



SECURING OIL AND GAS PRODUCTION SYSTEMS FROM CYBER-ATTACK

Aleksander Gorkowienko

- Principal IT Security Consultant, CREST ACE certified
- More than 14 years in IT business, wide experience
- Areas of special interest:
 - Web application security
 - Security of IoT and embedded devices
 - Security of ICS/SCADA
 - Mobile security
 - Social engineering
- Author of exploitation tools and security training courses
- Contact: Aleksander.Gorkowienko@paconsulting.com

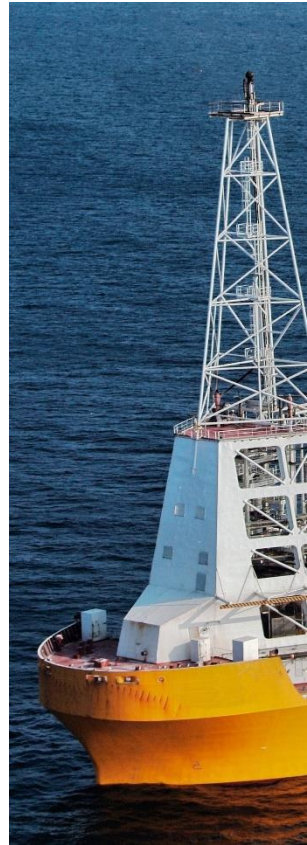
What FPSO is?

A **floating production storage and offloading (FPSO)** unit is a floating vessel used by the offshore oil and gas industry 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 or, less frequently, transported through a pipeline.

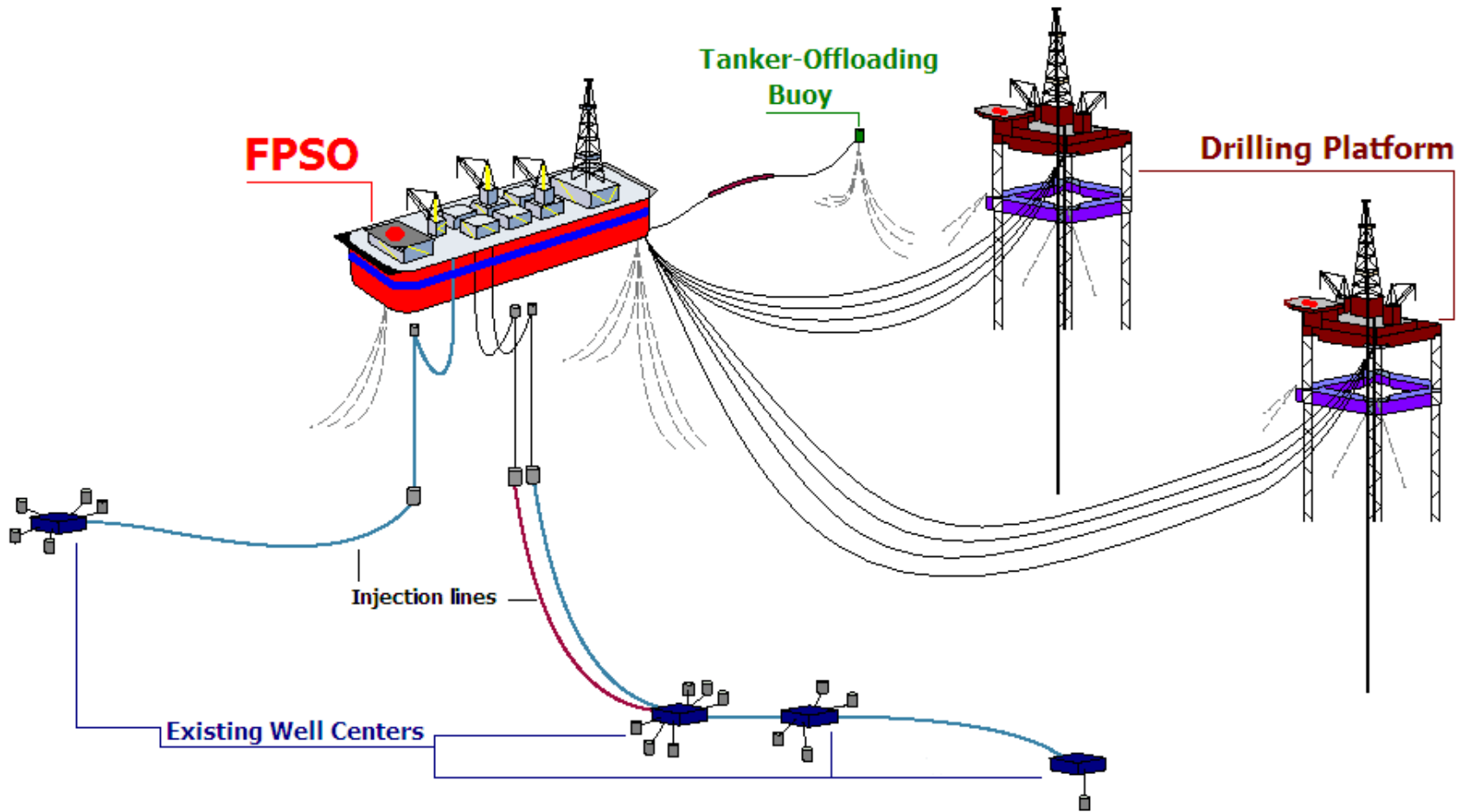
FPSOs are preferred in frontier offshore regions as they are easy to install, and do not require a local pipeline infrastructure to export oil.

FPSOs can be a conversion of an oil tanker or can be a vessel built specially for the application.



Source: https://en.wikipedia.org/wiki/Floating_production_storage_and_offloading

What FPSO is?

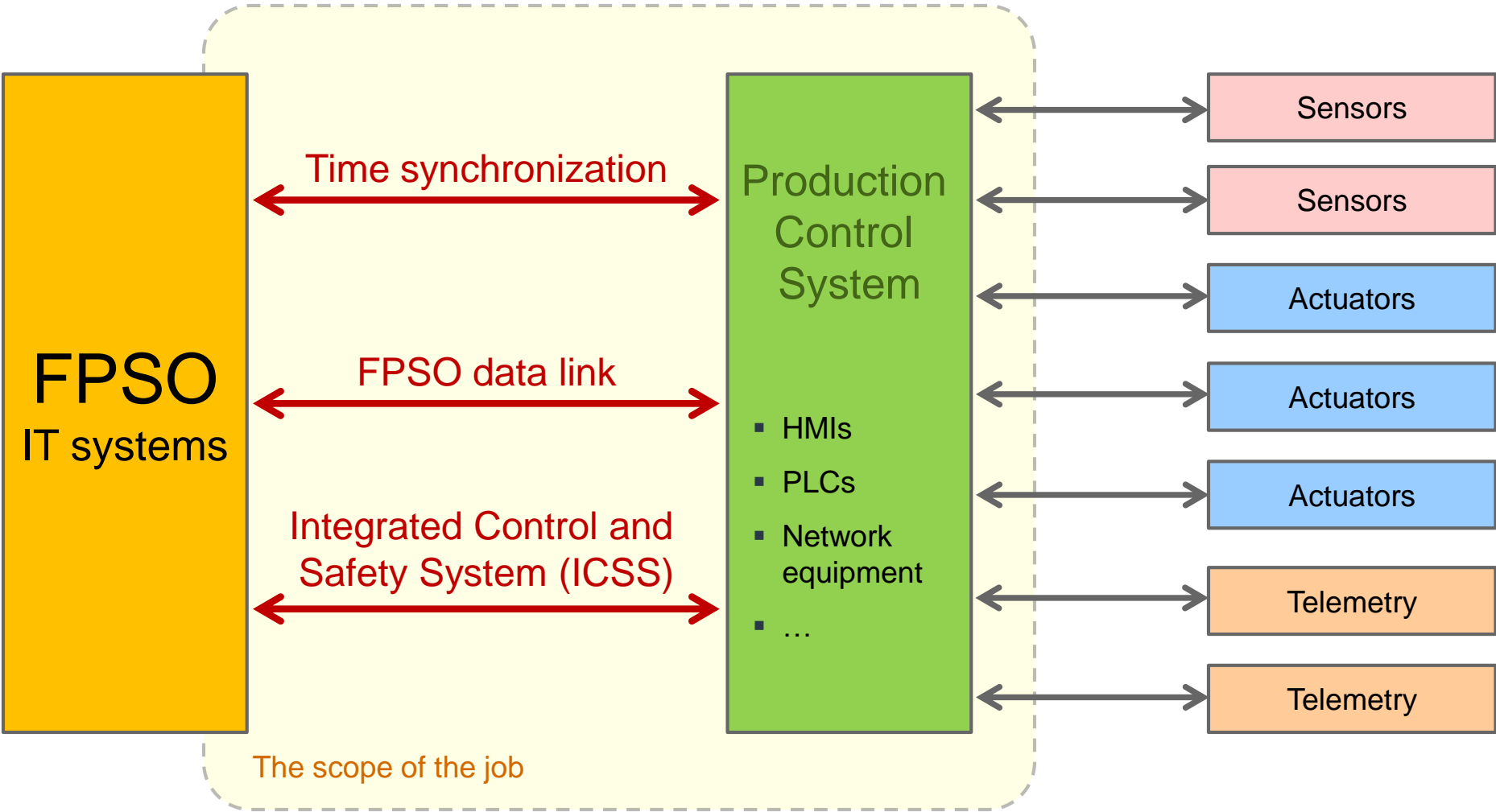


Source: https://en.wikipedia.org/wiki/Floating_production_storage_and_offloading

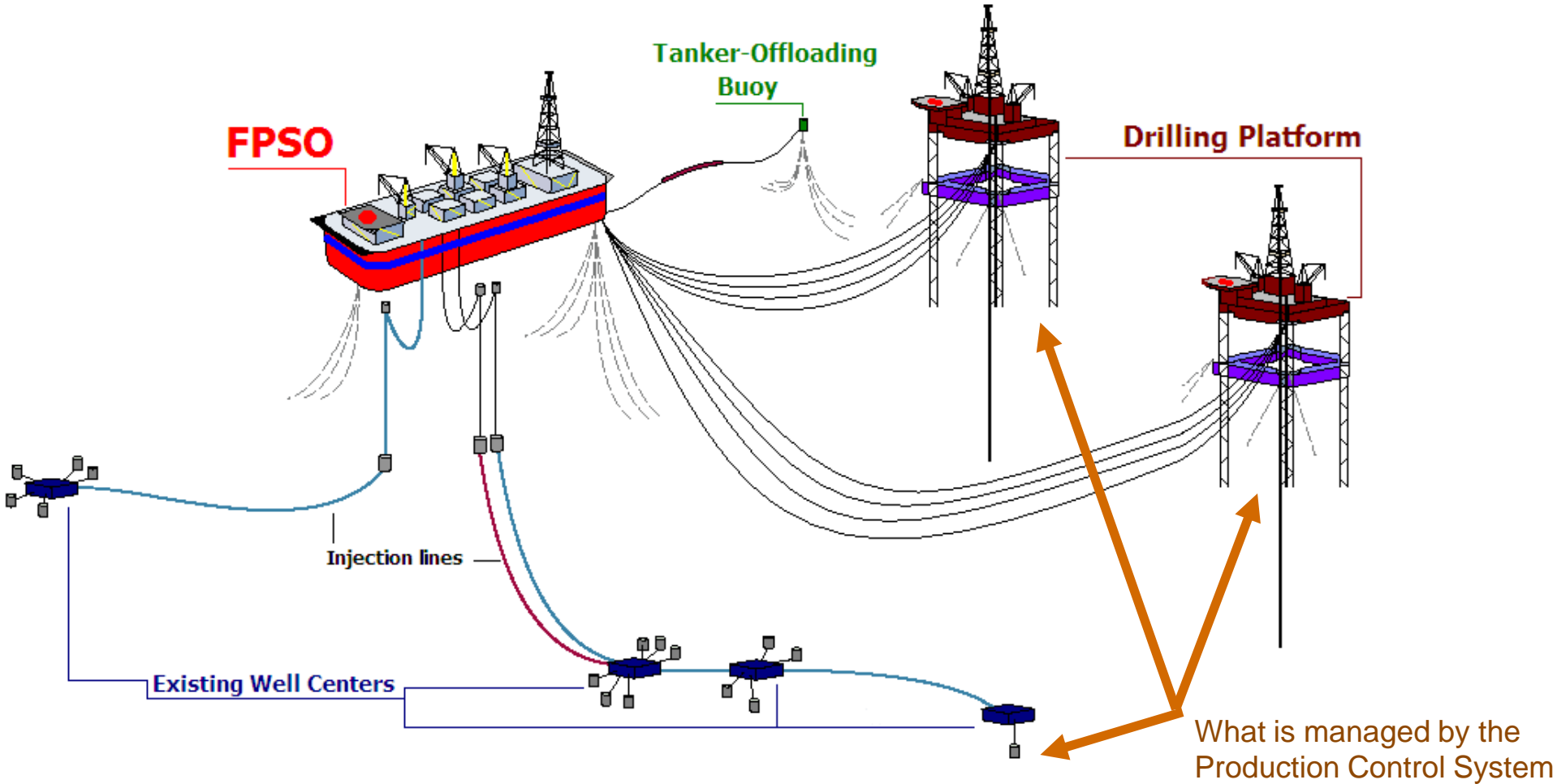
The objective

- Review security features of the Oil and Gas Production System solution provided by the vendor/supplier. The production system featured a number of servers, HMIs, PLCs, Ethernet networks and associated networking equipment that were crucial for the operation of the system
- Identify and rank vulnerabilities
- Test intrusion detection and response capabilities of the system
- Test the solution from both: unauthorised and authorised user perspective
- Check the network resilience to a denial of service attack
- Verify portable media security

The objective



Oil and gas production managed by the solution we have tested



Source: https://en.wikipedia.org/wiki/Floating_production_storage_and_offloading

Interesting facts

- The Production Control System (the one in scope) was designed in a number of years by a group of world-class engineers and software developers.
- The average price for offshore oil-drilling rigs is approximately £650 million up to £1 billion
- The average cost of daily operation on oil rig is £150000 - £250000
- Oil rigs are commonly referred to as “floating cities,” since many different people live on them at any given time. It’s also fun to note that most offshore oil rigs are taller than the world’s biggest skyscrapers.
- World’s Deepest Offshore Well: Back in September 2009, Transocean’s Deepwater Horizon hit a depth of 10,683 meters, making it the deepest well in the world. The record was short-lived as the Deepwater Horizon blew up just over six months later.



Source: <http://www.offshore-mag.com>

Findings

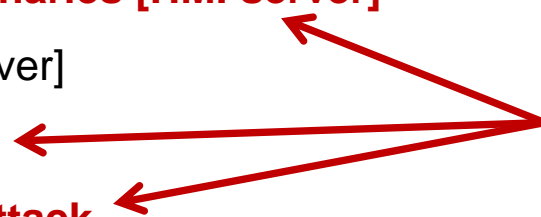
FINDINGS



Non-exhaustive list of findings

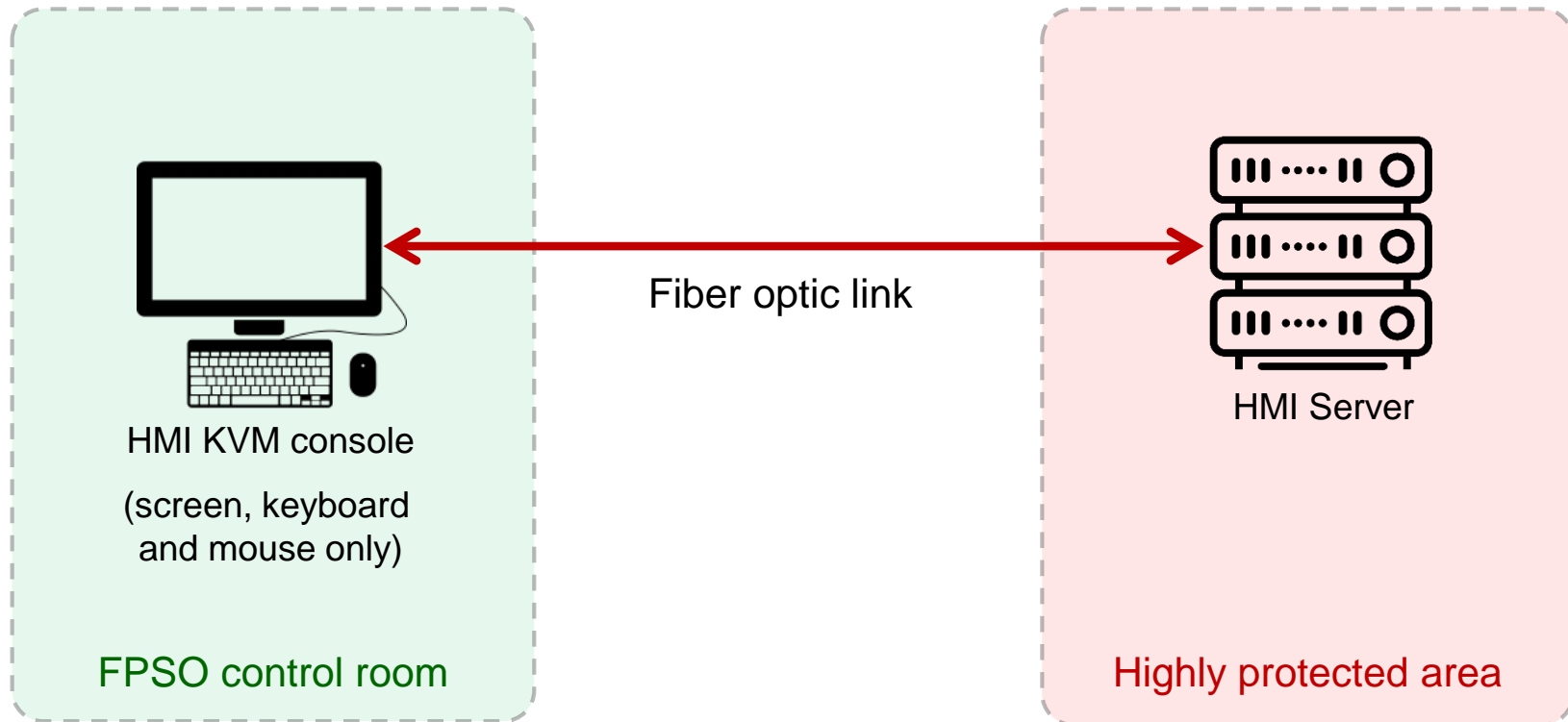
- ...
- **Unauthorised bidirectional transfer of data and binaries [HMI server]**
- Unauthorised Access & Privilege Escalation [HMI server]
- **PLC is Vulnerable to the Man in the Middle Attack**
- **NTP Server Vulnerable to the Man in the Middle Attack**
- Windows Services Can Be Reconfigured By Non-Admin Users [HMI server]
- Insecure Permissions on Program Files and Services [HMI server]
- Potentially Unnecessary Open Ports [HMI workstation subnet, PDI]
- Multiple Transport Layer Encryption Weaknesses
- ...
- ...

**We shall focus
on these issues
only**



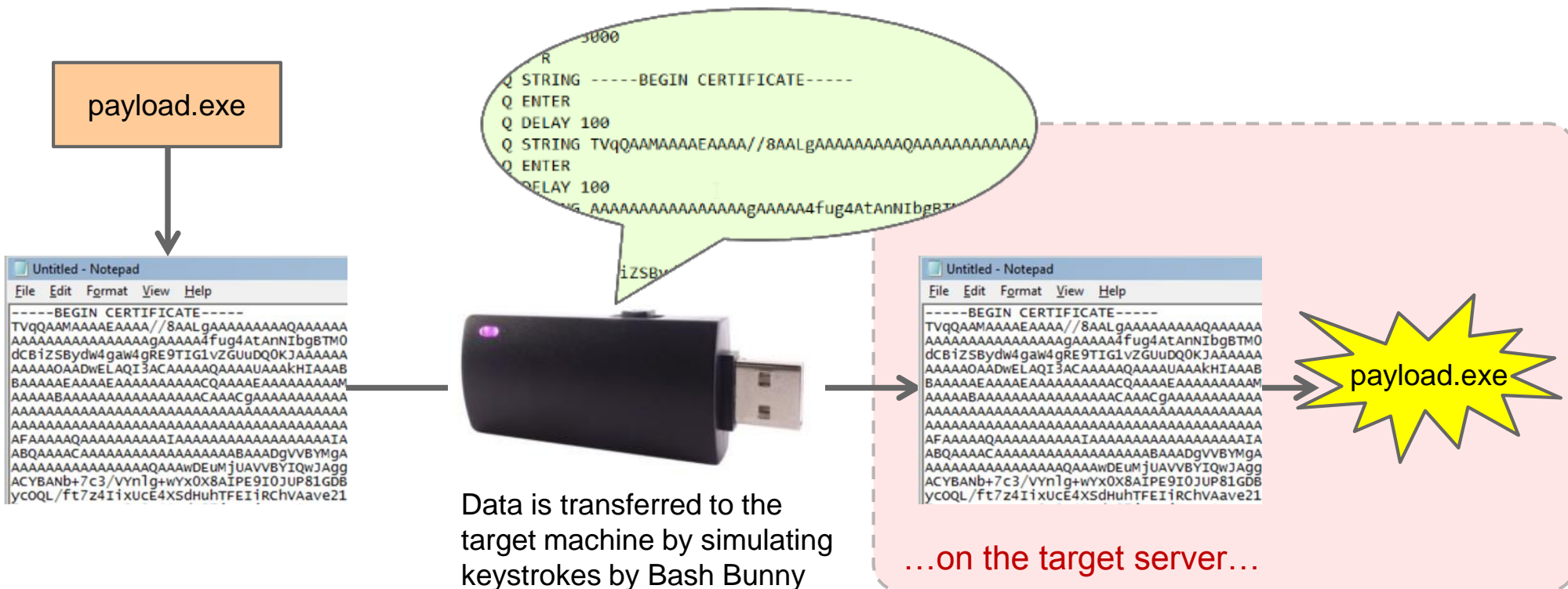
Takeover the “air gapped” server

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



Transferring any binary to the server using a “virtual keyboard”

- Windows 7 was identified on the server
- The certutil.exe tool was found on the server (a part of the default installation). Yes, notepad.exe was also there. :-)
- Bash Bunny connected to the KVM instead of the whitelisted keyboard mimicking the exact USB device ID
- The “malicious” binary has been successfully transferred to the remote server and recovered by certutil.exe



Transferring data back from the remote server

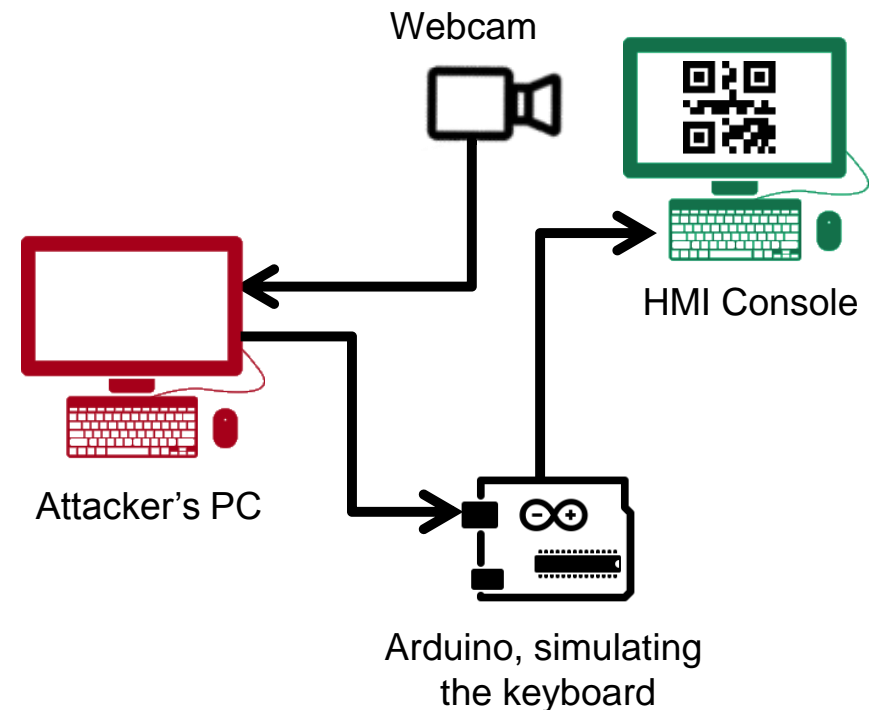
- Transferring a custom-built utility (.exe) to the target server using the technique described in the previous step
- Run the utility, drag-and-drop any file to it – the content is on the screen transformed to a QR codes!



Further steps

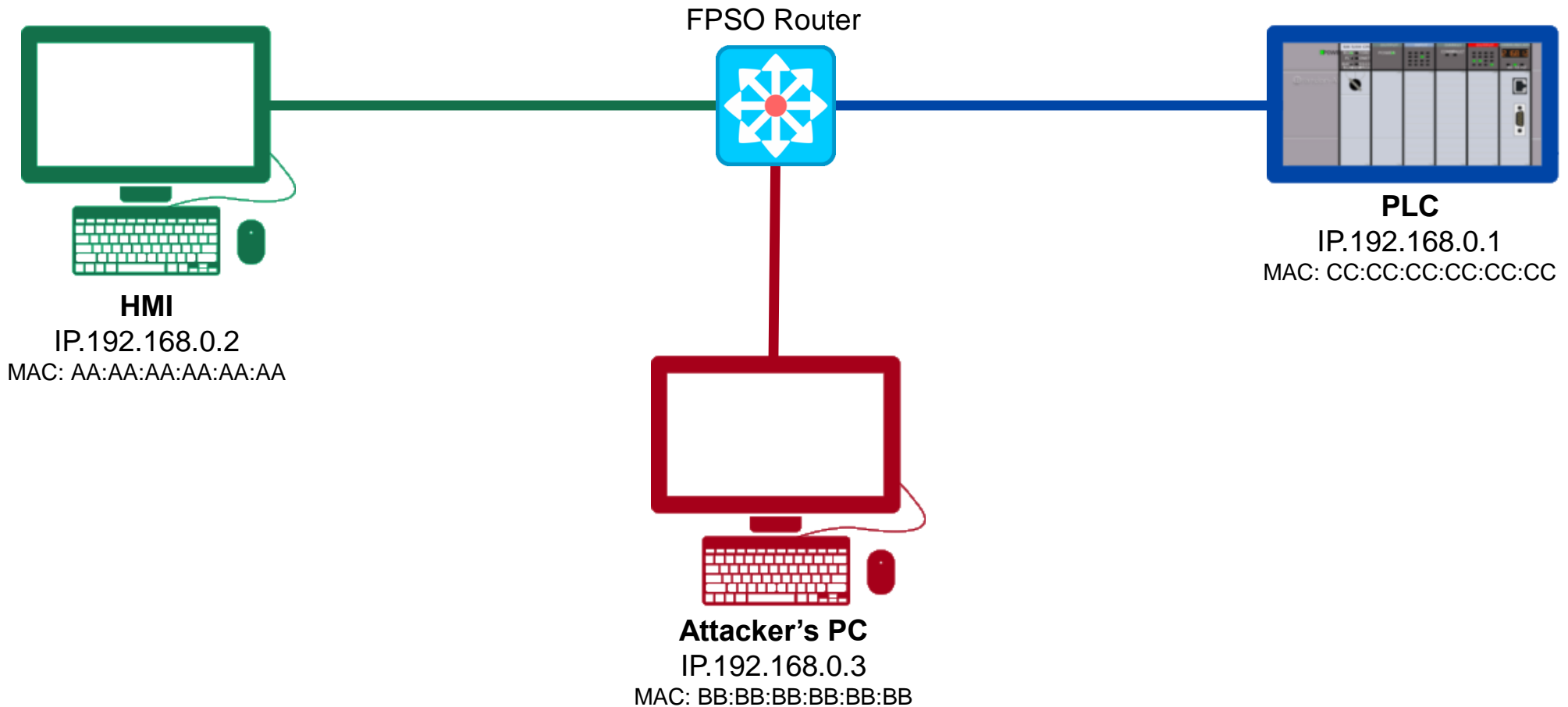
IP over QRcode

- Source project:
<https://github.com/seiferteric/qrtun>
- Implementation of a tunnel (tun) interface to send bidirectional data using QR codes displayed on a monitor and read using a webcam :)
- Proof of concept with a webcam facing the HMI screen (“reading” data) and Arduino Leonardo simulating a keyboard (“writing” data).
- The approach can provide much better (but still quite slow) access to the remote machine



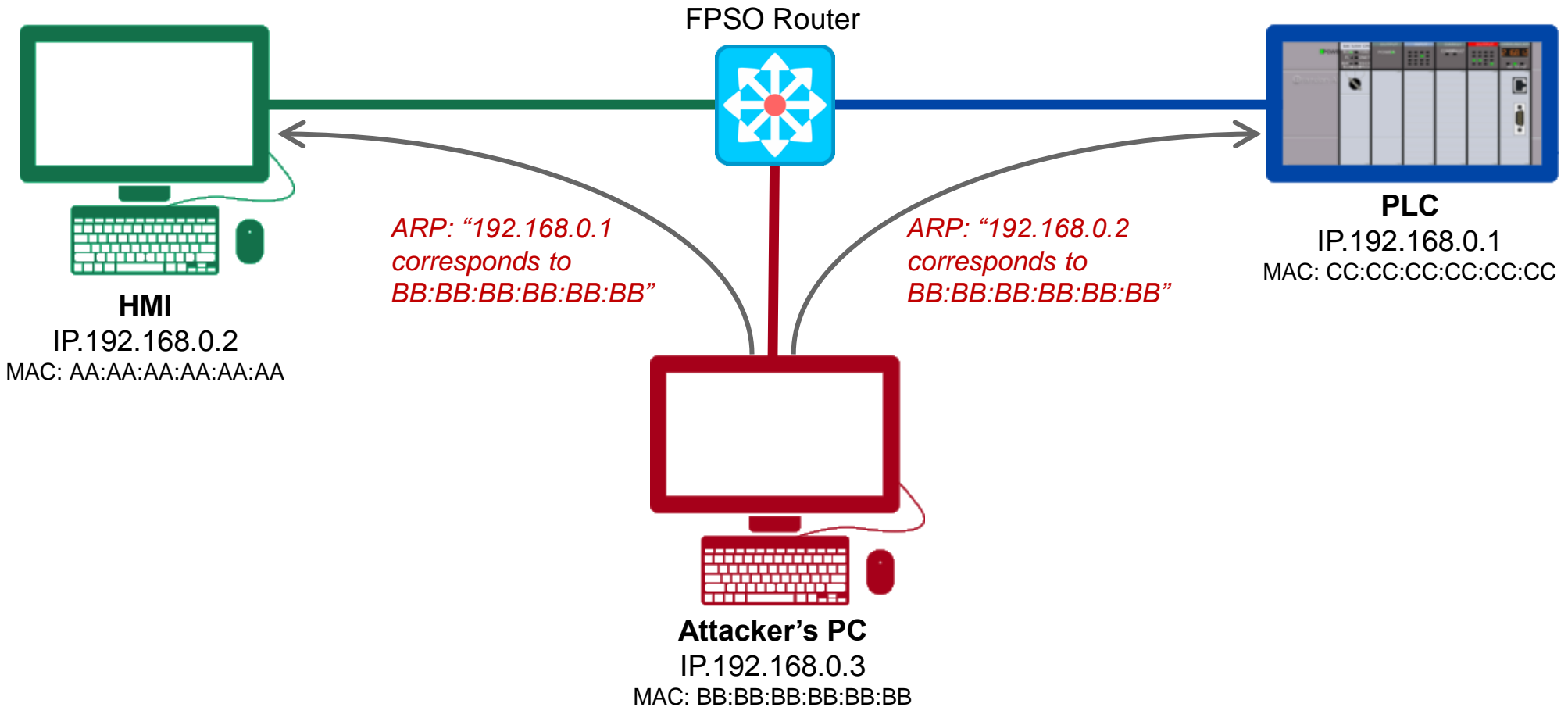
Man in The Middle (MiTM) attack

- MiTM attack was successfully conducted by exploiting the ARP spoofing technique



Man in The Middle (MiTM) attack

- The attacker is sending ARP messages, redirecting all traffic between parties to himself.



The tool we used for MiTM

- We have used ettercap tool from the Kali Linux distro

```
Terminal - root@KALI: ~/PLC MITM 2017/MITM/modbus-swap-request-static-1563
File Edit View Terminal Tabs Help
ettercap 0.8.2 copyright 2001-2015 Ettercap Development Team
Content filters loaded from ./mb_mitm_modbus_swap_request.ig...
Listening on:
  eth0 -> [redacted]
[redacted]
[redacted]

SSL dissection needs a valid 'redir_command_on' script in the etter.conf file
Privileges dropped to EUID 65534 EGID 65534...

  33 plugins
  42 protocol dissectors
  57 ports monitored
20388 mac vendor fingerprint
1766 tcp OS fingerprint
2182 known services
Lua: no scripts were specified, not starting up!

Randomizing 1023 hosts for scanning...
Scanning the whole netmask for 1023 hosts...
* |=====>| 100.00 %

Scanning for merged targets (1 hosts)...
* |=====>| 100.00 %
```

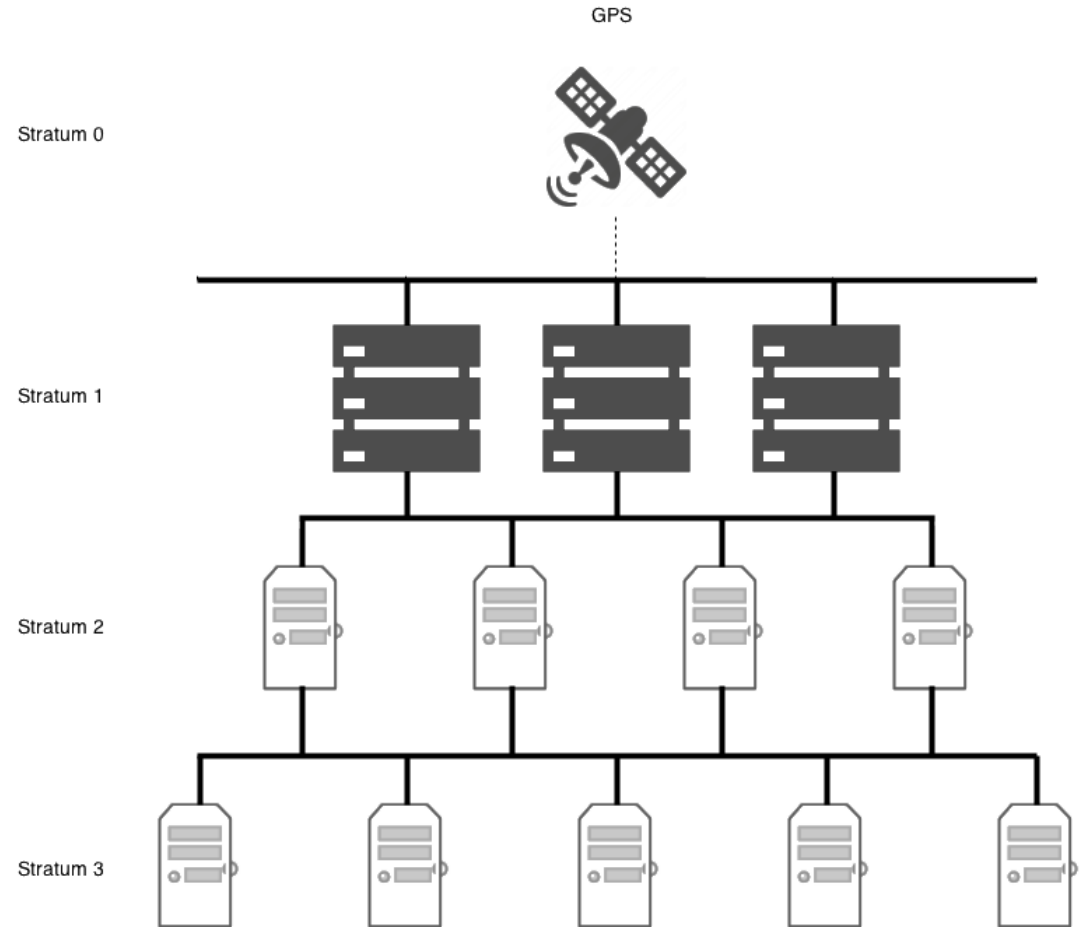
What attacker could do with MiTM?

- Attacker can sniff network traffic and passively collect sensitive plain text information
- 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 time stamp for operation logs and all dependent devices



Attacking NTP server

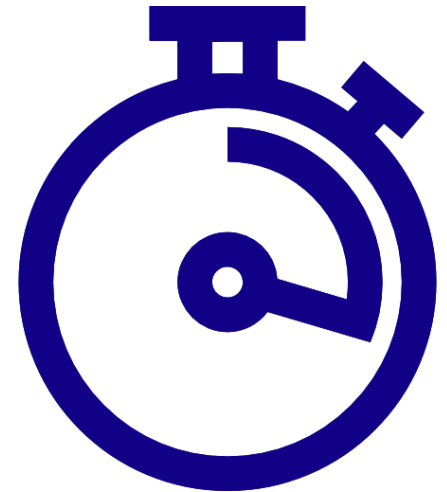
Network Time Protocol is a hierarchical protocol and is divided into stratum which define the distance from the reference clock. A reference clock source that relays UTC (Coordinated Universal Time) time and has little or no delay is known as a stratum-0 device.



The Challenge

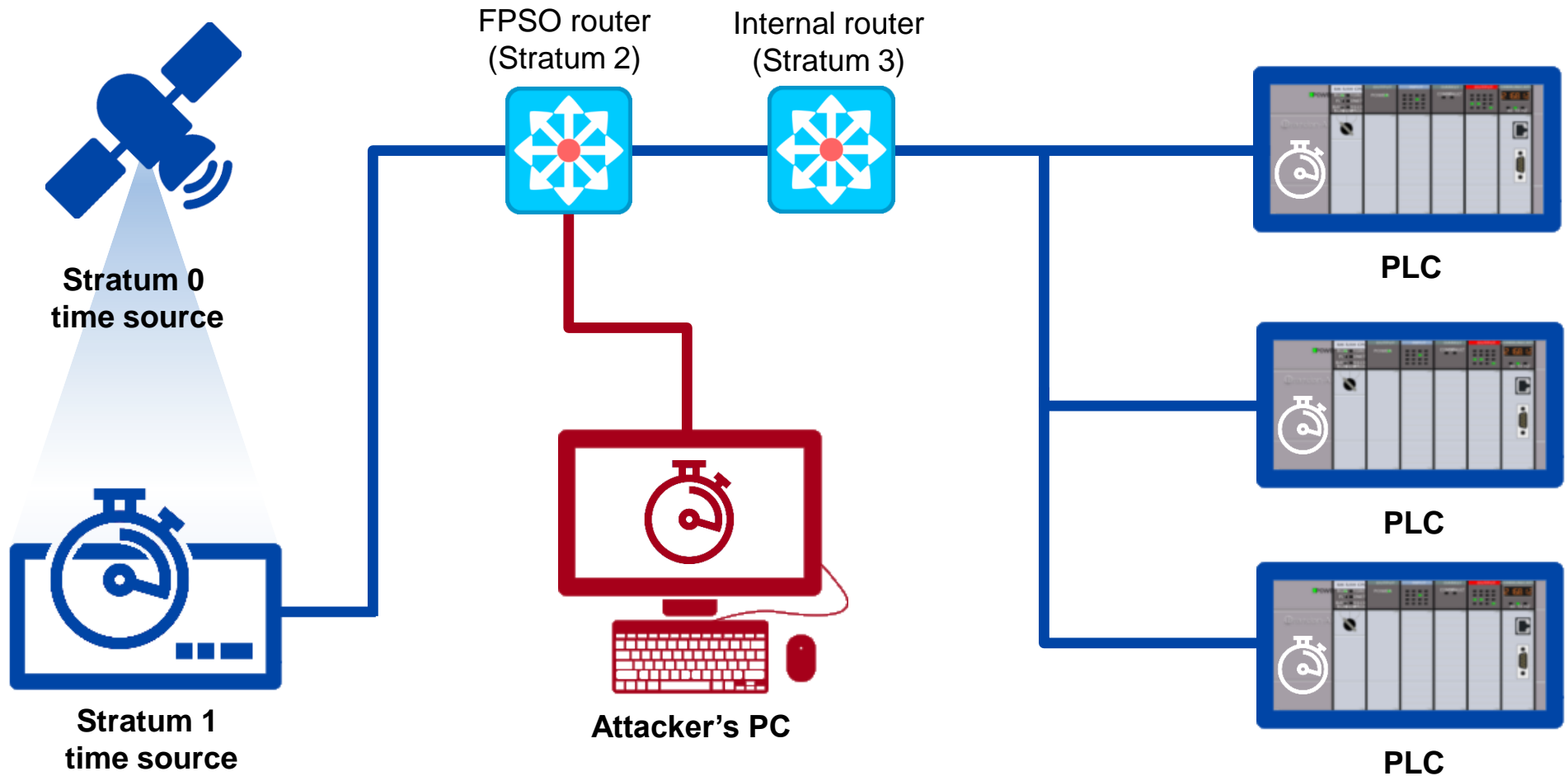
If a network switch detects that the time difference between the timestamp from its internal clock and the data provided by the NTP server is too big – it will ignore the source of the incorrect information. So the “fake” NTP server will be blacklisted.

We can do a Denial of Service (DoS) attack, that’s true. But can we still enforce the switch to use the incorrect timestamp?...



Yes, we can!

- We can gradually “drift” from the correct time and increase the time difference error step by step



The algorithm on the attacker's PC

1. Set the TimeDelta variable to zero
2. Intercept the NTP packet (response from the NTP server)
3. Increase TimeDelta variable ($\text{TimeDelta} = \text{TimeDelta} + 1 \text{ sec}$)
4. Replace time stamp in the intercepted packet with the new fake data
5. Pass through the modified NTP packet back to its destination
6. Wait for another intercepted NTP packet



...

Lessons learned

Lessons learned for the vendor

- Never “assume security”. Always test it!
- Know: it is always better (and cheaper) to prevent disaster rather than react
- Beware of attacks from malicious insiders. These are very difficult to detect.
- Apply the Principle of Least Privilege globally
- Get rid of unnecessary software on your workstations and servers
- Security should be an integral part of the software (and hardware) development cycle

...

Questions?...

...

Thank you!