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-3: Essential Protection for Energy Control Networks

Overview

- Overview of the main TCP/IP security protocols
- Endpoint protection, such as HMIs and servers
- Final remarks
- References and sources

Topic-3: Essential Protection for Energy Control Networks

Overview

- Overview of the main TCP/IP security protocols
- Endpoint protection, such as HMIs and servers
- **Final remarks**
- References and sources

Final remarks

- In this topic, we have seen how existing **TCP/IP security protocols can protect the communication channels** between two peers in the network
  - They are essential to safeguard a minimum of protection during the communications, in terms of confidentiality, integrity and authentication, such as TLS or IPSec
- **Preventive measures at endpoints** (the 'peers') must also be protected from penetrations or unauthorised accesses
  - For this purpose, the most recurrent measures such as isolation or segregation of nodes and network domains, but also inspection techniques at the level of ports and network services have been considered
  - Note that although we have explored two techniques in detail, there are many other security measures at the OS or network level (e.g. intrusion detection/prevention systems) that should be prioritised and reflected in regulatory frameworks (e.g. security policies)
  - In fact, detection and monitoring techniques are extensively developed in the following topic

Topic-3: Essential Protection for Energy Control Networks

Overview

- Overview of the main TCP/IP security protocols
- Endpoint protection, such as HMIs and servers
- Final remarks
- **References and sources**

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. NIST, NIST SP 800-113, 2008
   URL: https://csrc.nist.gov/pubs/sp/800/113/final
4. IETF, IP Security Protocol (IPSec), 2003-2004
   URL: https://datatracker.ietf.org/wg/ipsec/about/
5. IETF, IP Security (IPSec) and Internet Key Exchange (IKE) Document Roadmap,2011
   URL: https://datatracker.ietf.org/doc/html/rfc6071
6. QACafe, CloudShark, 2024
   URL: https://www.qacafe.com/analysis-tools/cloudshark/
7. Wireshark, 2024
   URL: https://www.wireshark.org
8. IETF, "Internet Security Association and Key Management Protocol (ISAKMP)", RFC 2408
   URL: https://datatracker.ietf.org/doc/html/rfc2408
9. CloudShark, "wireshark-capture-ipsec-ah-esp-transport.pcap", 2024.
   URL:https://www.cloudshark.org/captures/b7e2a9ad7a06
10. Ubuntu, UFW, Ubuntu documentation, 2024
    URL: https://help.ubuntu.com/community/UFW

References and sources

10. Archlinux, iptables, 2024
URL: https://wiki.archlinux.org/title/iptables
11. CloudShark, "IKE-1-MainMode-IKE-2-QuickMode.pcap", 2024.
URL: https://www.cloudshark.org/captures/d242b4ff850f
12. Source: William Stallings, Cryptography and Network Security: Principles and Practice, Fifth Edition
13. What is IPsec? | How IPsec VPNs work | Cloudflare
URL: https://www.cloudflare.com/en-gb/learning/network-layer/what-is-ipsec/
14. K. Brown, How to install and use telnet on Kali Linux, Linuxconfig.cong, 2021.
URL: https://linuxconfig.org/how-to-install-and-use-telnet-on-kali-linux
15. PhoenixNAP, How to Install FTP Server on Ubuntu with vsftpd, 2024.
URL: https://phoenixnap.com/kb/install-ftp-server-on-ubuntu-vsftpd
16. K. Scarfone and P. Hoffman, "Guidelines on Firewalls and Firewall Policy", NIST SP 800-41-rev1, NIST, Sept. 2009
17. Archlinux, nftables, 2024
URL: https://wiki.archlinux.org/title/nftables
18. NIST, "Cybersecurity Framework (CSF) 2.0 Reference Tool", 2024.
URL: https://csrc.nist.gov/Projects/Cybersecurity-Framework/Filters#/csf/filters
19. NIST, "Guidelines for Smart Grid Cybersecurity", NIST IR 7628 Rev. 1, 2024.
URL: https://csrc.nist.gov/pubs/ir/7628/r1/final
20. ENISA, "Appropriate security measures for smart grids. Guidelines to assess the sophistication of security measures implementation", 2012
URL: https://www.enisa.europa.eu/publications/appropriate-security-measures-for-smart-grids

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