Next session in

black hat ASIA 2023

MAY 11-12

ARSENAL

The Positive Way

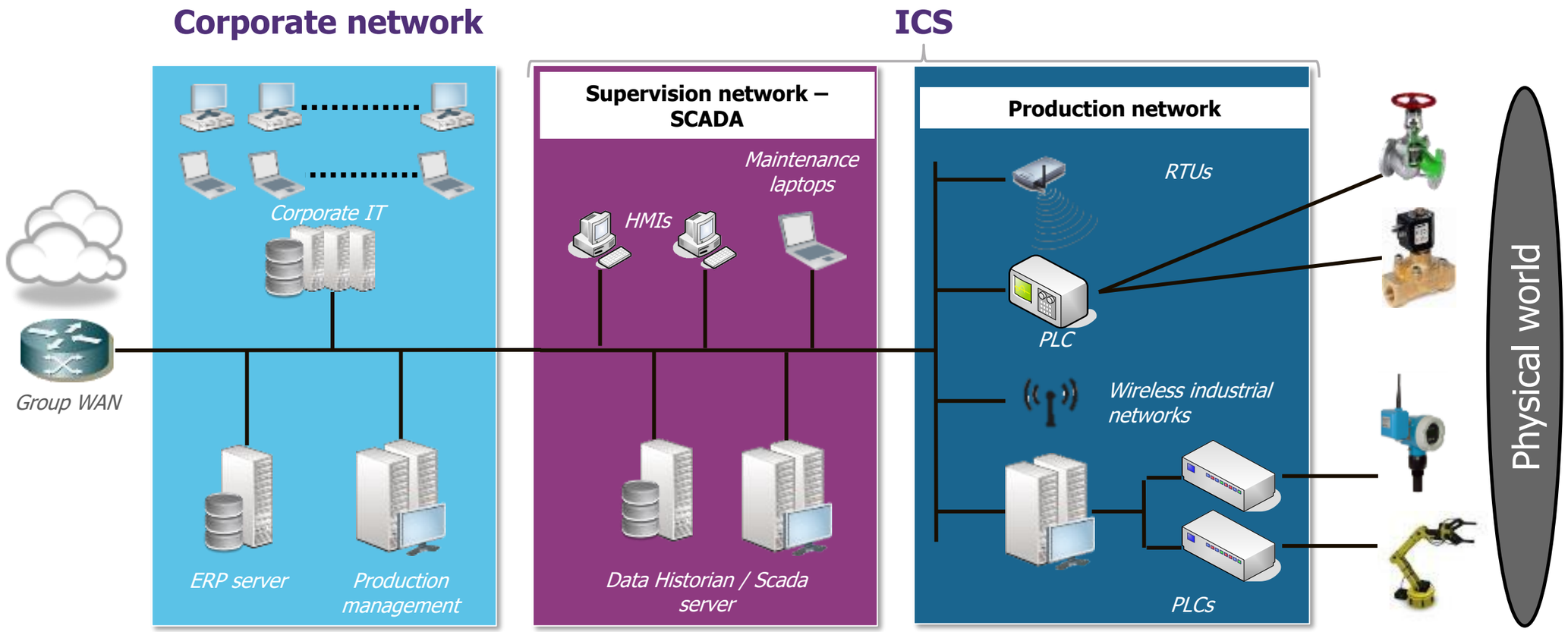
WAVESTONE

OPC-U-HACK!

An introduction to a modern Industrial Control Systems protocol

Arnaud Soullié
Paris office
@arnaudsoullie

Romain GAGLIARDI
Singapore office



Corporate IT handle data

≠

ICS handle interfaces data with physical world (cyber-physical systems)

OPC-UA protocol

Most legacy ICS protocols don't offer any security at all:

- *No authentication*
- *No encryption*

The OPC suite of protocols was developed in the 90s to allow easier integration of IT and ICS

- *Protocols were based on DCOM (Microsoft) technologies*
- *Several variants (OPC-DA / OPC A&E / OPC HAD / OPC-DX)*

OPC-UA is a brand-new protocol created in 2006

- *Cross-platform*
- *Available for free*
- *Provides security features!*

OPC-UA security

OPC-UA features 3 security modes:

- *None*
- *Sign*
- *Sign & Encrypt*

The security policies then define the type of algorithms to be used (SHA256 /)

In addition, OPC-UA provides user **authentication** & **authorization**, using **passwords** or **certificates**

https://opcfoundation.org/security/

But: ***implementations and configurations are not flawless!***

OPC-UA protocol

Our challenges for today

1. Identify OPC-UA services
2. Gather information
3. Try to take control of the robotic arms using OPC-UA!

Instructions at:
https://github.com/wavestone-cdt/bhasia23-opcuhack

CTFd platform at:
http://185.64.246.121:8000

Step 1: Scanning

Scanning live ICS environments in dangerous
Legacy equipment sometimes doesn't like a lot of packets and/or a lot of unclosed TCP connections.

A few general recommendations

Scan all TCP ports (not to be performed in real ICS environments)

```
nmap -p- IP_ADDRESS
```

(IP address is on a post-it on your laptop)

Step 2: Get OPC-UA endpoints

Identify which ports correspond to the OPC-UA service(s)

Using opcua-scanner

```
cd opcua-scanner

./opcua_scan.py hello -i IP_ADRESS
    -p 'PORT1, PORT2, PORT3'

./opcua_scan.py server_config
-t 'opc.tcp://IP:PORT/endpoint'
```

(IP address is on a post-it on your laptop)

Step 3: Try to read & write data

Using opcua-scanner

```
cd opcua-scanner

./opcua_scan.py read_data
-t 'opc.tcp://IP:PORT/ENDPOINT'

./opcua_scan.py read_data
-t 'opc.tcp://IP:PORT/ENDPOINT'
-r 'ns=2;s=XXX.YYY'

./opcua_scan.py write_data -t
'opc.tcp://IP:PORT/ENDPOINT' -r
'ns=2;s=XXX.YYY' --data True
```

Dynamic tags

Is a feature that allows to reference directly the memory zone you want to access.
This way, you do not have to create a tag for each value, you can directly pass the address.

This feature, of course, has some security implication because it can be used to bypass access control enforced on static tags.

```
cd opcua-scan

./opcua_scan.py read_data -t
'opc.tcp://IP:PORT/ENDPOINT' -r
'ns=2;s=XXX.YYY' --single True
```

Next session in

black hat ASIA 2023

MAY 11–12

ARSENAL

The Positive Way

WAVESTONE

Slides and code snippets at:

https://github.com/wavestone-cdt/bhasia23-opcuhack

Arnaud Soullié
Paris office
@arnaudsoullie

Romain GAGLIARDI
Singapore office