Vulnerability Assessment of Industrial Control System

By:
Ashish Gahlot

Acknowledgement

- Dr. Sandeep K Shukla, IIT Kanpur
- Mr. Rohit Negi, IIT Kanpur
- Colleagues

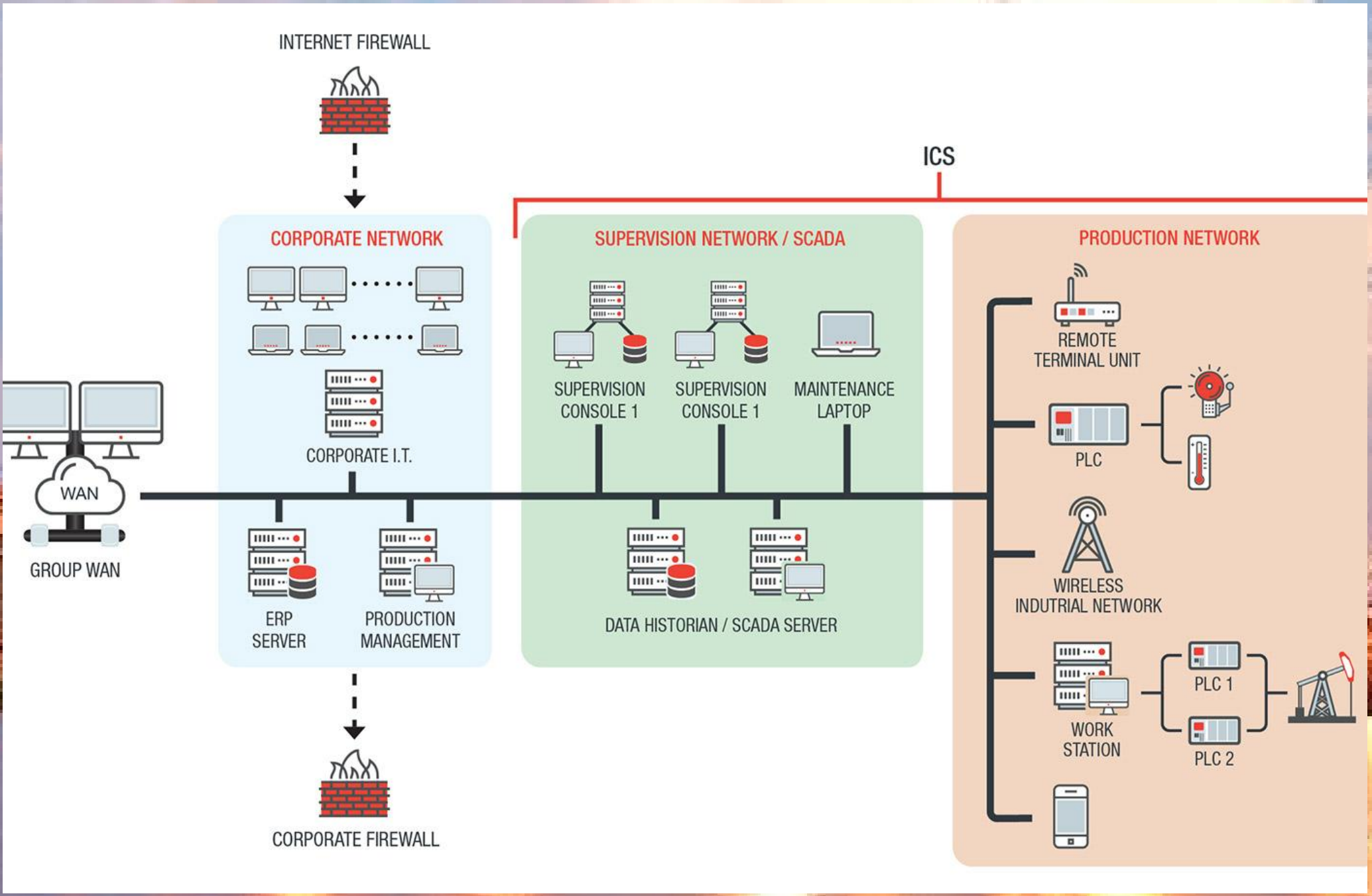
ICS: Introduction

- What is ICS
- Talk about Fundamental human needs
- National importance
- Economy

Introduction

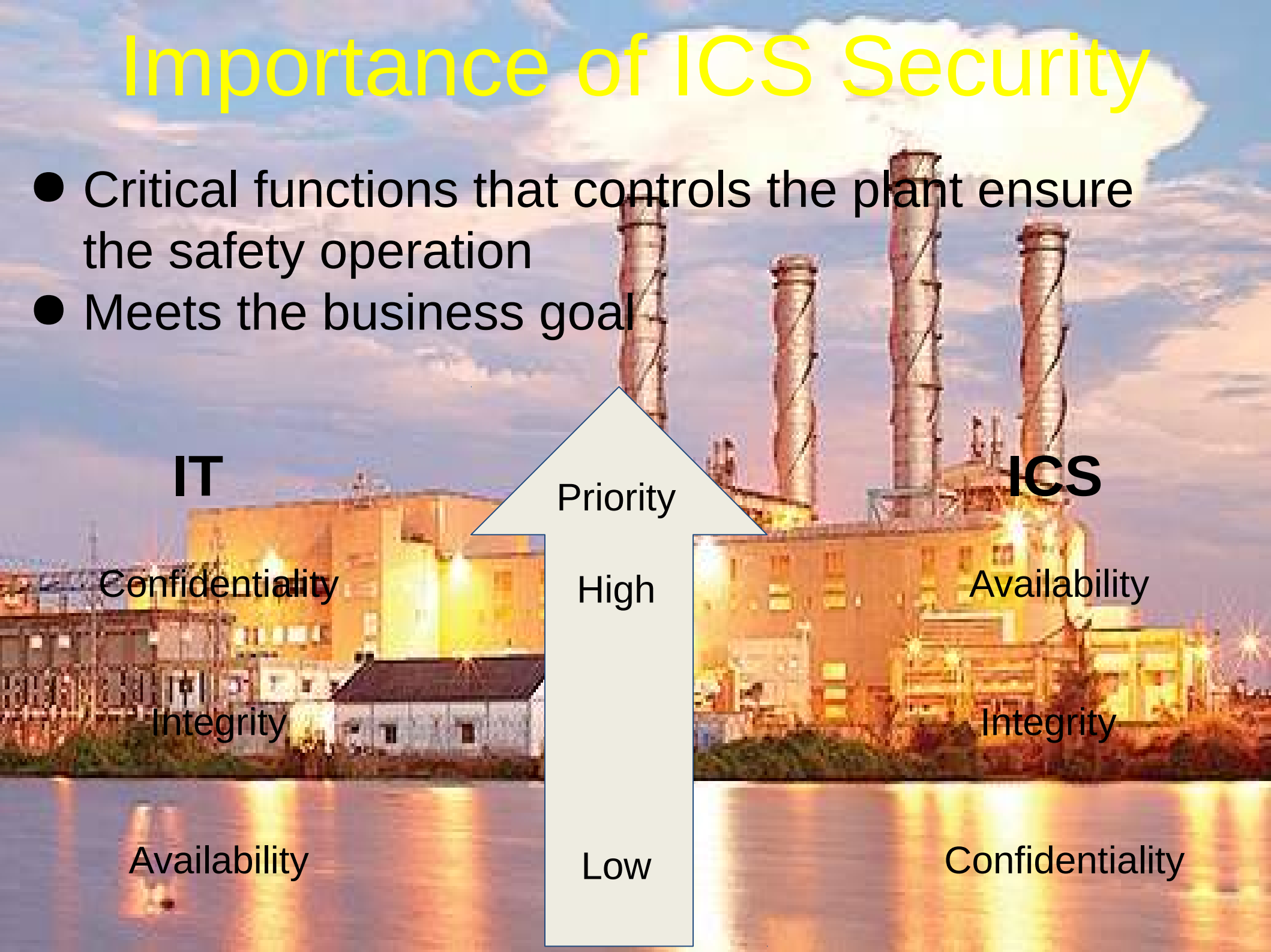
- PLCs are computers used to automate mechanical device processes.
- PLCs are used in oil, nuclear, defence and many other things.
- These devices are insecure
- They are in all terms propetiary

Architecture



Importance of ICS Security

- Critical functions that controls the plant ensure the safety operation
- Meets the business goal

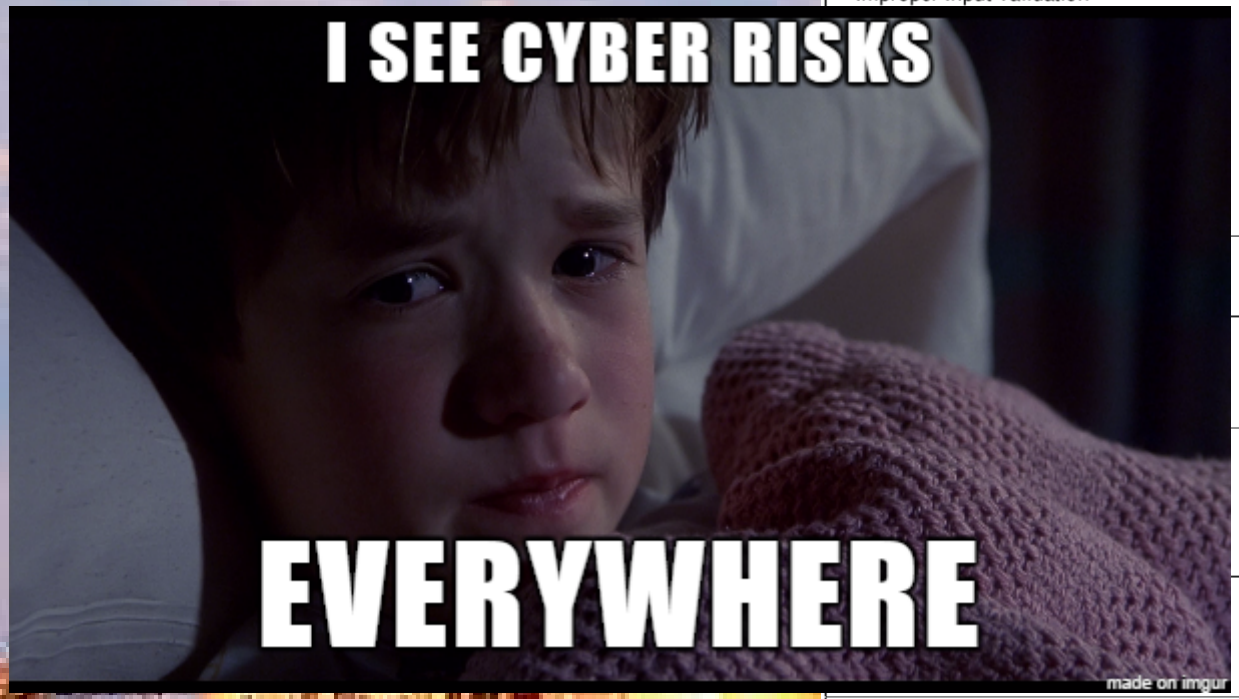


Attack Surface

Publicized ICS Attacks		
Year	**Incident**	**Location**
2000	Sewage-processing plant attack by a former employee	Maroochy, Australia
2003	Nuclear power plant system was disabled via the Slammer worm	Ohio, USA
2008	Train derailment due to hacking	Lodz, Poland
2009	Traffic signal system hacked	LA, California, USA
2010	Stuxnet worm destroyed uranium centrifuge operations	Natanz, Iran
2011	Ambulance service disrupted via a malware infection	New Zealand
2013	Banking and broadcasting services were disrupted	South Korea

By Trend Micro

Attack Surface



Category	Common Vulnerability
Improper Input Validation	Buffer overflow
	Lack of bounds checking
	Command injection • OS command injection • SQL injection
	Cross-site scripting
	Path traversal
	Use of potentially dangerous function
	NULL pointer dereference
	Improper access control (authorization)
	Execution with unnecessary privileges • Incorrect default permissions
	Authentication bypass issues
	Missing authentication for critical function Use of client-side authentication Channel accessible by nonendpoint (MitM)
	Cross-site request forgery
	Missing support for integrity check
	Download of code without integrity check
Cryptographic Issues	Missing encryption of sensitive data • Clear-text transmission of sensitive information
	Use of a broken or risky cryptographic algorithm
Credentials Management	Insufficiently protected credentials • Plaintext storage of a password • Unprotected transport of credentials
	Use of hard-coded credentials
ICS Software Security Configuration and Maintenance	Poor patch management • Unpatched or Old Versions of Third-party Applications Incorporated into ICS Software
	Improper security configuration • Security functions/options not used during development • Information exposure through debug information

https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/DHS_Common_Cybersecurity_Vulnerabilities_ICS_2010.pdf

Assessment in Three Easy Steps

- **Reconnaissance**

  Active :

  Port scanning, Patched against publicly disclosed vulnerabilities

  Passive:

  Monitoring network traffic

- **Exploration**

  Conduct some documentation research

  Look for attack vectors

  Vulnerabilities pertaining to Published, Web, Input validation, Database, Improper authentication and authorization, **ICS data and command message manipulation and injection**

- **Exploit**

  Exploit the identified problem

STUXNET

- Attacked Siemens PLC
- Took advantage of Windows and vulnerable Siemens products
- Printer shared on network is accessible by anyone as a Guest user in order to print documents
- Stuxnet used "printer spooler service" to make RPC to write a malware to disk

Reconnaissance

- Nmap
- plcscan

Reconnaissance

Google-FU + SHODAN =

Shodan | Developers | Book | View All... | Show API Key

SHODAN | port:502 country:"FR" | Explore | Downloads | Reports | Enterprise Access | Contact Us | My Account | Upgrade

Exploits | Maps | Share Search | Download Results | Create Report

TOTAL RESULTS

1,129

TOP COUNTRIES

France 1,129

TOP CITIES

Paris	27
Nevers	17
Villeurbanne	3
Vienne	2
Sélestat	2

TOP ORGANIZATIONS

Orange	730
SFR	139
Free SAS	67
Orange France Wireless	58
Bouygues Telecom	57

TOP OPERATING SYSTEMS

5.48.199.231
i19-les02-th2-5-48-199-231.sfr.lns.abo.bbox.fr
Bouygues Telecom
Added on 2017-07-06 06:41:52 GMT
France, Toulouse
Details
ICS

```
Unit ID: 0
-- Slave ID Data: Illegal Function (Error)
-- Device Identification: Illegal Function (Error)

Unit ID: 1
-- Slave ID Data: Illegal Function (Error)
-- Device Identification: Illegal Function (Error)

Unit ID: 2
-- Slave ID Data: Illegal Function (Error)
-- Device Identification: Illeg...
```

109.0.146.60
60.146.0.109.rev.sfr.net
SFR
Added on 2017-07-06 06:30:48 GMT
France
Details
ICS

```
Unit ID: 1
-- Device Identification: Schneider Electric TM221ME32TK V2.2

Unit ID: 2
-- Device Identification: Schneider Electric TM221ME32TK V2.2

Unit ID: 3
-- Device Identification: Schneider Electric TM221ME32TK V2.2

Unit ID: 4
-- Device Identification: Schneider Electric TM221ME32TK V2.2...
```

80.11.202.124
LStLambert-658-1-171-124.w80-11.abo.wanadoo.fr

```
Unit ID: 0
```

Reconnaissance

Reconnaissance

ashish : zsh — Konsole

File Edit View Bookmarks Settings Help

```
Completed NSE at 20:23, 11.33s elapsed
Initiating NSE at 20:23
Completed NSE at 20:23, 0.00s elapsed
Nmap scan report for 192.168.100.40
Host is up (0.0063s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd (before 2.0.8) or WU-FTPD
80/tcp open  http    Schneider-WEB 2.2.0
|_http-favicon: Unknown favicon MD5: 8C291E32E7C7C65124D19EB17BCECA87
| http-methods:
|_  Supported Methods: GET HEAD
|_http-server-header: Schneider-WEB/V2.2.0
| http-title: Site doesn't have a title (text/html).
|_Requested resource was http://192.168.100.40/index.htm
MAC Address: 00:80:F4:14:F2:32 (Telemecanique Electrique)
Device type: general purpose
Running: Wind River VxWorks
OS CPE: cpe:/o:windriver:vxworks
OS details: VxWorks
Uptime guess: 0.016 days (since Wed Jul  5 20:00:05 2017)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=262 (Good luck!)
IP ID Sequence Generation: Incrementing by 2

TRACEROUTE
HOP RTT     ADDRESS
1   6.34 ms 192.168.100.40

NSE: Script Post-scanning.
Initiating NSE at 20:23
Completed NSE at 20:23, 0.00s elapsed
Initiating NSE at 20:23
Completed NSE at 20:23, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 26.44 seconds
           Raw packets sent: 1472 (65.514KB) | Rcvd: 1016 (41.098KB)
➜  ~
```

ashish : zsh

➜ ~ sudo nmap - [redacted] 192.168.100.40

Reconnaissance

ashish : zsh — Konsole

File Edit View Bookmarks Settings Help

```
Completed NSE at 20:22, 8.32s elapsed
Initiating NSE at 20:22
Completed NSE at 20:22, 0.00s elapsed
Nmap scan report for 192.168.100.10
Host is up (0.0050s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd (before 2.0.8) or WU-FTPD
80/tcp open  http    Schneider-WEB 2.1.0
|_http-favicon: Unknown favicon MD5: 8C291E32E7C7C65124D19EB17BCECA87
| http-methods:
|_  Supported Methods: GET HEAD
|_http-server-header: Schneider-WEB/V2.1.0
| http-title: Site doesn't have a title (text/html).
|_Requested resource was http://192.168.100.10/index.htm
MAC Address: 00:80:F4:15:2B:0F (Telemecanique Electrique)
Device type: general purpose
Running: Wind River VxWorks
OS CPE: cpe:/o:windriver:vxworks
OS details: VxWorks
Uptime guess: 0.016 days (since Wed Jul  5 19:59:11 2017)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=258 (Good luck!)
IP ID Sequence Generation: Incremental

TRACEROUTE
HOP RTT     ADDRESS
1   5.00 ms 192.168.100.10

NSE: Script Post-scanning.
Initiating NSE at 20:22
Completed NSE at 20:22, 0.00s elapsed
Initiating NSE at 20:22
Completed NSE at 20:22, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 22.73 seconds
           Raw packets sent: 1477 (65.734KB) | Rcvd: 2030 (82.128KB)
➜  ~
```

ashish : zsh

➜ ~ sudo nmap [redacted] 192.168.100.10

Reconnaissance

trunk : zsh — Konsole

File Edit View Bookmarks Settings Help

```
→  trunk python2.7 plcscan.py --timeout 2 90.63.[redacted]
Scan start...
90.63.[redacted]:502 Modbus/TCP
  Unit ID: 0
    Device: Schneider Electric BMX NOE 0100 V2.80
  Unit ID: 255
    Device: Schneider Electric BMX NOE 0100 V2.80
Scan complete
→  trunk
```

→ ~ python plcscan.py –timeout 2 90.63.[redacted]

Reconnaissance

ashish : ftp — Konsole

File Edit View Bookmarks Settings Help

```
➜  ~ ftp 192.168.100.10
Connected to 192.168.100.10.
220 host FTP server (VxWorks 6.4) ready.
Name (192.168.100.10:ashish): sysdiag
331 Password required for sysdiag.
Password:
230 User sysdiag logged in.
Remote system type is VxWorks:.
ftp> ls
200 PORT command successful.
150 Opening ASCII mode data connection for 'file list'.
drwxrwxAwx  1 0       0                 1024 Jan  1 00:00 wwwroot
drwxrwxAwx  1 0       0                  512 Jan  1 00:00 ftp
drwxrwxAwx  1 0       0                  512 Jan  1 00:01 rdt
-rwxrwxAwx  1 0       0                  179 Sep  7 15:00 http.ini
-rwxrwxAwx  1 0       0                  110 Sep  7 15:00 webloader.ini
-rwxrwxAwx  1 0       0                  612 Sep  7 15:00 UserWebFiles.ftp
-rwxrwxAwx  1 0       0                56604 Sep  7 15:00 datalogging.jar
-rwxrwxAwx  1 0       0                59012 Sep  7 15:00 email.jar
-rwxrwxAwx  1 0       0                 5192 Sep  7 15:00 plc.jar
-rwxrwxAwx  1 0       0                 1625 Sep  7 15:00 DC.properties
-rwxrwxAwx  1 0       0                  803 Sep  7 15:00 factorycast.properties
-rwxrwxAwx  1 0       0                 1939 Sep  7 15:00 logserver.properties
226 Transfer complete.
ftp>
```

Hadcoded Username/Password

ashish : ftp

➜ ~ ftp 192.168.100.10

Industrial Communication

- **Famous Protocols:**
  ControlNet, DeviceNet, ProfiNet, Modbus TCP

Modbus TCP is one of the widely used communication protocol

- Is it Secure ?????

Modbus Packet

modbus.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression...

No.	Time	Source	Destination	Protocol	Length	Info
274	2.703354	192.168.100.40	192.168.100.115	Modbus…	107	Response: Trans: 0; Unit: 255, Func: 3: Read Holding Registers
275	2.703741	192.168.100.115	192.168.100.40	TCP	60	12737 → 502 [ACK] Seq=579 Ack=2077 Win=32754 Len=0
276	2.713090	192.168.100.115	192.168.100.40	Modbus…	68	Query: Trans: 0; Unit: 255, Func: 15: Write Multiple Coils
277	2.713159	192.168.100.9	192.168.100.40	Modbus…	68	Query: Trans: 0; Unit: 255, Func: 15: Write Multiple Coils
278	2.724031	192.168.100.40	192.168.100.9	Modbus…	66	Response: Trans: 0; Unit: 255, Func: 15: Write Multiple Coils
279	2.724099	192.168.100.40	192.168.100.115	Modbus…	66	Response: Trans: 0; Unit: 255, Func: 15: Write Multiple Coils
280	2.724440	192.168.100.115	192.168.100.40	TCP	60	12737 → 502 [ACK] Seq=593 Ack=2089 Win=32765 Len=0
281	2.733106	192.168.100.115	192.168.100.40	Modbus…	66	Query: Trans: 0; Unit: 255, Func: 3: Read Holding Registers
282	2.733168	192.168.100.9	192.168.100.40	Modbus…	66	Query: Trans: 0; Unit: 255, Func: 3: Read Holding Registers
283	2.740126	192.168.100.40	192.168.100.9	Modbus…	91	Response: Trans: 0; Unit: 255, Func: 3: Read Holding Registers
284	2.740179	192.168.100.40	192.168.100.115	Modbus…	91	Response: Trans: 0; Unit: 255, Func: 3: Read Holding Registers

```
> Frame 276: 68 bytes on wire (544 bits), 68 bytes captured (544 bits) on interface 0
> Ethernet II, Src: DigitalE_3e:86:3c (00:01:23:3e:86:3c), Dst: AsustekC_c5:33:d4 (d8:50:e6:c5:33:d4)
> Internet Protocol Version 4, Src: 192.168.100.115, Dst: 192.168.100.40
> Transmission Control Protocol, Src Port: 12737, Dst Port: 502, Seq: 579, Ack: 2077, Len: 14
v Modbus/TCP
    Transaction Identifier: 0
    Protocol Identifier: 0
    Length: 8
    Unit Identifier: 255
v Modbus
    .000 1111 = Function Code: Write Multiple Coils (15)
    Reference Number: 119
    Bit Count: 1
    Byte Count: 1
    Data: 01
```

```
0000  d8 50 e6 c5 33 d4 00 01  23 3e 86 3c 08 00 45 00   .P..3... #>.<..E.
0010  00 36 2a 1f 40 00 ff 06  07 b6 c0 a8 64 73 c0 a8   .6*.@... ....ds..
0020  64 28 31 c1 01 f6 b7 1d  52 81 cc 8f 7b 98 50 18   d(1..... R...{.P.
0030  80 00 5f c2 00 00 00 00  00 00 00 08 ff 0f 00 77   .._..... .......w
0040  00 01 01 01                                        ....
```

modbus | Packets: 1721 · Displayed: 1721 (100.0%) · Load time: 0:0.40 | Profile: Default

Modbus Packet

modbus.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression...

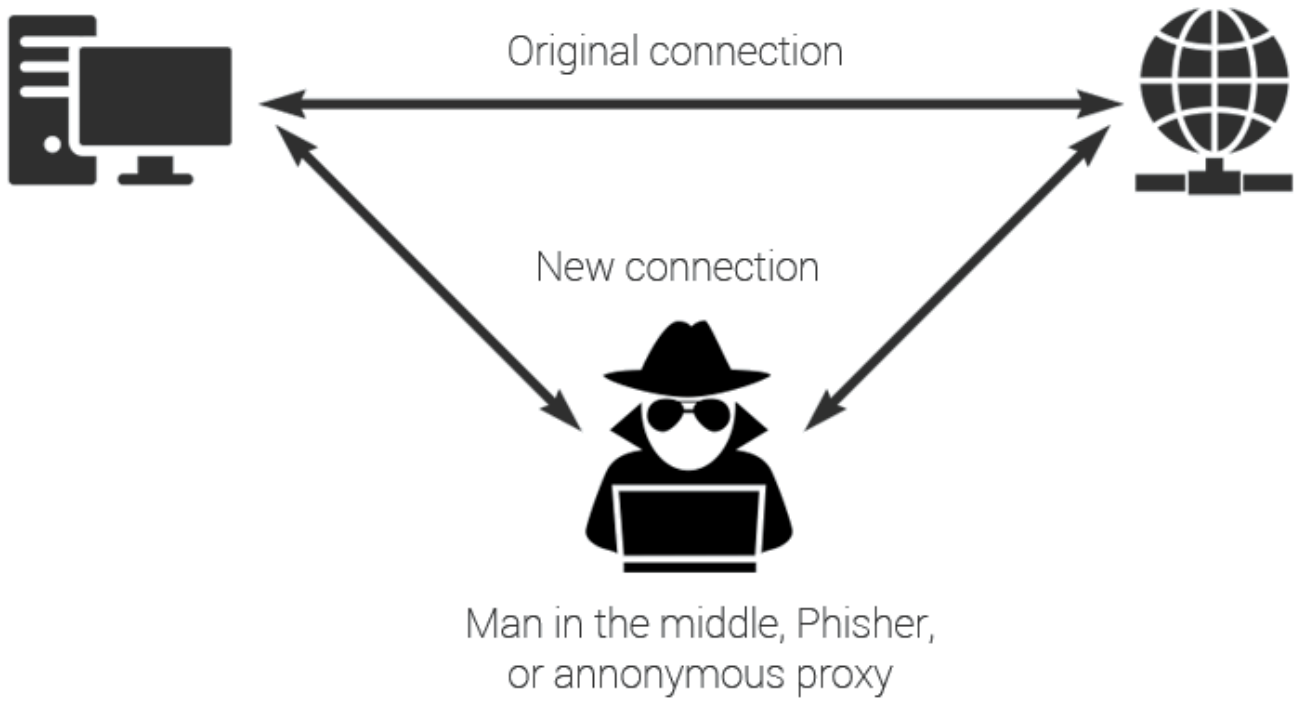
No.	Time	Source	Destination	Protocol	Length	Info
288	2.752124	192.168.100.40	192.168.100.9	Modbus…	179	Response: Trans: 0; Unit: 255, Func: 3: Read Holding Registers
289	2.752184	192.168.100.40	192.168.100.115	Modbus…	179	Response: Trans: 0; Unit: 255, Func: 3: Read Holding Registers
290	2.752610	192.168.100.115	192.168.100.40	TCP	60	12737 → 502 [ACK] Seq=617 Ack=2251 Win=32736 Len=0
291	2.762891	192.168.100.115	192.168.100.40	Modbus…	66	Query: Trans: 0; Unit: 255, Func: 1: Read Coils
292	2.763013	192.168.100.9	192.168.100.40	Modbus…	66	Query: Trans: 0; Unit: 255, Func: 1: Read Coils
293	2.771957	192.168.100.40	192.168.100.9	Modbus…	64	Response: Trans: 0; Unit: 255, Func: 1: Read Coils
294	2.772024	192.168.100.40	192.168.100.115	Modbus…	64	Response: Trans: 0; Unit: 255, Func: 1: Read Coils
295	2.772387	192.168.100.115	192.168.100.40	TCP	60	12737 → 502 [ACK] Seq=629 Ack=2261 Win=32765 Len=0
296	2.808420	192.168.100.9	192.168.100.40	TCP	54	41243 → 502 [ACK] Seq=629 Ack=2261 Win=29200 Len=0
297	2.912077	192.168.100.115	192.168.100.40	Modbus…	68	Query: Trans: 0; Unit: 255, Func: 15: Write Multiple Coils
298	2.912145	192.168.100.9	192.168.100.40	Modbus…	68	Query: Trans: 0; Unit: 255, Func: 15: Write Multiple Coils

```
> Frame 297: 68 bytes on wire (544 bits), 68 bytes captured (544 bits) on interface 0
> Ethernet II, Src: DigitalE_3e:86:3c (00:01:23:3e:86:3c), Dst: AsustekC_c5:33:d4 (d8:50:e6:c5:33:d4)
> Internet Protocol Version 4, Src: 192.168.100.115, Dst: 192.168.100.40
> Transmission Control Protocol, Src Port: 12737, Dst Port: 502, Seq: 629, Ack: 2261, Len: 14
v Modbus/TCP
    Transaction Identifier: 0
    Protocol Identifier: 0
    Length: 8
    Unit Identifier: 255
v Modbus
    .000 1111 = Function Code: Write Multiple Coils (15)
    Reference Number: 119
    Bit Count: 1
    Byte Count: 1
    Data: 00
```

```
0000  d8 50 e6 c5 33 d4 00 01  23 3e 86 3c 08 00 45 00   .P..3... #>.<..E.
0010  00 36 32 1f 40 00 ff 06  ff b5 c0 a8 64 73 c0 a8   .62.@... ....ds..
0020  64 28 31 c1 01 f6 b7 1d  52 b3 cc 8f 7c 50 50 18   d(1..... R...|PP.
0030  80 00 5e d9 00 00 00 00  00 00 00 08 ff 0f 00 77   ..^..... .......w
0040  00 01 01 00                                        ....
```

Reference Number (modbus.reference_num), 2 bytes | Packets: 1721 · Displayed: 1721 (100.0%) · Load time: 0:0.40 | Profile: Default

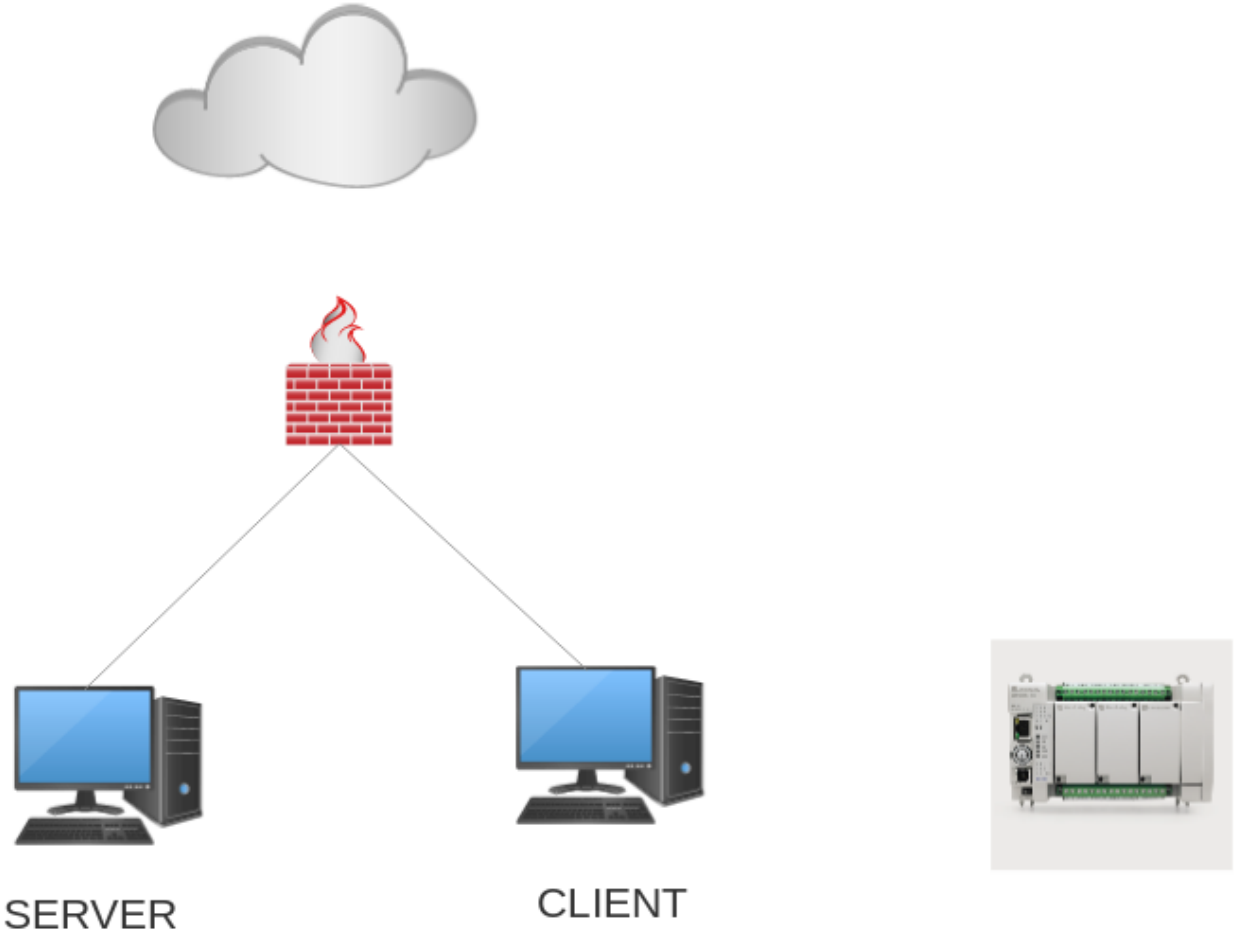
Classical MITM



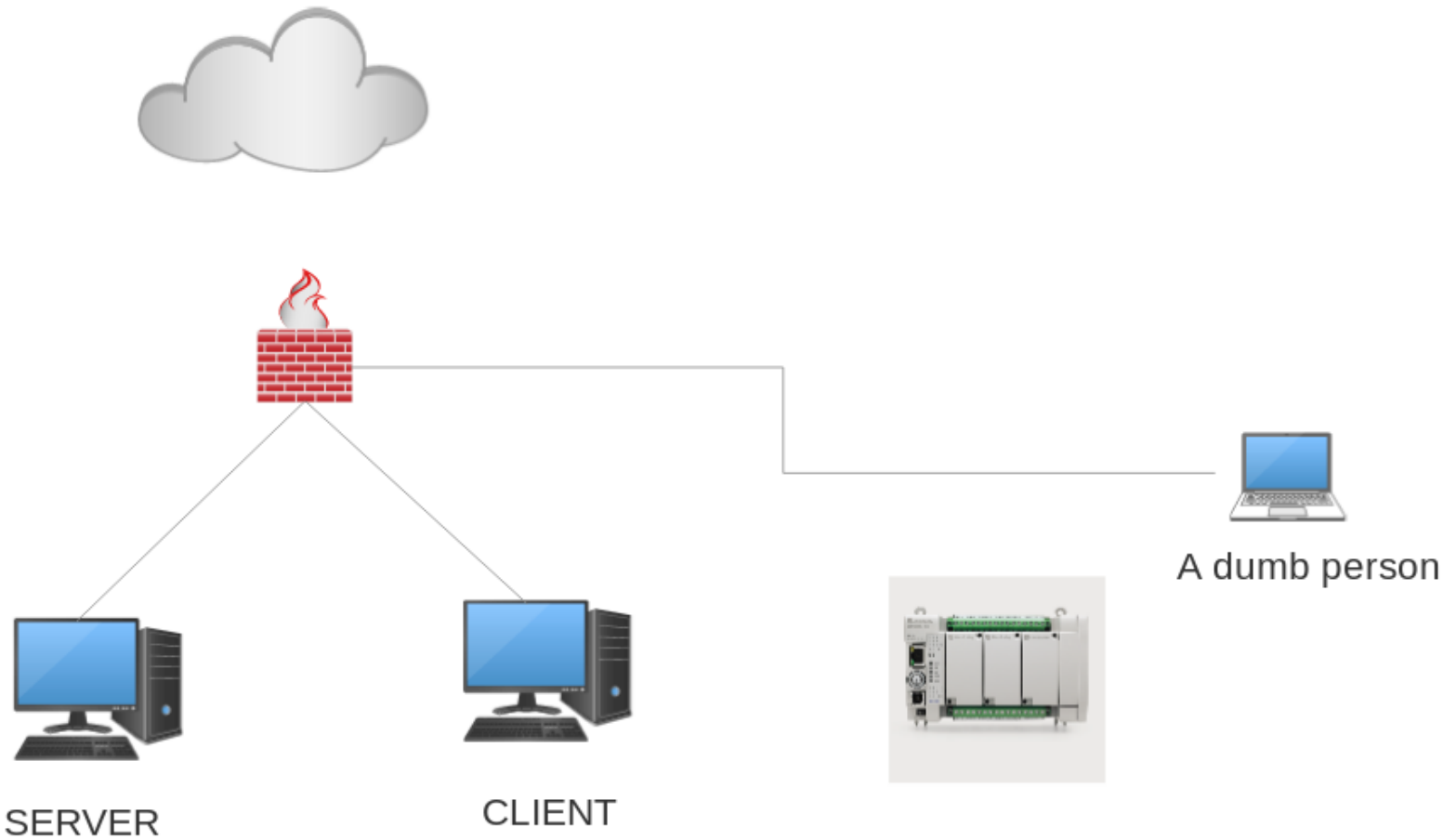
Attack Vector and Process

- Perform arpspoof to forward all the traffic from the client to the attacker machine
- Use IPTABLES to forward it to local port
- Keep an application listening on that local port and modify the payload
- Send back the packet along with modified payload to server

Advance MITM

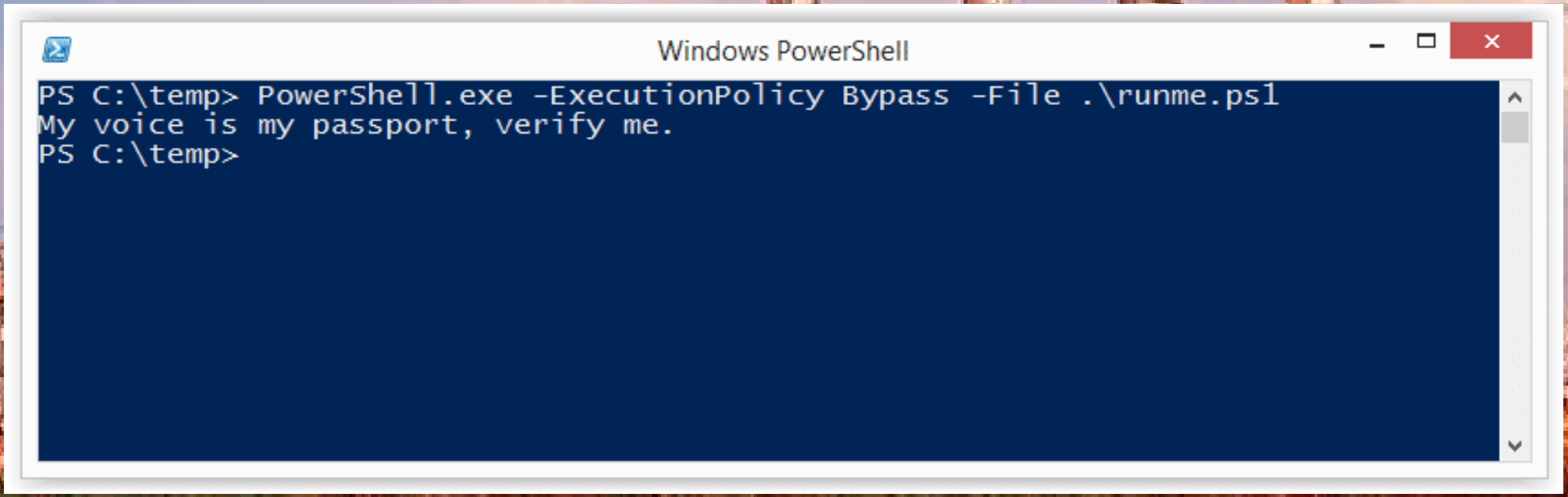


Advance MITM



Worm Execution

- Powershell default policy set to “Restricted”
- Use the “Bypass” Execution Policy Flag



Countermeasures

- Restrict Network Shares
- Update Firmwares
- USB Lockdown
- Do not expose ICS devices on the internet

Future Work

- Reversing VxWorks
- Moving to Windows


Thank You