ICSNet: A Hybrid-Interaction Honeynet for Industrial Control Systems

Luis Salazar[1], Efren Lopez-Morales[2], **Juan Lozano** [1],
Carlos Rubio-Medrano[2] and Alvaro A. Cardenas[1],

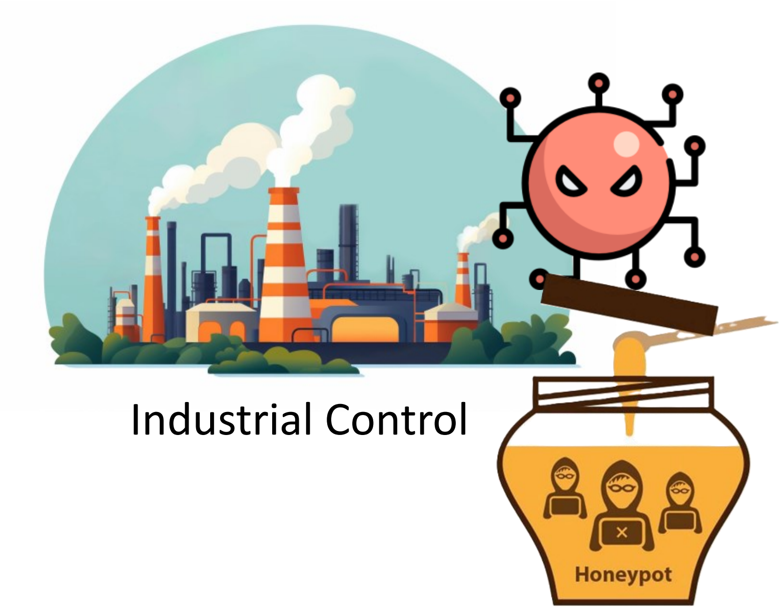
1 University of California, Santa Cruz
2 Texas A&M University, Corpus Christi

CPSIoTSec 2024. October 18th, Salt Lake City, U.S.A

Cyber-Physical Systems

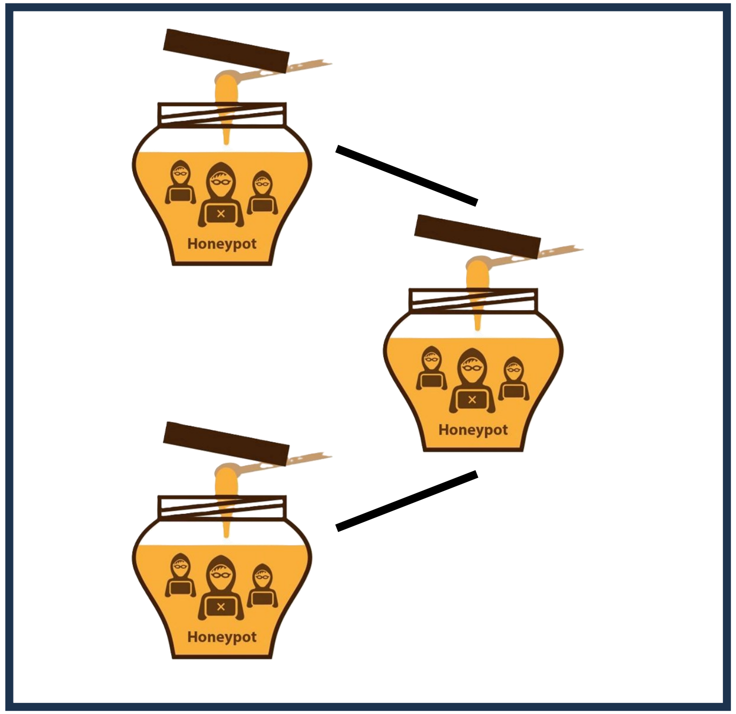
Industrial Control

Cyber-Physical Systems



Industrial Control

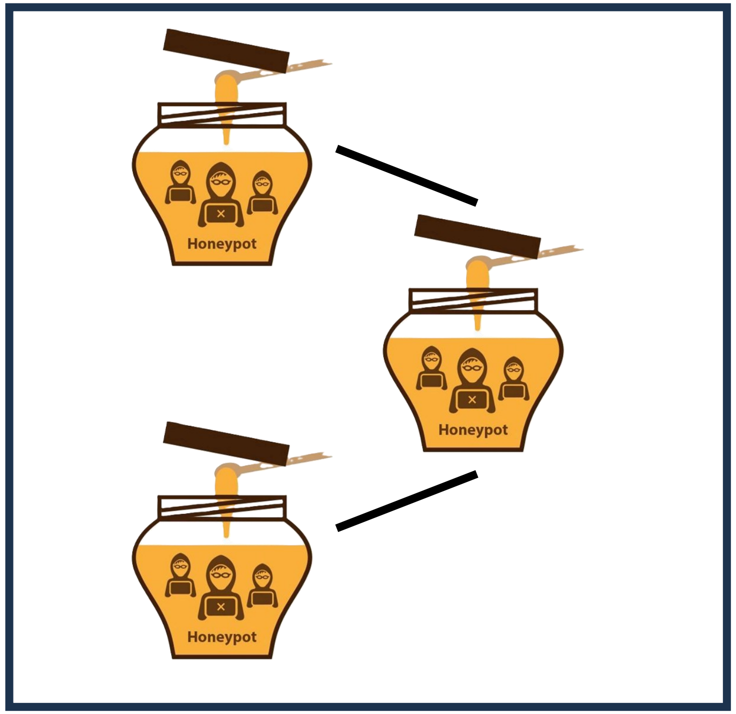
Honeypots and Honeynets



Honeynet

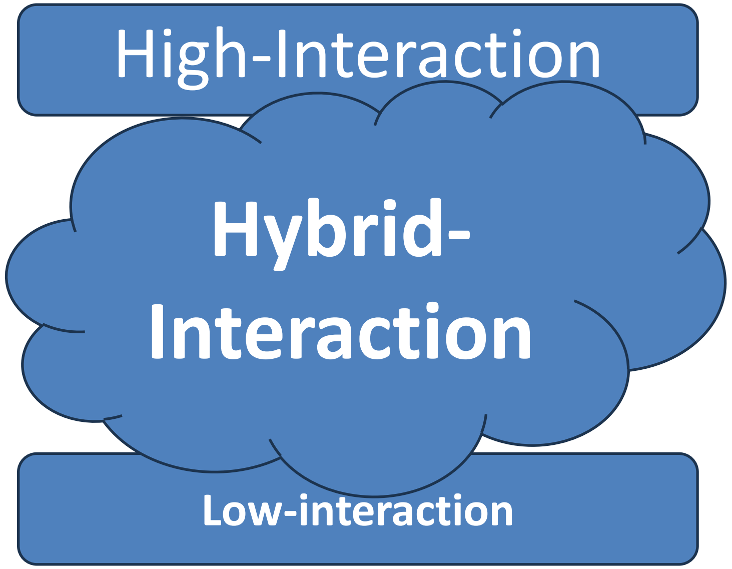
Honeynets interact with attacker; thus, learning its goals, patterns, and techniques, and then provides data to better prepare defense strategies and countermeasures.

Honeypots and Honeynets



Honeynet

Honeynets interact with attacker; thus, learning its goals, patterns, and techniques, and then provides data to better prepare defense strategies and countermeasures.



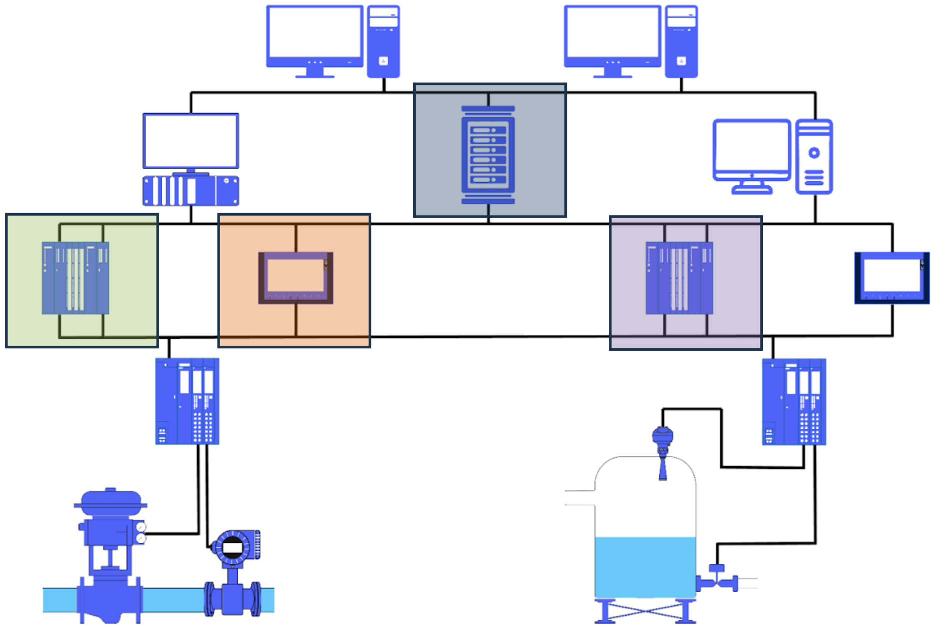
High-Interaction

Hybrid-Interaction

Low-interaction

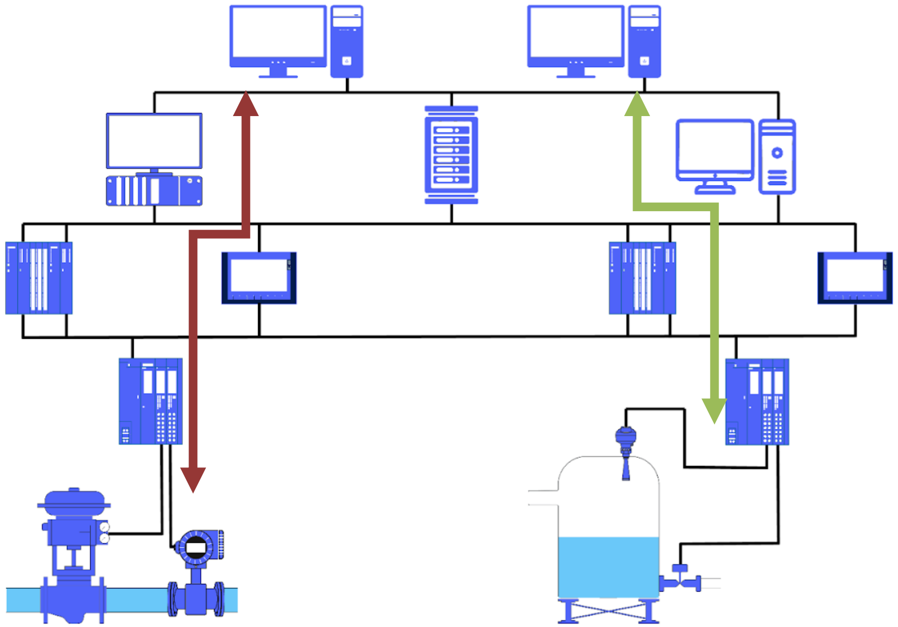
Challenges: ICS Nature

- Diversity of vendors



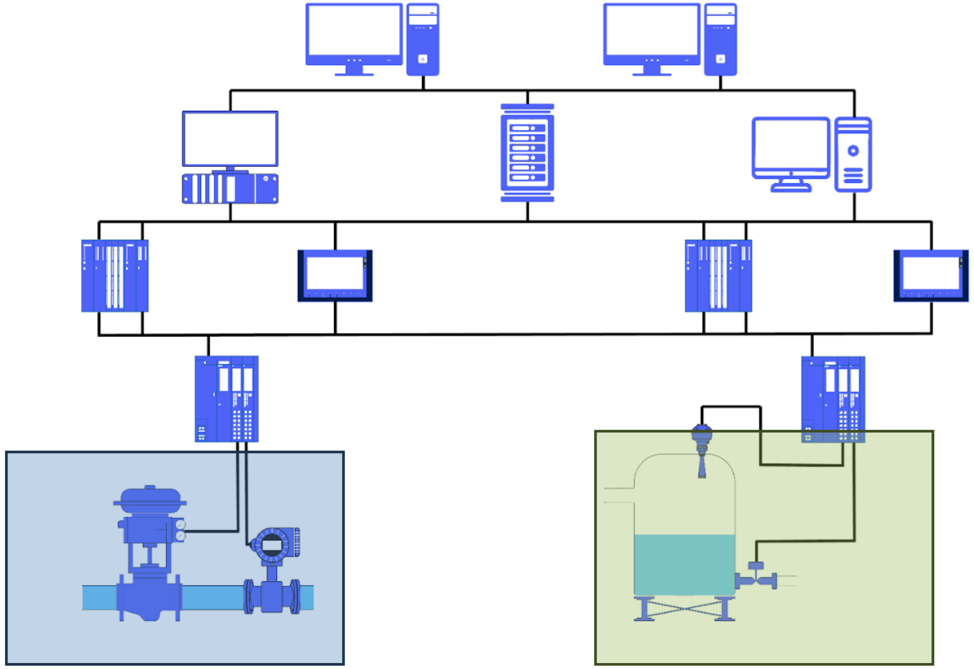
Challenges: ICS Nature

- Diversity of vendors
- Diversity of industrial protocols



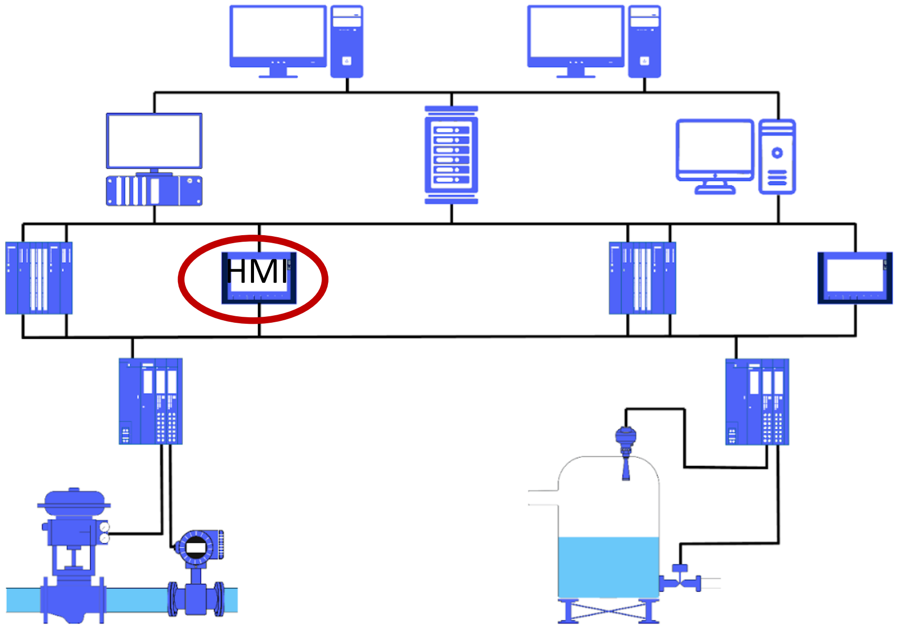
Challenges: ICS Nature

- Diversity of vendors
- Diversity of industrial protocols
- Diverse physical processes



Challenges: ICS Nature

- Diversity of vendors
- Diversity of industrial protocols
- Diverse physical processes
- Different Functionalities (e.g. HMI)



Contribution

	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	ICSNet
Supported ICS Devices	1	1	1	2	NS	2	5	7	12

[1] SCADA HoneyNet Project
[2] Xiao et al, S7CommTrace
[3] Wade, Scada Honeynets
[4] Vestergaard, Conpot
[5] Srinivasa et al, Interaction matters
[6] Conti et al, ICSPot
[7] Lopez-Morales et al, HoneyPLC
[8] Lucchese et al, HoneyICS

NS: Not Specified

Contribution

	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	ICSNet
Supported ICS Devices	1	1	1	2	NS	2	5	7	12
Interaction Level	L	H	H	L	Y	H	H	H	Y

[1] SCADA HoneyNet Project
[2] Xiao et al, S7CommTrace
[3] Wade, Scada Honeynets
[4] Vestergaard, Conpot

[5] Srinivasa et al, Interaction matters
[6] Conti et al, ICSPot
[7] Lopez-Morales et al, HoneyPLC
[8] Lucchese et al, HoneyICS

H: High Interaction; **L:** Low Interaction; **Y:** Hybrid interaction; **NS:** Not Specified

Contribution

	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	ICSNet
Supported ICS Devices	1	1	1	2	NS	2	5	7	12
Interaction Level	L	H	H	L	Y	H	H	H	Y
Network protocols	3	1	1	3	4	4	3	2	5

[1] SCADA HoneyNet Project
[2] Xiao et al, S7CommTrace
[3] Wade, Scada Honeynets
[4] Vestergaard, Conpot
[5] Srinivasa et al, Interaction matters
[6] Conti et al, ICSPot
[7] Lopez-Morales et al, HoneyPLC
[8] Lucchese et al, HoneyICS

H: High Interaction; **L:** Low Interaction; **Y:** Hybrid interaction; **NS:** Not Specified

Contribution

	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	ICSNet
Supported ICS Devices	1	1	1	2	NS	2	5	7	12
Interaction Level	L	H	H	L	Y	H	H	H	Y
Network protocols	3	1	1	3	4	4	3	2	5
Physical Process Simulation	✗	✗	✗	✗	✗	✓	✗	✓	✓

[1] SCADA HoneyNet Project
[2] Xiao et al, S7CommTrace
[3] Wade, Scada Honeynets
[4] Vestergaard, Conpot
[5] Srinivasa et al, Interaction matters
[6] Conti et al, ICSPot
[7] Lopez-Morales et al, HoneyPLC
[8] Lucchese et al, HoneyICS

H: High Interaction; **L:** Low Interaction; **Y:** Hybrid interaction; **NS:** Not Specified

Contribution

	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	ICSNet
Supported ICS Devices	1	1	1	2	NS	2	5	7	12
Interaction Level	L	H	H	L	Y	H	H	H	Y
Network protocols	3	1	1	3	4	4	3	2	5
Physical Process Simulation	✗	✗	✗	✗	✗	✓	✗	✓	✓
Modularity	✗	✗	✗	✓	✓	✓	✓	✓	✓

H: High Interaction; **L:** Low Interaction; **Y:** Hybrid interaction; **NS:** Not Specified

Contribution

	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	ICSNet
Supported ICS Devices	1	1	1	2	NS	2	5	7	12
Interaction Level	L	H	H	L	Y	H	H	H	Y
Network protocols	3	1	1	3	4	4	3	2	5
Physical Process Simulation	✗	✗	✗	✗	✗	✓	✗	✓	✓
Modularity	✗	✗	✗	✓	✓	✓	✓	✓	✓
Honeynet	✓	✗	✓	✗	✗	✗	✗	✓	✓

H: High Interaction; **L:** Low Interaction; **Y:** Hybrid interaction; **NS:** Not Specified

Contribution

	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	ICSNet
Supported ICS Devices	1	1	1	2	NS	2	5	7	12
Interaction Level	L	H	H	L	Y	H	H	H	Y
Network protocols	3	1	1	3	4	4	3	2	5
Physical Process Simulation	✗	✗	✗	✗	✗	✓	✗	✓	✓
Modularity	✗	✗	✗	✓	✓	✓	✓	✓	✓
Honeynet	✓	✗	✓	✗	✗	✗	✗	✓	✓
Supported Manufacturers	1	1	1	2	NS	3	3	3	6

H: High Interaction; **L:** Low Interaction; **Y:** Hybrid interaction; **NS:** Not Specified

Contribution

We designed ICSNet, an open-source ICS honeynet that has **advanced** features for device, protocol and physical process simulation.

https://anonymous.4open.science/r/ics-virtual-testbed-766D

Contribution

We designed ICSNet, an open-source ICS honeynet that has **advanced** features for device, protocol and physical process simulation.

Contribution

We designed ICSNet, an open-source ICS honeynet that has **advanced** features for device, protocol and physical process simulation.

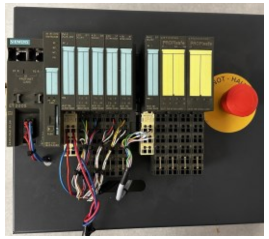
Personality Engine: Device List

We have access to 12 ICS devices from different vendors and diverse functionality.

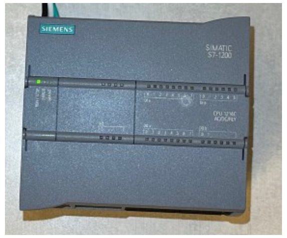
Contribution: Devices

Siemens ET 200

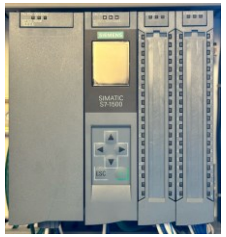
Siemens ET 200s



Siemens S7-1200



Siemens S7-1500



Allen-Bradley MicroLogix 1400

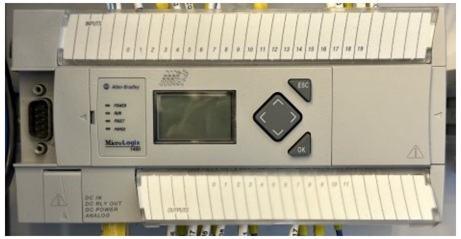
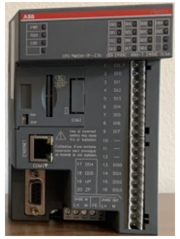
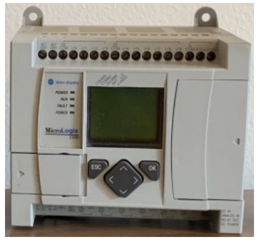


ABB PM554-TP-ETH



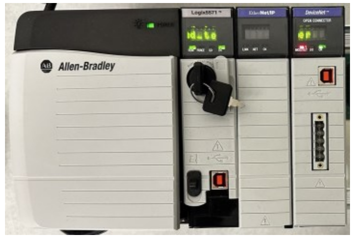
Allen-Bradley Micrologix 1100



Moxa EDS-405A Switch

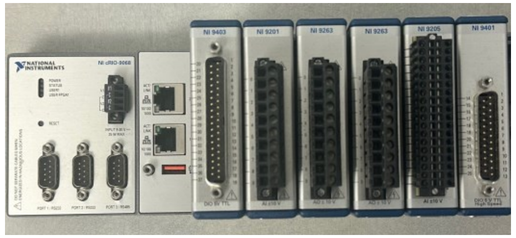
N. I. cRIO-9024

Allen-Bradley ENBT



Siemens S7-300

N. I. cRIO-9068



Contribution

We designed ICSNet, an open-source ICS honeynet that has **advanced** features for device, protocol and physical process simulation.

Personality Engine: Fingerprints

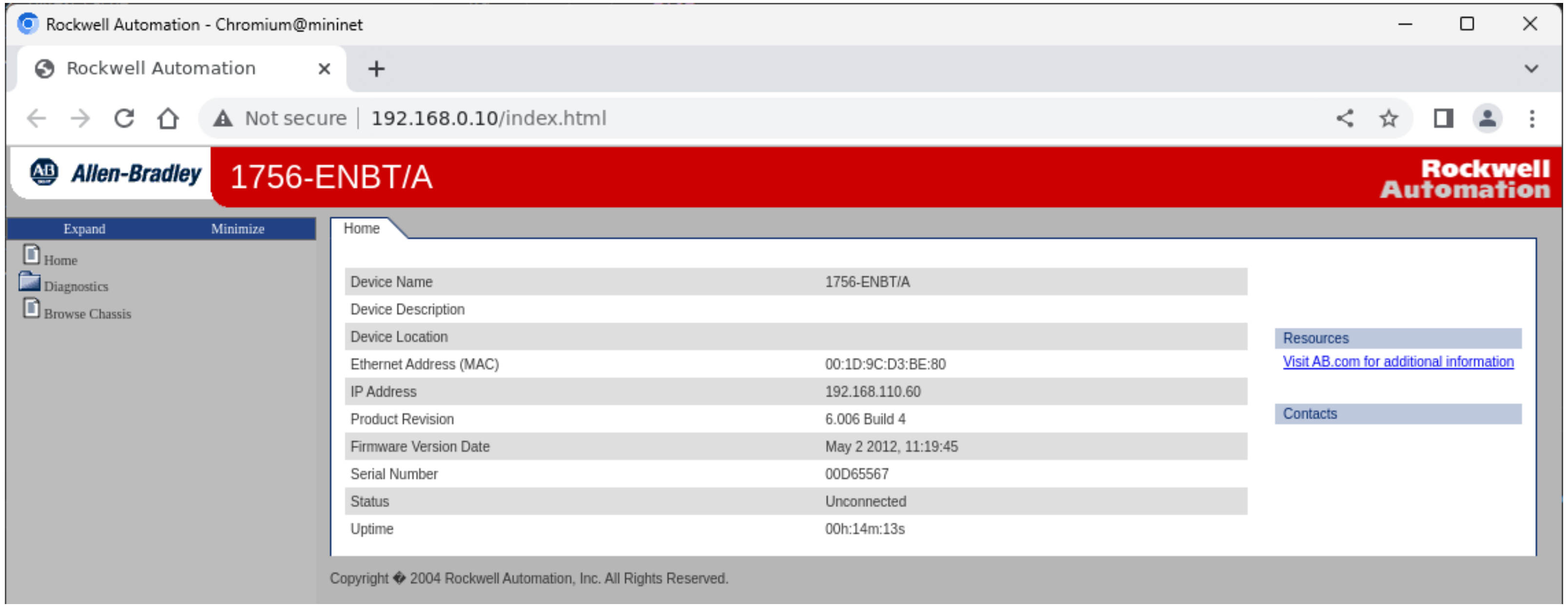
There was no fingerprints for those devices in the open access Nmap database

We used Nmap to extract fingerprints of said devices and use it in our personality engine.

Contribution

We designed ICSNet, an open-source ICS honeynet that has **advanced** features for device, protocol and physical process simulation.

Personality Engine: Web scraping



1756-ENBT/A

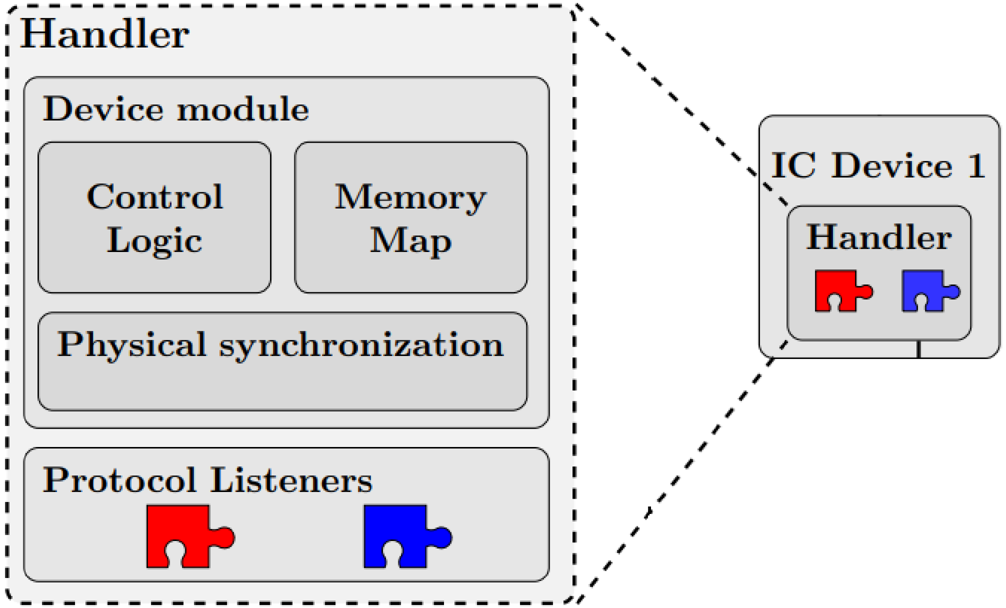
Device Name	1756-ENBT/A
Device Description	
Device Location	
Ethernet Address (MAC)	00:1D:9C:D3:BE:80
IP Address	192.168.110.60
Product Revision	6.006 Build 4
Firmware Version Date	May 2 2012, 11:19:45
Serial Number	00D65567
Status	Unconnected
Uptime	00h:14m:13s

Copyright � 2004 Rockwell Automation, Inc. All Rights Reserved.

Contribution

We designed ICSNet, an open-source ICS honeynet that has **advanced** features for device, protocol and physical process simulation.

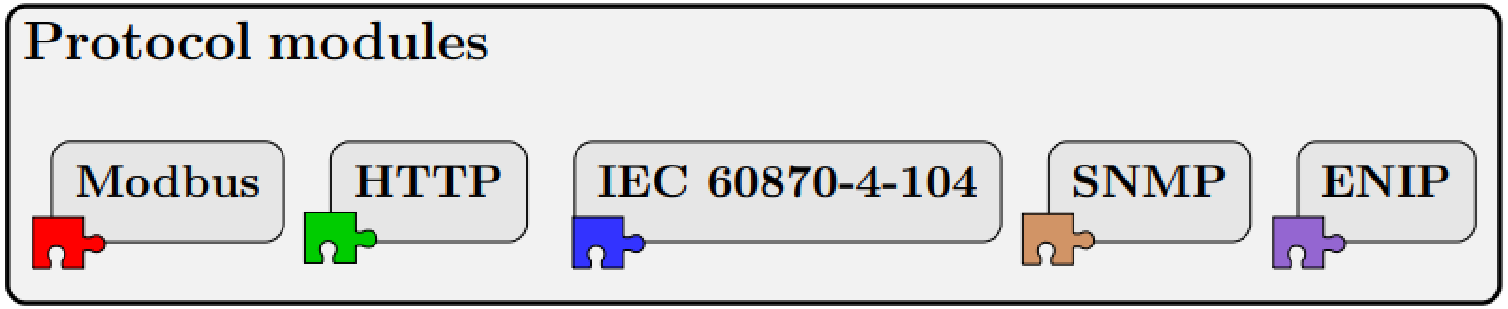
We developed libraries; Protocol Modules, for representative ICS network protocols and deployed them in device handlers as Protocol Listeners.



Contribution

We designed ICSNet, an open-source ICS honeynet that has **advanced** features for device, protocol and physical process simulation.

Representative Network Protocols in ICS



Contribution

We designed ICSNet, an open-source ICS honeynet that has **advanced** features for device, protocol and physical process simulation.

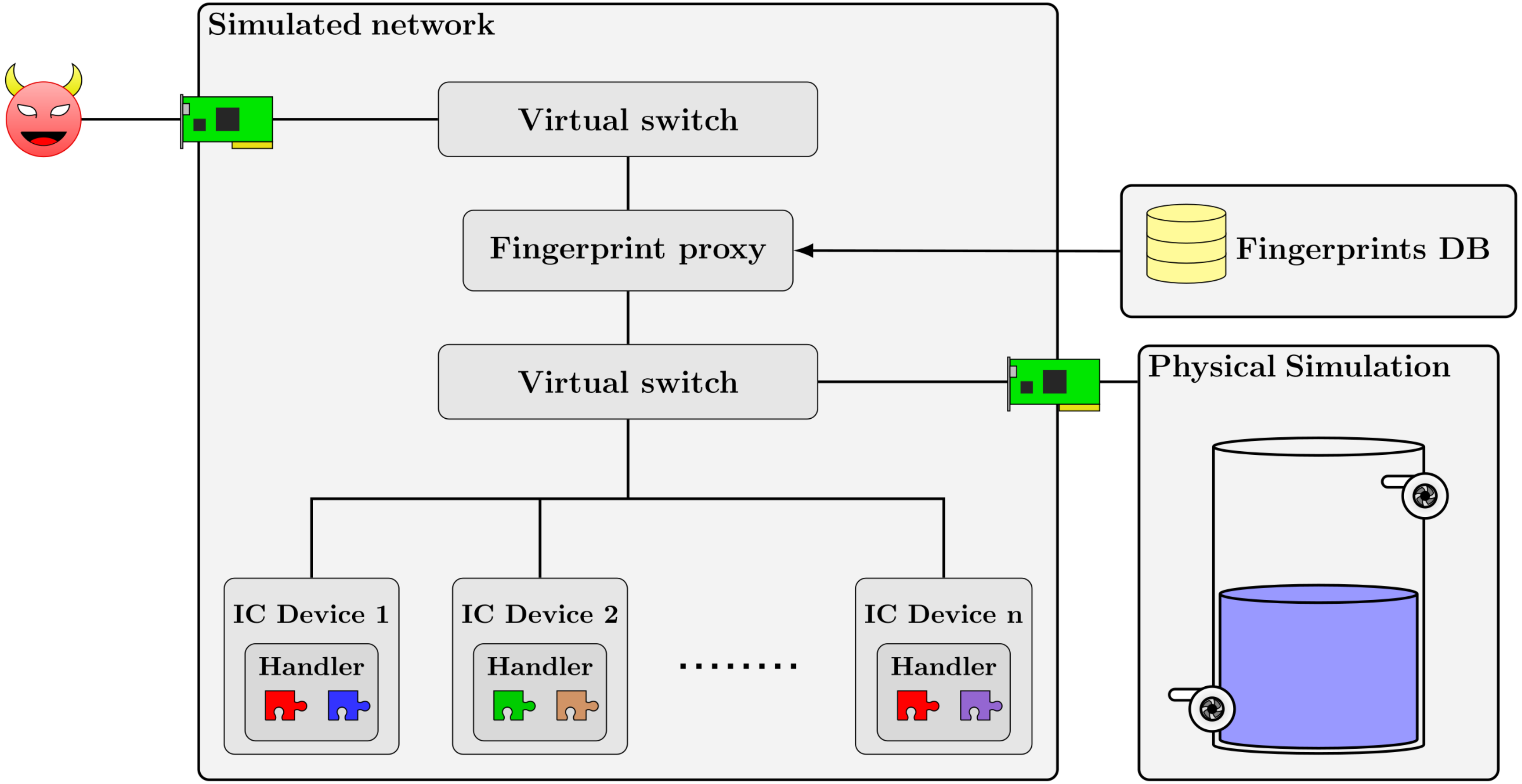
Contribution

We designed ICSNet, an open-source ICS honeynet that has **advanced** features for device, protocol and physical process simulation.

High Fidelity Physical Process Simulation

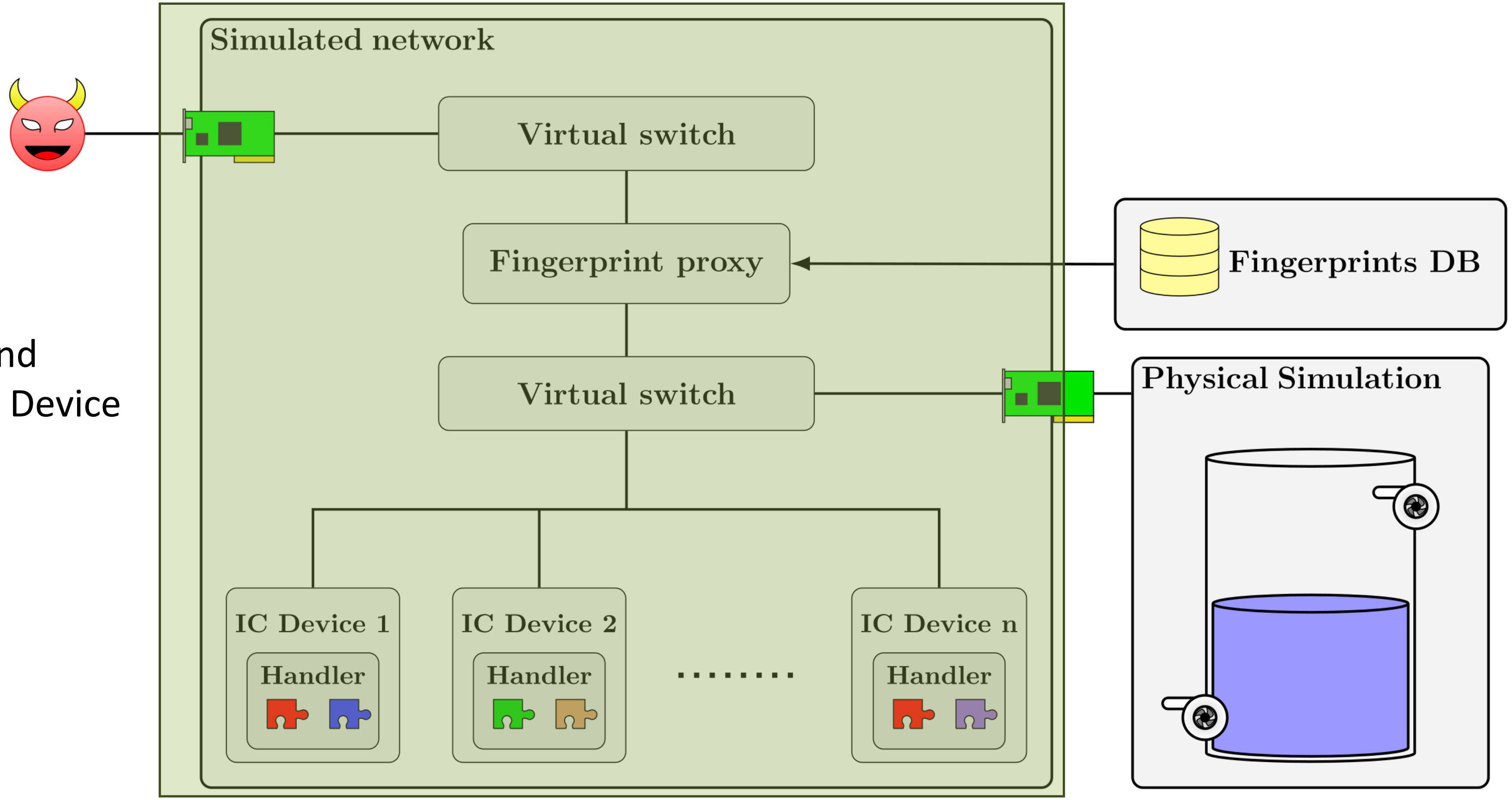
We used an external simulator or PLC trainer, named Factory I/O. We added an HMI via FUXA open-source software.

Architecture: Modularity

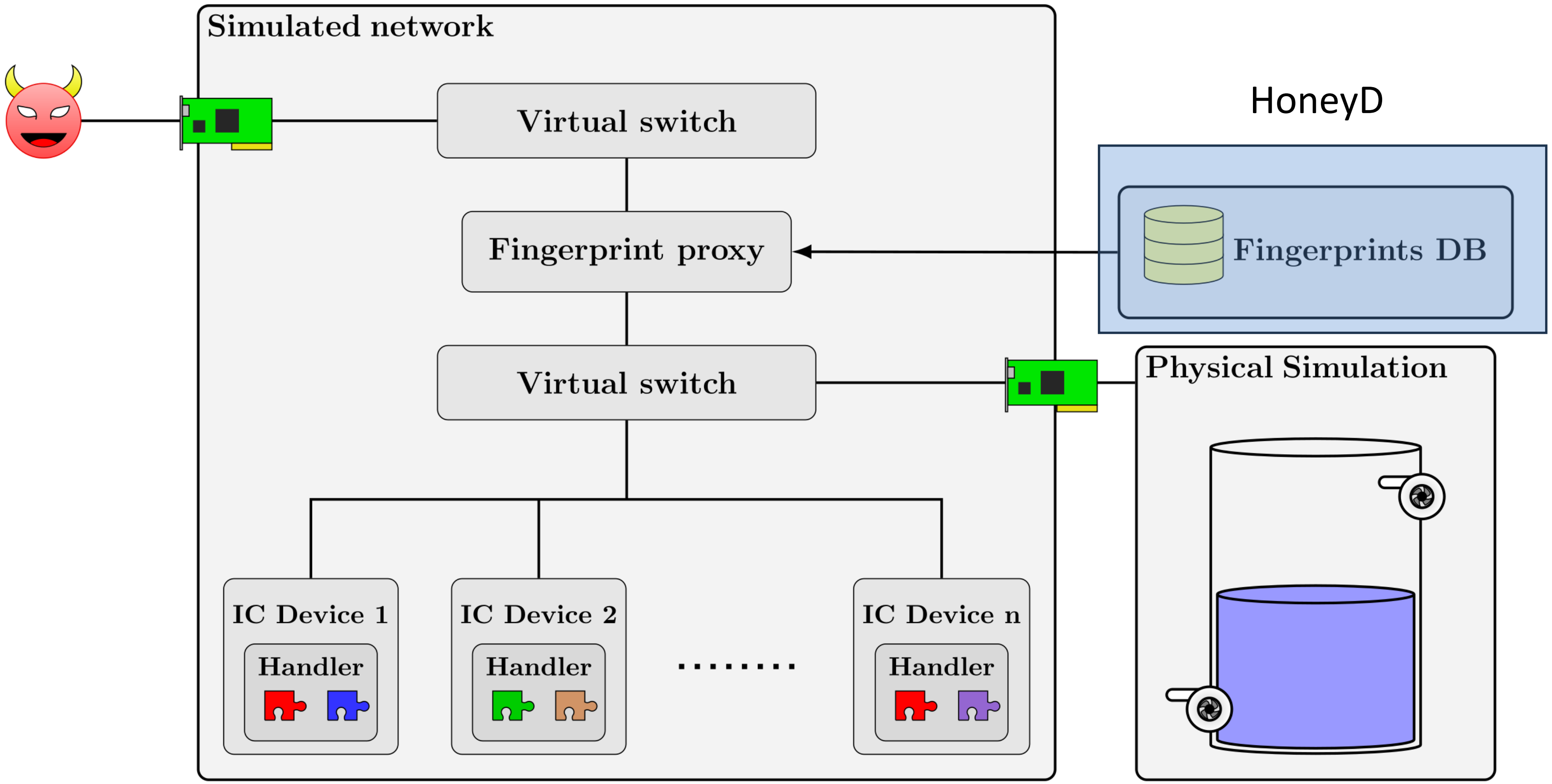


Architecture: Modularity

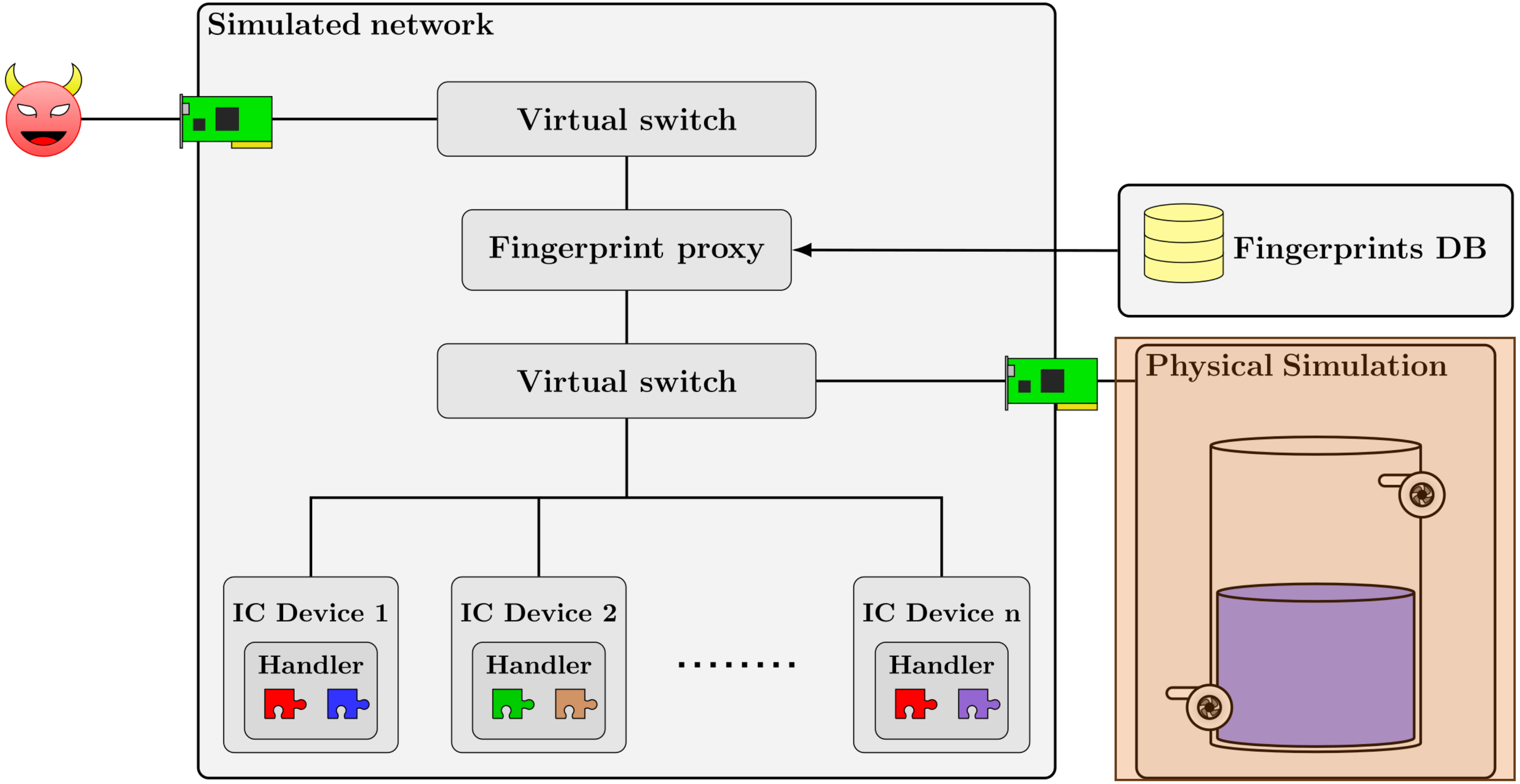
Mininet and specific IC Device Handler



Architecture: Modularity



Architecture: Modularity



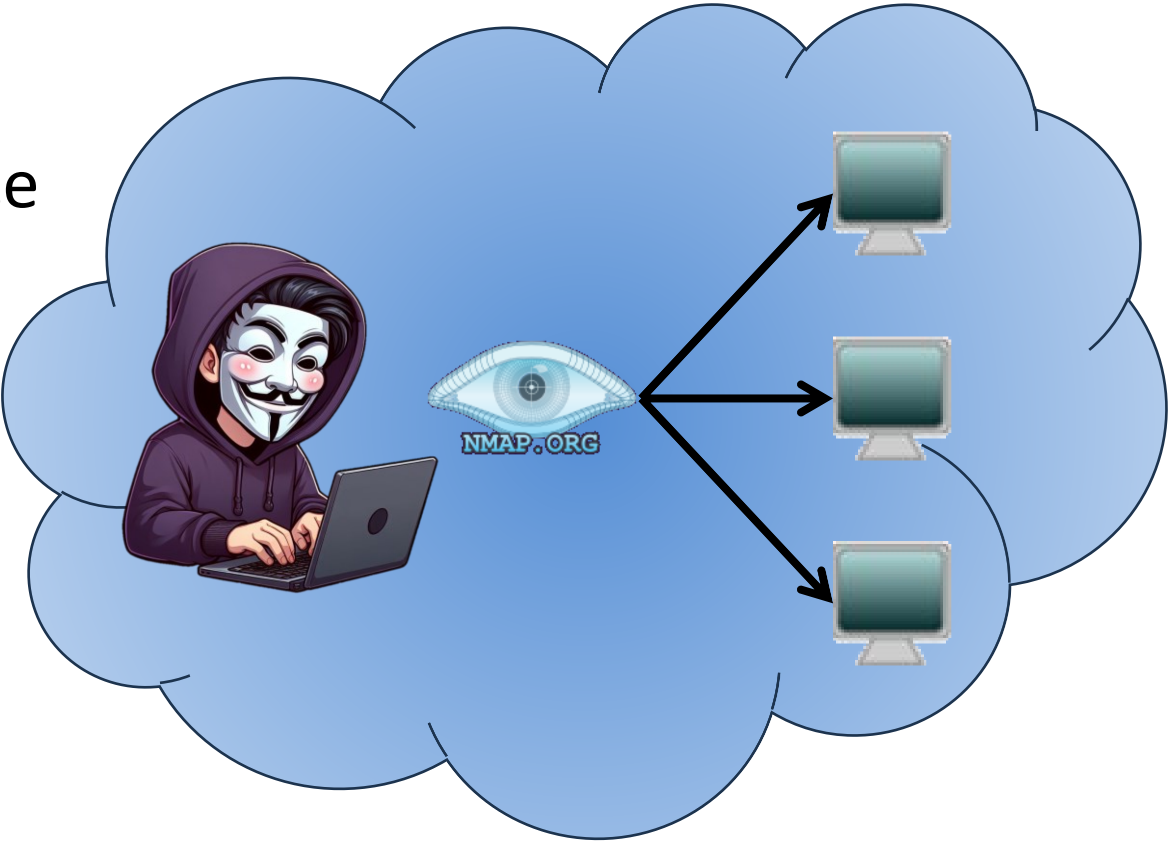
PLC Trainer

Threat Model

- The attacker already has a foothold in the network

- They will perform reconnaissance attacks.

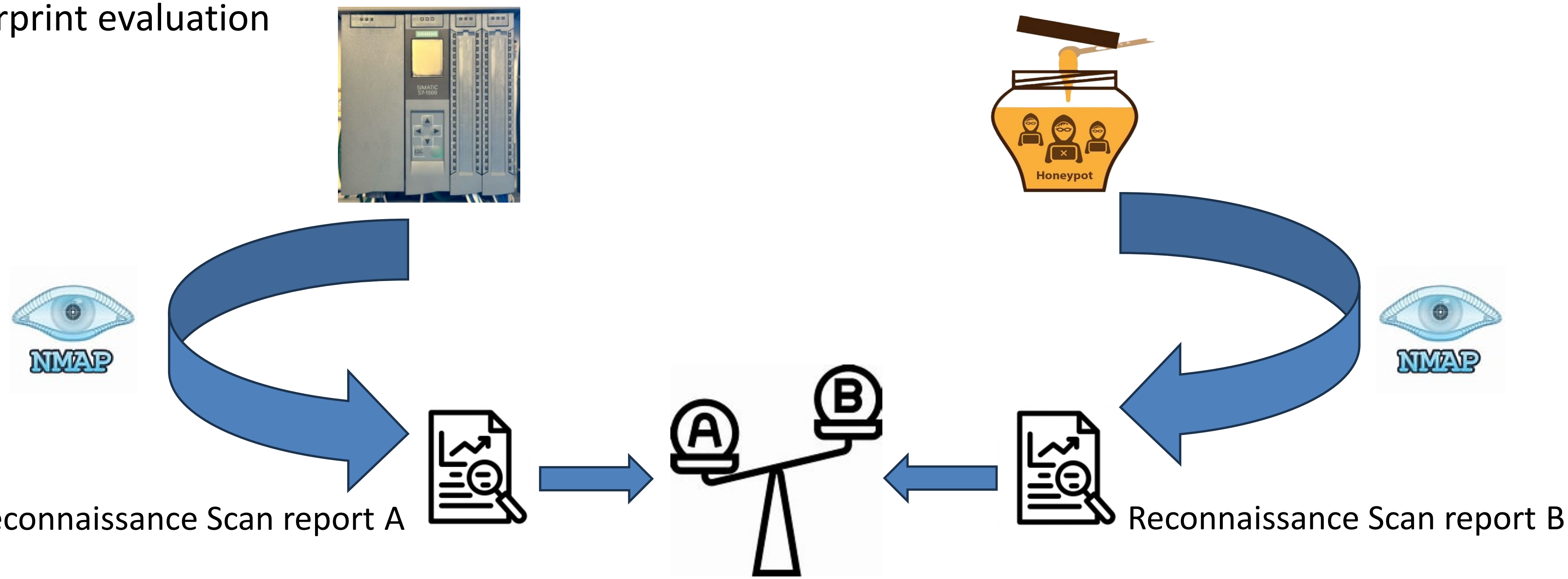
- We assume they use popular tools like NMap



ICSNet Evaluation

Fingerprint, Protocol and Web Evaluation consist in comparing our honeynet-emulated devices versus real devices, to do so we used widely adopted open-source tools like Nmap or Nikto:

1. Fingerprint evaluation



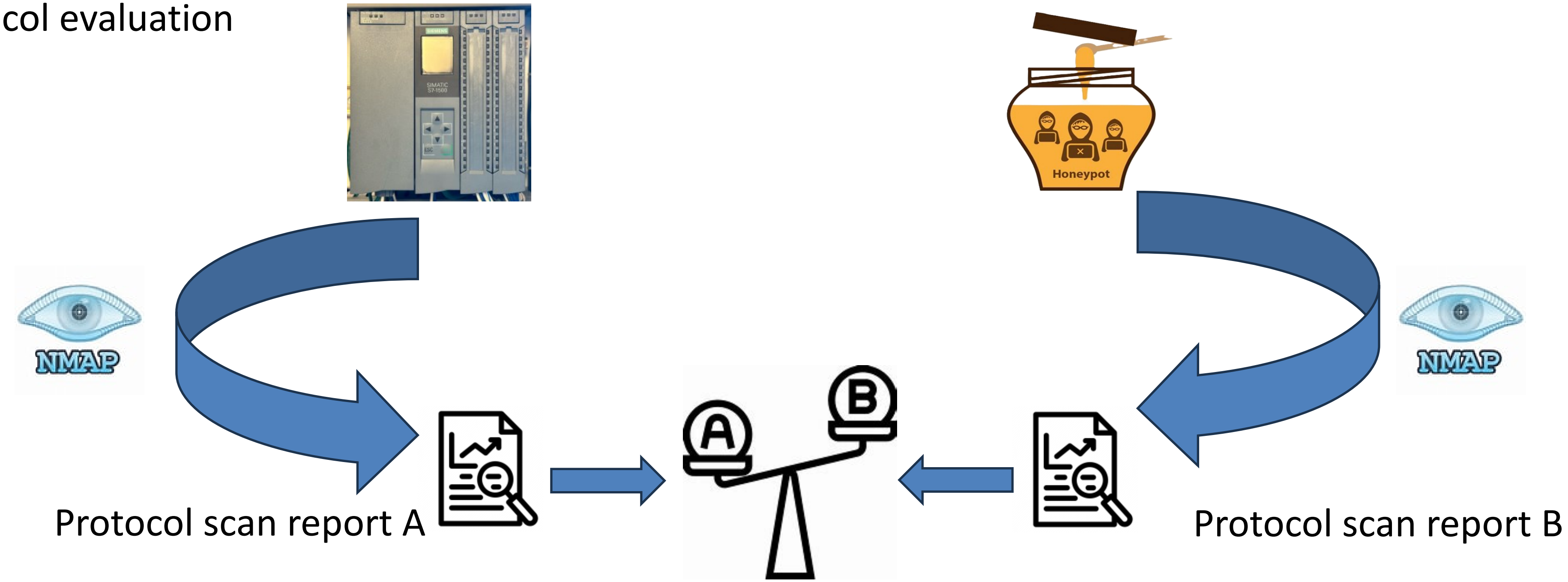
Reconnaissance Scan report A

Reconnaissance Scan report B

ICSNet Evaluation

Fingerprint, **Protocol** and Web Evaluation consist in comparing our honeynet-emulated devices versus real devices, to do so we used widely adopted open-source tools like Nmap or Nikto:

2. Protocol evaluation



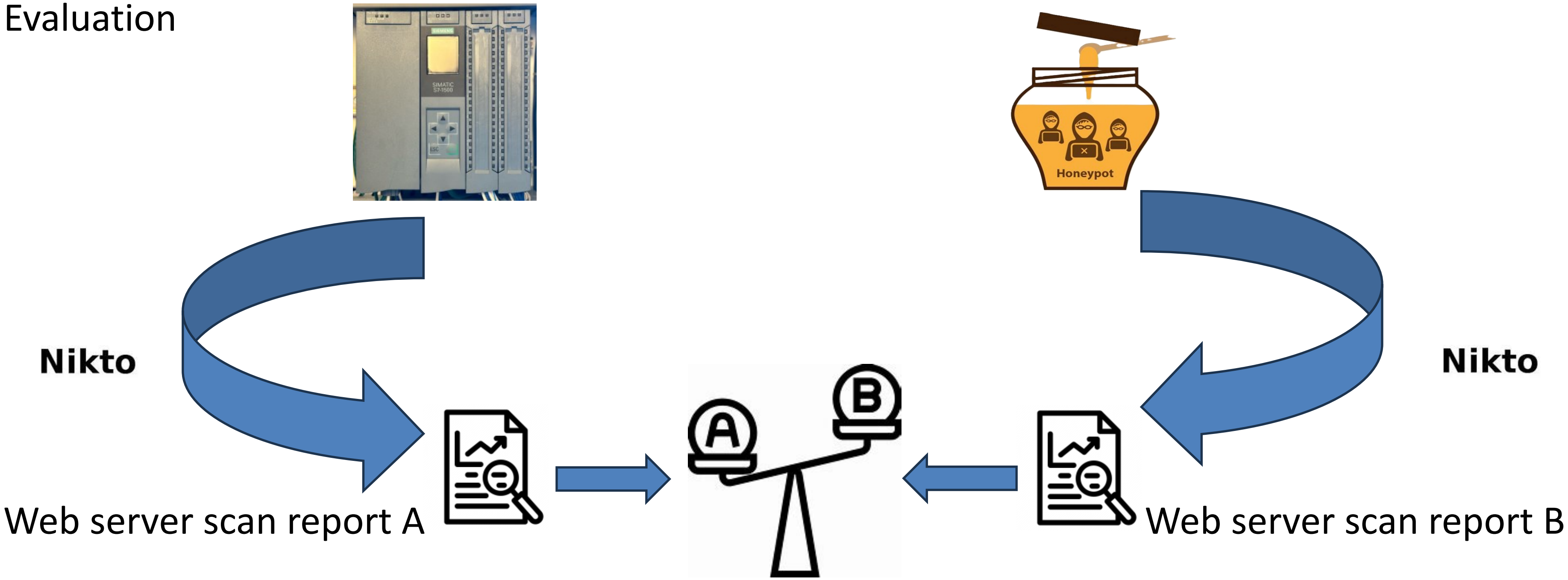
Protocol scan report A

Protocol scan report B

ICSNet Evaluation

Fingerprint, Protocol and **Web Evaluation** consist in comparing our honeynet-emulated devices versus real devices, to do so we used widely adopted open-source tools like Nmap or Nikto:

3. Web Evaluation



Nikto

Nikto

Web server scan report A

Web server scan report B

ICSNet Evaluation

Fingerprint, Protocol and Web Evaluation consist in comparing our honeynet-emulated devices versus real devices, to do so we used widely adopted open-source tools like Nmap or Nikto.

Additionally, we want to know if an attacker can interact with physical process parameters and furthermore exploit known protocol vulnerabilities (**Physical process evaluation**)

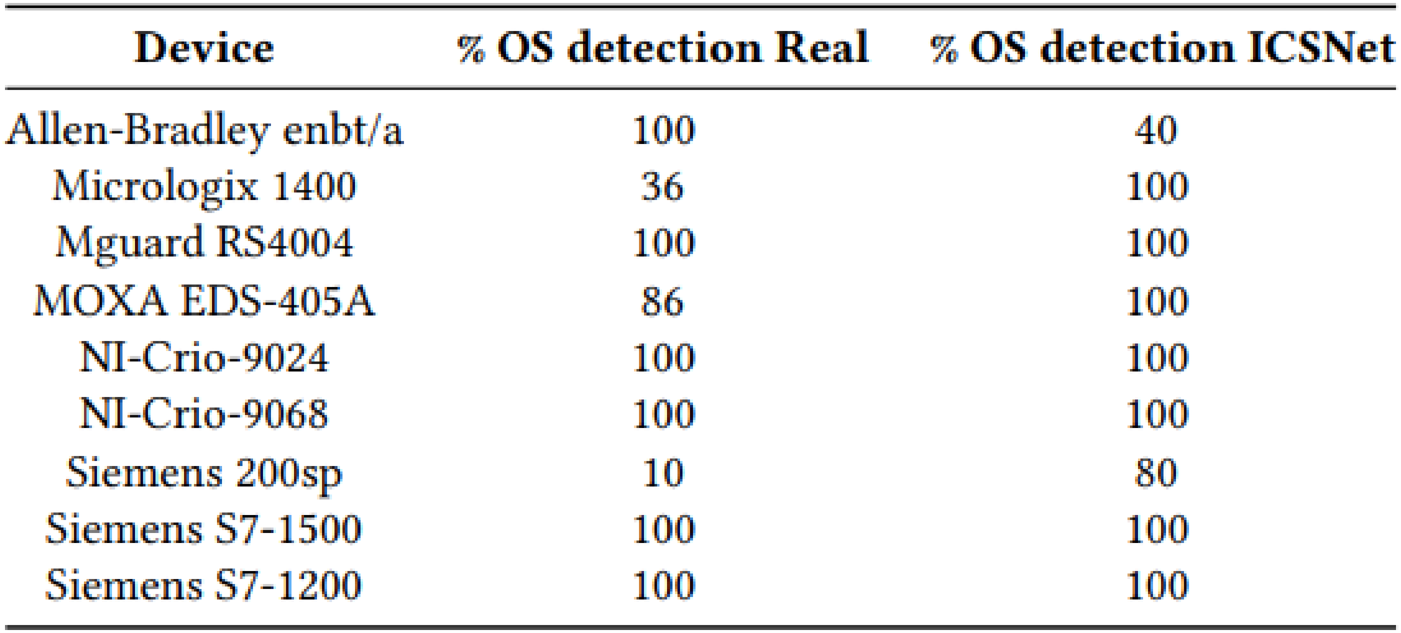
ICSNet Evaluation

1. Device Fingerprint Evaluation

We ran Nmap reconnaissance commands from a machine connected to ICSNet, and we compare those findings running the same commands on the real devices.

ICSNet Evaluation

1. Device Fingerprint Evaluation



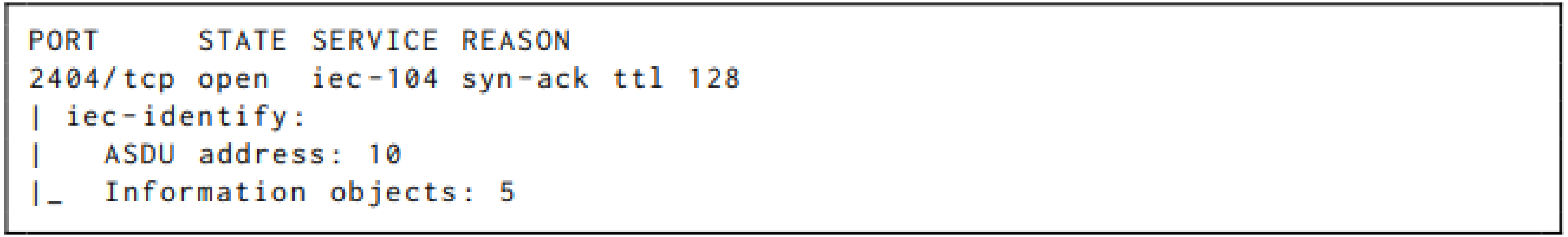
Device	% OS detection Real	% OS detection ICSNet
Allen-Bradley enbt/a	100	40
Micrologix 1400	36	100
Mguard RS4004	100	100
MOXA EDS-405A	86	100
NI-Crio-9024	100	100
NI-Crio-9068	100	100
Siemens 200sp	10	80
Siemens S7-1500	100	100
Siemens S7-1200	100	100

ICSNet Evaluation

2. ICS Protocol Evaluation

We used specific protocol identification using Nmap on the ICSNet emulated devices.

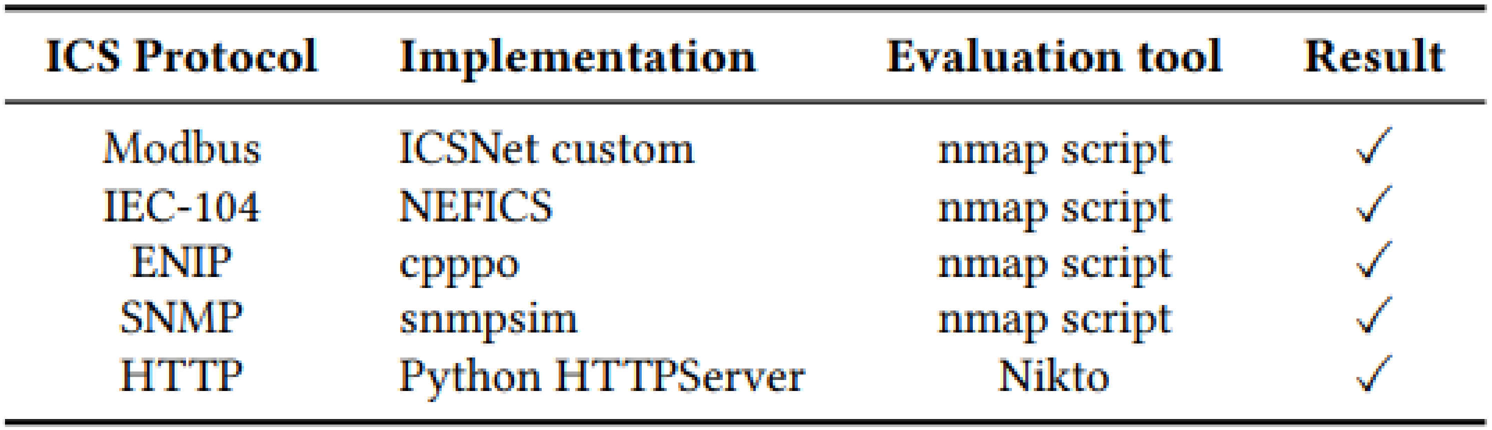
nmap -p 2404 -v -v -v -n -Pn –script=iec-identify 10.0.0.10.



```
PORT      STATE SERVICE REASON
2404/tcp open  iec-104 syn-ack ttl 128
| iec-identify:
|   ASDU address: 10
|_  Information objects: 5
```

ICSNet Evaluation

2. ICS Protocol Evaluation



ICS Protocol	Implementation	Evaluation tool	Result
Modbus	ICSNet custom	nmap script	✓
IEC-104	NEFICS	nmap script	✓
ENIP	cpppo	nmap script	✓
SNMP	snmpsim	nmap script	✓
HTTP	Python HTTPServer	Nikto	✓

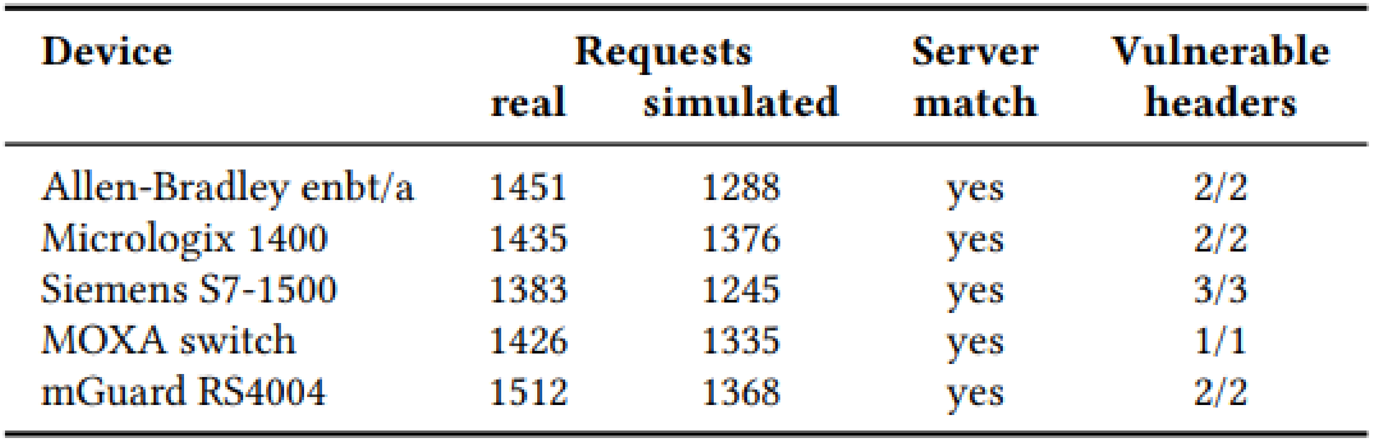
ICSNet Evaluation

3. Web Evaluation

We ran Nikto on subset of devices that have a webpage service in both real devices and ICSNet simulated devices and compare the web server detection.
Nikto also provides a list of http header vulnerabilities and report of web server requests.

ICSNet Evaluation

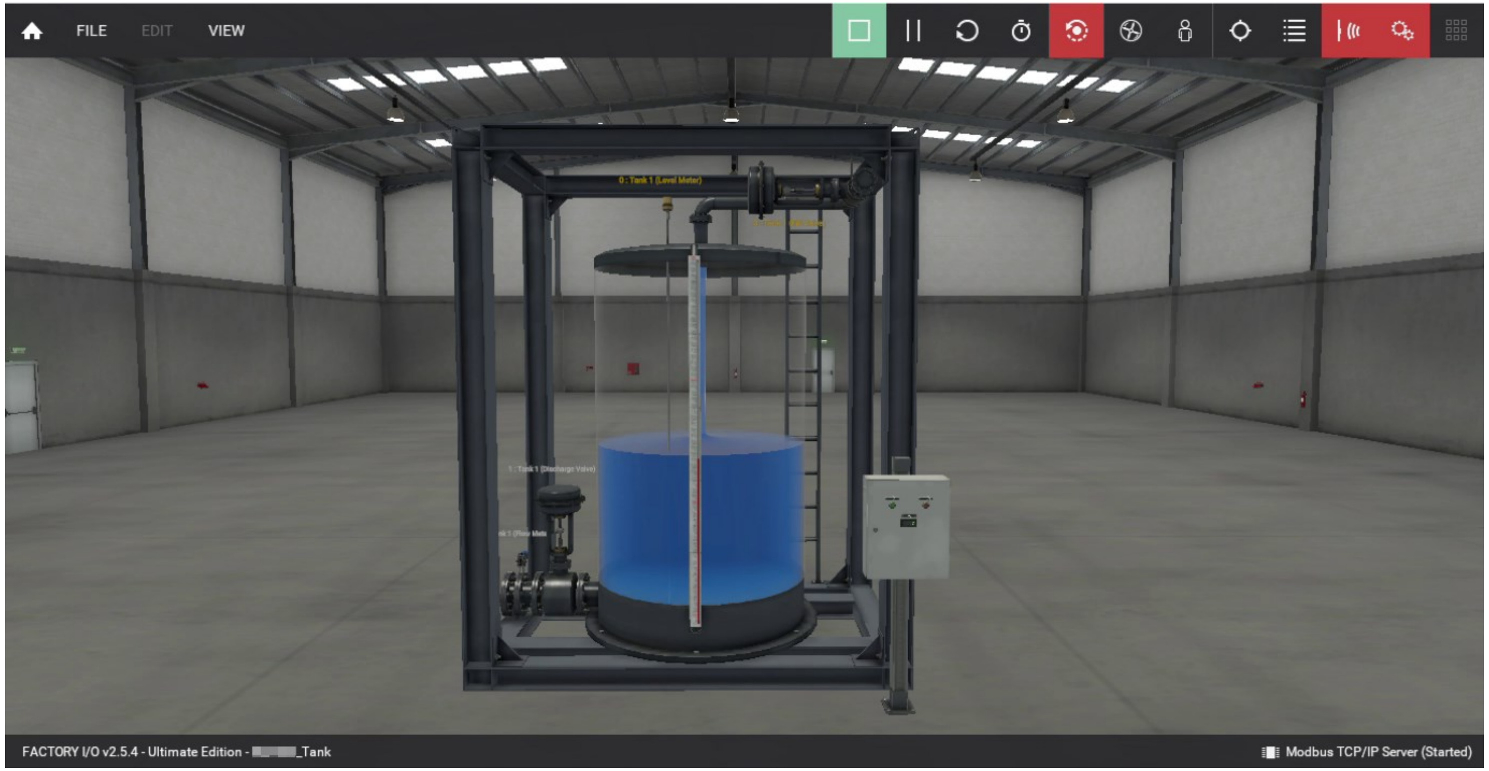
3. Web Evaluation



Device	Requests		Server	Vulnerable
	real	simulated	match	headers
Allen-Bradley enbt/a	1451	1288	yes	2/2
Micrologix 1400	1435	1376	yes	2/2
Siemens S7-1500	1383	1245	yes	3/3
MOXA switch	1426	1335	yes	1/1
mGuard RS4004	1512	1368	yes	2/2

ICSNet Evaluation

4. Physical Process Evaluation

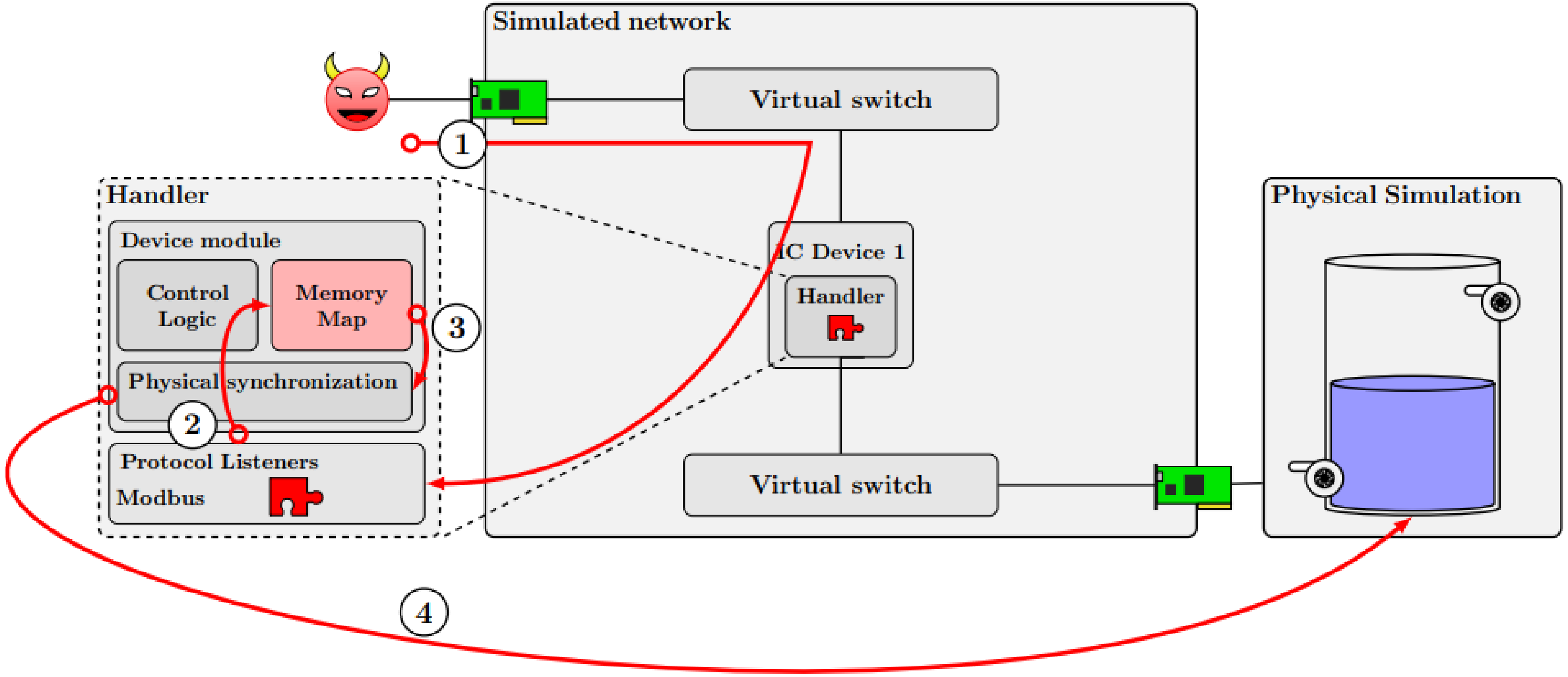


FACTORY I/O v2.5.4 - Ultimate Edition - [redacted]_Tank

Modbus TCP/IP Server (Started)

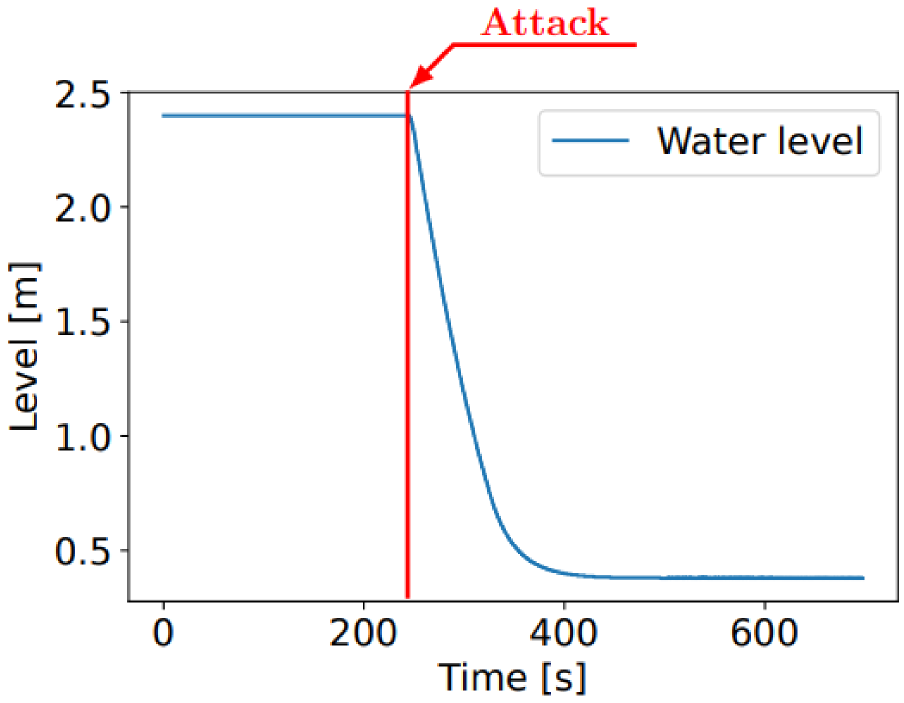
ICSNet Evaluation

4. Physical Process Evaluation



ICSNet Evaluation

4. Physical Process Evaluation



Conclusions and Future Work

We present ICSNet, an industrial honeynet supporting the largest set of devices, protocols, and physical processes

Questions

UC SANTA CRUZ TEXAS A&M UNIVERSITY CORPUS CHRISTI