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-1: Introduction to Energy Control Network Protection

Overview

- Introduction to the application scenario and the main security challenges in power control systems
- Taxonomy of threats and case studies
- Final remarks
- References and sources

Topic-1: Introduction to Energy Control Network Protection

Overview

- Introduction to the application scenario and the main security challenges in power control systems
- **Taxonomy of threats and case studies**
- Final remarks
- References and sources

Therefore, which threats may affect energy control systems?

With the new landscape of control networks and the adaptation of the new technologies to the operational environment

.... **EVERYTHING !!!**

Threats and taxonomy in "control networks"

- Control networks are mainly based on cyber-physical and IIoT devices, but also IT devices for interconnection such as routers, switches and proxies
  - Thus, the **targets** in control networks could be, for example:
    - SCADA master, servers
    - Controllers, sensors, actuators
    - Proxies
    - Routers
    - Switches
- In this module, we **classify the threats** following the general category provided by the ISO 7498-2 model – **AIC+A/A**
  - Availability (A)
  - Integrity (I)
  - Confidentiality (C)
  - Authentication / Authorization (A/A)

TAXONOMY OF THREATS

AVAILABILITY

INTEGRITY

CONFIDENTIALITY

AUTHENTICATION/ AUTHORIZATION

Threats and taxonomy in "control networks"

- Control networks are mainly based on cyber-physical and IIoT devices, but also IT devices for interconnection such as routers,

IMPORTANT:

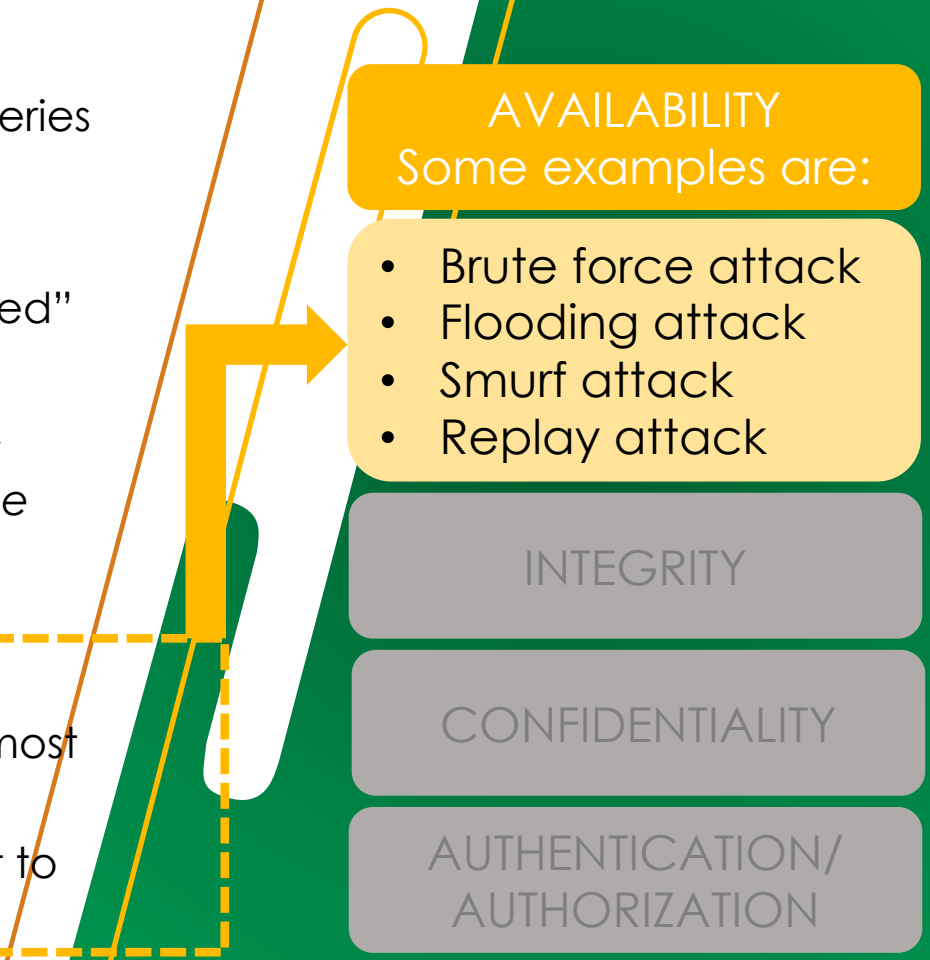
- IT IS NECESSARY TO PERFORM THE ATTACKS WITHIN THE NETWORK ESTABLISHED FOR THE PRACTICAL ACTIVITIES; I.E. WITHIN THE VIRTUAL MACHINES IN GNS 3.0 OR IN THE LOCAL/PERSONAL MACHINE
- IN OTHER WORDS, ANY ACTION MUST BE CARRIED OUT AGAINST THE VIRTUAL MACHINES FOR THE TRAINING AND WITHOUT LEAVING THE NETWORK OF THE "HOME LAN"
- YOU MUST TAKE THE UTMOST CAUTION IN THIS REGARD

  - Confidentiality
  - Authentication / Authorization

AUTHENTICATION/ AUTHORIZATION

Threats and taxonomy in "control networks" - AVAILABILITY

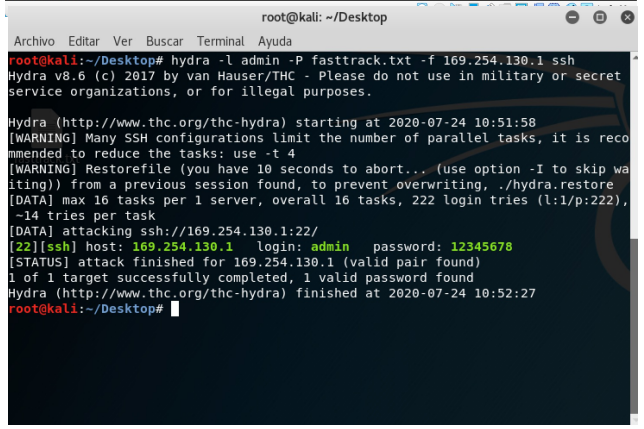
- **Exhaustion of limited HW/SW resources**
  - As commented previously, CPS/IIoT objects powered by batteries may be targeted by Denial of Service (DoS) attacks
- **Wireless channel integrity**
  - It is a type of DoS attack where the communication is "jammed"
- **Subtraction of Devices**
  - CPS/IIoT may be stolen due to their deployments - *isolated or unattended substations, which are generally configured in the critical physical objects or embedded into them such as generators, pylons or transformers*
- **(Distributed) Denial of Service Attacks (DDoS)**
  - External services may be rendered unavailable through the most common and traditional attacks (e.g. a botnet)
  - CPS/IIoT may be more difficult to reach, but it takes less effort to bring them down

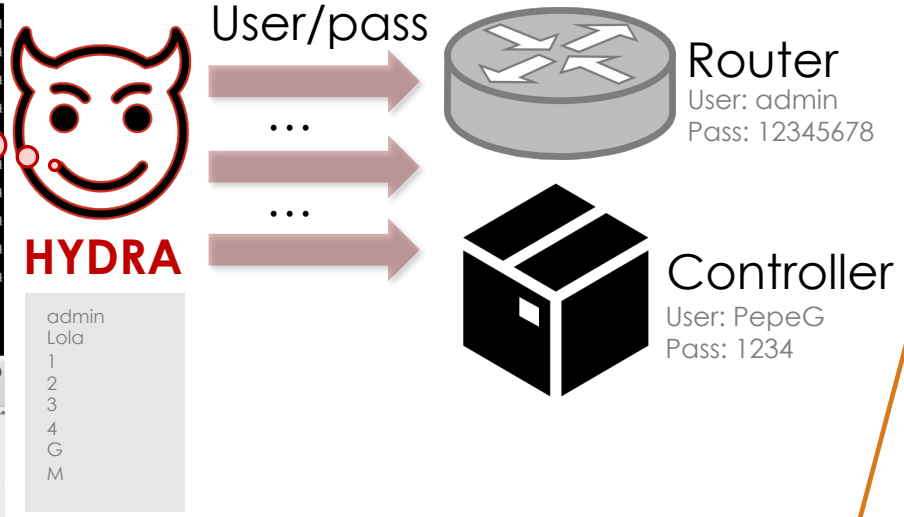


TAXONOMY OF THREATS

Threats and taxonomy in "control networks" - AVAILABILITY

- **Brute force attack / Dictionary attack**
  - CPS/IIoT/IT devices in networks, such as controllers or routers, require access via traditional credential (username-password) using default protection





With **HYDRA (Linux tool,** https://www.kali.org/tools/hydra/), attackers may create a file with possible combinations of credentials (dictionary) to attack

TAXONOMY OF THREATS

AVAILABILITY
Some examples are:

- **Brute force attack**
- Flooding attack
- Smurf attack
- Replay attack

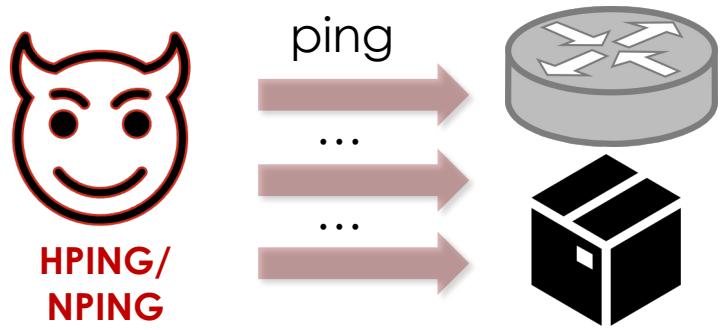
INTEGRITY

CONFIDENTIALITY

AUTHENTICATION/ AUTHORIZATION

Threats and taxonomy in "control networks" - AVAILABILITY

- **Flooding attack**
  - A flooding attack is the generation of spurious messages to increase network traffic, thus consuming server or network resources
  - Thus, the attack is designed to bring down a service or network by flooding it with large amounts of messages (traffic), so the threat is normally intended to deter peer-to-peer connections
  - Types of attacks:
    - **MAC flooding**
    - **TCP SYN flooding**
    - **UDP flooding**
    - **ICMP flooding**



  - With **HPING** (https://www.kali.org/tools/hping3/)**/NPING** (https://man7.org/linux/man-pages/man1/nping.1.html)
    - Linux tools, in which attackers may provoke different types of flooding attacks, such as ICMP/TCP floods

TAXONOMY OF THREATS

AVAILABILITY
Some examples are:

- Brute force attack
- **Flooding attack**
- Smurf attack
- Replay attack

INTEGRITY

CONFIDENTIALITY

AUTHENTICATION/
AUTHORIZATION

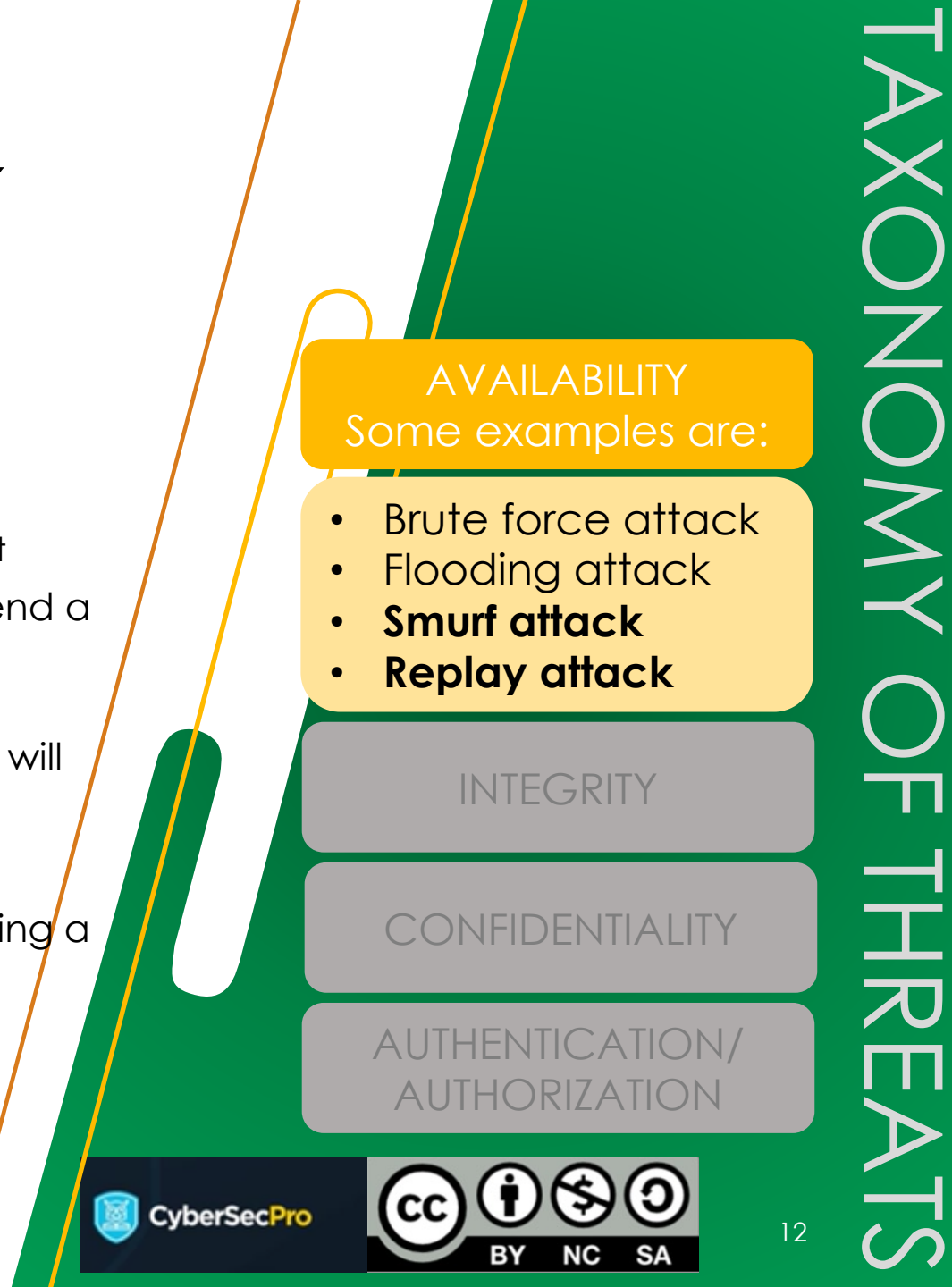
Homework: DoS Attack using HPING3

- **Objective**: to enhance your practical skills, it is crucial to engage in hands-on work. The aim of this exercise is to simulate real-world network interactions for providing a denial-of-service attack against a target machine
- **Guidelines**: Follow the steps below to set up a controlled, simulation-based lab environment using virtual machines (victims and an attacker). This setup will enable you to perform packet analysis on the target devices in a safe and isolated setting
  1. Use the GNS3 network simulator to create a topology with a node (victim machine) and a Kali Linux machine acting as the attacker
  2. Ensure you install these machines on your preferred virtual machine software and integrate them with the GNS3 server
  3. Ensure the installation of the hping3 tool on your Kali Linux
- **Task**:
  - Use hping3 to simulate a TCP SYN flood attack on port 80 of the target machine
  - Check whether the target machine is able to visit any websites
  - Extend your attack to include another target port
  - Make a comparison between the network bandwidth before and during the attack. You could use iPerf3 (also you are free to use any other tools) for this task
  - Report the results and show how the target machine was affected by the attack

OPTIONAL PRACTICAL TASKS

Threats and taxonomy in "control networks" - AVAILABILITY

- **Smurf attack**
  - This is a type of ICMP flooding (e.g. using hping3), in which an attacker
    1. Impersonates a legitimate node (e.g. by using the victim's IP)
    2. Causes a multicast or broadcast flood by sending an ICMP packet
  - Each system receiving the request (ICMP echo request) will send a response (echo reply) to the victim system rather than to the attacker
  - As a result, the victim system will be flooded and the attacker will deny service
- **Replay attack**
  - This attack aims to cause a drastic denial of service by replaying a previous message several times against a specific target
  - To do so, the attacker first needs to intercept the communication channels



Threats and taxonomy in "control networks" - INTEGRITY

- **Misconfiguration**
  - This type of attack can be accidental (human error) or planned
- **Hijacking (e.g. injection of malware)**
  - Not only due to vulnerabilities, but also due to aspects such as misconfiguration / human error, phishing, etc.
- **Alteration of the control network and its main resources**
  - Man-in-the-middle
  - Alteration of the firmware or the Operating System
  - Abuse of the insecure protocols such as telnet, FTP or HTTP
  - Code injection for malicious Command & Control (C&C) actions
  - …
- NOTE: In control networks, these threats depend on several factors: location of targets, type of authorisation and permissions, activity and movements (to derive stealth attacks or targeted attacks such as **Advanced Persistent Threats (APTs)**) ….

TAXONOMY OF THREATS

AVAILABILITY

INTEGRITY
Some examples are:

- False injection
- Code Injection
- APTs

CONFIDENTIALITY

AUTHENTICATION/
AUTHORIZATION

Threats and taxonomy in "control networks" - INTEGRITY

- **False injection**
  - Attackers may be able to inject spoofed packets into the control network, even impersonating the sender

  - **Scapy** (https://scapy.net) is a Linux tool that provides the capacities to modify or inject packets

TAXONOMY OF THREATS

AVAILABILITY

INTEGRITY
Some examples are:

- **False injection**
- Code Injection
- APTs

CONFIDENTIALITY

AUTHENTICATION/ AUTHORIZATION

Homework: Scapy Packet Injection

- **Objective**: to enhance your practical skills, it is crucial to engage in hands-on work. The aim of this exercise is to simulate real-world network interactions by injecting packets towards a victim machine
- **Guidelines**: follow the steps below to set up a controlled, simulation-based lab environment using virtual machines (victims and an attacker). This setup will enable you to perform packet injection using Scapy in a safe and isolated setting
  1. Use the GNS3 network simulator to create a topology with one node (victim machine) and a Kali Linux machine acting as the attacker.
  2. Ensure you install these machines on your preferred virtual machine software and integrate them with the GNS3 server.
  3. Ensure the installation of the Scapy tool on your Kali Linux machine. Also, install Wireshark on your victim machine.
- **Task**:
  - Use Scapy to create and send a packet to the target machine
  - Catch the transmitted packet using the Wireshark tool
  - Extend your attack to send many packets at the same time to perform a DoS attack
  - Make a comparison between the network bandwidth before and during the attack. You could use iPerf3, although you can use any other tools for this task
  - Report the results and show how the target machine was affected by the attack

OPTIONAL PRACTICAL TASKS

Threats and taxonomy in "control networks" - INTEGRITY

- **Code injection**
  - Code injection attacks involve injecting malicious code into vulnerable systems to alter their behavior
  - This type of malicious code is also known as "malware", and may be inserted via other attacks such as **social engineering** or **supply chain attacks**
- **Malware**
  - Malware is malicious software created to harm computers, networks, or servers
  - It includes subsets like ransomware, trojans, spyware, viruses, worms, keyloggers, bots, and cryptojacking
- **Supply chain attack**
  - This attack targets trusted third-party vendors in the supply chain by injecting malicious code into software or compromising hardware components to infect users
  - Software supply chains are vulnerable due to their reliance on various off-the-shelf components like third-party APIs, open-source code, and proprietary software from vendors

TAXONOMY OF THREATS

AVAILABILITY

INTEGRITY
Some examples are:

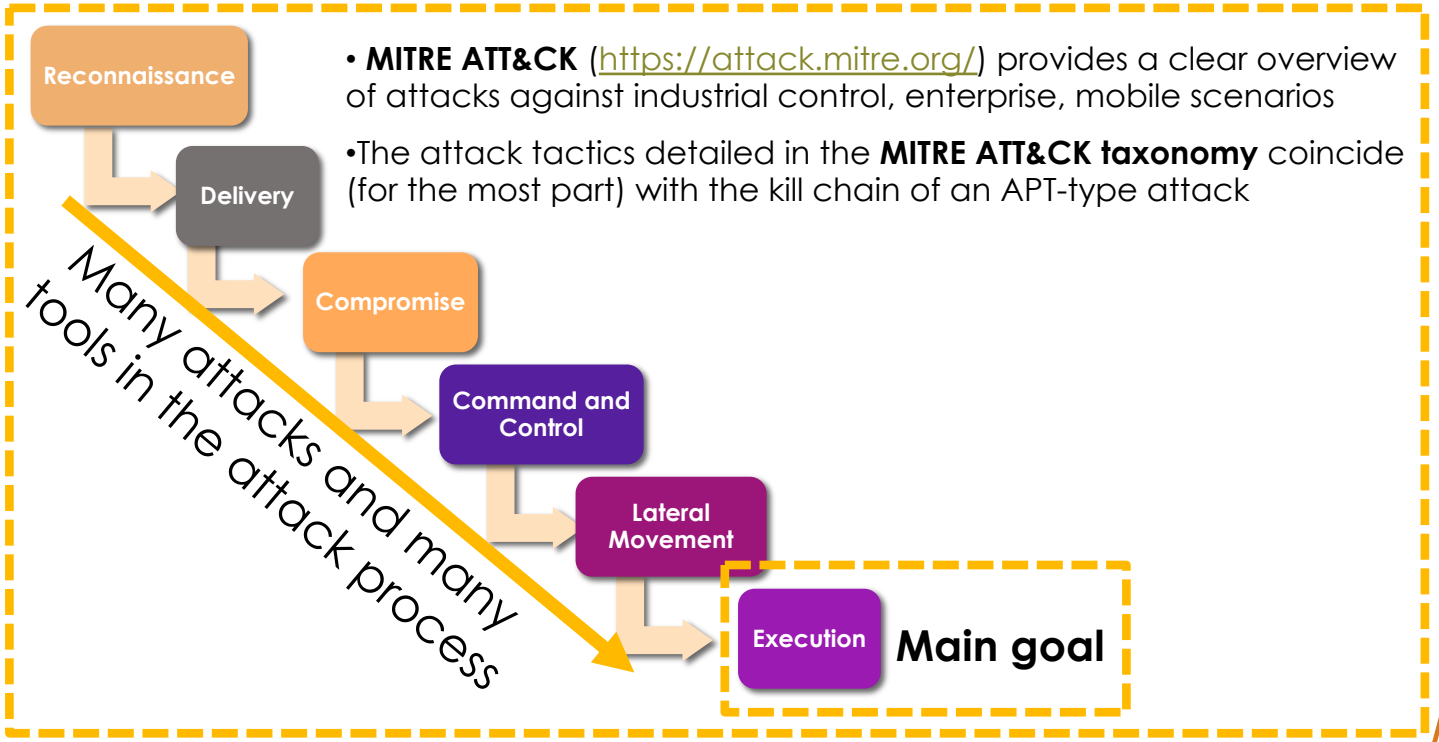
- **False injection**
- Code Injection
- APTs

CONFIDENTIALITY

AUTHENTICATION/
AUTHORIZATION

Threats and taxonomy in "control networks" - INTEGRITY

- **APTs in networks**
  - Beyond data exfiltration (as part of confidentiality), another main stage of APTs is the **destruction of critical resources** such as generators by taking control of controllers



TAXONOMY OF THREATS

AVAILABILITY

INTEGRITY
Some examples are:

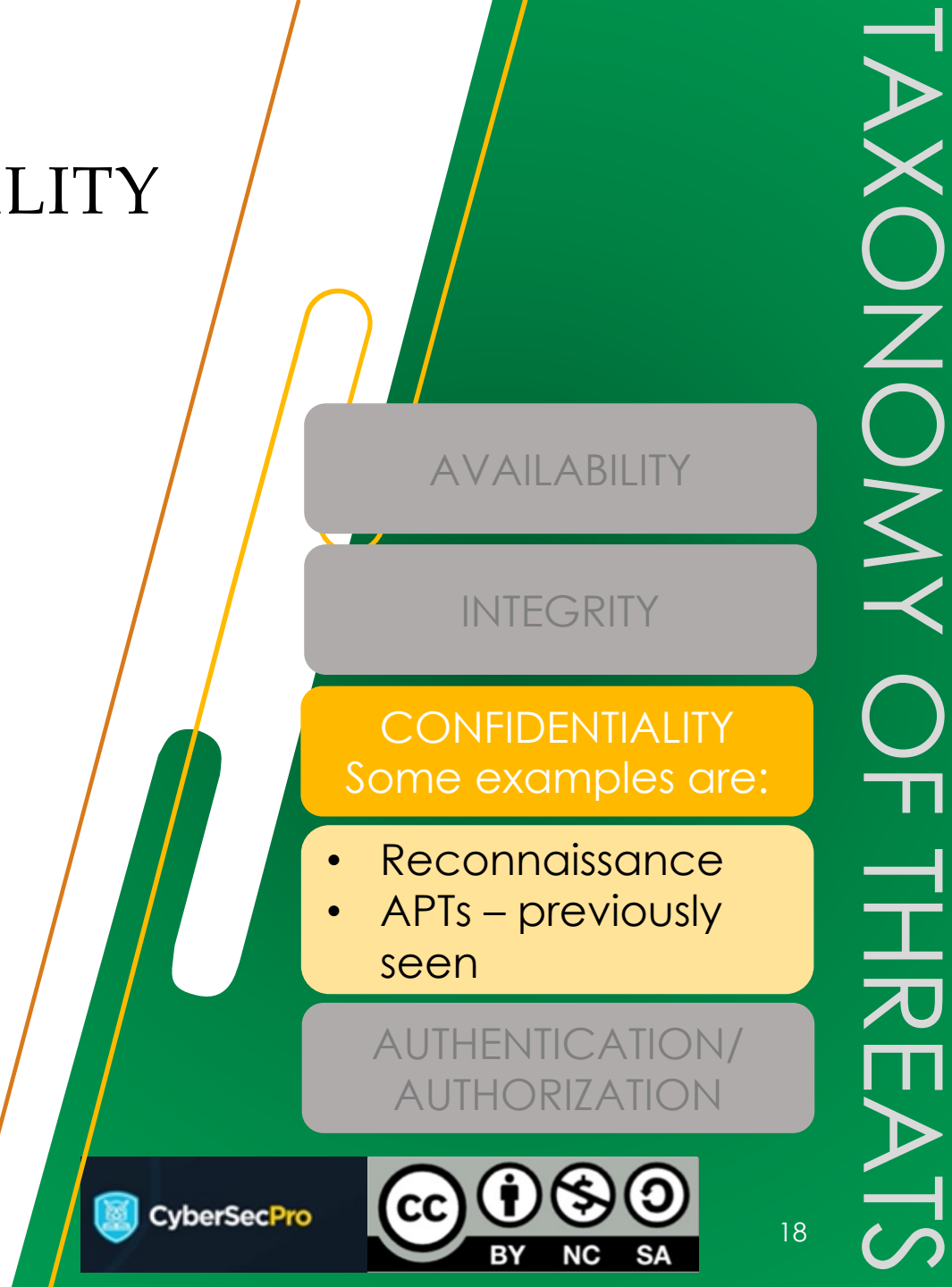
- False injection
- Code Injection
- **APTs**

CONFIDENTIALITY

AUTHENTICATION/ AUTHORIZATION

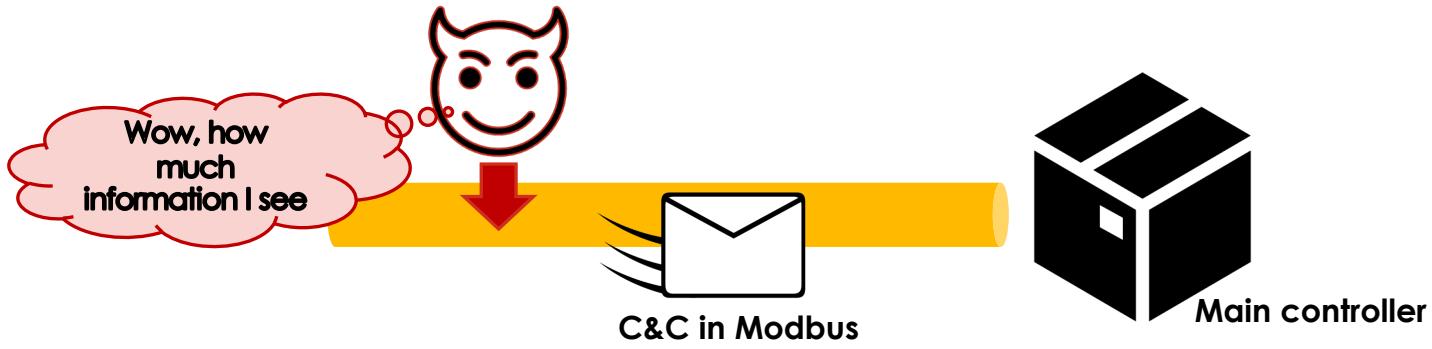
Threats and taxonomy in "control networks" - CONFIDENTIALITY

- **Data eavesdropping**
  - It is normally lead by a Man-in-the-Middle
- **Data exfiltration**
  - May be performed in multiple ways:
    - **Network traffic analysis / network reconnaissance**
    - **Device analysis**
    - …
  - May provoke data leakage to competitors:
    - Infrastructure information
    - Operational information
    - Process information
    - Security information
    - Human information
    - …



Threats and taxonomy in "control networks" - CONFIDENTIALITY

- **Network reconnaissance**
  - As discussed, an attacker may need to first explore the application context (the scenario) before its final exploitation
  - To do so, the attacker might need to perform various attacks related to social engineering (e.g. phishing) or passive observation of the network using:
    - **Wireshark**, https://www.wireshark.org
    - **Nmap/Zenmap**, https://nmap.org/zenmap/
    - **Etherape**, https://juncotic.com/etherape-monitoreando-el-trafico-de-red/
    - **LEGION**, https://www.kali.org/tools/legion/



TAXONOMY OF THREATS

AVAILABILITY

INTEGRITY

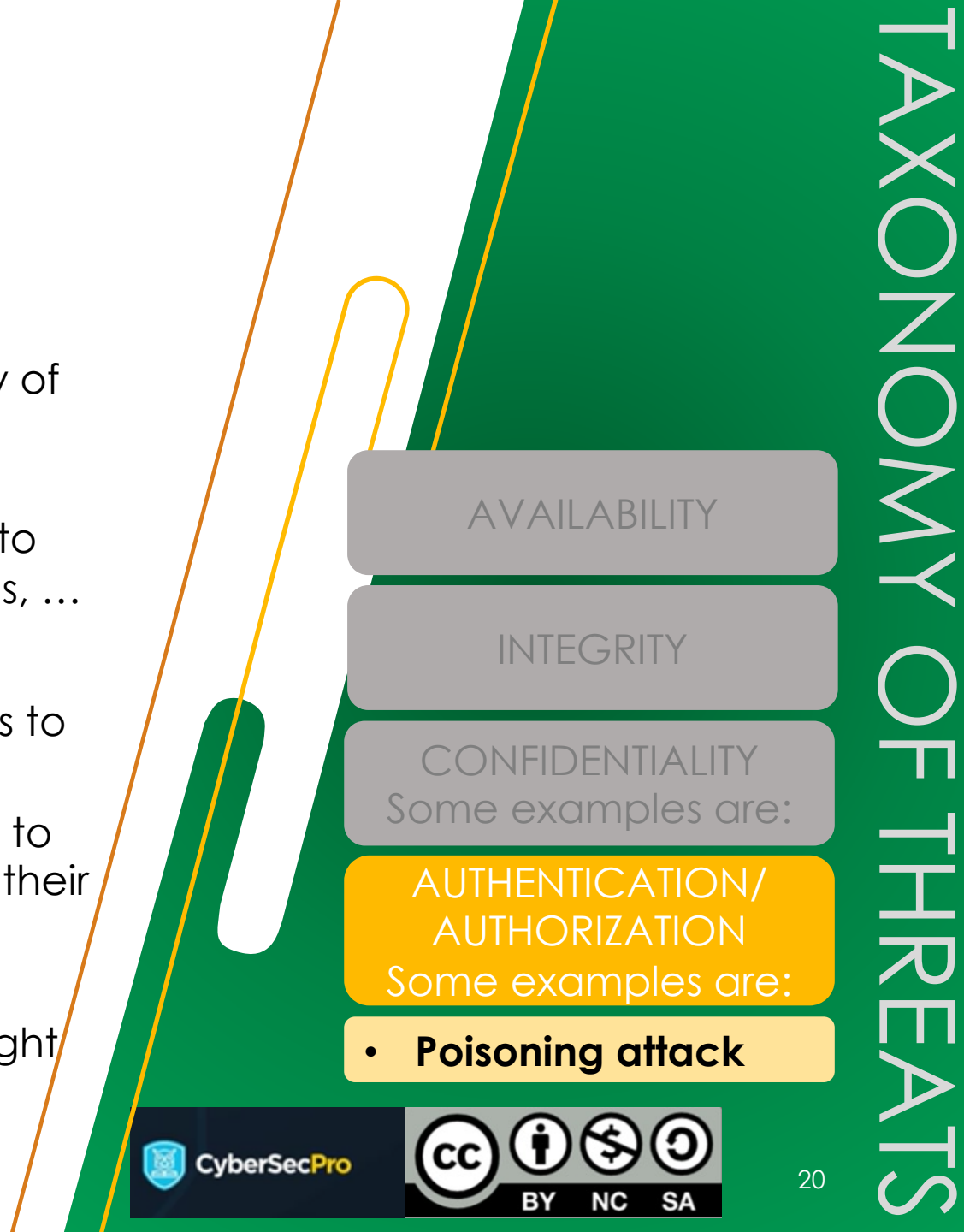
CONFIDENTIALITY
Some examples are:

- **Reconnaissance**
- APTs – previously seen

AUTHENTICATION/ AUTHORIZATION

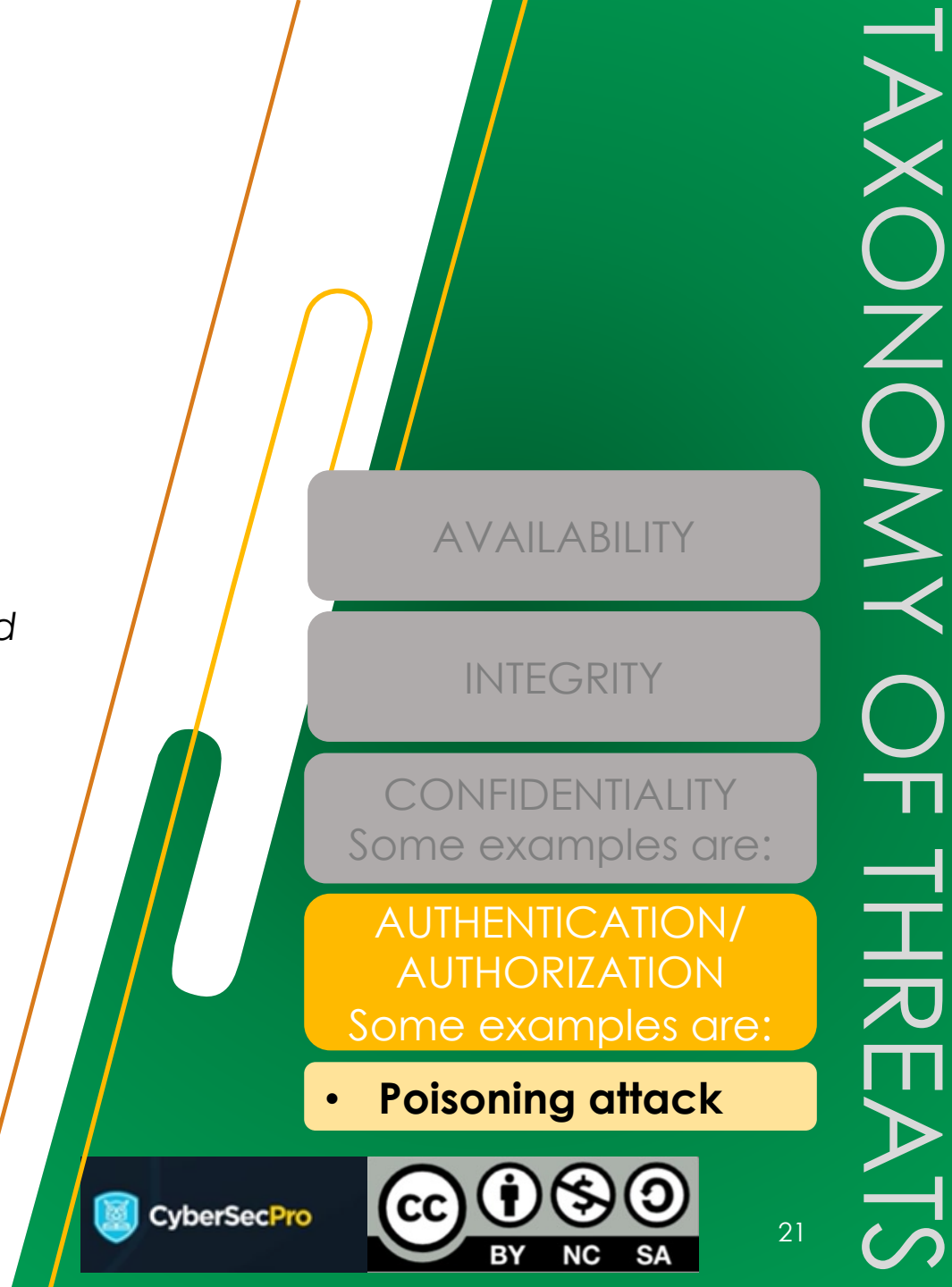
Threats and taxonomy in "control networks" – A/A

- **Entity impersonation (spoofing attack)**
  - The goal of this attack is to steal and use the identity of another legitime nodes, such as controller
  - This type of attacker may lead to other subsequent attacks: a man-in-the-middle, unauthorized access to critical devices, eavesdropping the communications, …
- **Privilege escalation**
  - The aim of this attack is to escalate access privileges to critical resources such as operating devices
  - This type of attack may be initiated by insiders - due to the ease of access to the application domains and their critical resources
  - NOTE: special attention should be paid in DT-based networks, as intellectual property may be located right there (in digital twin models)



Threats and taxonomy in "control networks" – A/A

- **Poisoning attack**
  - The aim of the attack is to inject false data (known as contamination) in order to bypass or corrupt the final operation or performance of the target node
  - Among the most common attacks:
    - **ARP poisoning** – *typical for Man-in-the-middle and discussed later*
    - **DHCP poisoning**
    - **ICMP poisoning**
    - **DNS (cache) poisoning**



Industry APTs, Case 1: STUXNET (2009)

- **Scenario:** Iranian nuclear power plants
  - Traditional SCADA network: IT connected to OT network
  - Use of SCADA/PLC protocols/programs
- **Goal:** sabotage the PLCs controlling the nuclear centrifuges
- **Steps:**
  - *Infection/compromise*: infected USB keys installing malware
  - *Lateral Movement*: vulnerabilities (print Spooler, SMB, WinCC), hardcoded passwords in SCADA HMI machines, harvesting credentials
  - *Final infection*: infection of the controller (the PLC), and manipulation of the PLC code
  - *Result*: the malware (in the PLC) destroys the well performance of the centrifuges, and the effects are hidden

Industry APTs, Case 1: STUXNET (2009)

- **Causes:**
  - Discovery of **zero-day vulnerabilities** ☹
  - **Industrial network without internal defensive measures** ☹
    - All defences located at the perimeter but not in the network perimeter and their hosts
  - **Malware infection** ☹
- **Threats:**
  - *Availability:* hardware availability (DoS against centrifuges)
  - *Integrity*: hijacking (malware)
  - *A/A*: privilege escalation (IT machine accessing core OT elements)
- **Lessons learnt:**
  - 'Birth' of the industrial intrusion detection industry
  - Development of specialized USB management machines for industry

Industry APTs, Case 2: BackEnergy (2015-2016)

- **Scenario:** Ukraine energy network
  - Both IT (management) and OT (energy systems) network
- **Goal:** Infiltration of IT/OT power grids, and destruction
  - Malware is installed and hidden, waiting for malicious C&C instructions
  - When instructions are received, the malware disrupts both IT and OT elements
- **Steps:**
  - *Infection/compromise*: spear-phishing, vulnerabilities, Trojans
  - *Persistence*: malware, local privilege escalation, keep the SSH server in the system
  - *Lateral movement*: Windows admin shares (authenticated sessions)
  - *Exfiltration*: exfiltrate data according to commands from C&C
  - *Destruction*: IT (delete files), OT (disrupt circuit breakers)
  - *Result*: the energy infrastructure is crippled

Industry APTs, Case 2: BackEnergy (2015-2016)

- **Causes:**
  - Again, use of **vulnerabilities**
  - Again, **industrial network without internal defensive measures** - however, this attack also targeted IT networks! (no incorporated defence measures either!)
  - Also, **phishing, Trojans, …**
- **Threats:**
  - *Availability*: destruction of physical and logical services
  - *Integrity*: hijacking (malware)
  - *Confidentiality*: data exfiltration
  - *AAA*: privilege escalation (within infected IT machines, for persistence)
- **Lessons learnt:**
  - It is recommended to continue with detection & protection measures (in terms of malware, penetration, response, recovery, etc.)

More real cases in the energy sector

Year	Location	Attack Objects	Type	Impact
2014	International	Energy companies	NA	250 US and Western European companies were infected for espionage
2015	Ukraine	Electricity operators	DDoS	30 substations disconnected, 8 provinces without power for hours
2015	UAE	Energy companies	Trojan "Laziok"	Espionage, strategically important data theft
2017	Turkey	Electric network in Istanbul	Trojan	Power system failure, blackout in the city over 2 hours
2019	Utah, USA	Wind farms	Trojan	Power system failure
2020	USA	Energy department	Trojan	Power system failure
2021	Denmark	Wind turbines of Vestas company	Trojan	Vestas, top wind turbine supplier, data compromised in suspected 22.11.21 cyberattack
2022	Ukraine	Ukranian electrical substations	Industroyer2	April 2022 virus targets Ukrainian high-voltage substations, controls switches and circuit breakers using Industrial control system (ICS) protocols. Detected and mitigated before blackout
2022	Austria	Wind turbines of Enercon company	NA	Around 5,800 wind turbines in Europe, generating 11,000 MW, were affected by the malfunction. It took weeks to become controlled again
2022	Germany	Wind turbines of Windtechnik company	NA	Deutsche Wind Technik faced a cyberattack on April 12, 2022, after the attack was detected, all remote data monitoring connections to the wind turbines were disconnected for security reasons
2022	Germany	Wind Turbine Giant Nordex	Bazar Loader TrickBot	The cyber-attack was detected by IT security team early. Nordex revealed that the necessary response protocols were taken and IT systems across multiple locations and business units were shut down

Sources: Fursov, Ihor, Klym Yamkovyi, and Oleksandr Shmatko. "Smart Grid and wind generators: an overview of cyber threats and vulnerabilities of power supply networks." Radioelectronic and Computer Systems 4 (2022): 50-63

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