

RSAC[®]Conference2020

San Francisco | February 24 – 28 | Moscone Center

HUMAN
ELEMENT

SESSION ID: SBX1-W3

SCADA/ICS Inherited Insecurity: From Nuclear Power Plants to Oil Rigs



Aleksander Gorkowienko

Managing Consultant
Spirent Communications

#RSAC

ICS/SCADA 1-0-1

Where Are Industrial Control Systems (ICS) Used?

- Industrial processes
- Manufacturing processes
- Power generation
 - Critical national infrastructure
 - Electricity transmission
 - Water treatment and distribution
 - Oil and gas pipelines
 - Transportation
 - Vehicles and infrastructure (trains, metro, tankers, airplanes, etc.)

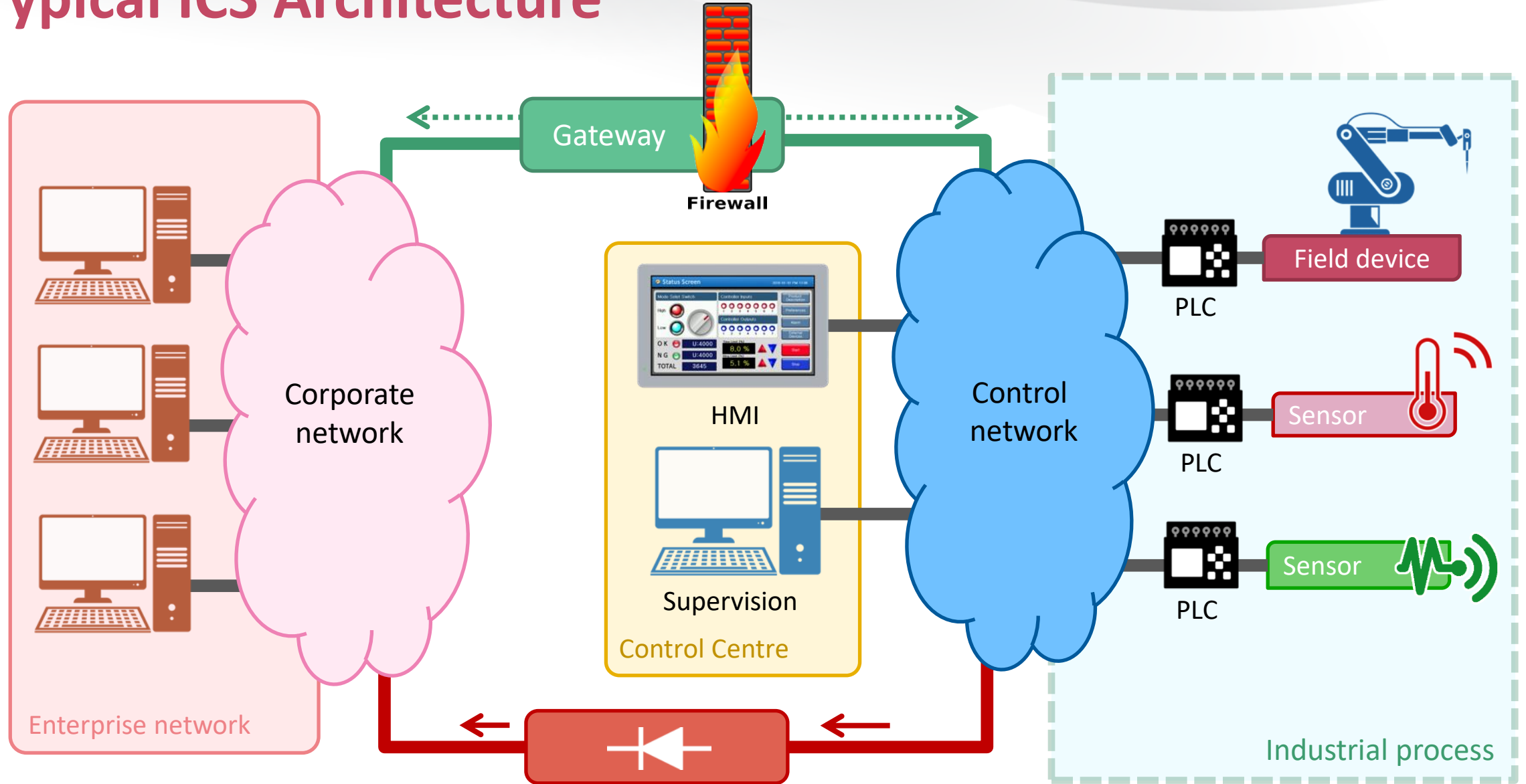


What Is So Special About ICS?

- Proprietary systems
- Long service life span (sometimes beyond 20 years)
- Not easily upgradable (sometimes not upgradable at all)
- Specialized communication, including many legacy ICS protocols wrapped in TCP or UDP
- Most often not designed with security in mind
- **VERY HACKABLE...**



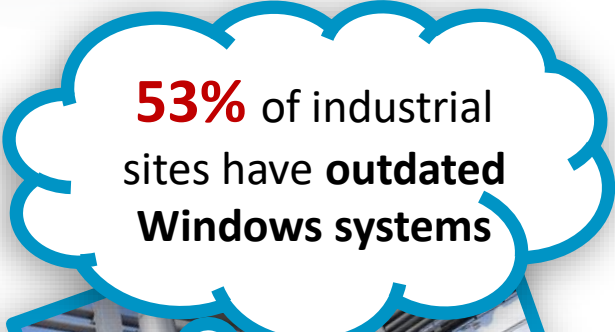
Typical ICS Architecture




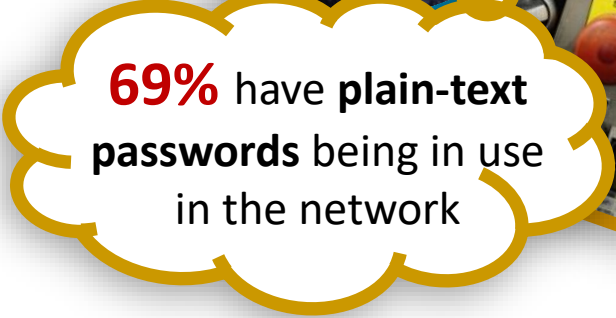
ICS/SCADA (IN) SECURITY

Typical Issues With ICS/SCADA Security

- ICS/SCADA is **managed by engineers**, not IT
- **Legacy systems** working side-by-side with the newest solutions. Very difficult to enforce unified security.
- ICS/SCADA systems are **much more vulnerable to Denial of Service (DoS)** attacks
- Many critical systems feature **proprietary protocols** which are designed (and operating) in a non-secure way
- **Security by obscurity** (in reality it means: no security)
- **Myth of “security by air gapping”**. OT can never be fully separated from IT.



53% of industrial sites have **outdated Windows systems**



69% have **plain-text passwords** being in use in the network

Exploiting ICS May Cost Human Life

- If someone hacks a web server – you can restart it and restore the data, but generally, no major harm is done (*yes, we can always debate...*)
- If someone hacks a power plant, oil refinery or manufactory – the **consequences are very tangible, very physical**, sometimes lethal, seriously damaging infrastructure and **affecting the safety and security of people.**
- **People's life is at stake**



Breaking The Air Gap

- Malicious USB pen drives (yes, the good old Stuxnet way still works)
- Hacking through supply chain (exploit ICS vendors first, then go to main target)
- Technicians and field engineers (vulnerable laptops and field devices)
- Sniffing communication (wired, radio, etc.)
- Attacking unmanned field sites



RSA[®]Conference2020



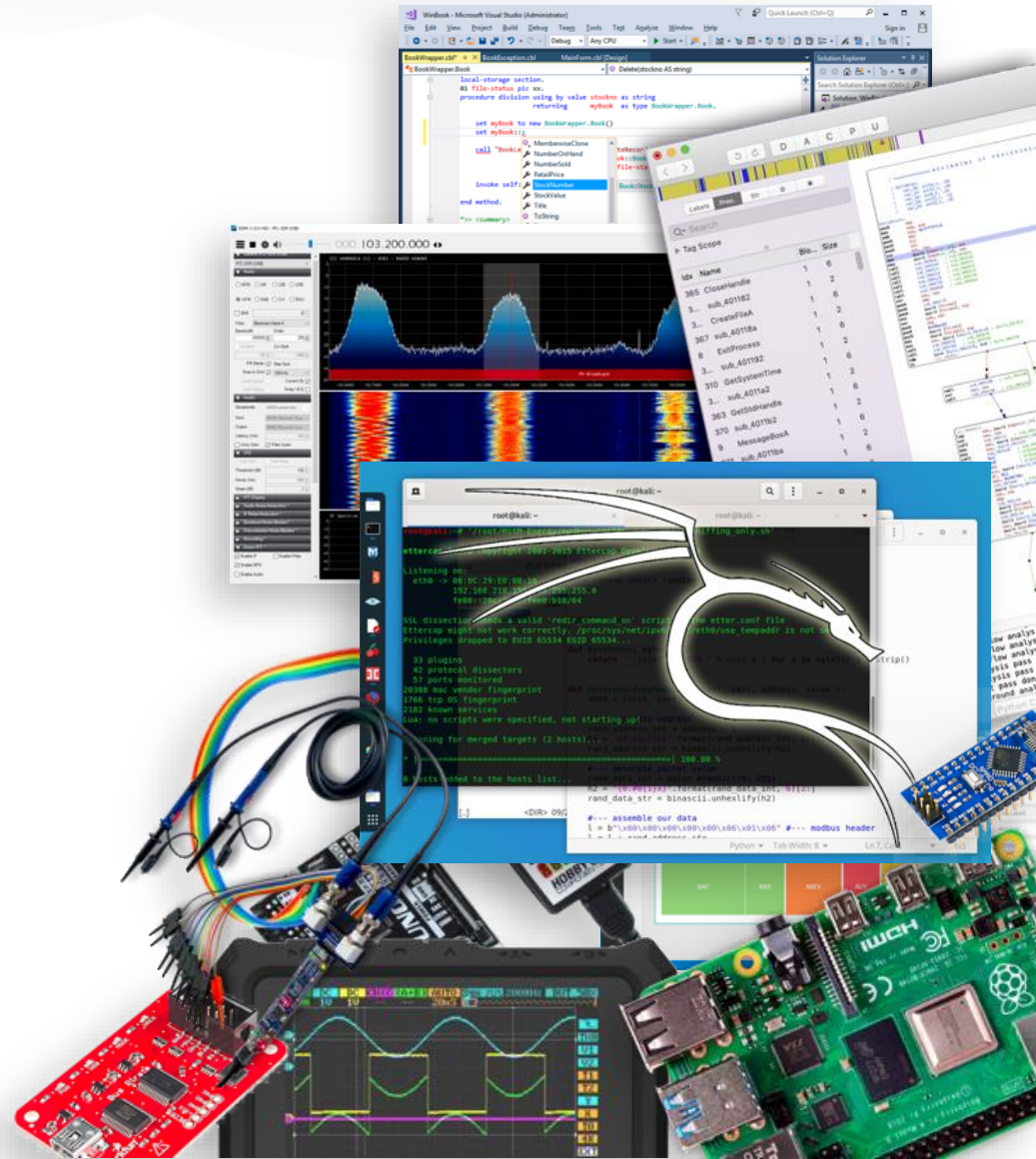
New Generation of ICS Remote Clients

- Web applications are more and more common
- Mobile devices are also now in use in the ICS world
- Various web APIs are available
- All of above creates additional and well-known attack surface: SQLi, XSS, direct object reference, LFI, RFI, etc. = **paradise for hackers**

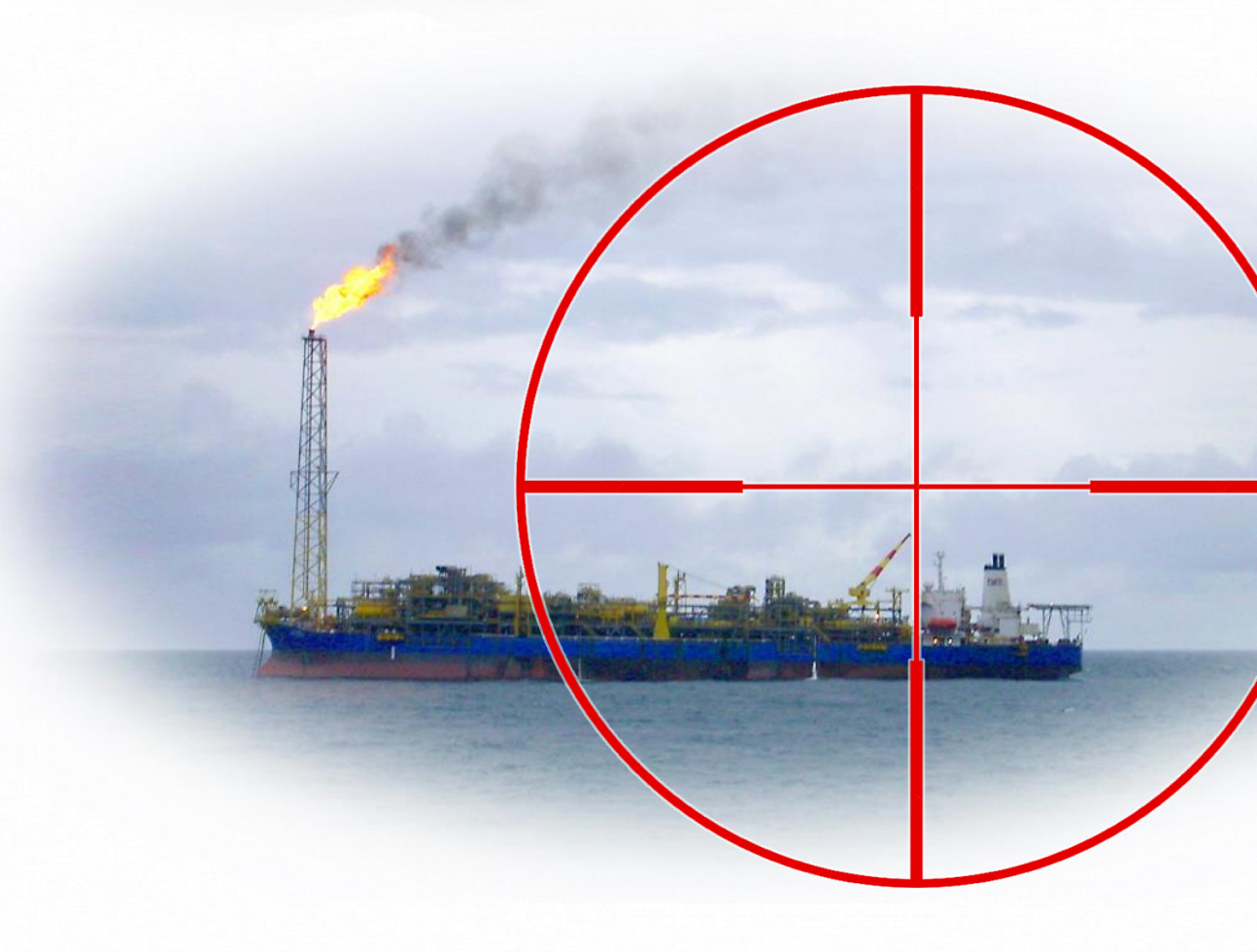


What Tools Does An Attacker Need?

- Common network tools and techniques as modern ICS networks are more and more featuring TCP-IP
- Tools for network traffic sniffing, analysis and reverse engineering
- Scripting and packets crafting (Python or any programming language you prefer)
- Hardware for connecting to ICS systems
- Enough time and curiosity



HACKING FPSO



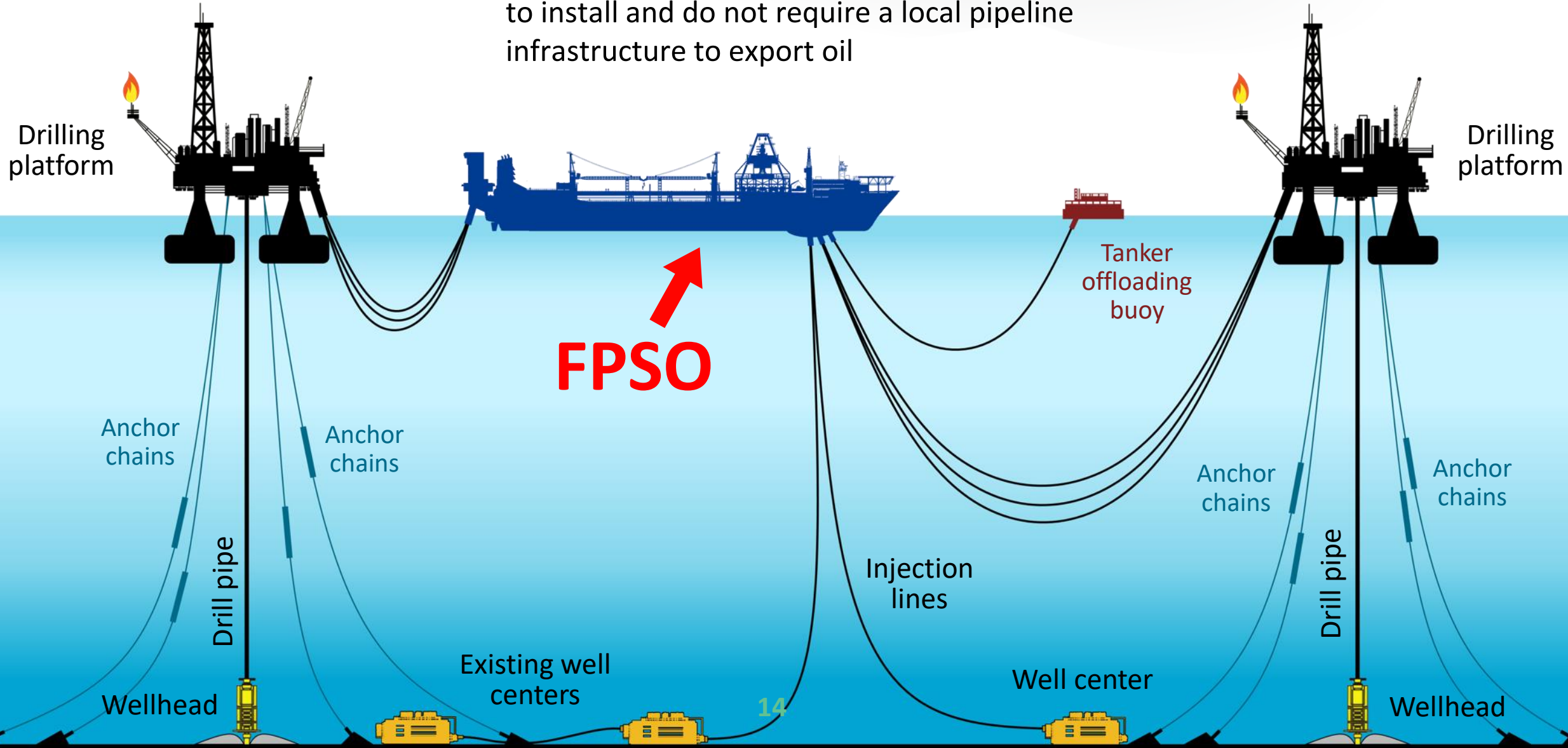
What FPSO is?

- A **Floating Production Storage and Offloading (FPSO)** is a vessel used by the offshore oil and gas industry. It is used for the production and processing of hydrocarbons, and for the storage of oil.
- A FPSO vessel is designed to receive hydrocarbons produced by itself or from nearby platforms or subsea template, process them, and store oil until it can be offloaded onto a tanker (less frequently: transported through a pipeline).



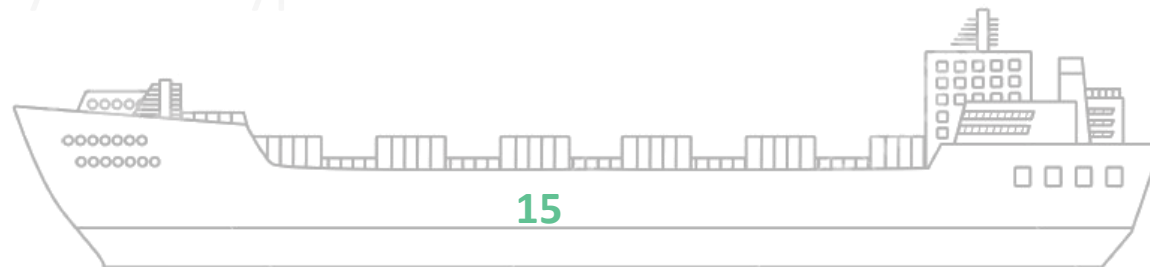
What FPSO is?

FPSOs are popular because they are relatively easy to install and do not require a local pipeline infrastructure to export oil



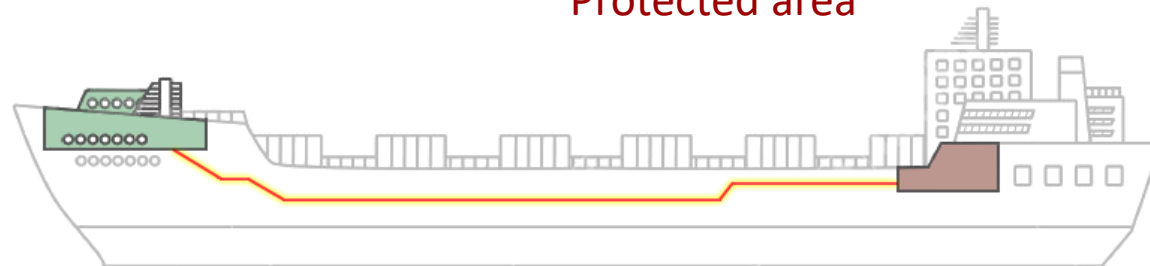
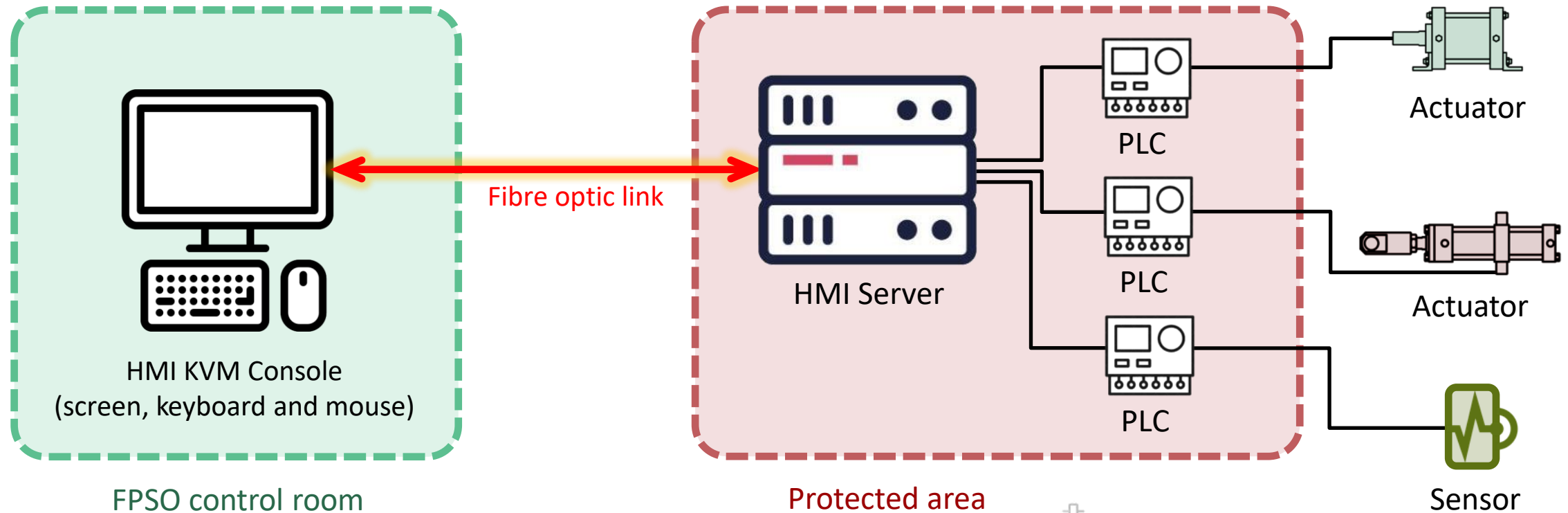
Findings From Our Assessment

- ...
 - **Unauthorized bidirectional transfer of data and binaries to and from the air gapped HMI server**
 - Unauthorized access and privilege escalation
 - **PLC is vulnerable to the Man in the Middle attack**
 - **NTP Server is vulnerable to the Man in the Middle attack**
 - Windows services can be reconfigured by non-admin users [HMI server]
 - Insecure permissions on program files and services [HMI server]
 - Unnecessary open ports [HMI workstation subnet]
 - Multiple transport layer encryption weaknesses
- We will discuss these issues



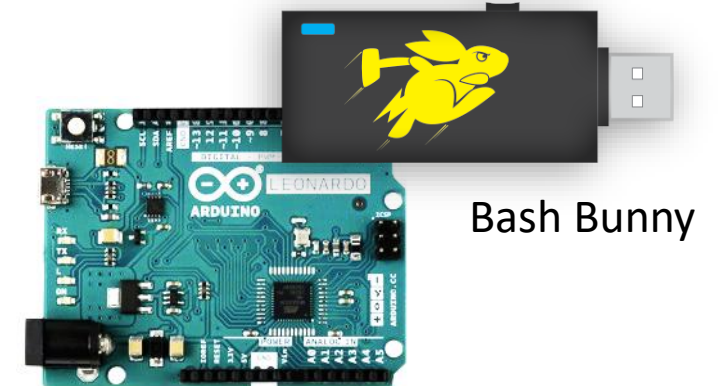
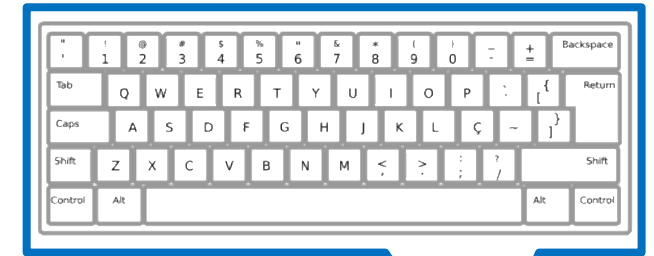
Let's Take Over The "Air Gapped" Server First

- The HMI server can only be accessed from the console over KVM
- It was assumed by architects that there is no way to transfer anything to the server over KVM...



Transferring (Malicious) Binary To The HMI Server

- We have identified **Windows 7** installed on the HMI server (unpatched!) with no AV (HMI supposed to be working as a “kiosk” with no access to the OS)
- The **certutil.exe** tool was found on the server (a part of the default installation) and **notepad.exe** too
- **Bash Bunny** connected to the KVM instead of the whitelisted keyboard mimicking the exact USB device ID
- The “malicious” binary has been transferred to the remote server and recovered by certutil.exe

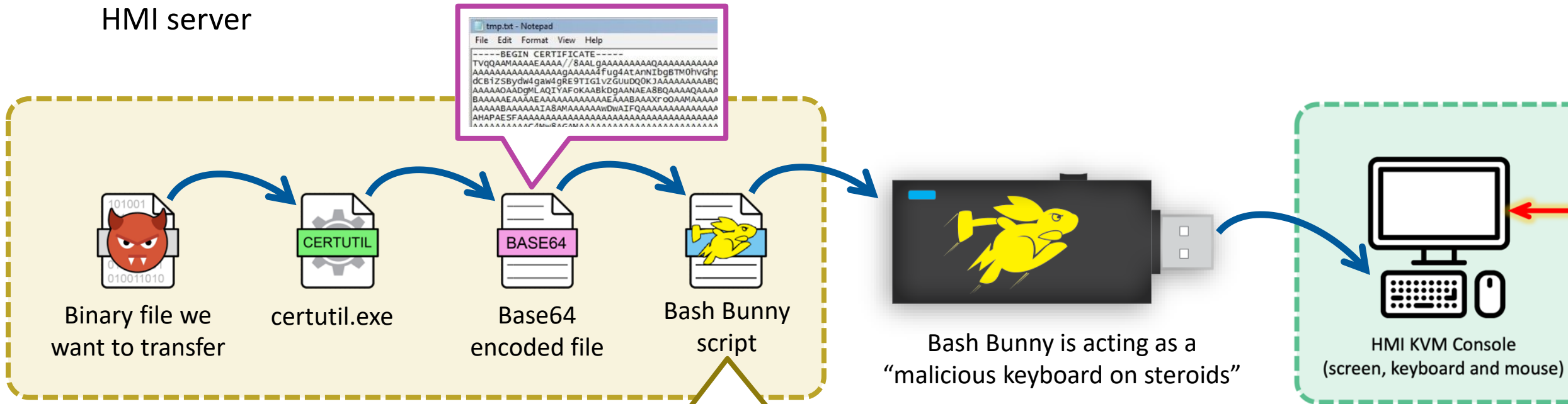


Bash Bunny

Arduino Leonardo

Transferring (Malicious) Binary To The HMI Server

- We have converted a payload (binary file) to the set of instructions for Bash Bunny
- Bash Bunny was connected to the KVM instead of the keyboard
- We simulated keystrokes and copied the Base 64 encoded file to an empty text file on HMI server



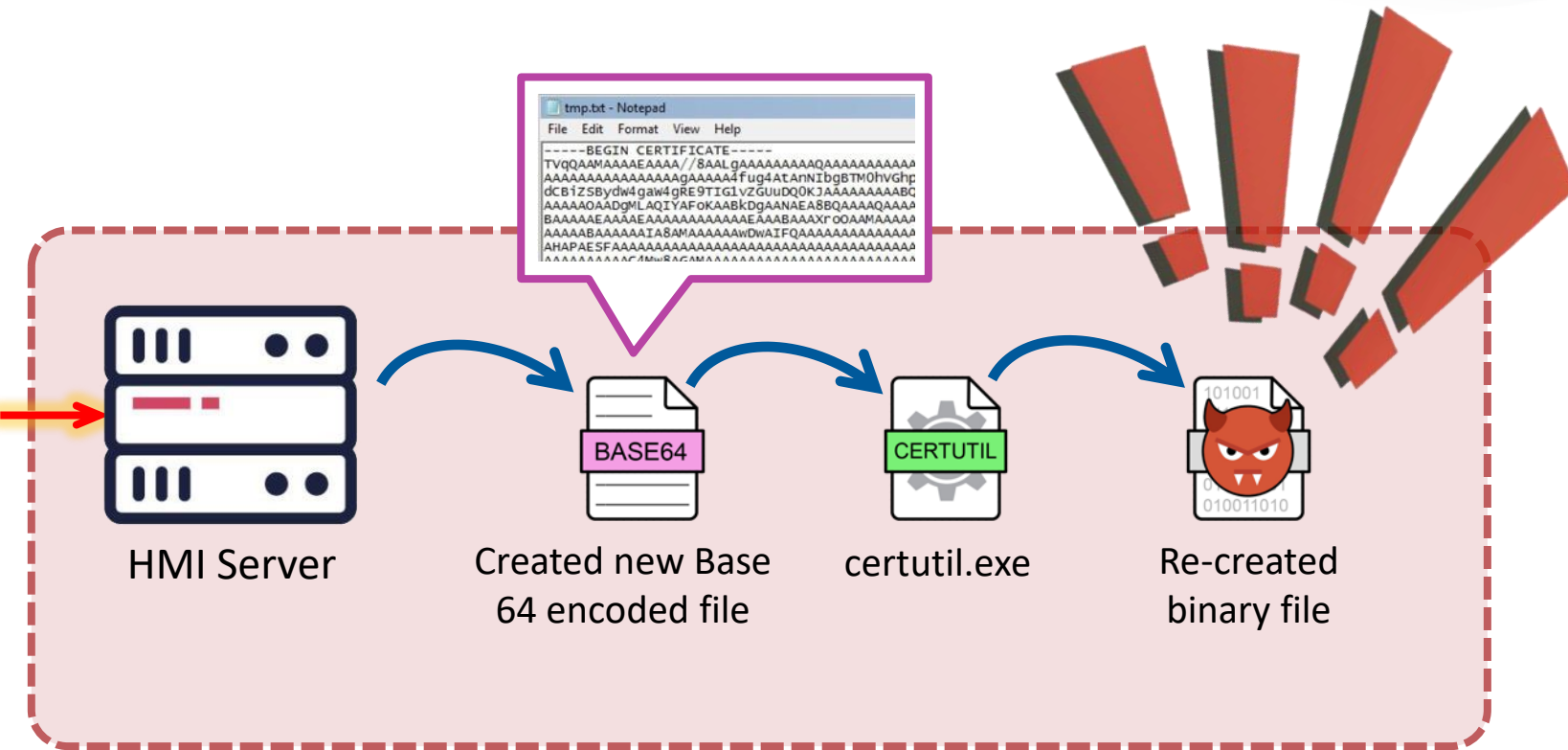
```

tmp.txt - Notepad
File Edit Format View Help
-----BEGIN CERTIFICATE-----
TVqQAAAAAAAAAAAA//8AALgAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAA4fug4AtAnNIbgBTM0hVgHpcyBwcm9ncmFtIGNhbm5v
dCB1ZSBydw4gaw4gRE9TIG1vZGUuDQ0KJAAAAAAAAABQRQAATAEDAPx+fjoAAAAA
AAAAAAAAAADgMLAQIYAF0KAAABDgAANAeA8BQAAAAAAAAAAAA
BAAAAEAAAAEAAAAAAAAAAAAAAAAEAAABAAAXG00AAAMAAAAA
AAAAABAAAAATABAMAAAAAAWdWAIQAAAAAAAAAAAAAAAAAAAA
AHAPAESFAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAACAmuBACMAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
  
```

```

1 DELAY 3000
2 STRING -----BEGIN CERTIFICATE-----
3 ENTER
4 DELAY 100
5 STRING TVqQAAAAAAAAAAAA//8AALgAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
6 ENTER
7 DELAY 100
8 STRING AAAAAAAAAAAAAAAAAAAAAA4fug4AtAnNIbgBTM0hVgHpcyBwcm9ncmFtIGNhbm5v
9 ENTER
10 DELAY 100
11 STRING dCB1ZSBydw4gaw4gRE9TIG1vZGUuDQ0KJAAAAAAAAABQRQAATAEDAPx+fjoAAAAA
12 ENTER
13 DELAY 100
14 STRING AAAAAAADgMLAQI3ACAAAAAQAAAAUAAAKHIAABgAAAAQAAAAABAAAAQAAAAgAA
  
```

Transferring (Malicious) Binary To The HMI Server

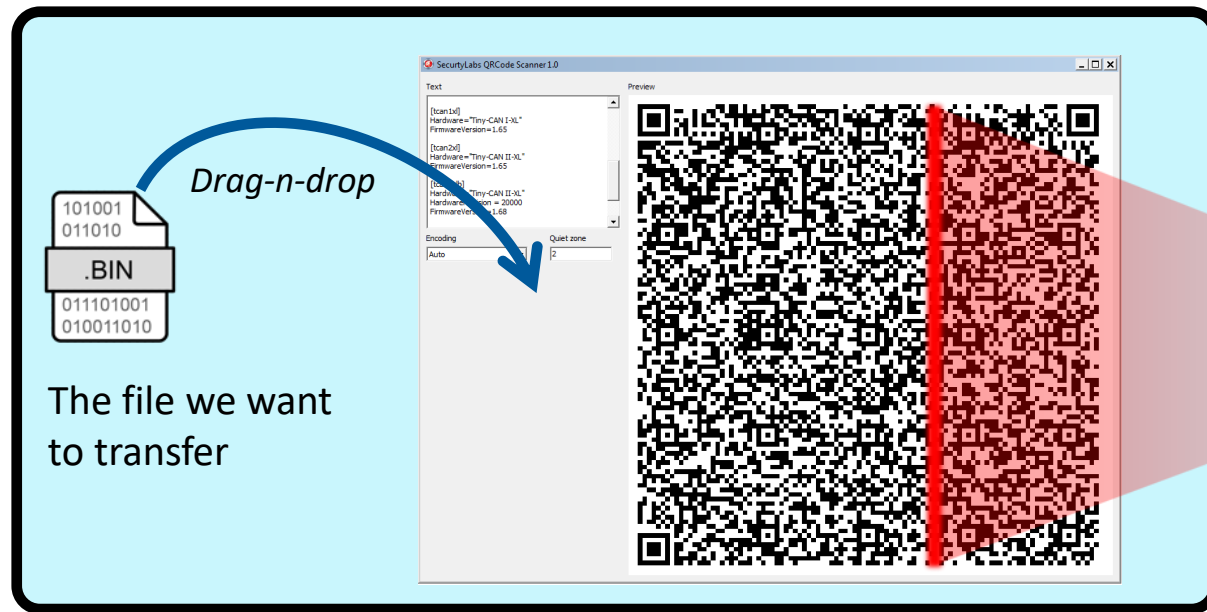


On the HMI Server...

- We ran certutil.exe on the HMI server again and converted back the Base 64 encoded file to the original binary form
- We can run our binary on the server without restrictions
- Job done!

Transferring Data Back From The HMI Server

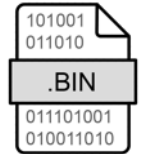
- Step 1: Transferring a small custom-built utility (.exe) to the target server
- Step 2: Run the utility, drag-and-drop any file to it – the content is on the screen transformed to a QR code!
- Step 3: Read the code by the mobile app and you've got the file



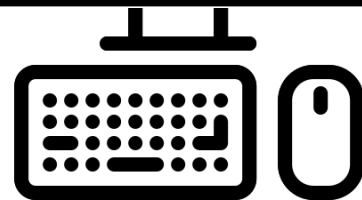
The file we want to transfer



The QR code can be read from the KVM screen by the mobile app and converted back to the original file

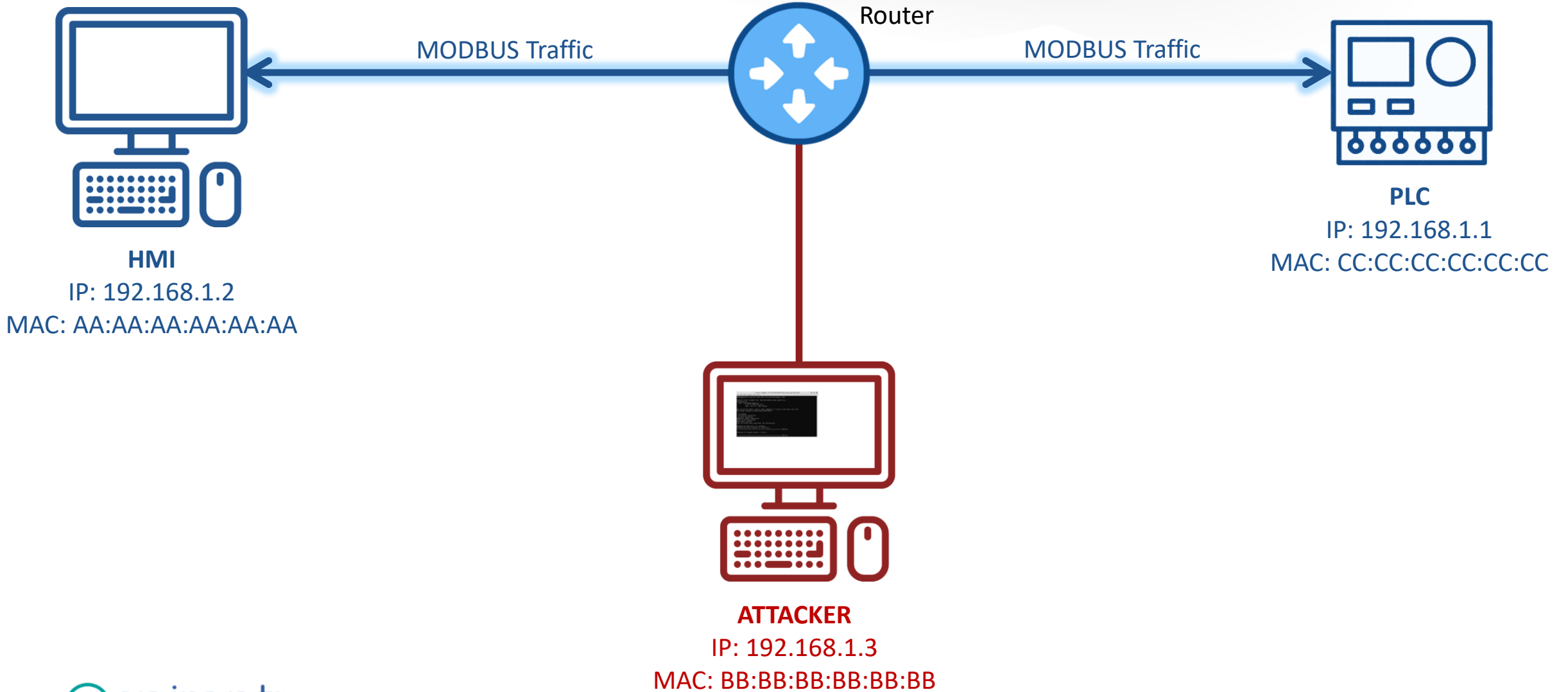


We have our file!

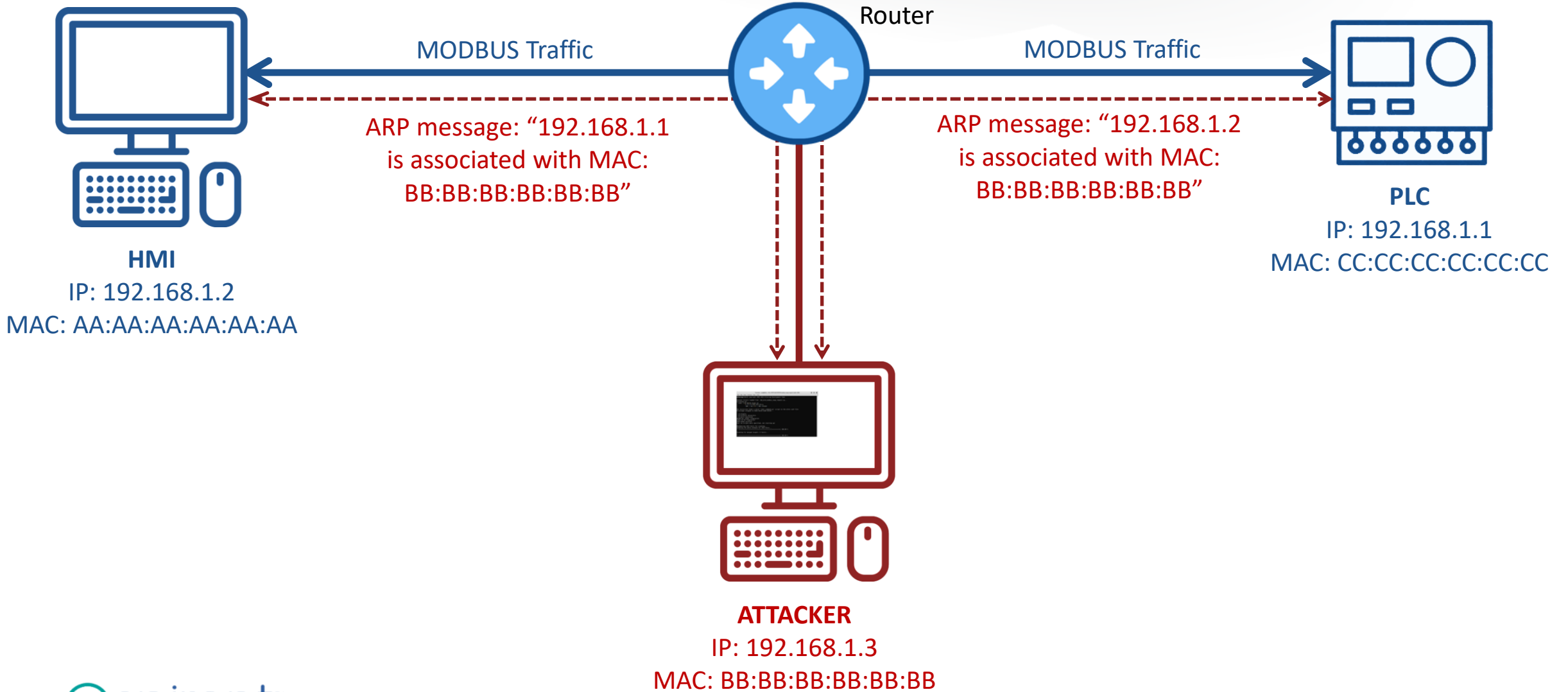


HMI KVM Console

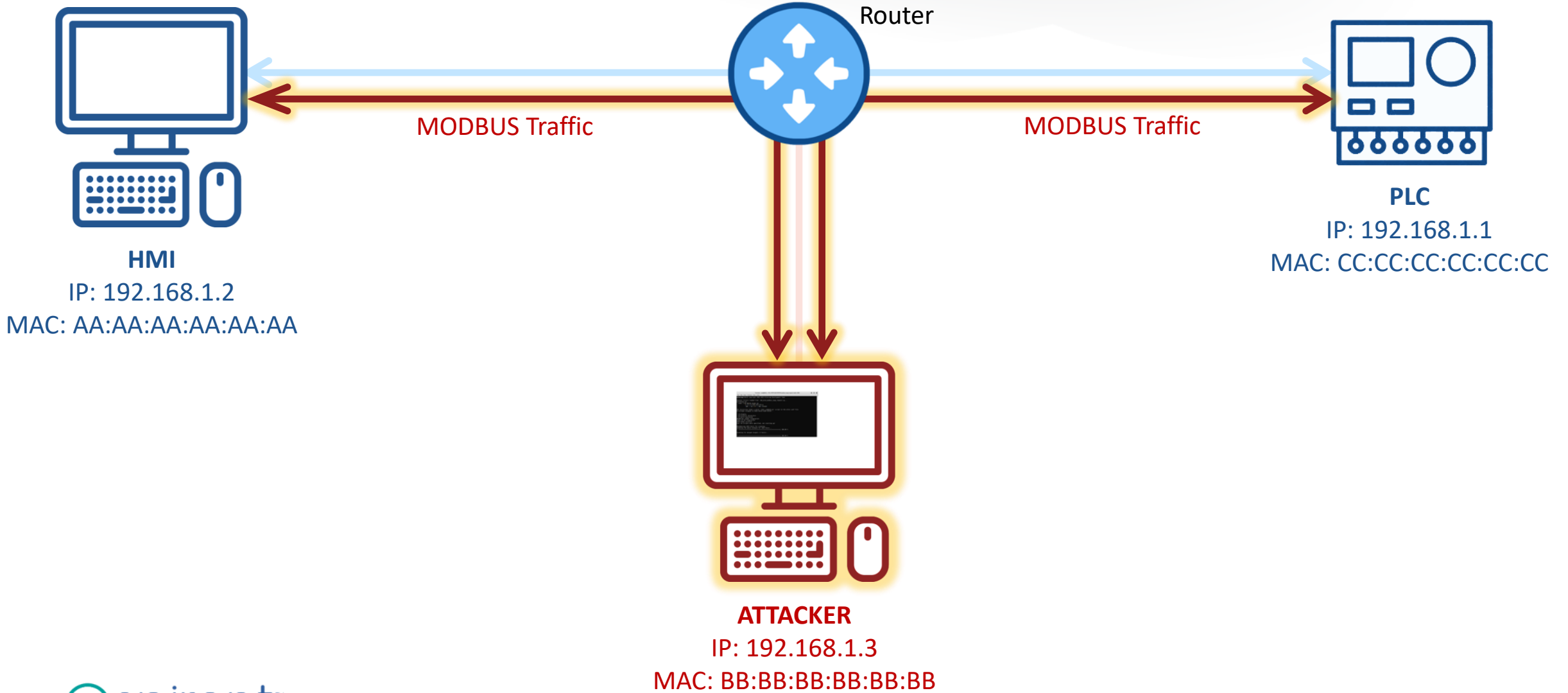
Man in The Middle (MiTM) attack



Man in The Middle (MiTM) attack



Man in The Middle (MiTM) attack



What Could The Attacker Do With MiTM?

- An attacker can **sniff network traffic** and passively collect sensitive plain text information
- An attacker can **tamper the information** exchanged between parties at the same time staying undetected
- In our case we were able to:
 - Intercept and modify queries to PLC
 - Swap “read register” requests to PLC with “write register”
 - Intercept and modify queries to the central NTP server, changing the reference timestamp for operation logs and all dependent devices



Attacking The NTP Server

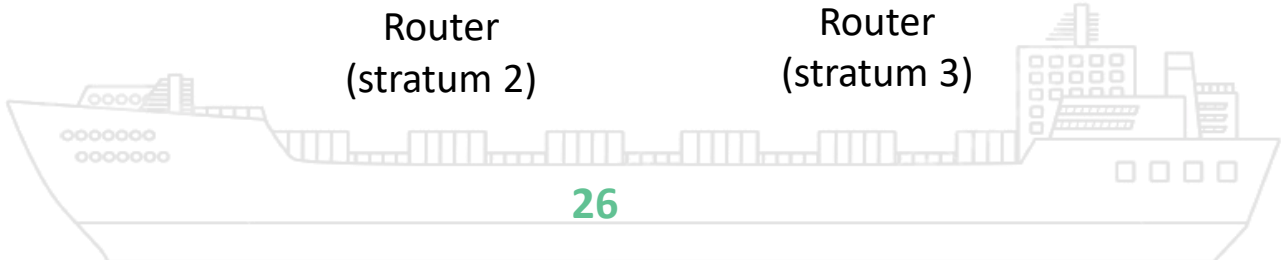
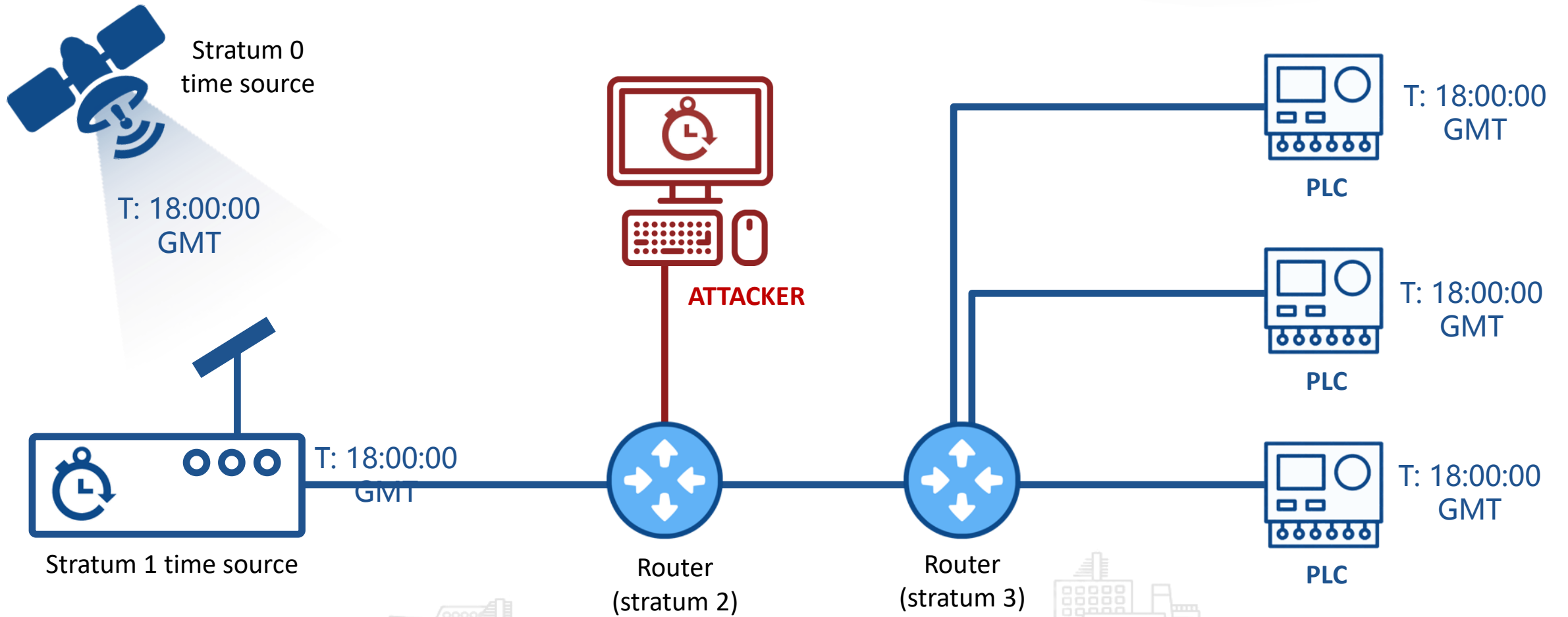
The Challenge

- We can conduct a Denial of Service (DoS) attack. Can we enforce routers to use the incorrect timestamp?..
- If the time difference between the timestamp from the router's internal clock and the data provided by the NTP server is too big, it will ignore the source of the incorrect information.
- The “fake” NTP server will be blacklisted.



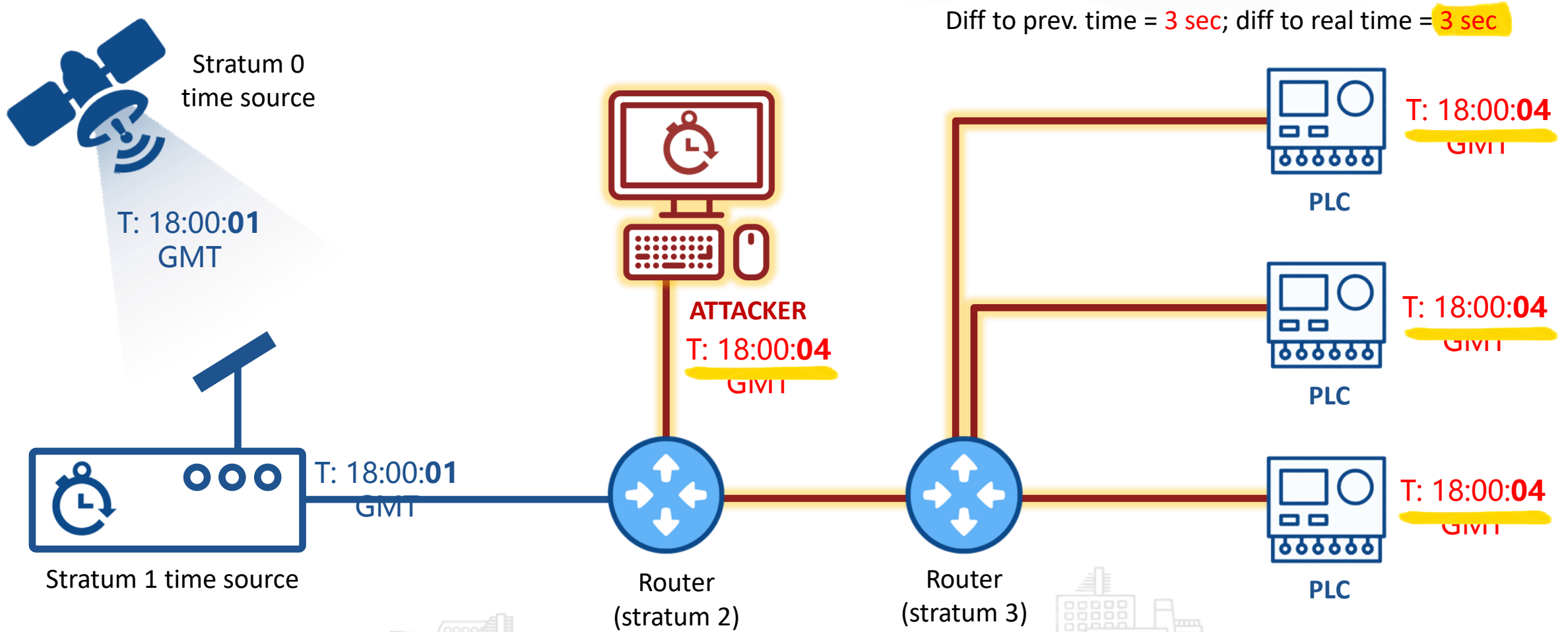
Attacking The NTP Server

We can gradually “drift” from the correct time and increase the time difference in small steps



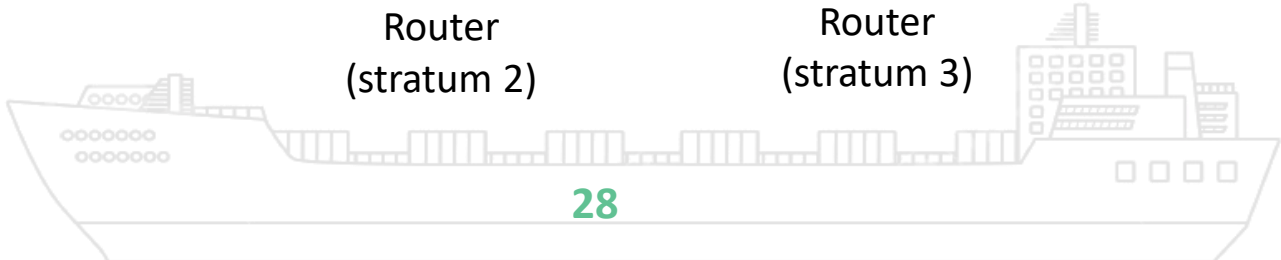
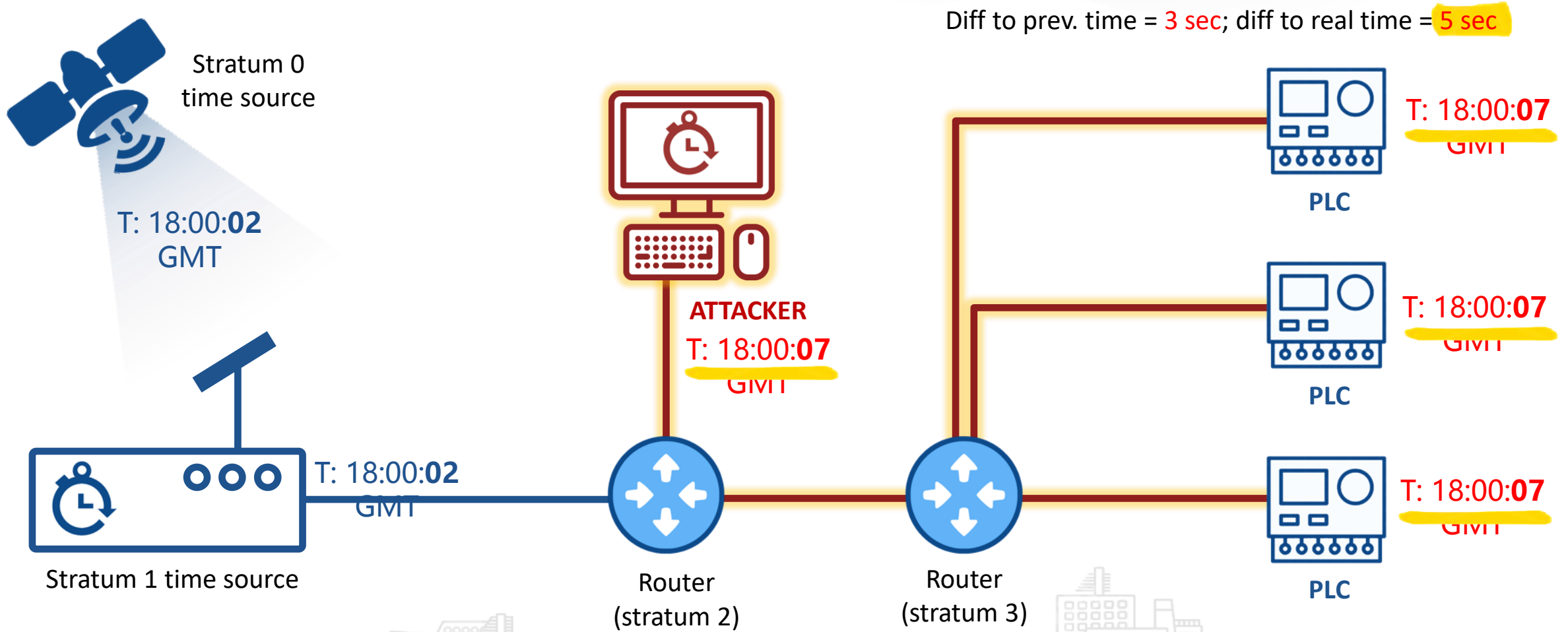
Attacking The NTP Server

We can gradually “drift” from the correct time and increase the time difference in small steps



Attacking The NTP Server

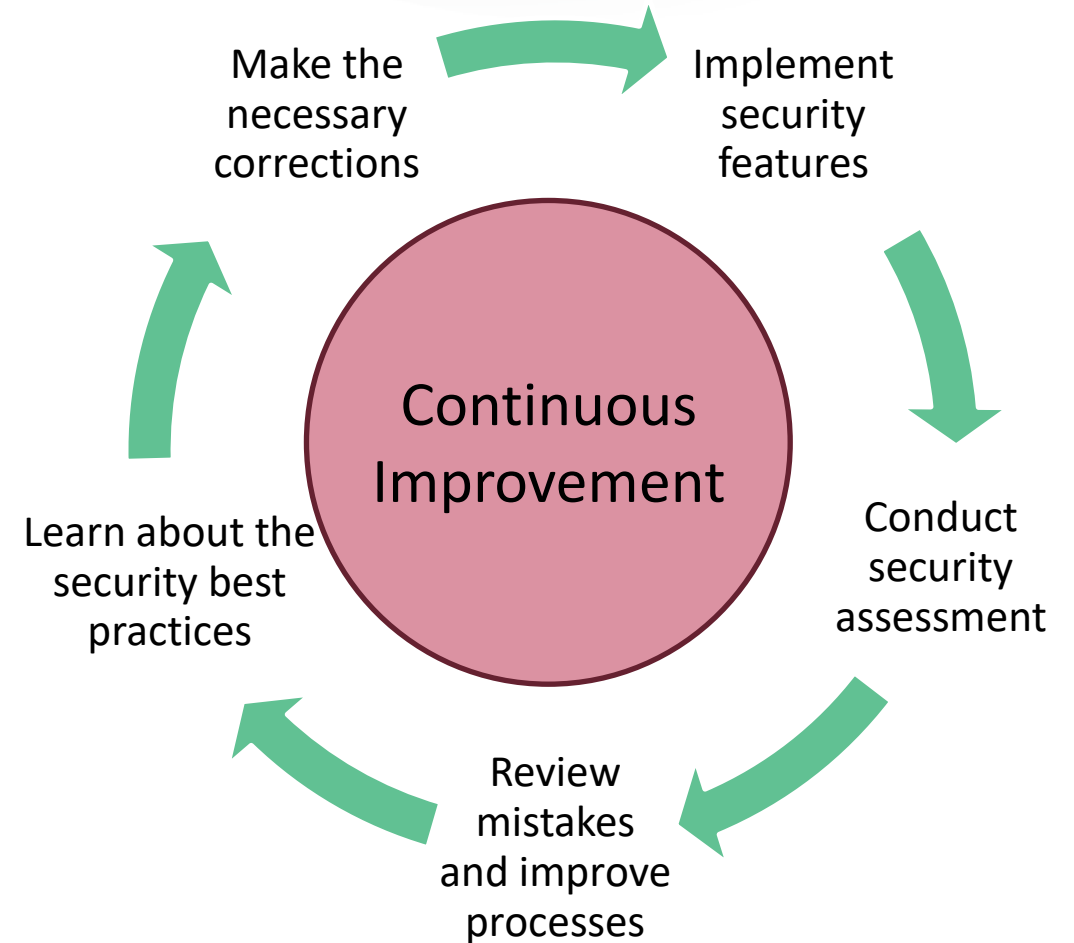
We can gradually “drift” from the correct time and increase the time difference in small steps



IMPROVING SECURITY OF ICS

Change Your Mindset First!

- Security is a **continuous process**, where an organization is learning and improving their processes and the security posture all the time
- Security is a **system property**, not a feature
- Security is a **continual process**, not a product



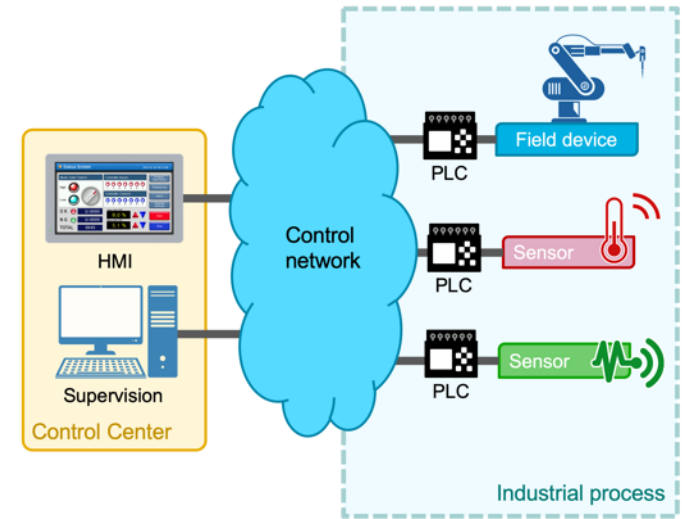
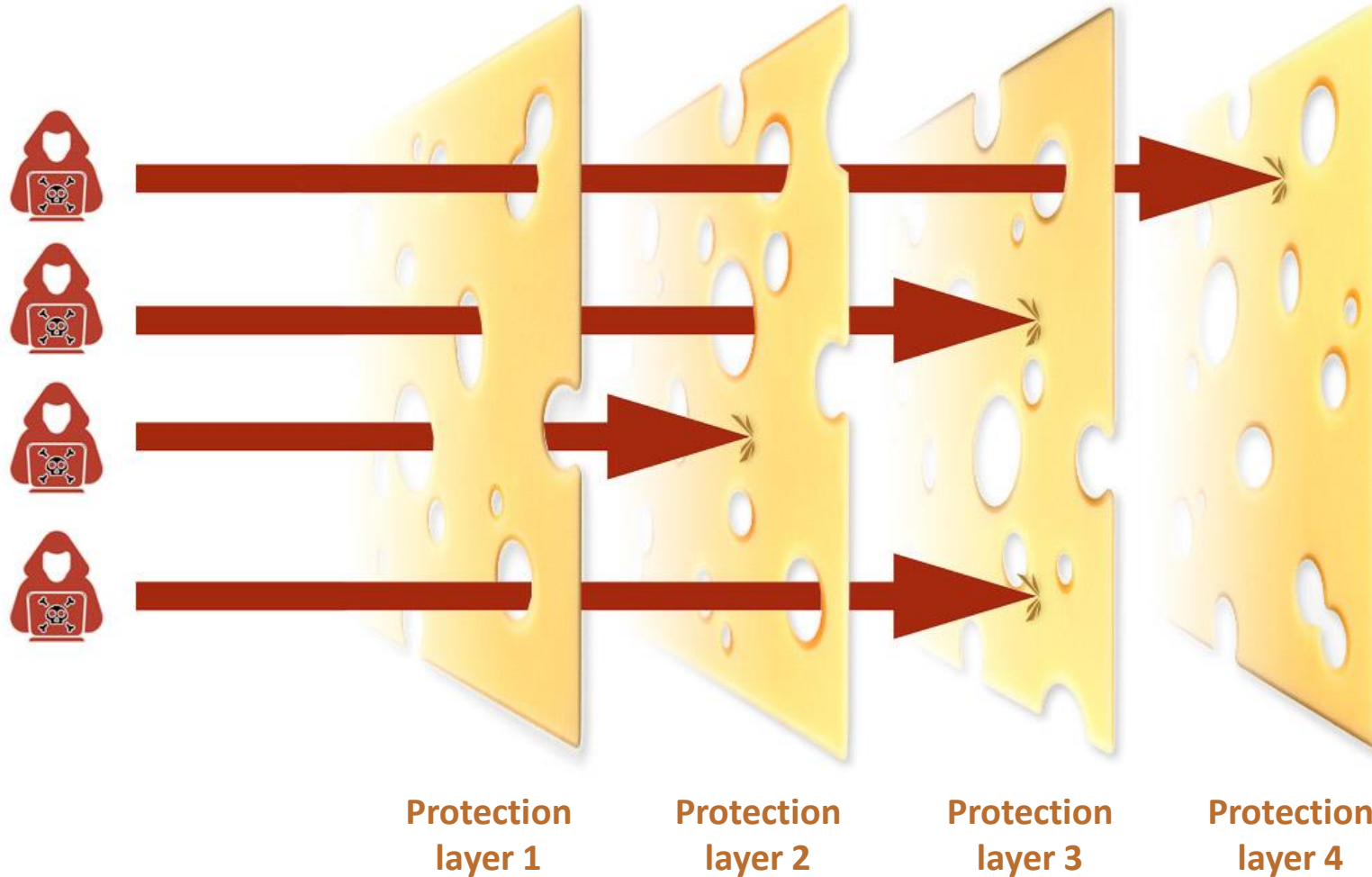
ICS/SCADA – How To Make It More Secure?

1. Map the network
2. Identify all your IT assets
3. Identify critical systems
4. Reduce the attack surface
5. Patch and update
6. Never “assume” security. Always have it tested!



Defense In Depth Is As Swiss Cheese...

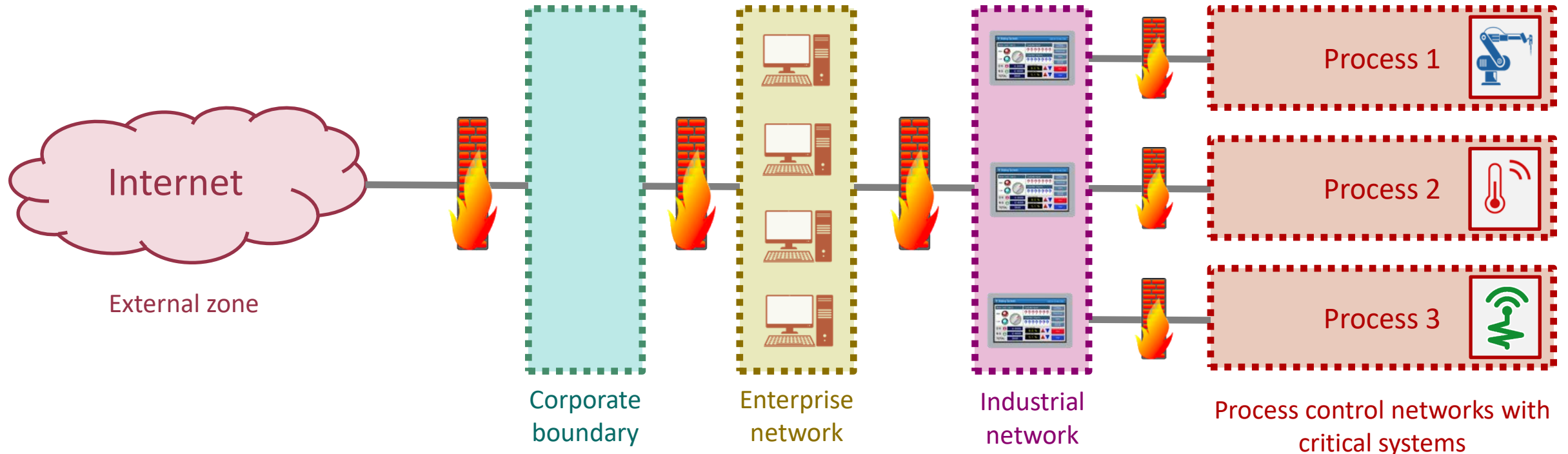
ATTACKS



Industrial network, ICS/SCADA systems

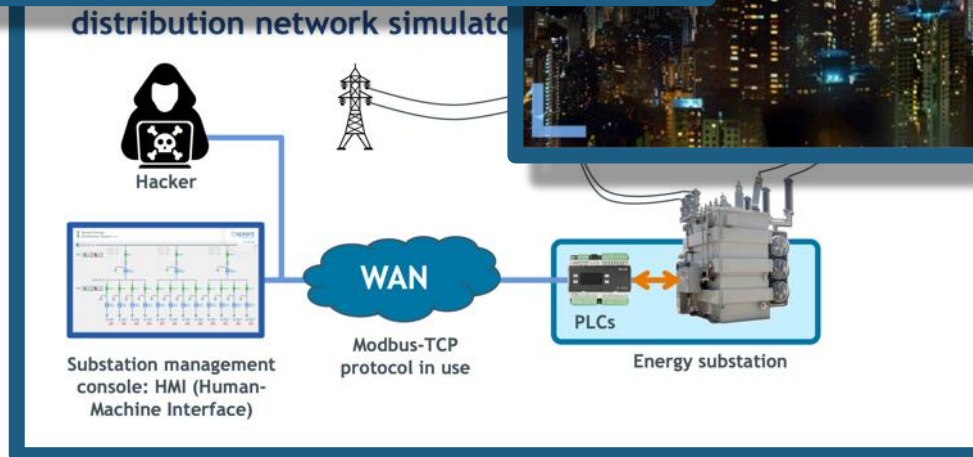
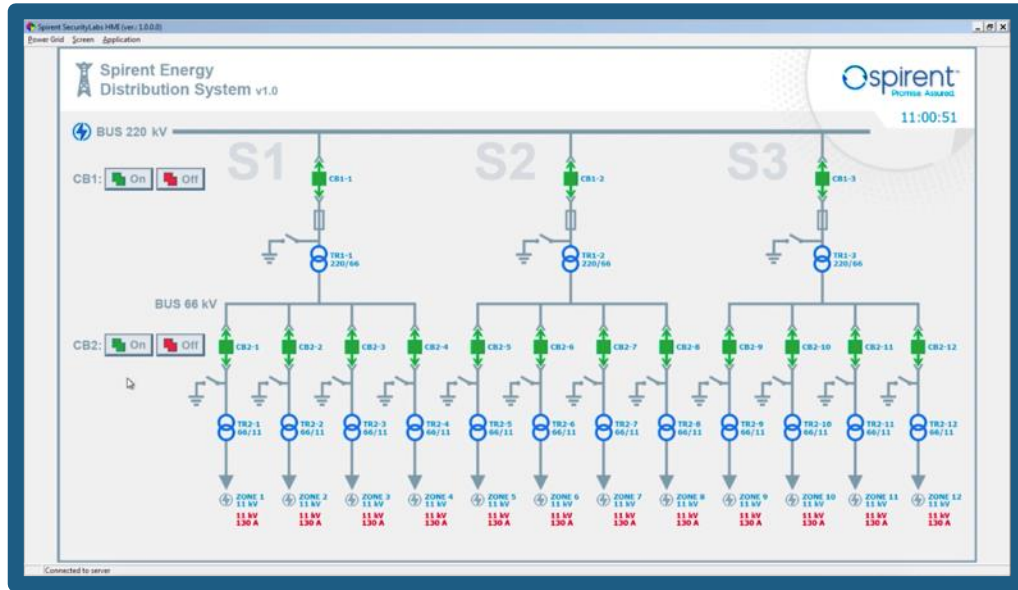
Use Network Segmentation

- **Physical segmentation** generally would be the best approach but might not be easy to implement in the already existing environment
- **Virtual network segmentation** is a logical separation of the network to VLANs with a thorough traffic control



Education Is a Key To Success

Hacking Energy Distribution System
(live demo at the Spirent booth)



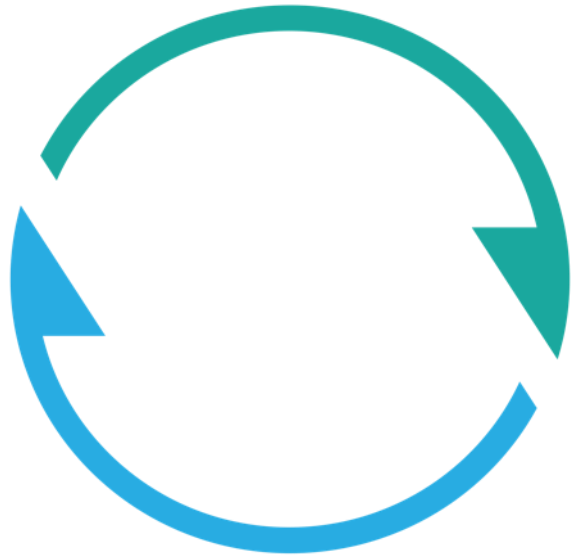
KEY TAKEAWAYS

Key Takeaways

- A **holistic approach** to security is a key to success
- People are (still) making **mistakes**, no matter what they do
- The newest **technology does not help** if the right policies are not in place
- There is **no perfect airgap**. Let's just admit it. And there will never be.
- WEB AND Mobile ICS remote clients bring **well-known attack vectors to ICS** (XSS, SQL inj., CSRF, LFI, RFI, etc.)
- Applying basic security principles, such as **“defense in depth”** and network segmentation help to secure the environment and slow down attacks



QUESTIONS



Thank you!

w: <https://www.spirent.com/Products/SecurityLabs>

e: securityLabs@spirent.com

Aleksander Gorkowienko

e: aleksander.gorkowienko@spirent.com

m: +44 (0) 7974431025