Network Protection for Energy Control Systems

CSP004_C_E

PRESENTATION BY:

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

CyberSecPro
CC BY NC SA

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*

CyberSecPro CC BY NC SA

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

CyberSecPro
CC BY NC SA

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

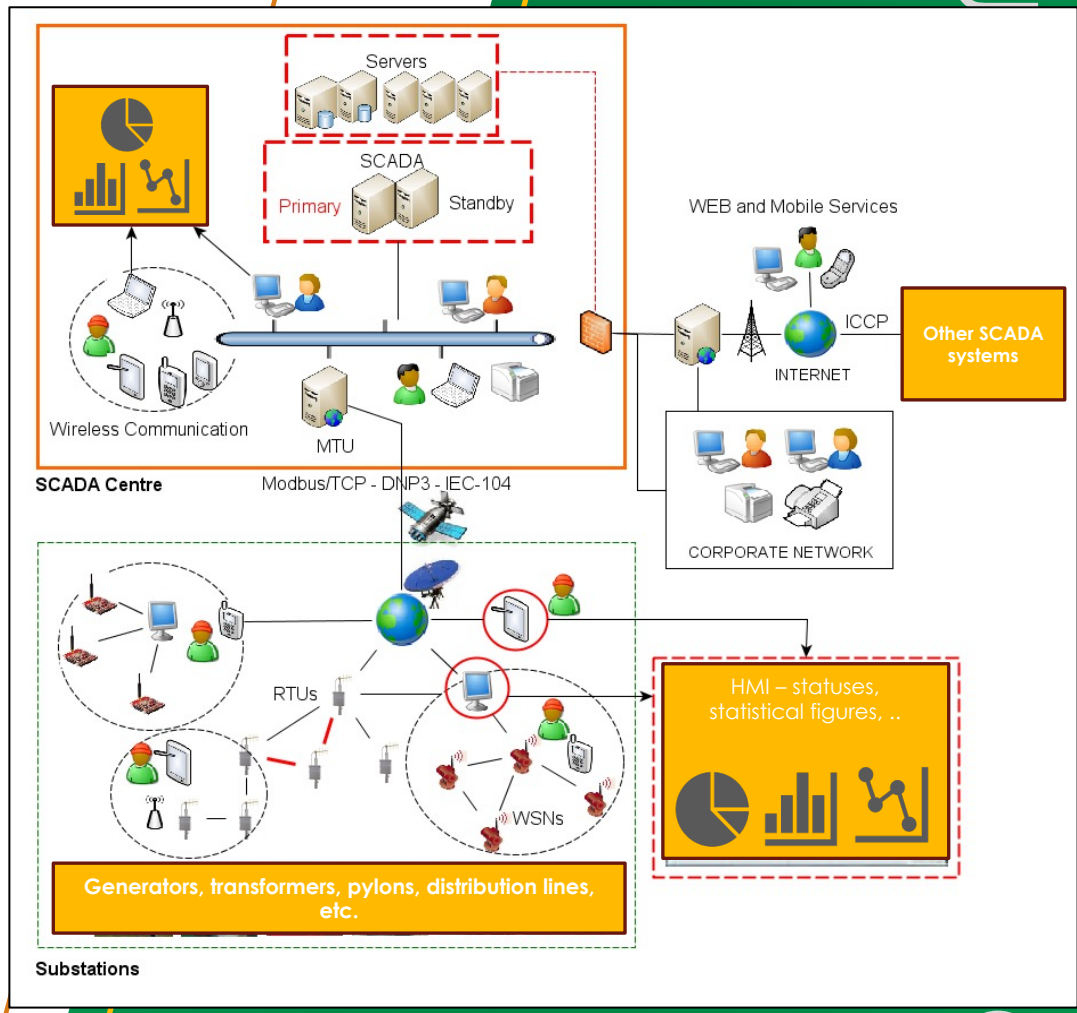
CSP004_C_E – TOPIC 2:
Cristina Alcaraz, University of Malaga, Spain

CyberSecPro
CC BY NC SA

Control networks and their protocols

- As we saw in Topic 1, control networks are mainly based on industrial communication protocols:
  - ModbusTCP, DNP3, IEC-104, PROFIBUS, PROFINET, CIP, HART/IP, WirelessHART, ISA1001.11a, ZigBee PRO, etc.

- Unfortunately:
  - **Not all industrial protocols offer sufficient security guarantees** in terms of confidentiality, integrity, availability and authentication/authorization
  - Moreover, most of them run over TCP/IP and **inherit security weaknesses from the TCP/IP stack**
  - Most control network infrastructures rely on **wireless resources and IIoT/IoT infrastructures**



Control networks and their protocols

Some protocols	WIRED/WIRELESS Communications	Security features
ModbusTCP	• Master/slave • TCP/IP comm.	• **Does not provide confidentiality and authentication mechanisms**, and only verifies determined parts of the packets • **Lacks anti-replay mechanisms** to control DoS attacks, and **does not include CRC** because it is included by the TCP/IP layers
PROFIBUS	• Master/slave • Token-based comm. in multipoint busses	• Offers multiple control services: PROFIsafe and PROFIdrive • PROFIsafe **offers integrity mechanisms**, and PROFIdrive **guarantees location-based interaction**
PROFINET	• Works over Ethernet and TCP/IP	• **Offers** multiple control services: **diagnosis, alerting, configuration, maintenance, and synchronization** • Extends the PROFIBUS profiles to add extra functionality, so a PROFINET network can control a PROFIBUS network through interfaces PROFINET IO or a proxy
OPC-UA	• Object-based comm., where each device is encapsuled on an object	• Uses data codification based on XML-RPC (XML over HTTP), and is based on two protocols: TCP/IP-based binary protocol for performance in real time, and SOAP-based protocol to manage the network through Web services • **Offers** service and device discovery, data exchange, **event management and alert**
CIP	• Object-based comm., where each device is encapsuled on an object • Ethernet/IP	• **Offers** multiple services: control in real time, **operational safety**, power control, synchronization and **prioritisation, authentication via TLS/DTLS in Ethernet/IP, access control, integrity and confidentiality**

- From the table, we note that there are advances in the security of some industrial protocols
  - However, there are protocols that are quite widespread in industrial environments, such as ModbusTCP, which do not add any security measures to protect data in transit

There are some security measures, but not really enough !

CyberSecPro
CC BY NC SA

Control networks and their protocols

Some protocols	WIRELESS Communications	Security features
WirelessHART	• Controllers/gateways and field devices • P2P comm. and mesh networks • Wireless comm. based on the IEEE **802.15.4** (low-rate wireless personal area networks (LR-WPANs)) • Command-oriented comm. based on the HART (TCP)	• **Offers** services for **frequency hopping and blacklisting** methods • **Applies cryptography and authentication measures** • **Susceptible to multiple threats** due to wireless communication
ISA100.11a	• Controllers/gateways and field devices • P2P comm. and mesh networks • Wireless comm. based on the IEEE **802.15.4** • Object-oriented comm. under UDP • Compatibility with 6LowPAN	• **Offers** services for **frequency hopping and blacklisting** methods • **Applies cryptography and authentication measures** • **Susceptible to multiple threats** due to wireless communication
ZigBee	• Controllers/gateways and field devices • P2P comm. and mesh networks • Wireless comm. based on the IEEE **802.15.4**	• **Offers** services for **addressing schemes (stochastic, group), frequency agility**, and **cryptography and authentication** • **Susceptible to multiple threats** due to wireless communication

- Indeed, **wireless communication** are:
  - **Vulnerable to multiple types of threats** (even more than wired networks)
  - **Unstable to noisy, vibration or high interference contexts** ➔ it is very common in industrial environments !
  - **Susceptible to manage coexistence issues** when multiple wireless networks or protocols are present in the same environment

Some security measures are therefore in place, but they are not enough! Protective measures are still necessary

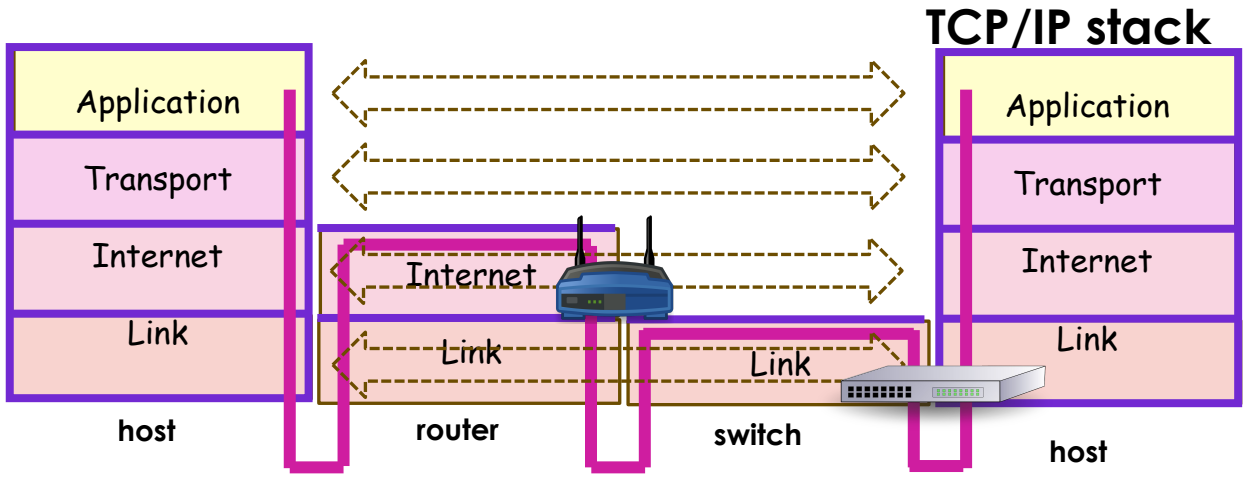
SECURITY ISSUES AND COMINGS

CyberSecPro

CC BY NC SA

Inheritance of security weaknesses in the TCP/IP stack

- Moreover, for the interconnection of control networks with other remote networks or sub-networks, e.g. substations, it is very common to connect via the Internet following the TCP/IP model
- This type of interconnection requires the application of the well-known TCP/IP model and IT devices, such as:
  - **Router**: operates only up to the Internet level and only understands IP addresses
  - **Switch**: works up to the link level and only understands MAC addresses
  - **Hub**: works up to the physical level

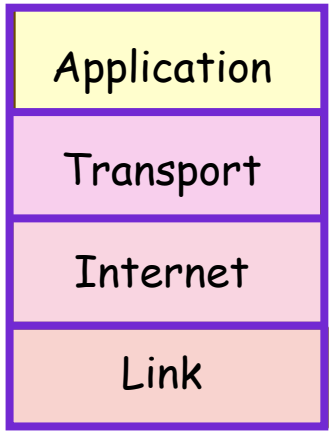


SECURITY SHORTCOMINGS

CyberSecPro
CC BY NC SA

Inheritance of security weaknesses in the TCP/IP stack

- Each TCP/IP layer leads a set of actions:



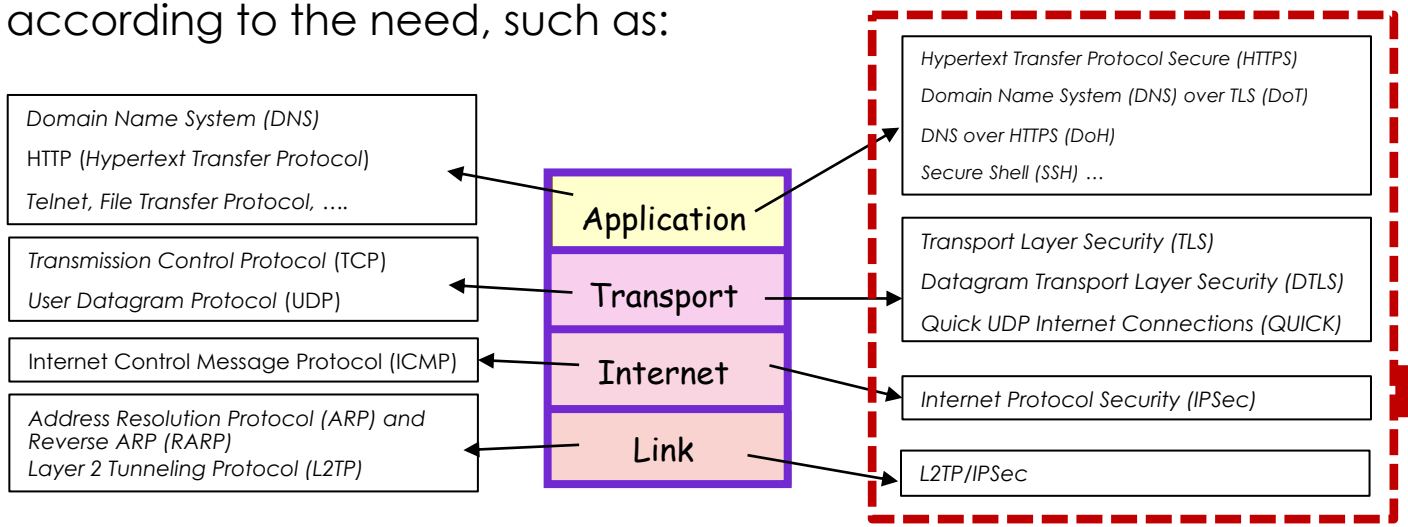
- **Application layer**: facilitates standardized data exchange for applications, and deals with the actual application data
- **Transport**: ensures end-to-end communications across the network
- **Internet**: deals with packets and connects independent networks to transport the packets across network boundaries
- **Link**: operates at the link level, connecting nodes or hosts within a network

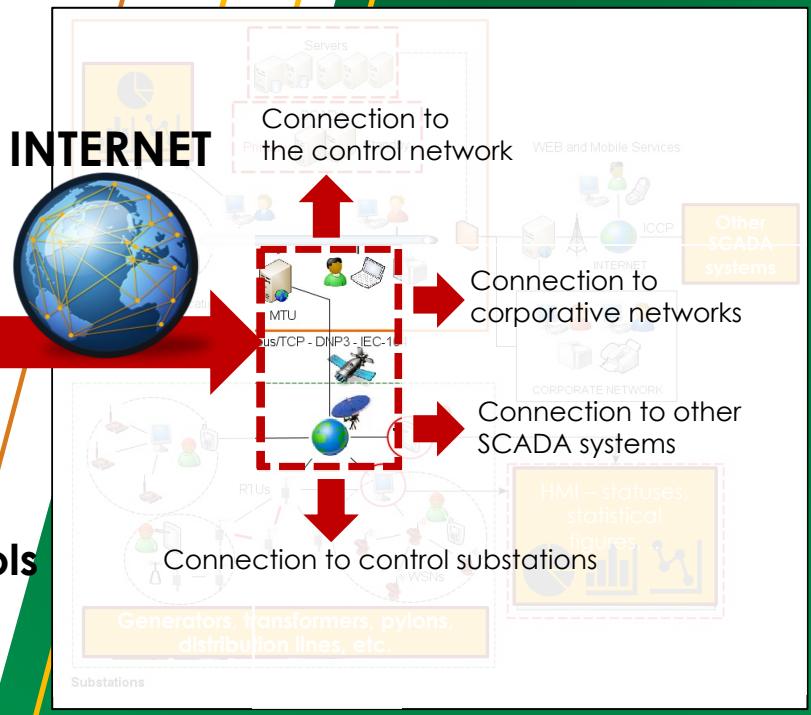
Source: K. Yasar, M. E. Shacklett, A. Novotny, "TCP/IP", 2024
URL: https://www.techtarget.com/searchnetworking/definition/TCP-IP

CyberSecPro
BY NC SA

Inheritance of security weaknesses in the TCP/IP stack

- However, the TCP/IP stack is based on a set of specific protocols, some originally developed for the stack, and others have been designed according to the need, such as:



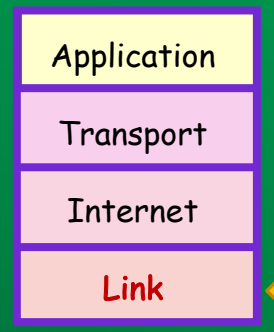


- The reasons for incorporating security protocols into the TCP/IP stack were due to the **security weaknesses found in the traditional protocols**
  - Most TCP/IP protocols were originally designed without security measures in mind
  - This also means that if protective measures are NOT properly applied in control networks, this level of insecurity may be extended to those critical communications, e.g. between a slave and a master in ModbusTCP

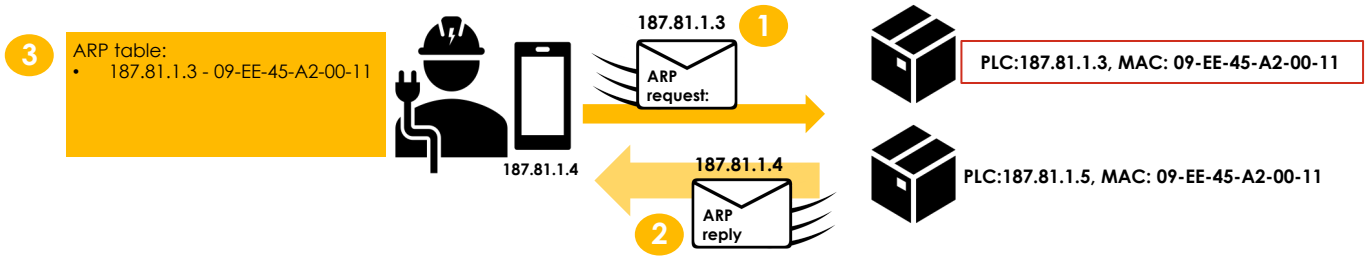
SECURITY SHORTCOMINGS

CyberSecPro
CC BY NC SA

TCP/IP Security weaknesses: link layer



- **Address Resolution**
  - **Main protocols**: ARP and RARP
  - **Goal**: ARP aims to resolve the conversion of an IP address (logical address) → MAC (physical address), whereas RARP would be MAC → IP
    - In ARP, when devices connect to the network, they first have to discover the MAC address of the destination node to update the internal ARP table and send the datagram with the corresponding IP of the destination node
    - With this MAC address, the node can connect to the switch, which only understands MAC addresses



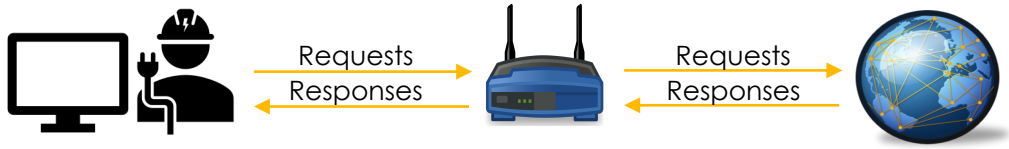
  - **Main security weaknesses**: ARP was originally designed without any kind of security that allows to verify that the sending device is really who it claims to be
    - Therefore, the protocol is susceptible to fake ARP messages, and all these messages are accepted by the involved devices
    - Among the attacks using ARP messages, we highlight **ARPSpoofing**

SECURITY SHORTCOMINGS

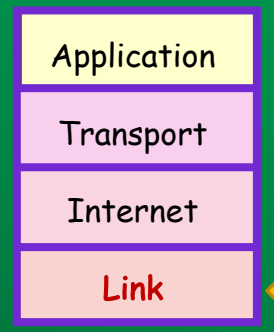
CyberSecPro
CC BY NC SA

<*Short break*>: ARPSpoofing

- ARP spoofing, also known as **ARP poisoning**, is a deceptive technique used by attackers to intercept data
  - In this attack, the attacker tricks a device into sending its data to him/her instead of to the intended recipient



  - By doing so, the attacker may access the targeted device's communications, potentially obtaining sensitive information like passwords and credit card details
  - Attackers may use ARP spoofing for spying the communications through a man-in-the-middle or leading other cyber-attacks, such as a DoS (e.g. a black hole or selective forwarding attack)



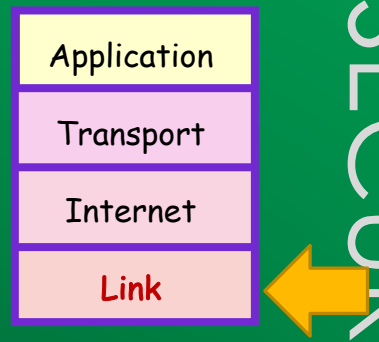
CyberSecPro
BY NC SA

Homework: ARP Spoofing/Poisoning

- **Objective**: 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 performing an ARP Poisoning/Spoofing attack. This attack positions the attacker in the middle of all data transmissions between the victim machine and the gateway (i.e., Main in the Middle)
- **Guidelines**: follow the steps below to set up a controlled, simulation-based lab environment using virtual machines (a victim and an attacker). This setup will enable you to perform the simulated attack 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 **arpspoof** tool on your Kali Linux machine
- **Tasks**:
  - Use **arpspoof** to execute the attack. To do so, mislead the gateway into believing that the attacker's device is the legitimate one, and deceive the legitimate device into thinking that the attacker is the gateway
  - Verify the ARP table on the target side before and after the attack
  - Compare the ARP table before and after the attack to assess the changes
  - Repeat the process, but this time using **Ettercap** - https://www.ettercap-project.org

OPTIONAL PRACTICAL TASKS

TCP/IP Security weaknesses: link layer



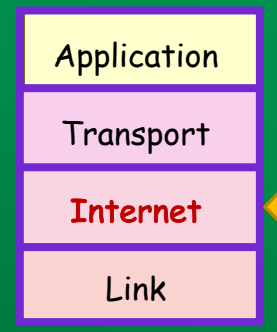
- **Tunnelling between networks**
  - **Main protocols**: there are several protocols like L2TP
  - **Goal**: L2TP aims to transfer of information between networks of different nature, either in terms of communication and format
    - However, the term also applies to the encryption of datagrams (the packet) to send information securely between two peers
    - The term is also associated to VPN (Virtual Private Network)

  - **Main security weaknesses**: although L2TP allows the connection of different types of networks, it was designed without security in mind such as encryption, authentication and integrity measures
    - Therefore, L2TP is susceptible to multiple types of attacks

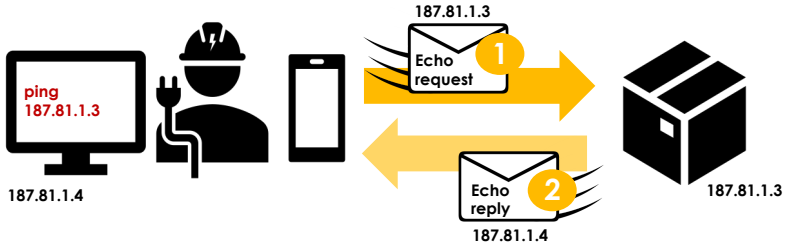
SECURITY SHORTCOMINGS

CyberSecPro
BY NC SA

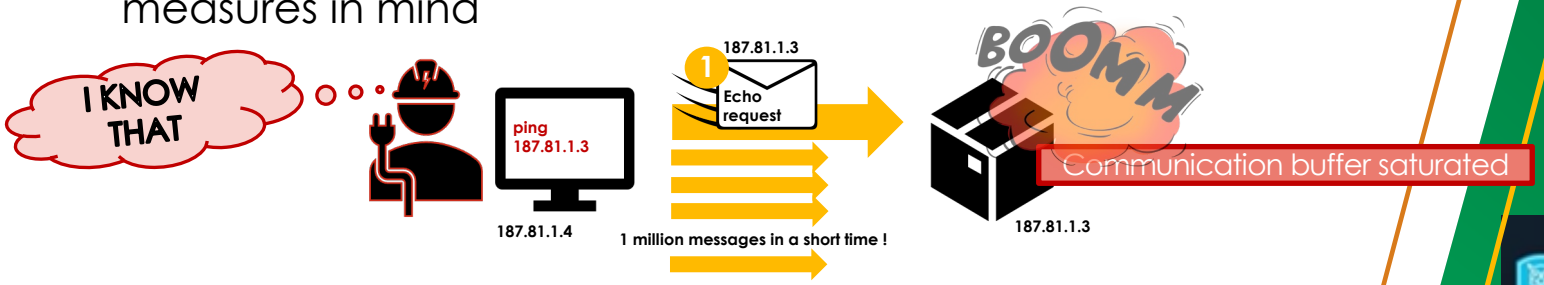
TCP/IP Security weaknesses: Internet layer



- **Network and device/resource diagnosis**
  - **Main protocol**: ICMP
  - **Goal**: check the health status of a node or a network
    - Note: ICMP operates with the "ping" command, which allows sending echo request packets to the destination node in order to receive an ICMP packet containing the "echo reply" → **$ ping 187.81.1.3**



  - **Main security weaknesses**: many of the DoS attacks come from the ICMP protocol, as it was designed without any security measures in mind

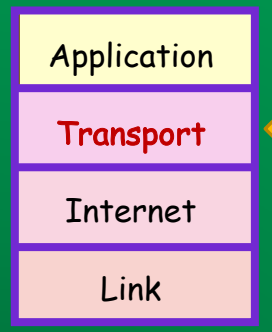


SECURITY SHORTCOMINGS

CyberSecPro
CC BY NC SA

TCP/IP Security weaknesses: transport layer

- **Network and device/resource diagnosis**
  - **Main protocols**: TCP and UDP
  - **Goal**: both protocols are responsible for fragmenting and reassembling data datagrams under a service-oriented connection
    - Service-oriented means that all fragments arrive at their destination in an ordered and complete manner
  - **Main security weaknesses**: both protocols were designed without security measures in mind



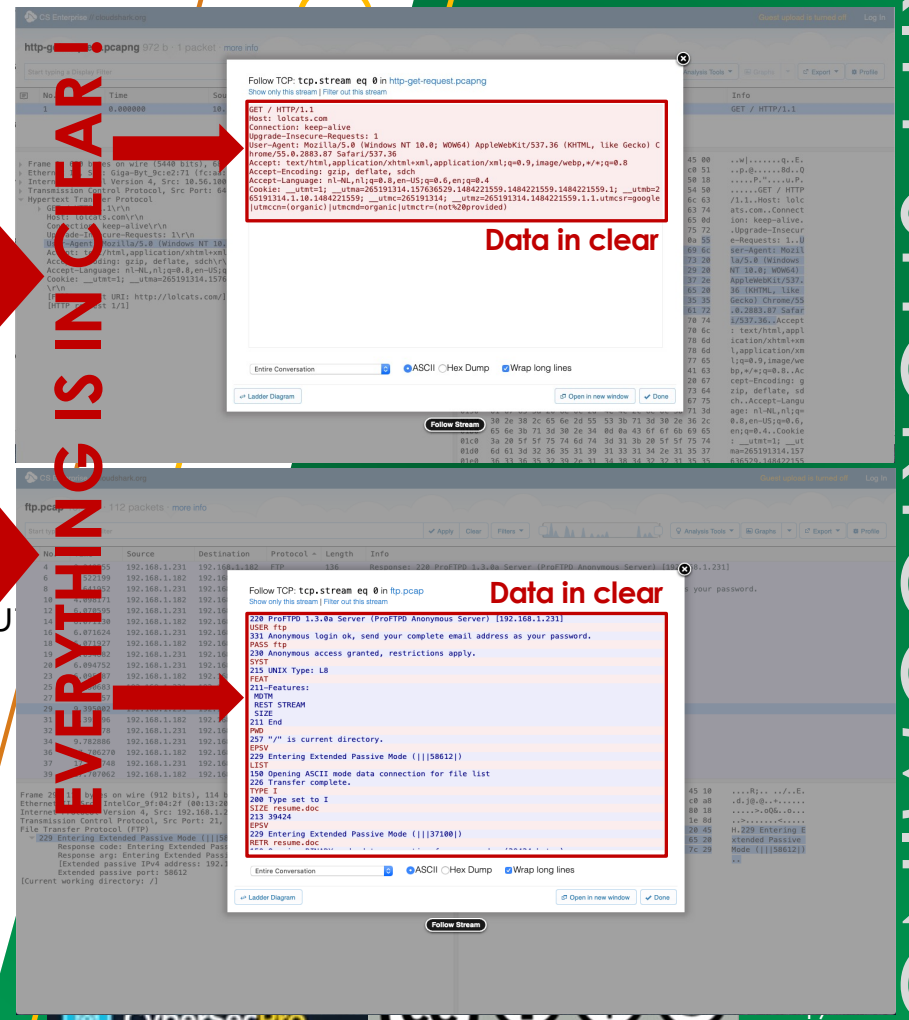
SECURITY SHORTCOMINGS

CyberSecPro

CC BY NC SA

TCP/IP Security weaknesses: application layer

- **Information transfer and communication**
  - **Main protocols**: HTTP and FTP
  - **Goal**:
    - HTTP is considered the Internet protocol and constitutes the basis of the WWW (World Wide Web), in which hypertext documents (texts interpreted by network devices) may include links to other network resources, globalising connections and the navigation of pages and resources on the Internet
    - FTP for data transference through the ports TCP-20-21
  - **Main security weaknesses**: both protocols were designed without security measures in mind
    - This means that the transference of data is done in clear and anyone with a dissection tool may be able to intercept the communications and read the network traffic – as also appreciated in the two captures of both figures

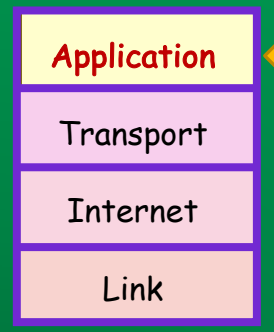


SECURITY SHORTCOMINGS

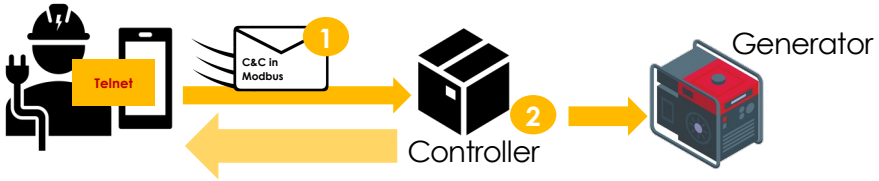
Source and figure source: CloudShark, "http-get-request.pcapng", 2024
https://www.cloudshark.org/captures/83390916ab62
Source and figure source: CloudShark, "ftp.pcap", 2024
URL:https://www.cloudshark.org/captures/abdc8742488f

CyberSecPro
BY NC SA

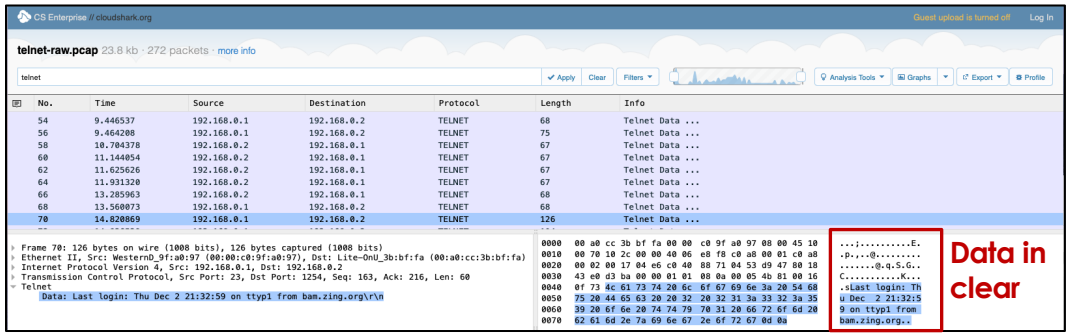
TCP/IP Security weaknesses: application layer



- **Remote control**
  - **Main protocol**: Telnet
  - **Goal**: this protocol establishes remote connection via TCP-port 23



  - **Main security weaknesses**: telnet presents similar problems to FTP and HTTP



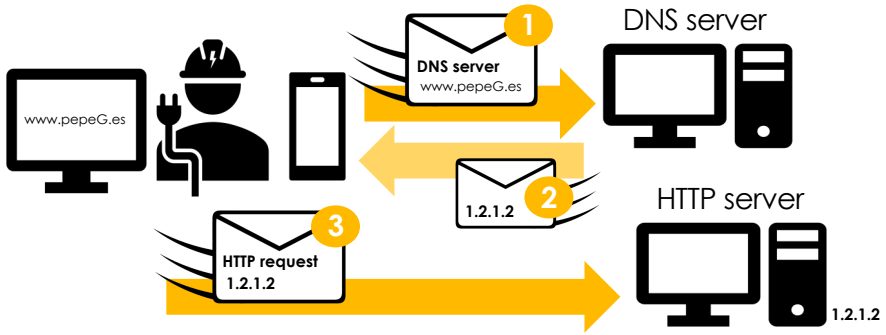
    - Unfortunately, legacy operational devices may still rely on these types of protocols !
    - Attackers may take advantage of the unsecure nature of the protocols (port 23, 21, 80) to lead: eavesdropping, DoS or modifications

Source and figure source: CloudShark "telnet-client-server.pcapng", accessed in 2024
URL: https://www.cloudshark.org/captures/818ceaef07b8?filter=telnet

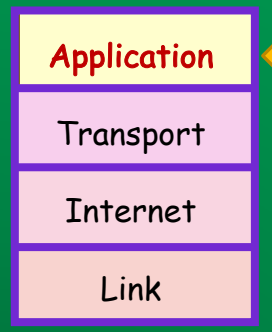
CyberSecPro
CC BY NC SA

TCP/IP Security weaknesses: application layer

- **Translation of www addresses**
  - **Main protocols**: DNS
  - **Goal**: allow the translation of IP addresses into human-readable and human-understandable names:
    - E.g. www.pepeG.es ➔ 1.2.1.2



  - **Main security weaknesses**: the protocol presents some security risks when translations are transferred www → IP
    - They are transferred in plaintext, with no guarantee of authentication and validity of the records
    - This lack of authentication makes the protocol susceptible to MitM and spoofing attacks, in which fake servers may impersonate legitimate servers, providing fake IPs (e.g. for subsequent forwarding)



SECURITY SHORTCOMINGS

CyberSecPro
CC BY NC SA

Homework: Telnet and FPT + Wireshark

- **Task**: considering the installation of two virtual machines or two PCs configured in the same local area network (e.g. home LAN):
  1. Install a **telnet client and server** to analyse the traffic between the two nodes using Wireshark
     - To do this, it is recommended to activate Wireshark before the telnet connection
     - Then, transfer commands via telnet, and analyse the Wireshark captures in order to verify that the transferred commands are sent in clear (or unencrypted) between the two peers
  2. Perform the same exercise, but this time installing an **FTP client-server** (Linux) to analyse the traffic between the two nodes using Wireshark
     - To do so, it is recommended to install the **Vsftpd** tool on Linux ($ sudo apt install vsftpd), and transfer FTP commands to be captured in Wireshark
     - Analyse the captures to verify that such commands are sent in clear as well

OPTIONAL PRACTICAL TASKS

Source for telnet (guidelines): 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
Source for FTP (guidelines): PhoenixNAP, How to Install FTP Server on Ubuntu with vsftpd, 2024.
URL: https://phoenixnap.com/kb/install-ftp-server-on-ubuntu-vsftpd

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

CyberSecPro

CC BY NC SA