Network Protection for Energy Control Systems

CSP004_C_E

PRESENTATION BY:

- **CRISTINA ALCARAZ**
  UNIVERSITY OF MALAGA, SPAIN

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*

Topic-2: Common Security Weaknesses and Attacks in Energy Control Networks

Overview

- Weaknesses in the operational protocols and security deficiencies of TCP/IP communication protocols
- Offensive tools against confidentiality, integrity and availability
- Best practices, recommendations and guidelines
- Final remarks
- References and sources

CSP004_C_E – TOPIC 2:
Cristina Alcaraz, University of Malaga, Spain

Topic-2: Common Security Weaknesses and Attacks in Energy Control Networks

Overview

- Weaknesses in the operational protocols and security deficiencies of TCP/IP communication protocols
- Offensive tools against confidentiality, integrity and availability
- Best practices, recommendations and guidelines
- **Final remarks**
- References and sources

Final remarks

- Throughout this module, we have seen that **industrial** communication **protocols do not guarantee sufficient security measures** in terms of:
  - Availability, integrity, confidentiality and authentication/authorization
- This also means that industrial protocols depend on the **security protocols of the TCP/IP stack**
  - This stack is fundamental in energy control networks as it enables greater connectivity of elements and resources (e.g. CPS, IoT or IIoT devices)
- However, we have also seen that **the TCP/IP stack** itself **has a significant number of security breaches** and there are multiple offensive tools that may corrupt their performance
  - Therefore, the use of stack-specific security protocols becomes a primary requirement
  - These security protocols will be presented under the following topic
- Among the first protective actions, it is recommended to be aware of the existing **standards, recommendations and guidelines**, which can help to identify and deploy security measures in energy control networks
  - There are interactive tools that allow us to navigate between the different regulatory frameworks, facilitating their correct use

Topic-2: Common Security Weaknesses and Attacks in Energy Control Networks

Overview

- Weaknesses in the operational protocols and security deficiencies of TCP/IP communication protocols
- Offensive tools against confidentiality, integrity and availability
- Best practices, recommendations and guidelines
- Final remarks
- **References and sources**

CSP004_C_E – TOPIC 2:
Cristina Alcaraz, University of Malaga, Spain

References and sources

1. Some figures are attributed from Vecteezy,
   URL: https://www.vecteezy.com/ - thanks !
2. DeepL Translator for proofreading.
   URL: https://www.deepl.com/translator
3. CloudShark.org – modbus-bug0.pcapng
   URL: https://www.cloudshark.org/captures/4b8f9f3579b3
4. K. Yasar, M. E. Shacklett, A. Novotny, "TCP/IP", 2024
   URL: https://www.techtarget.com/searchnetworking/definition/TCP-IP
5. CloudShark, "http-get-request.pcapng", 2024
   https://www.cloudshark.org/captures/83390916ab62
6. CloudShark, "ftp.pcap", 2024
   URL:https://www.cloudshark.org/captures/abdc8742488f
7. CloudShark "telnet-client-server.pcapng", accessed in 2024
   URL: https://www.cloudshark.org/captures/818ceaef07b8?filter=telnet
8. NIST, "Defence-in-depth", Computer Security Resource Center, Glossary, 2024
   URL: https://csrc.nist.gov/glossary/term/defense_in_depth
9. NIST, "Cybersecurity Framework (CSF) 2.0 Reference Tool", 2024
   URL: https://csrc.nist.gov/Projects/Cybersecurity-Framework/Filters#/csf/filters
10. ENISA, "Minimum Security Measures for Operators of Essentials Services", 2024
    URL: https://www.enisa.europa.eu/topics/cybersecurity-policy/nis-directive-new/minimum-security-measures-for-operators-of-essentials-services

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:

- Cristina Alcaraz
  Associate Professor
  University of Malaga
  alcaraz@uma.es