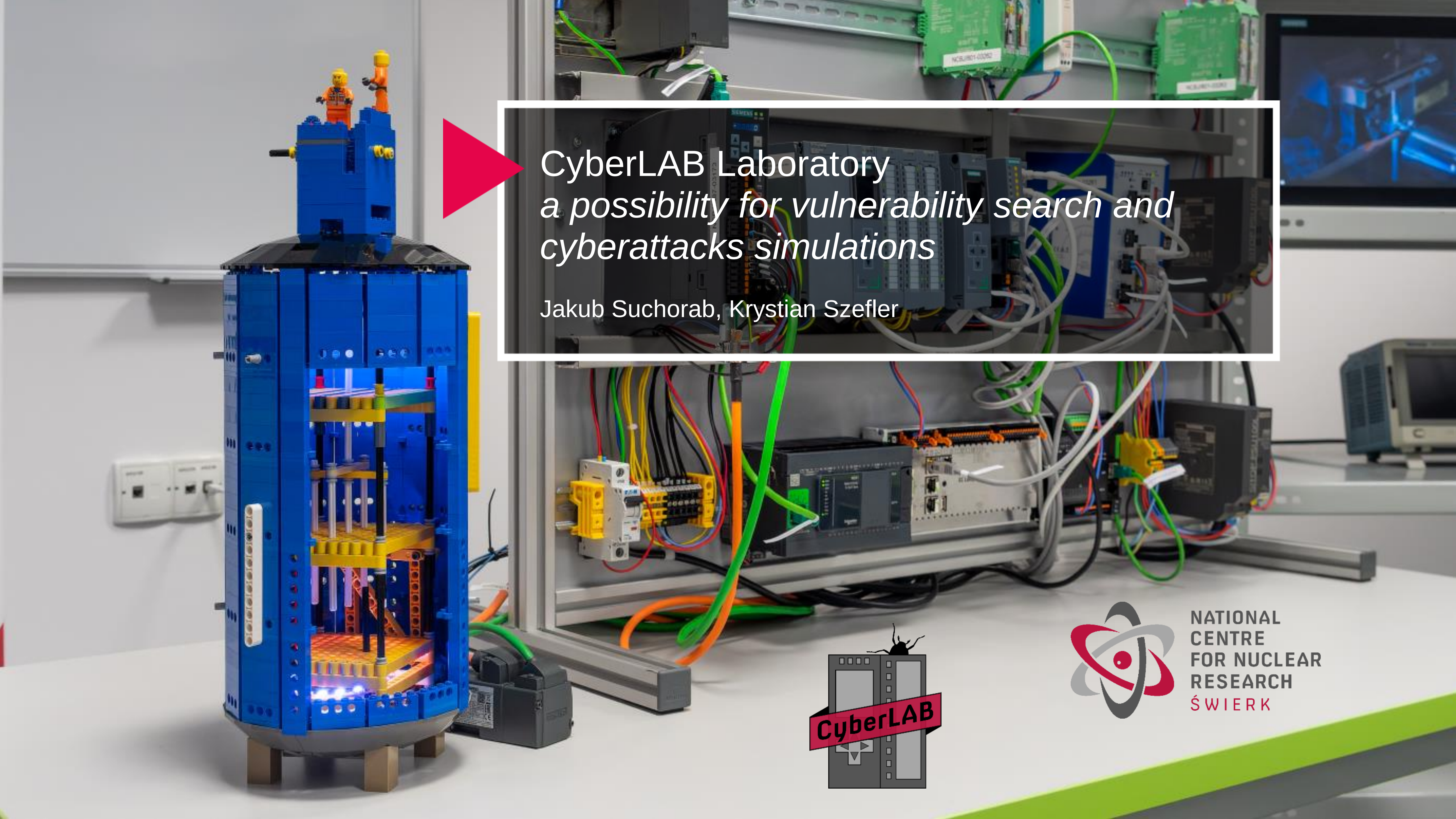


CyberLAB Laboratory

a possibility for vulnerability search and cyberattacks simulations

Jakub Suchorab, Krystian Szefler

CyberLAB

NATIONAL
CENTRE
FOR NUCLEAR
RESEARCH
ŚWIERK

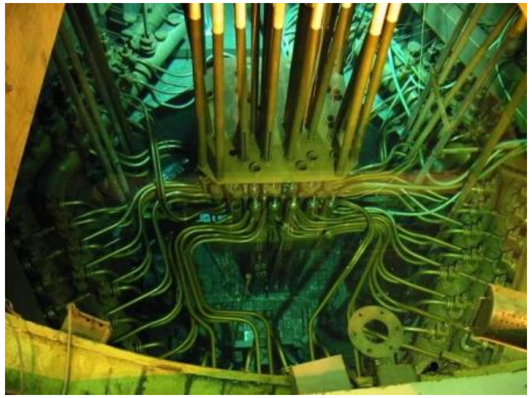
Presentation outline

- Creation of CyberLAB
- Industrial devices vulnerability testing
- Threat scenario for a nuclear power plant
- Summary

National Centre for Nuclear Research (NCBJ)

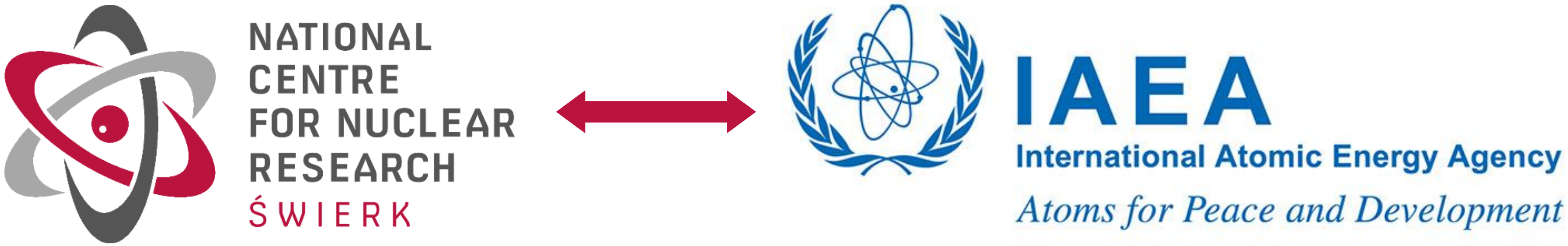
NATIONAL CENTRE FOR NUCLEAR RESEARCH ŚWIERK

- The largest research Institute in Poland (over 1100 employees, about 70 Professors, over 200 PhDs);
- The sole research nuclear reactor in Poland – MARIA, power 30MW;
- Strategic goals:
  - developing nuclear technologies and promoting practical applications of nuclear physics methods;
  - developing specialized devices (accelerators, detectors) for research, industry and medicine;



NCBJ – IAEA cooperation

- Research grant for a cybersecurity project
- Project title: “Testing of PLCs Used in Nuclear Installations by Fuzzing methodology for Cyber Vulnerabilities”


NATIONAL CENTRE FOR NUCLEAR RESEARCH
ŚWIERK
IAEA
International Atomic Energy Agency
Atoms for Peace and Development

International project coordinated by IAEA (CRP)

„Enhancing Computer Security Incident Analysis at Nuclear Facilities”

Comisión Nacional de Energía Atómica

Austrian Institute of Technology

Areva

University of São Paulo

Canadian Nuclear Laboratories

Bruce Power

Tsinghua University

Otto von Guericke University Magdeburg

Nuclear Regulatory Authority

CrySyS Lab

Instituto Nacional de Investigaciones Nucleares

Korea Institute of Nuclear Nonproliferation and Control

Korea Atomic Energy Research Institute

Atomic Energy Commission

National Centre for Nuclear Research

Mitre

Idaho National Laboratory

Underwriters Laboratories

UMass Lowell

13 contries, 20 institutes

General project objectives

- Improve computer security capabilities at the nuclear facilities:
  - prevention of
  - detection of
  - response to

  computer security incidents that can affect nuclear safety and nuclear security

- Establish international community of experts to provide exchange of good practices in the field of computer security incident response at nuclear facilities;

CyberLAB

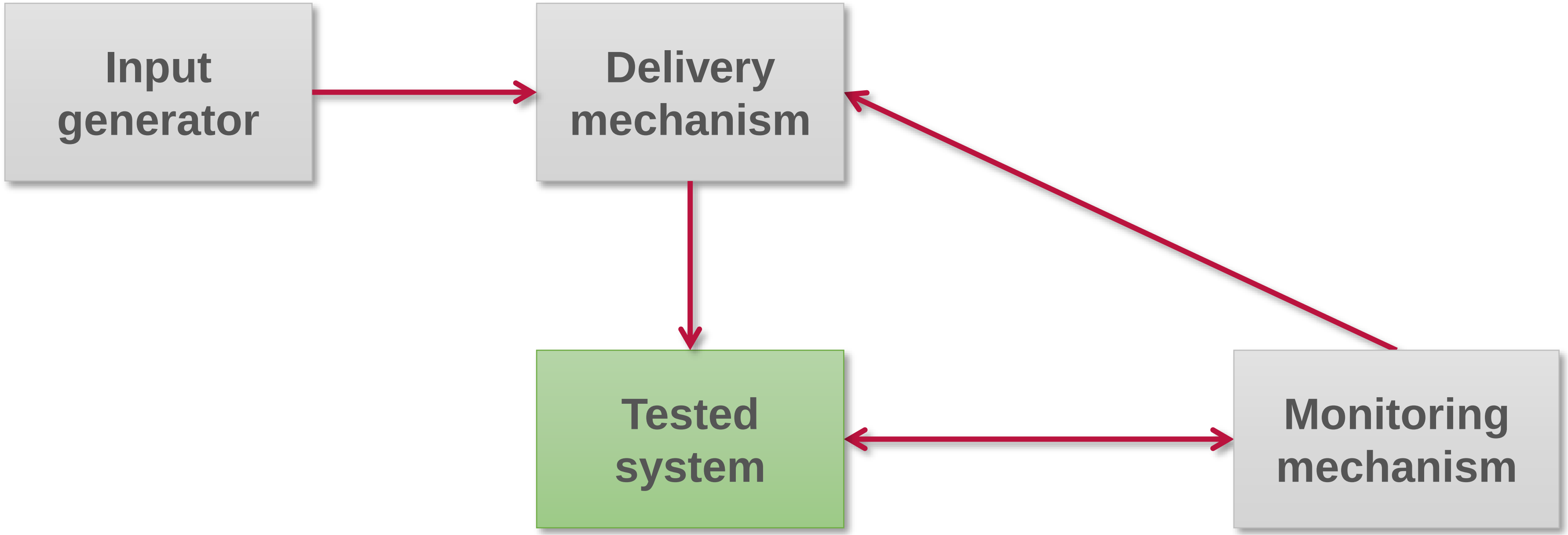
NATIONAL CENTRE FOR NUCLEAR RESEARCH ŚWIERK

- A research group focused on cybersecurity of industrial systems;
- Vulnerability research of programmable logic controllers (PLCs) using fuzz testing method;
- Preparing threat scenarios using a nuclear power plant simulator;

Ministerstwo Klimatu i Środowiska
Konferencja
Cyberbezpieczeństwo sektora energii – przedstawienie rekomendacji sektorowych
15 października 2021 r.

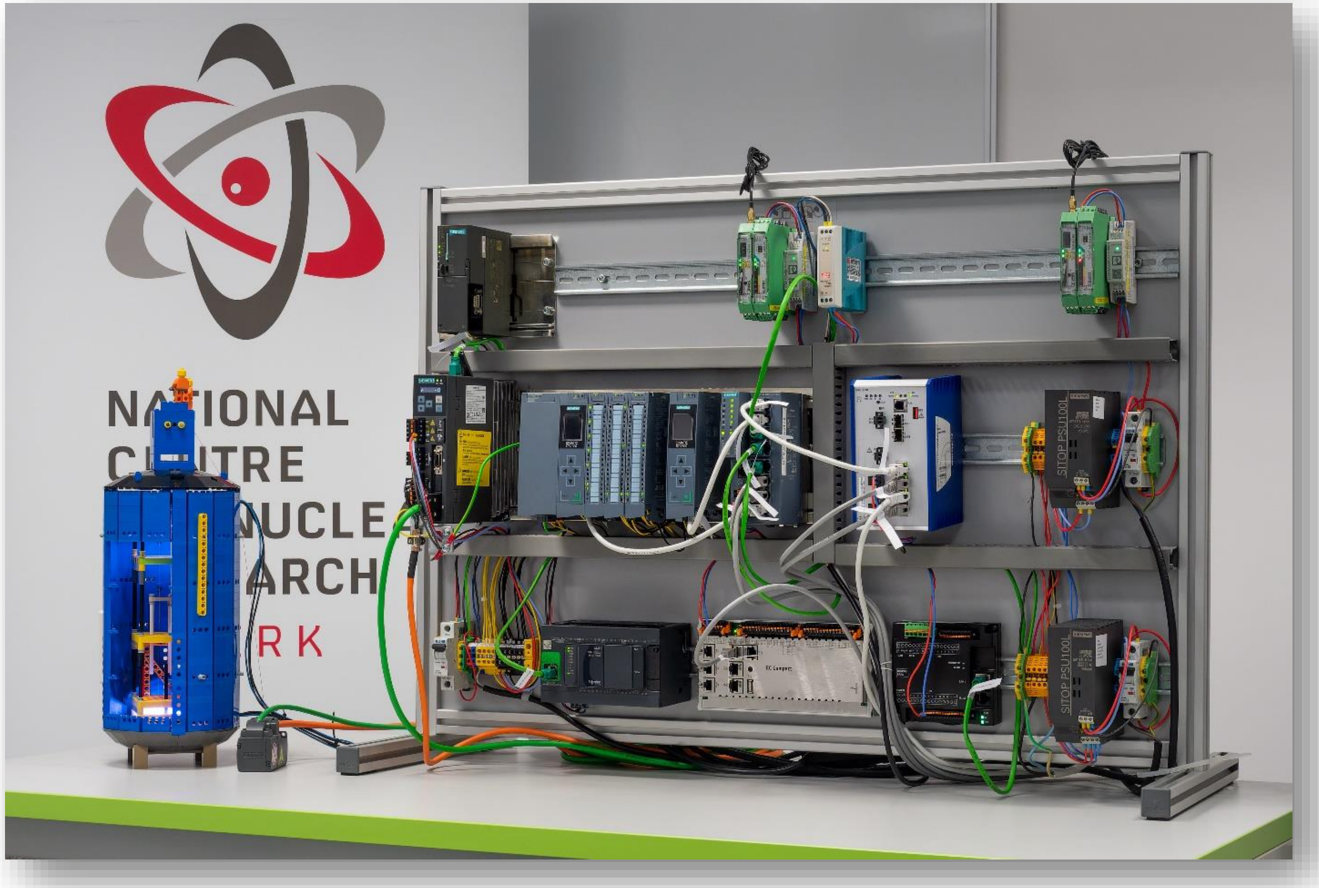
NATIONAL CENTRE FOR NUCLEAR RESEARCH ŚWIERK
EFFECTIVE FUZZ TESTING FOR PROGRAMMABLE LOGIC CONTROLLERS VULNERABILITY RESEARCH TO ENSURE NUCLEAR SAFETY
IAEA-CN-278/619 Paper presentation

Fuzzing



Source: M. Almgren, D. Balzarotti, J. Stijohann i E. Zambon *Report on automated vulnerability discovery techniques*

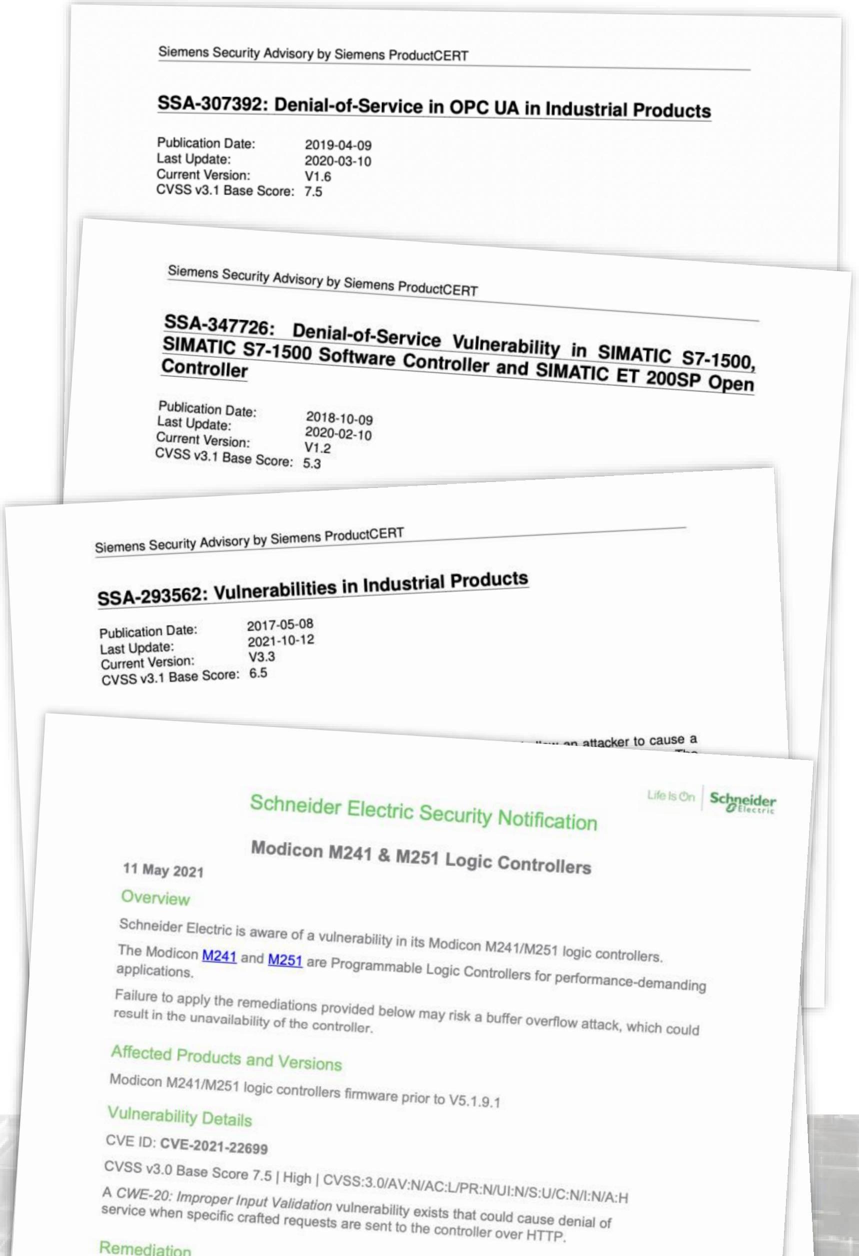
Laboratory


SITOP PSU100L
SITOP PSU100L

Fundamental research
The MARIA reactor
Radiopharmaceuticals
Materials science
www.ncbj.gov.pl

Found vulnerabilities

- A zero-day IPv4 vulnerability in Siemens S7-1500 PLCs;
- One previously known vulnerability in S7-300 PLCs in Profinet DCP;
- OPC-UA vulnerability in S7-1500 PLCs;
  (found by Siemens CERT just before us, fixed right after our discovery);
- A zero-day vulnerability in Schneider Electric M241 in HTTP;
- Potentially exploitable feature in SE M241 that allows a low cost DOS on TCP stack;



Siemens Security Advisory by Siemens ProductCERT

SSA-307392: Denial-of-Service in OPC UA in Industrial Products

Publication Date:	2019-04-09
Last Update:	2020-03-10
Current Version:	V1.6
CVSS v3.1 Base Score:	7.5

Siemens Security Advisory by Siemens ProductCERT

SSA-347726: Denial-of-Service Vulnerability in SIMATIC S7-1500, SIMATIC S7-1500 Software Controller and SIMATIC ET 200SP Open Controller

Publication Date:	2018-10-09
Last Update:	2020-02-10
Current Version:	V1.2
CVSS v3.1 Base Score:	5.3

Siemens Security Advisory by Siemens ProductCERT

SSA-293562: Vulnerabilities in Industrial Products

Publication Date:	2017-05-08
Last Update:	2021-10-12
Current Version:	V3.3
CVSS v3.1 Base Score:	6.5

an attacker to cause a

Schneider Electric Security Notification

Life Is On | Schneider Electric

Modicon M241 & M251 Logic Controllers

11 May 2021

Overview

Schneider Electric is aware of a vulnerability in its Modicon M241/M251 logic controllers.

The Modicon M241 and M251 are Programmable Logic Controllers for performance-demanding applications.

Failure to apply the remediations provided below may risk a buffer overflow attack, which could result in the unavailability of the controller.

Affected Products and Versions

Modicon M241/M251 logic controllers firmware prior to V5.1.9.1

Vulnerability Details

CVE ID: **CVE-2021-22699**

CVSS v3.0 Base Score 7.5 | High | CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

A *CWE-20: Improper Input Validation* vulnerability exists that could cause denial of service when specific crafted requests are sent to the controller over HTTP.

Remediation

NCBJ

IPv4 vulnerability in Siemens S7-1500

- IPv4 packet with a modified header sent about 33000 times;
- Result → **no communication with the PLC** using any IP-based protocols;
- A report including POC script sent to Siemens CERT (in line with *responsible disclosure* procedure);
- Classified as not previously known (**zero-day**);
- CVE-2018-13805 number assigned;
- The vulnerability affected all firmware versions for S7-1500 PLCs from 2.0 to 2.5;

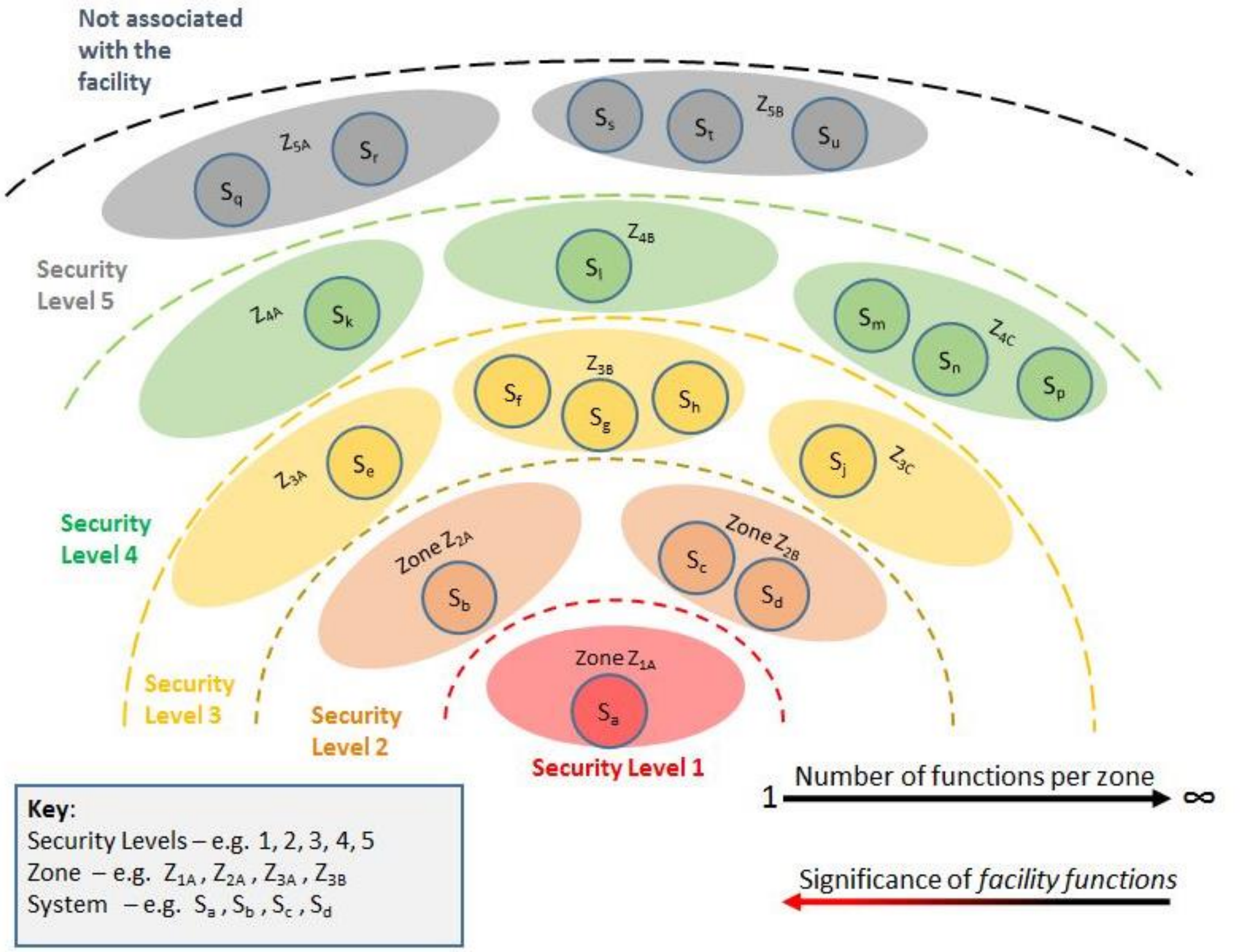
Asherah as…

- Nuclear Power Plan Simulator
  - **computer model** of nuclear power plant,
  - written in MATLAB Simulink,
  - **Hardware-in-the-loop** capable.

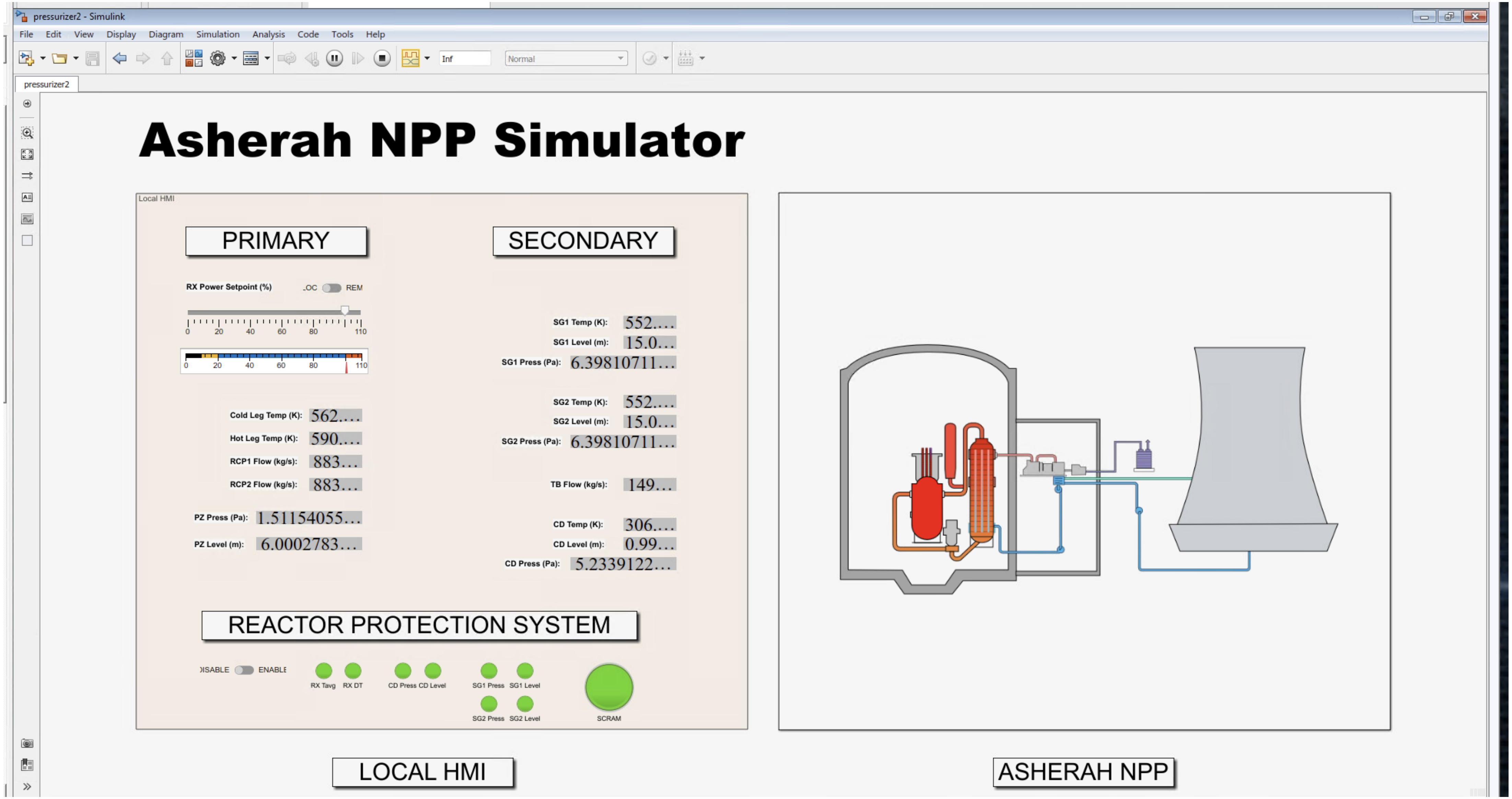
as well as

- Hypothetical facility

  built on basis of Defensive Computer Security Architecture (DCSA) proposed by the International Atomic Energy Agency (IAEA). Enforces division of the network infrastructure into security levels in order to ensure appropriate cybersecurity.



DCSA - division into security levels in nuclear power plant



Inf

Normal

Asherah NPP Simulator

PRIMARY

RX Power Setpoint (%) .OC REM

Cold Leg Temp (K): 562....

Hot Leg Temp (K): 590....

RCP1 Flow (kg/s): 883...

RCP2 Flow (kg/s): 883...

PZ Press (Pa): 1.51154055...

PZ Level (m): 6.0002783...

SECONDARY

SG1 Temp (K): 552....

SG1 Level (m): 15.0...

SG1 Press (Pa): 6.39810711...

SG2 Temp (K): 552....

SG2 Level (m): 15.0...

SG2 Press (Pa): 6.39810711...

TB Flow (kg/s): 149...

CD Temp (K): 306....

CD Level (m): 0.99...

CD Press (Pa): 5.2339122...

REACTOR PROTECTION SYSTEM

)ISABLE ENABLE

LOCAL HMI

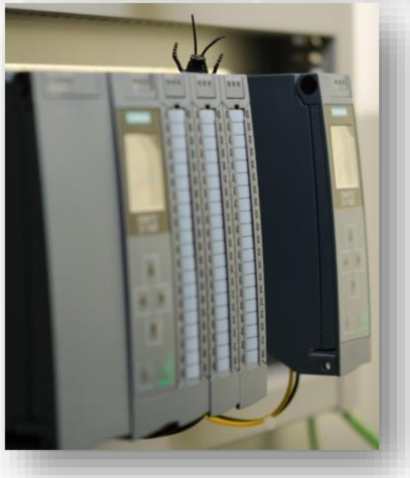
ASHERAH NPP

Test Bed

Server with VMware vSphere – ESXi + vCenter

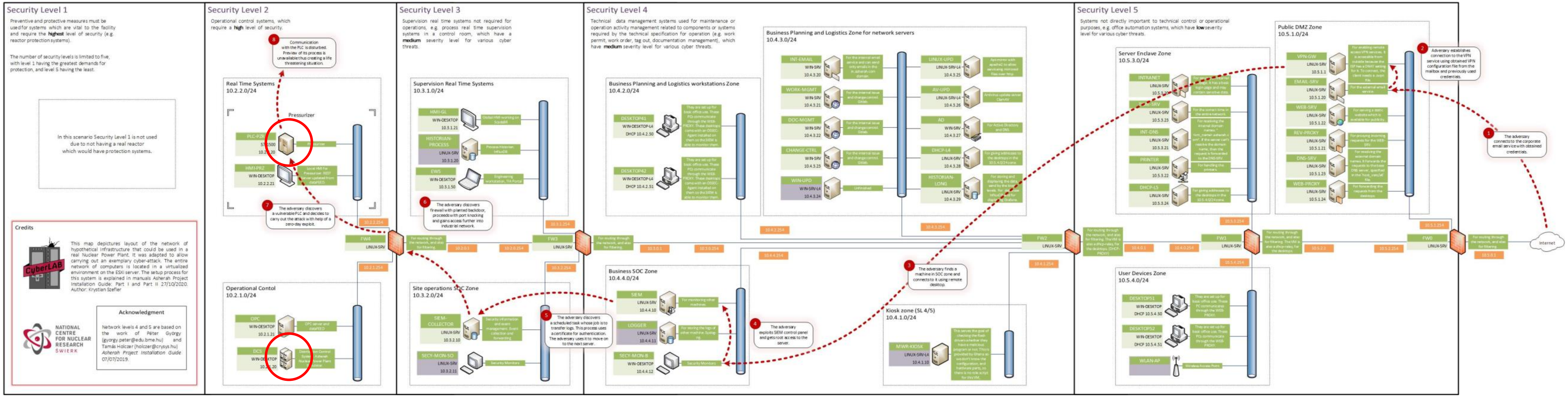
- in which is Asherah simulator
- and virtualized infrastructure of business and industrial networks (42 virtual machines)

PLC Siemens 1512C-1 PN



Siemens 1512C-1 PN

ESXi server



Security Level 1

Preventive and protective measures must be used for systems which are vital to the facility and require the **highest** level of security (e.g. reactor protection systems).

The number of security levels is limited to five, with level 1 having the greatest demands for protection, and level 5 having the least.

In this scenario Security Level 1 is not used due to not having a real reactor which would have protection systems.

Credits

This map depictures layout of the network of hypothetical infrastructure that could be used in a real Nuclear Power Plant. It was adapted to allow carrying out an exemplary cyber-attack. The entire network of computers is located in a virtualized environment on the ESXi server. The setup process for this system is explained in manuals Asherah Project Installation Guide: Part I and Part II 27/10/2020. Author: Krystian Szefler

Acknowledgment

Network levels 4 and 5 are based on the work of Péter György (gyorgy.peter@edu.bme.hu) and Tamás Holczer (holczer@crysys.hu) *Asherah Project Installation Guide* 07/07/2019.

Security Level 2

Operational control systems, which require a **high** level of security.

8 Communication with the PLC is disturbed. Preview of its process is unavailable thus creating a life threatening situation.

7 The adversary discovers a vulnerable PLC and decides to carry out the attack with help of a zero-day exploit.

Security Level 3

Supervision real time systems not required for operations, e.g. process real time supervision systems in a control room, which have a **medium** severity level for various cyber threats.

6 The adversary discovers firewall with planted backdoor, proceeds with port knocking and gains access further into industrial network.

5 The adversary discovers a scheduled task whose job is to transfer logs. This process uses a certificate for authentication. The adversary uses it to move on to the next server.

Security Level 4

Technical data management systems used for maintenance or operation activity management related to components or systems required by the technical specification for operation (e.g. work permit, work order, tag out, documentation management), which have **medium** severity level for various cyber threats.

4 The adversary exploits SIEM control panel and gets root access to the server.

3 The adversary finds a machine in SOC zone and connects to it using remote desktop.

Security Level 5

Systems not directly important to technical control or operational purposes, e.g. office automation systems, which have **low** severity level for various cyber threats.

2 Adversary establishes connection to the VPN service using obtained VPN configuration file from the mailbox and previously used credentials.

1 The adversary connects to the corporate email service with obtained credentials.

CyberLAB
NATIONAL CENTRE FOR NUCLEAR RESEARCH ŚWIERK
Real Time Systems 10.2.2.0/24
Pressurizer
PLC-PZR S7-1500 10.2.2.20
HMI-PRZ WIN-DESKTOP 10.2.2.21
Operational Contol 10.2.1.0/24
OPC WIN-DESKTOP 10.2.1.21
DCS WIN-DESKTOP 10.2.1.20
FW4 LINUX-SRV
10.2.2.254
10.2.1.254
10.2.0.1
10.2.0.254
Supervision Real Time Systems 10.3.1.0/24
HMI-GL WIN-DESKTOP 10.3.1.21
HISTORIAN-PROCESS LINUX-SRV 10.3.1.20
EWS WIN-DESKTOP 10.3.1.50
Site operations SOC Zone 10.3.2.0/24
SIEM-COLLECTOR LINUX-SRV 10.3.2.10
SECY-MON-SO LINUX-SRV 10.3.2.11
FW3 LINUX-SRV
10.3.1.254
10.3.2.254
10.3.0.1
10.3.0.254
Business Planning and Logistics workstations Zone 10.4.2.0/24
DESKTOP41 WIN-DESKTOP-L4 DHCP 10.4.2.50
DESKTOP42 WIN-DESKTOP-L4 DHCP 10.4.2.51
Business SOC Zone 10.4.4.0/24
SIEM LINUX-SRV 10.4.4.10
LOGGER LINUX-SRV 10.4.4.11
SECY-MON-B WIN-DESKTOP 10.4.4.12
Business Planning and Logistics Zone for network servers 10.4.3.0/24
INT-EMAIL WIN-SRV 10.4.3.20
WORK-MGMT WIN-SRV 10.4.3.21
DOC-MGMT WIN-SRV 10.4.3.22
CHANGE-CTRL WIN-SRV 10.4.3.23
WIN-UPD WIN-SRV-L4 10.4.3.24
LINUX-UPD LINUX-SRV-L4 10.4.3.25
AV-UPD LINUX-SRV-L4 10.4.3.26
AD WIN-SRV 10.4.3.27
DHCP-L4 LINUX-SRV 10.4.3.28
HISTORIAN-LONG LINUX-SRV 10.4.3.29
Kiosk zone (SL 4/5) 10.4.1.0/24
MWR-KIOSK LINUX-SRV-L4 10.4.1.10
10.4.2.254
10.4.3.254
10.4.4.254
10.4.1.254
FW2 LINUX-SRV
10.4.0.1
10.4.0.254
Server Enclave Zone 10.5.3.0/24
INTRANET LINUX-SRV 10.5.3.20
TIME-SRV LINUX-SRV 10.5.3.23
INT-DNS LINUX-SRV 10.5.3.21
PRINTER LINUX-SRV 10.5.3.22
DHCP-L5 LINUX-SRV 10.5.3.24
Public DMZ Zone 10.5.1.0/24
VPN-GW LINUX-SRV 10.5.1.1
EMAIL-SRV LINUX-SRV 10.5.1.20
WEB-SRV LINUX-SRV 10.5.1.22
REV-PROXY LINUX-SRV 10.5.1.21
DNS-SRV LINUX-SRV 10.5.1.23
WEB-PROXY LINUX-SRV 10.5.1.24
User Devices Zone 10.5.4.0/24
DESKTOP51 WIN-DESKTOP DHCP 10.5.4.50
DESKTOP52 WIN-DESKTOP DHCP 10.5.4.51
WLAN-AP
Wireless Access Point
FW1 LINUX-SRV
10.5.3.254
10.5.4.254
10.5.2.1
10.5.2.254
10.5.1.254
FW0 LINUX-SRV
10.5.0.1
Internet

A map of industrial network (SL2-3) along with business network (SL4-5) with marked out PLC controller and Asherah simulator.

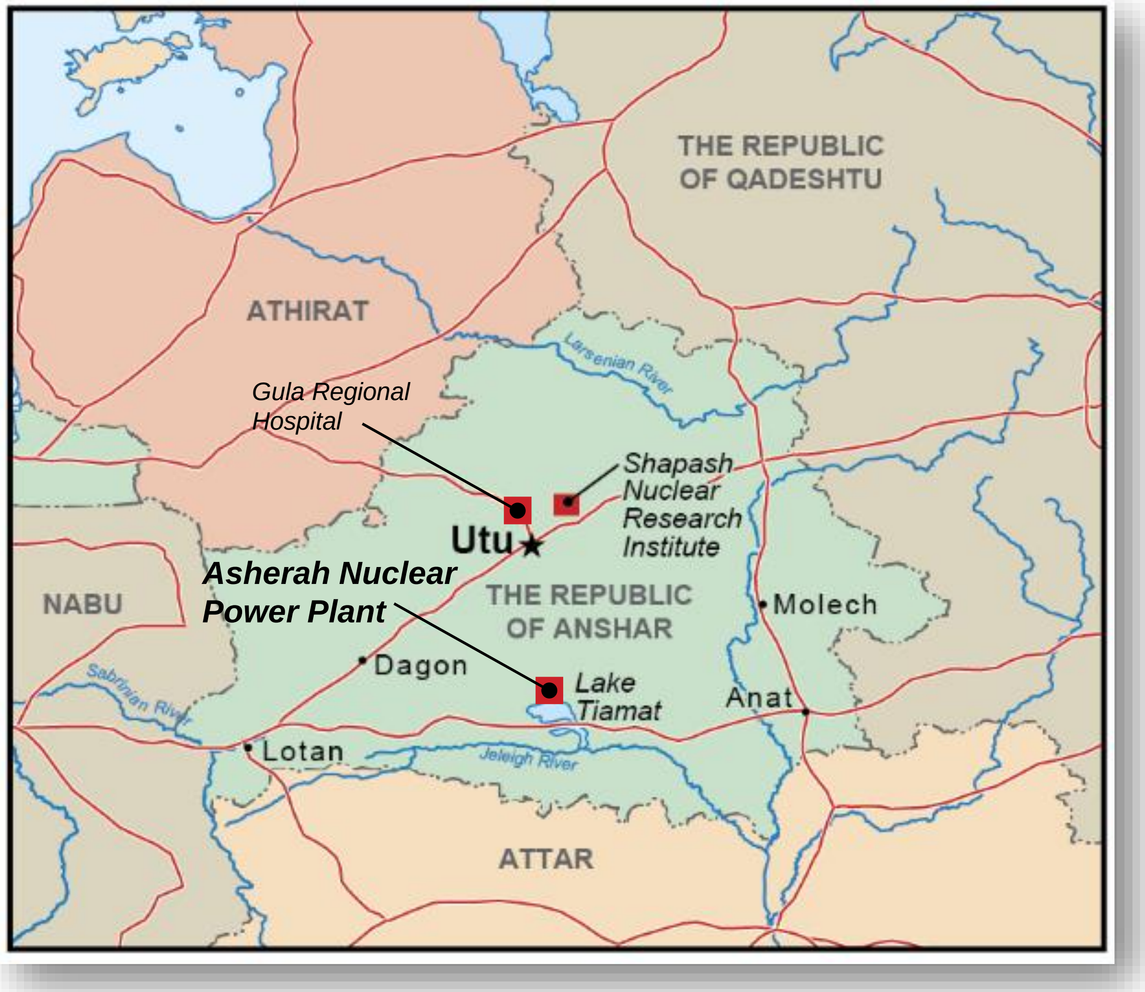
Attack scenario

Place

Republic of Anshar - a fictitious state created by the IAEA especially for academic purposes

Objective

Asherah Nuclear Power Plant (ANPP)



Map of Republic of Anshar with marked Asherah Plant

Supply chain implant with the help of partial modernization in the plant

ANPP’s authorities have released an invitation to tender. ANPP is looking for new firewalls.

One of the workers of the company that won the tender turns out to be a Sneaky Sloths group (SSG) member.

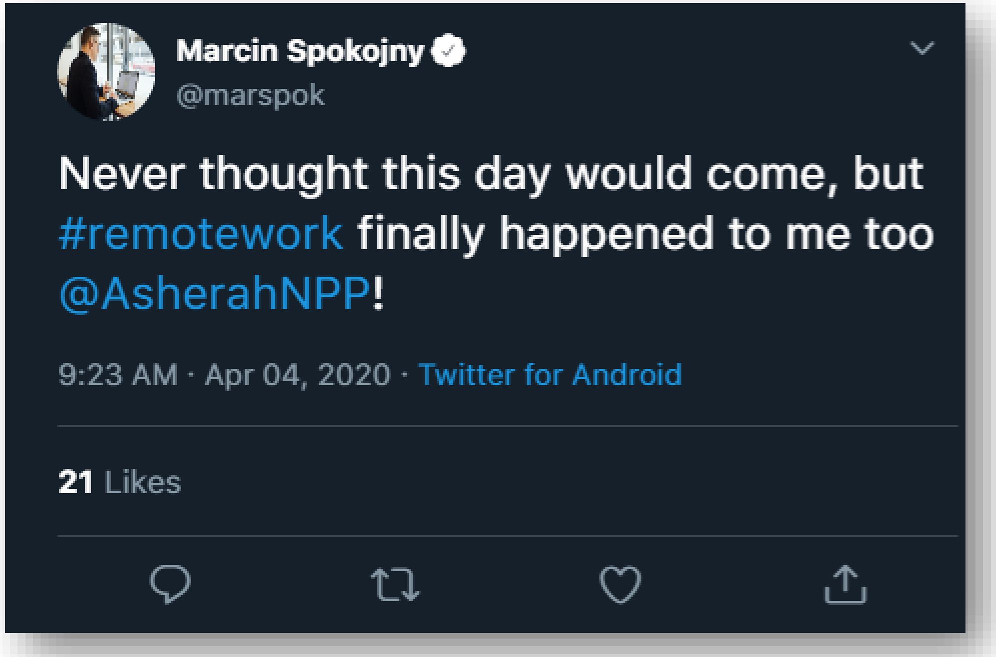
The firewalls were imperceptibly switched to specially crafted ones with installed backdoors.

Pandemic and its consequences

SSG has noticed that Marcin Spokojny, one of the IT employees of the ANPP, tweeted about starting remote work in the ANPP.

Due to pandemic the remote work has been introduced in the plant.

The adversary has a hunch that remote access to the plant has been configured in a hurry leaving some security flaws.



Marcin Spokojny
@marspok

Never thought this day would come, but #remotework finally happened to me too @AsherahNPP!

9:23 AM · Apr 04, 2020 · Twitter for Android

21 Likes

Initial access data acquisition

Adversary found Marcin’s login and password from leaked databases of an online store, easypc.an;

- email: marcin.spokojny@gmail.com
- password: D@NC1NG3l3f@nt**easypc**

Adversary notices that the password contains shop’s name – a technique used to create a unique password;

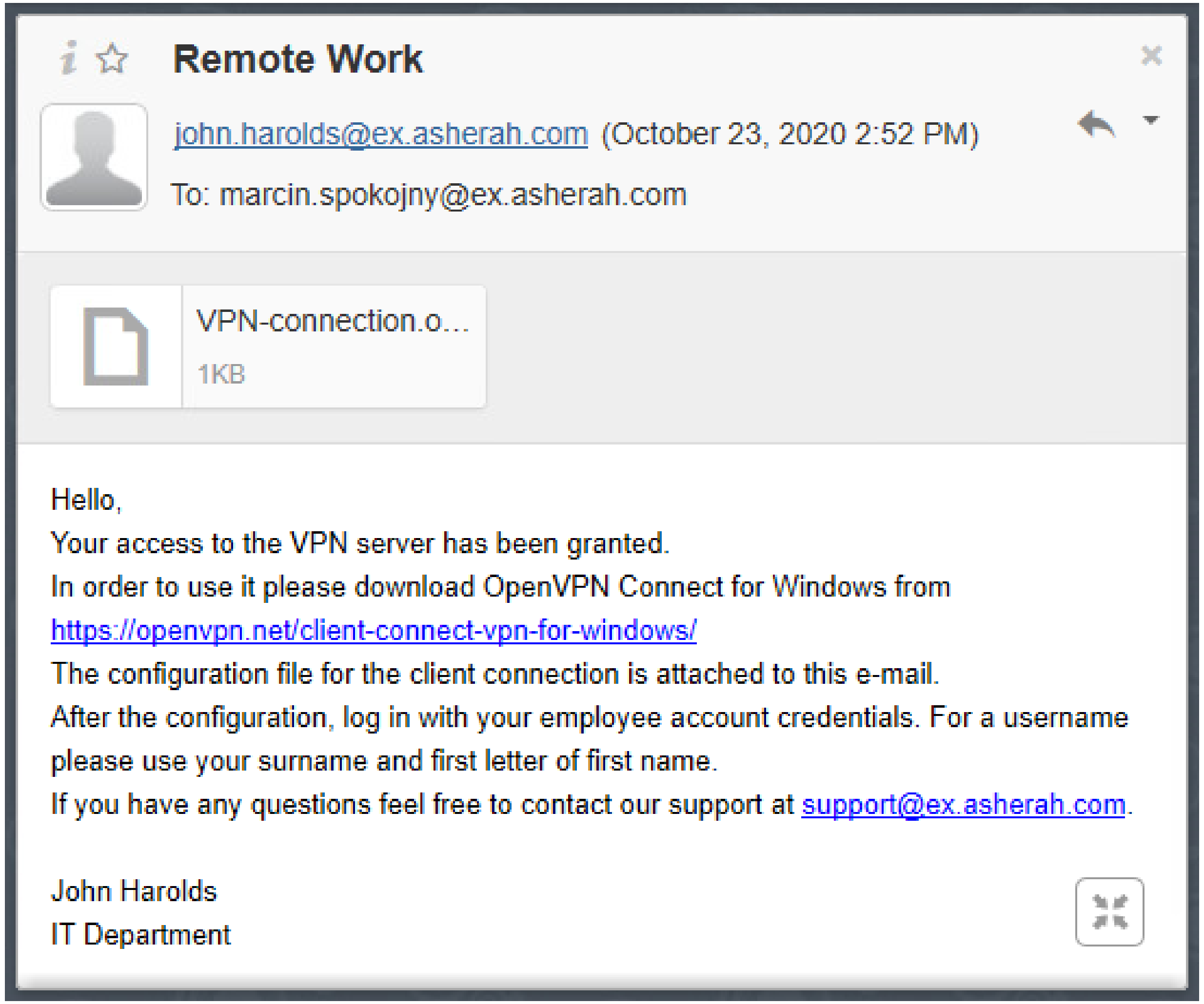
- password: D@NC1NG3l3f@nt**anpp** / D@NC1NG3l3f@nt**asherah** ?

From Asherah website they learn email’s template: name.surname@ex.asherah.com;

SGG gains access to the mailbox!

A corporate mailbox

In the mailbox SSG finds an email instructing them how to access the corporate network with the help of a VPN service.



john.harolds@ex.asherah.com (October 23, 2020 2:52 PM)

To: marcin.spokojny@ex.asherah.com

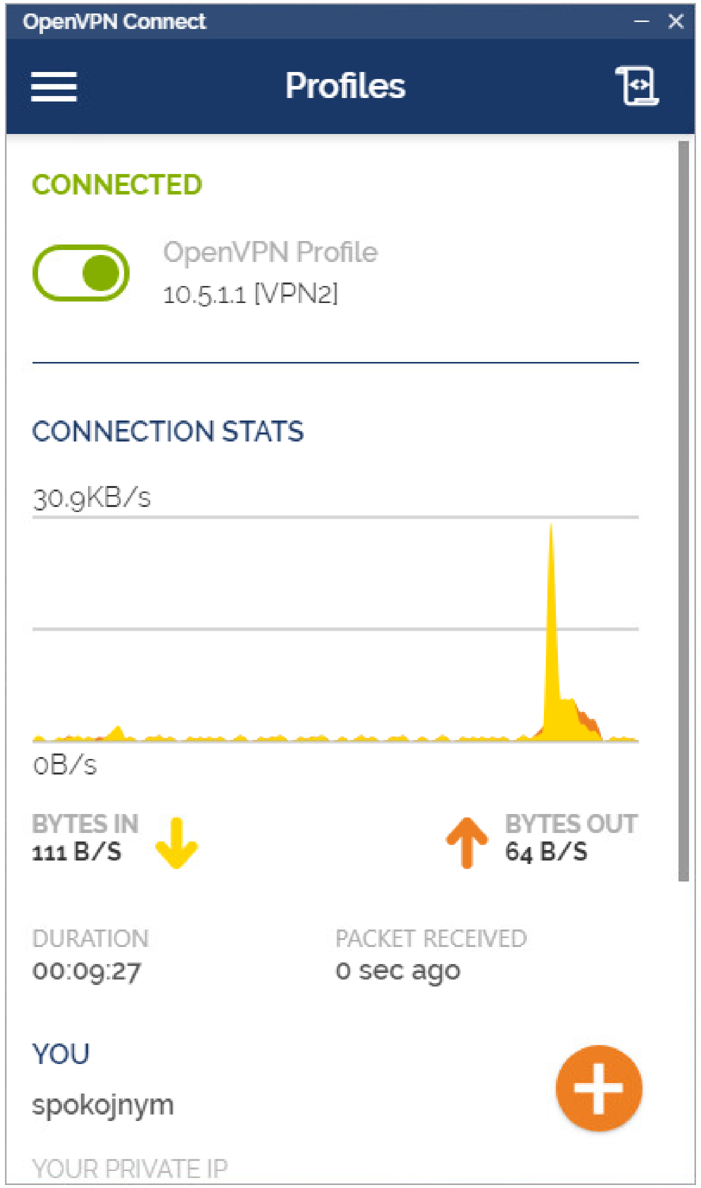
Hello,
Your access to the VPN server has been granted.
In order to use it please download OpenVPN Connect for Windows from
https://openvpn.net/client-connect-vpn-for-windows/
The configuration file for the client connection is attached to this e-mail.
After the configuration, log in with your employee account credentials. For a username please use your surname and first letter of first name.
If you have any questions feel free to contact our support at support@ex.asherah.com.

John Harolds
IT Department

Initial access

Having gathered information about the VPN, SSG tries to make use of it and initiates a VPN connection.

Fortunately for them, they gain access to the enterprise network of the ANPP on 5th security level.



OpenVPN Connect

Profiles

CONNECTED

OpenVPN Profile
10.5.1.1 [VPN2]

CONNECTION STATS

30.9KB/s

0B/s

BYTES IN
111 B/S

BYTES OUT
64 B/S

DURATION
00:09:27

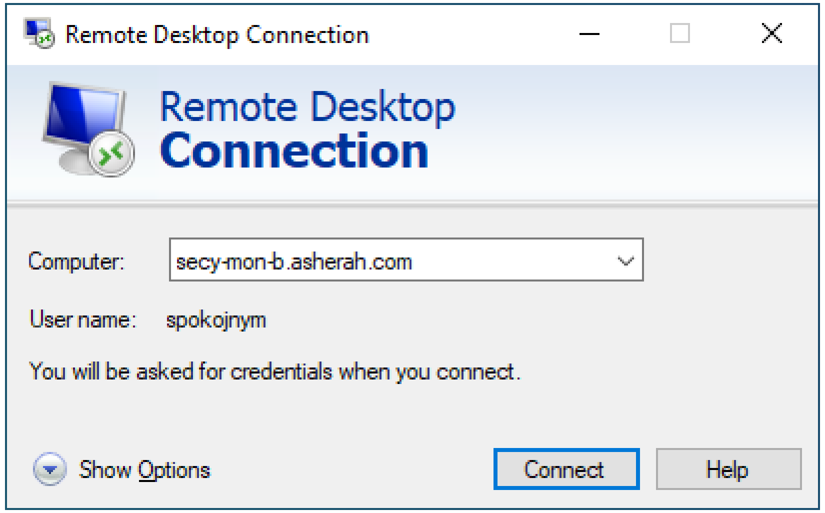
PACKET RECEIVED
0 sec ago

YOU
spokojnym

YOUR PRIVATE IP

Lateral Movement

SGG decided to scan a local DNS server. With a list of all computers they try to connect to all of the machines.



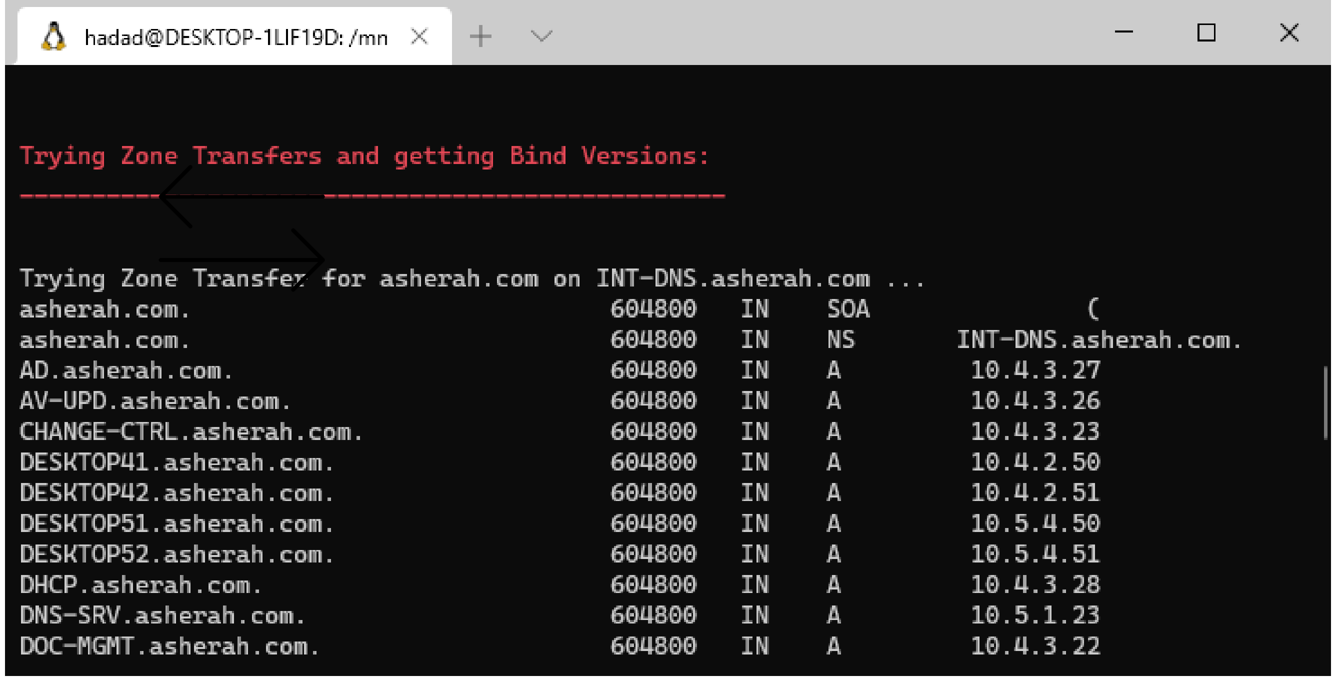
Remote Desktop Connection

Remote Desktop **Connection**

Computer: secy-mon-b.asherah.com

User name: spokojnym

You will be asked for credentials when you connect.

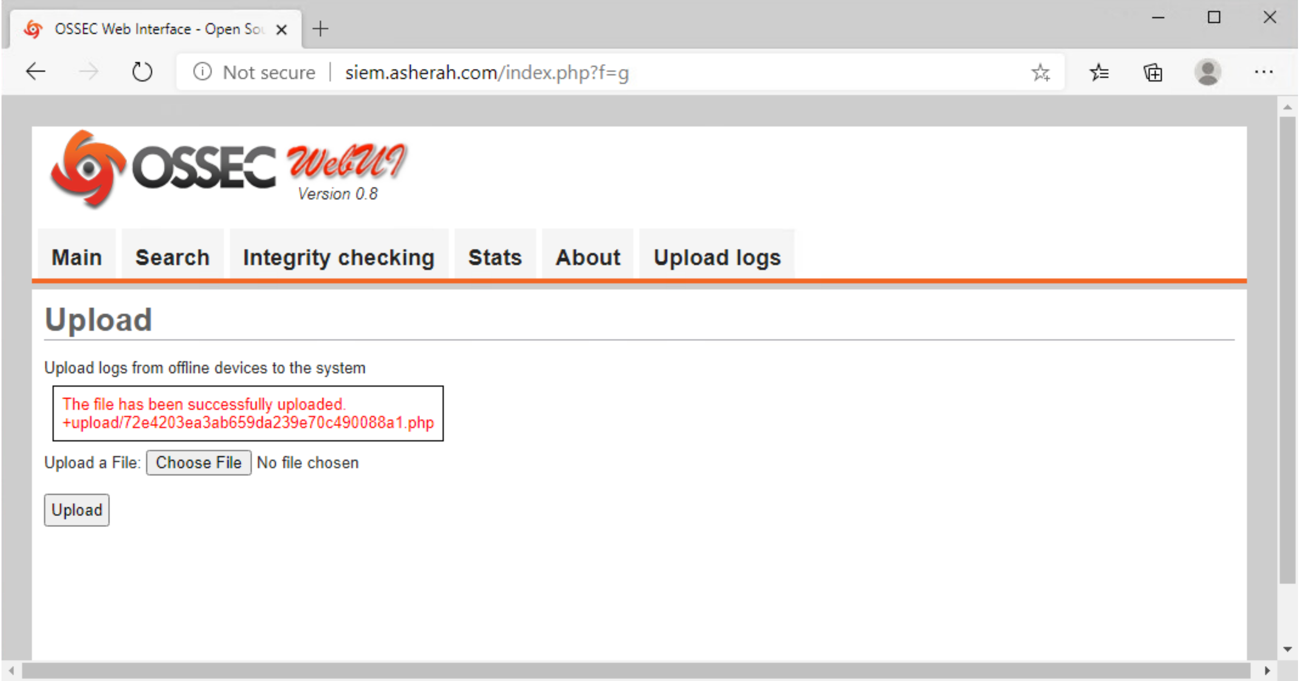


```
Trying Zone Transfers and getting Bind Versions:
-------------------------------------------------


Trying Zone Transfer for asherah.com on INT-DNS.asherah.com ...
asherah.com.                       604800   IN    SOA          (
asherah.com.                       604800   IN    NS      INT-DNS.asherah.com.
AD.asherah.com.                    604800   IN    A        10.4.3.27
AV-UPD.asherah.com.                604800   IN    A        10.4.3.26
CHANGE-CTRL.asherah.com.           604800   IN    A        10.4.3.23
DESKTOP41.asherah.com.             604800   IN    A        10.4.2.50
DESKTOP42.asherah.com.             604800   IN    A        10.4.2.51
DESKTOP51.asherah.com.             604800   IN    A        10.5.4.50
DESKTOP52.asherah.com.             604800   IN    A        10.5.4.51
DHCP.asherah.com.                  604800   IN    A        10.4.3.28
DNS-SRV.asherah.com.               604800   IN    A        10.5.1.23
DOC-MGMT.asherah.com.              604800   IN    A        10.4.3.22
```

PHP Injection

SSG discovers unsecured control panel for reviewing network logs. Panel contains a form allowing uploading log files to the system. SSG uses it to upload a webshell.


OSSEC Web Interface - Open So
Not secure | siem.asherah.com/index.php?f=g
OSSEC WebUI
Version 0.8
Main
Search
Integrity checking
Stats
About
Upload logs

Upload

Upload logs from offline devices to the system

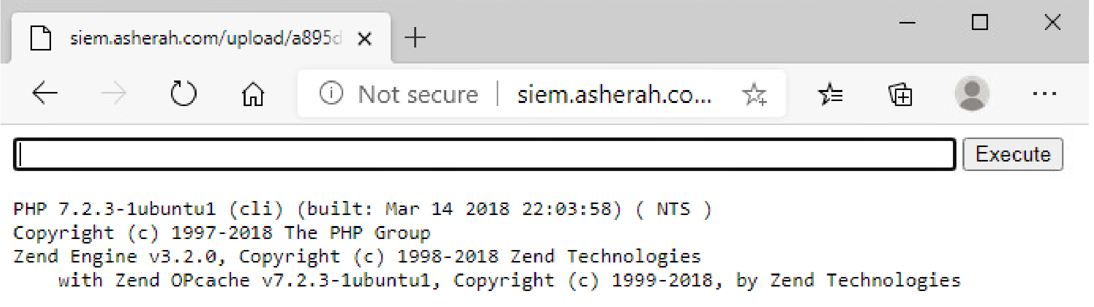
The file has been successfully uploaded.
+upload/72e4203ea3ab659da239e70c490088a1.php

Upload a File: Choose File No file chosen

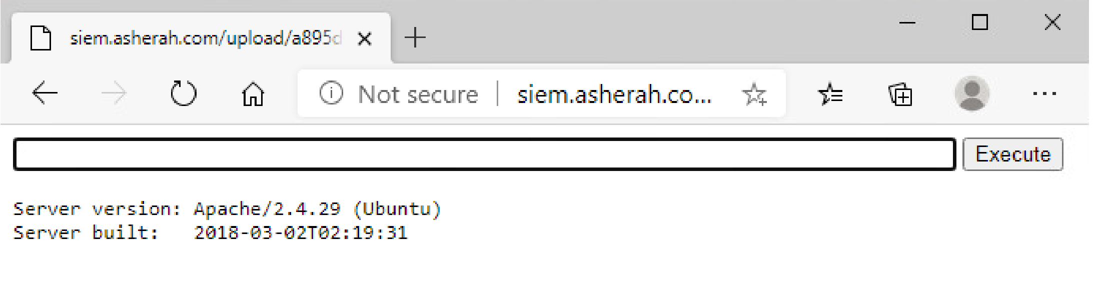
Upload

Not so up-to-date software

With the use of the webshell, information about the server is gathered in order to find a vulnerability to escalate privileges. It turns out that the Apache server and PHP Preprocessor are in an older version. Exploit is found and root access is gained.



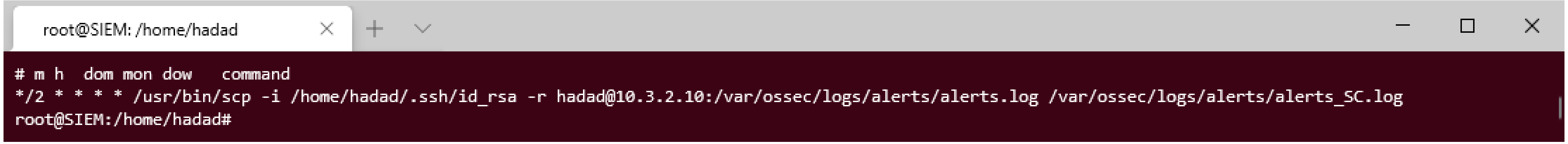
```
PHP 7.2.3-1ubuntu1 (cli) (built: Mar 14 2018 22:03:58) ( NTS )
Copyright (c) 1997-2018 The PHP Group
Zend Engine v3.2.0, Copyright (c) 1998-2018 Zend Technologies
    with Zend OPcache v7.2.3-1ubuntu1, Copyright (c) 1999-2018, by Zend Technologies
```



```
Server version: Apache/2.4.29 (Ubuntu)
Server built:   2018-03-02T02:19:31
```

Return of the backdoored firewall

Now with root access, a scheduled task in the server is discovered. Its job is to download logs from a machine located in Security Level 3. It is done by using SCP with a private key as authentication.



```
# m h  dom mon dow   command
*/2 * * * * /usr/bin/scp -i /home/hadad/.ssh/id_rsa -r hadad@10.3.2.10:/var/ossec/logs/alerts/alerts.log /var/ossec/logs/alerts/alerts_SC.log
root@SIEM:/home/hadad#
```

With the found private key it is possible to move to Security Level 3.

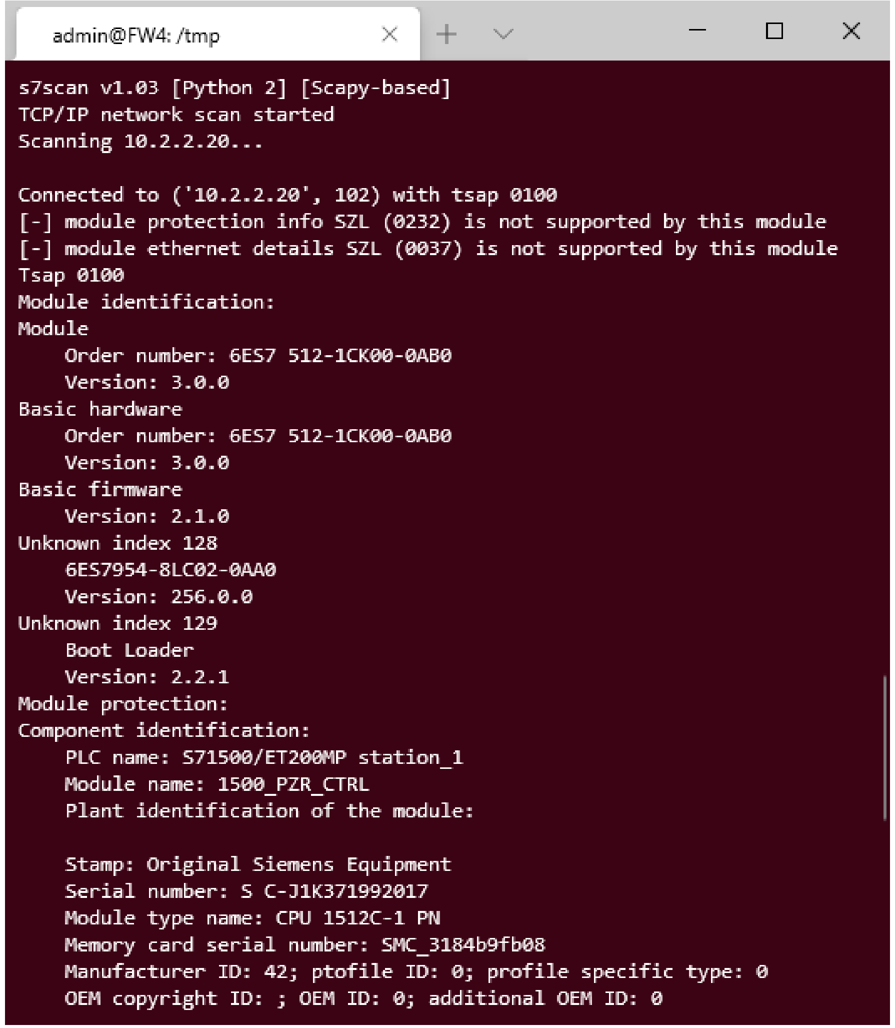
Next SSG finds their previously backdoored firewall bridging security level 3 and 2. Using port knocking they access it consequently gaining access to security level 2 – industrial network.

Industrial network

In the industrial network SSG discovers a PLC controller and enumerates its details. Its firmware is vulnerable to a zero-day exploit.

It is decided to carry out an attack…

Vulnerability of number CVE-2018-13805 used in the presentation has been discovered by CyberLAB team.



```
s7scan v1.03 [Python 2] [Scapy-based]
TCP/IP network scan started
Scanning 10.2.2.20...

Connected to ('10.2.2.20', 102) with tsap 0100
[-] module protection info SZL (0232) is not supported by this module
[-] module ethernet details SZL (0037) is not supported by this module
Tsap 0100
Module identification:
Module
    Order number: 6ES7 512-1CK00-0AB0
    Version: 3.0.0
Basic hardware
    Order number: 6ES7 512-1CK00-0AB0
    Version: 3.0.0
Basic firmware
    Version: 2.1.0
Unknown index 128
    6ES7954-8LC02-0AA0
    Version: 256.0.0
Unknown index 129
    Boot Loader
    Version: 2.2.1
Module protection:
Component identification:
    PLC name: S71500/ET200MP station_1
    Module name: 1500_PZR_CTRL
    Plant identification of the module:

    Stamp: Original Siemens Equipment
    Serial number: S C-J1K371992017
    Module type name: CPU 1512C-1 PN
    Memory card serial number: SMC_3184b9fb08
    Manufacturer ID: 42; ptofile ID: 0; profile specific type: 0
    OEM copyright ID: ; OEM ID: 0; additional OEM ID: 0
```

Exploitation

Conclusions

Presented attack scenario aka. kill chain was invented and then tested in a simulated plant. Even though fictitious **is even so realistic**! (all shortcomings have appeared before in actual security incidents).

Presented attack scenario takes advantage of human nature (sharing information on the Internet, schematic password), uses available exploits (including CyberLAB's one) as well as current world situation (pandemic).

The presented test bed and scenario **may bring great value to the cybersecurity community**, as these could be used, among others, for enhancing risk analysis, as a case study for awareness-raising demonstrations, or as part of incident response training.

As well as for testing security solutions of industrial control systems in realistic scenario attack.

Thank you for your attention!

NATIONAL CENTRE FOR NUCLEAR RESEARCH
ŚWIERK

CyberLAB

cyberlab@ncbj.gov.pl

10 February 2022