 2022, 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. Nasr, Tony, et al. "Power jacking your station: In-depth security analysis of electric vehicle charging station management systems." Computers & Security 112 (2022): 102511
5. Open Charge Point Protocol (OCPP) Security Explained (wevo.energy), accessed in March 2024
6. EV Charging Station Applications – a Growing Cyber Security Risk – Radware Blog, accessed in March 2024
7. 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.
8. MITRE, MITRE ATT&CK, https://attack.mitre.org
9. Figures attributed to Vecteezy, https://www.vecteezy.com, 2024 – Thanks!

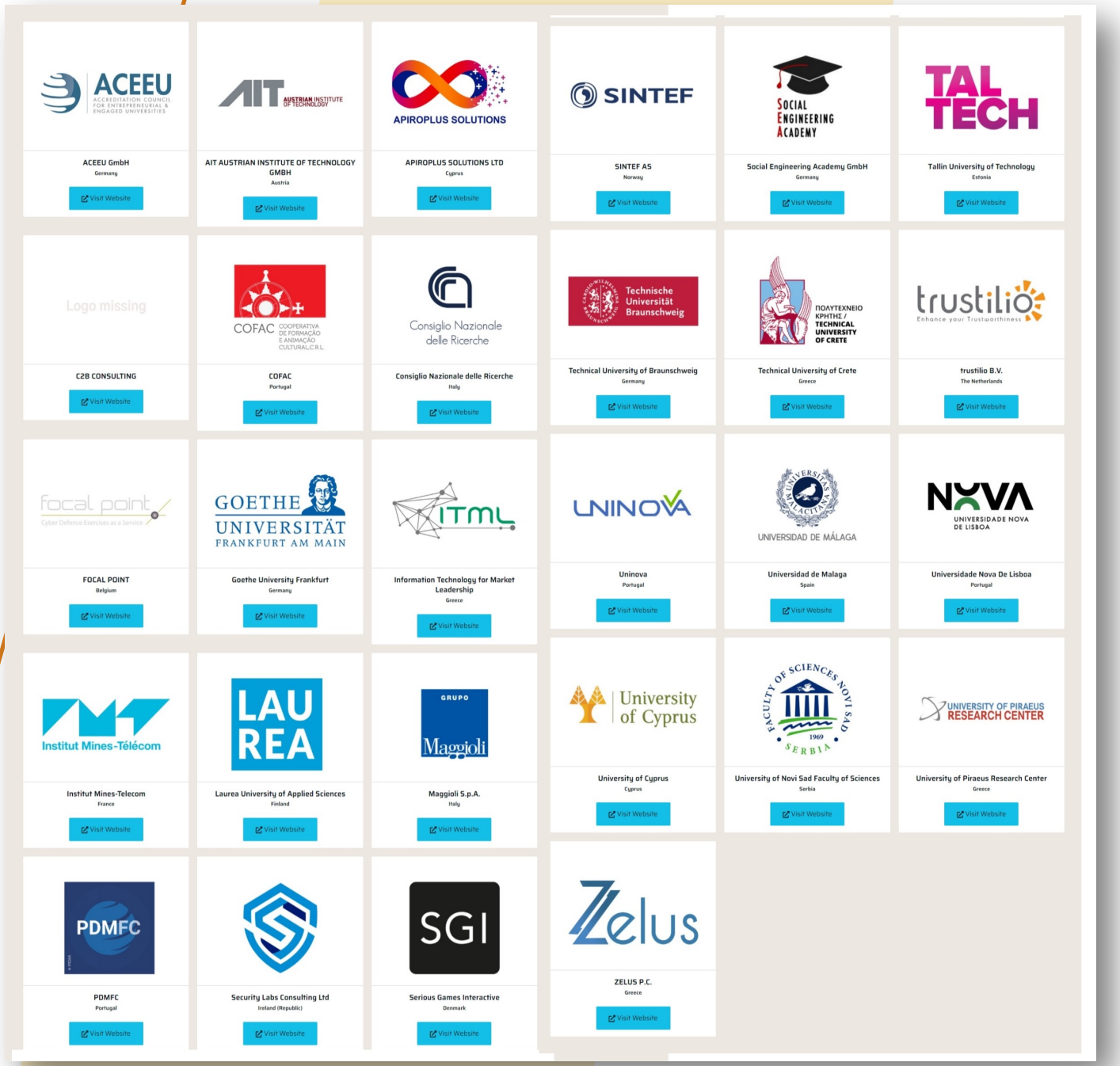
Registration: How to register and other practical information

The specific registration process for the Cybersecurity Essentials and Management training may vary depending on the training provider or institution

However, the general steps are detailed in the DCM platform

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
- Stefan Schauer
  stefan.schauer@ait.ac.at
- Elias Athanasopoulos
  athanasopoulos.elias@ucy.ac.cy

CyberSecPro