Honeypots

CPS and IoT Security

Alessandro Brighente

Master Degree in Cybersecurity

Università degli Studi di Padova

SPRITZ Security & Privacy Research Group

Other attacks in ICSs

- Stuxnet was the first example of a cyberattack against an ICSs, but not the only one
- In 2017 Triton malware was able to disable safety instrumented systems in a Saudi Arabian petrochemical plant
- In 2017, WannaCry ransomware took down a car manufactorying factory in Japan

Detection in ICSs

- To effectively protect ICSs it is necessary to develop new methods for attack detection and mitigation
- Firewalls and anti-virus solutions are reactive and require updates in order to detect/prevent new forms of malicious traffic
- Zero-day exploits can consequently penetrate networks and infect systems while being undetected
- Bring your own device makes it hard to define clear security perimeters

Honeypots

- A solution aiming at mitigating novel (potentially unknown) attacks is via *honeypots*
- Honeypots are systems with no inherent purpose rather than capturing attacks either on the internet of within a networks
- Generally, they do not receive any legitimate traffic
- Many different types of honeypots, ranging from emulating specific services (e.g., SSH) to fully fledged systems with multiple running services

Honeypots

SPRITZ Security & Privacy Research Group
Università degli Studi di Padova

- Proactive approach to security: adversaries are encouraged to attack these systems to reveal valuable threat intelligence
- This gives indication on new vulnerabilities and associated exploits
- Broader view of offensive tactics and techniques
- In 2020, honeypots helped in identifying four zero-day vulnerabilities in ICS, proving their effectiveness

Legal Caveat

- Entrapment: defense to criminal charges when it is established that the agent or official originated the idea of the crime and induced the accused to engage in it
- Other experts consider honeypots not only unethical, but a disadvantage to the computer world since they are “building the better hacker”
- However, pretty useful, nah?

Legal Caveat

- Entrapment: defense to criminal charges when it is established that the agent or official originated the idea of the crime and induced the accused to engage in it
- Other experts consider honeypots not only unethical, but a disadvantage to the computer world since they are “building the better hacker”
- However, pretty useful, nah?

Honeypots Types

- Honeypots can be either virtual or physical and are designed to be exploitable
- Virtual: install and simulate hosts on the network from different operating systems and simulate the whole TCP/IP stack. More frequent modality
- Physical: real machines with their own IP addresses simulating the behaviors modeled by the system. Higher price for purchasing and maintenance, so less frequent

Honeypots Types

- Honeypots can be either virtual or physical and are designed to be exploitable
- Research honeypots: facing the internet and deployed to gather information for research purposes
- Production honeypots: usually not directly accessible and deployed inside an organizational network
- Need to be configured with care to avoid the entrapment problem
- When compromised, they can generate alerts, deceive the attacker by diverting exploitation efforts away from the system

Honeynets

- A honeynet can be defined as two or more honeypots implemented on a system
- More specifically, it is a high interaction honeypot system of generation I, II, and III
- Usually, although using multiple honeypots in a system, the literature talks about honeypots

Generation I

- First appeared in 1999 with the goal of capturing actions from the black-hat community
- It consists of a firewall supported by an IDS at front and a honeypot in the back
- They can capture in-depth information and capture unknown attacks
- However, they can easily be detected by attackers

Generation II and III

- Generation II as developed in 2002 and had an honeynet sensor that serves the purpose of the IDS and of the firewall in Generation I
- The sensor works like a bridge, so it is more difficult for attackers to detect it
- Generation III was developed in 2004 and had the same architecture as Generation II
- However, it has improved deployment and management capabilities

Two Types

Low-interaction	High interaction
Solution emulates operating systems and services	No emulation, real operating systems and services are provided
• Easy to install and deploy. • Usually requires simply installing and configuring software on a computer. • Minimal risk, as the emulated services control what attackers can and cannot do. • Captures limited amounts of information mainly transactional data and some limited interaction	• Can capture far more information including new tools, communications, or attacker keystrokes. • Can be complex to install or deploy (commercial versions tend to be much simpler). • Increased risk, as attackers are provided real operating systems to interact with

The First ICS Honeypot

- The first honeynet for SCADA ICS was proposed by Cisco Systems' SCADA HoneyNet Project in 2004
- It is based on an open-source honeypot framework Honeyd
- It is a low interaction honeynet that supports the simulation of Modbus/TCP, FTP, Telnet, and HTTP services running on a PLC
- We need to simulate various entry points so that when the attacker encounters a perimeter device will be presented the same network as a SCADA network
- Router connected to Internet, Direct serial device, HMIs,...

Digital Bond SCADA HoneyNet

- The second honeynet for ICSs was proposed by Digital Bond in 2006 under the name of SCADA HoneyNet
- Two virtual machines
  - one simulates a PLC with Modbus/TCP, FTP, Telnet, HTTP, and SNP services
  - One is a Generation III Honeywall, i.e., a honeynet that monitors and controls the honeypot traffic and attacker interactions

Digital Bond SCADA HoneyNet

SPRITZ Security & Privacy Research Group

Università degli Studi di Padova

- From the attacker's perspective, the target is simply an internet facing machine
- The attacker can launch an nmap and discover open ports and services
- Furthermore, the attacker can type an URL (e.g., http://bld-control.iac.iastate.edu i) to find the homepage for Schneider Electric Modicon Modbus/TCP and get for instance diagnostic information

Digital Bond SCADA HoneyNet

- From the administrator's perspective, the attacker only reaches a second NIC on the physical machine hosting both the Honeywall and the Target VMs
- The honeywall bridge bridges the adversary with the target VM logging activities as it does so
- The administrator can manage the honeynet locally or remotely via a properly configured NIC

Making Target VM credible

- If the honeypot is too easy to attack, the attacker might get suspicious and detect that operations are actually happening inside a honeypot
- Services in the target VM are partially implemented to give the impression of a real system without providing the attacker too many opportunities for successful attacks
- For instance, Telnet will return banners that resemble a PLC but will not actually allow any login

Making Target VM credible

```
[root@kosh]# ftp 129.186.215.1
Connected to 129.186.215.1.
220 VxWorks FTP servers (VxWorks 5.3.1) ready.
534 Only TLS is supported.
534 Only TLS is supported.
KERBEROS_V4 rejected as an authentication type
Name (129.186.215.1:root): root
331 Need password for user root
Password:
431 Username and password do not match
Login failed.
ftp>
```

Conpot

- Conpot is one of the most famous ICS honeypots that have been used by researchers
- Open-source low-interaction honeypot developed under the Honeynet Project (Link to the Conpot project)
- It supports various industrial protocols including IEC 60870-5, Building Automation and Control Network, Ethernet/IP, Modbus, S7Comm and others such as HTTP, FTP, SNMP and TFTP
- It comes with templates for Siemens S7 PLCs, Guardian AST tank monitoring systems, and Kamstrup 382 smart meters

Nmap-ping Conpot

- Let’s use the Nmap scanner to see what Conpot exposes
  - nmap -A -v [IP Address]
  - nmap -A -v -Pn [IP Address]
  - nmap -A -v -Pn -p- [IP Address]
- The flag -A results in Nmap turning on version detection and other advanced and aggressive features (according to docs)
- Very intrusive and readily detected but provides a good representation on what to expect (if executed on a standard machine)

Nmap-ping Conpot

SPRITZ Security & Privacy Research Group

Università degli Studi di Padova

- Let's use the Nmap scanner to see what Conpot exposes
  - nmap -A -v [IP Address]
  - nmap -A -v -Pn [IP Address]
  - nmap -A -v -Pn -p- [IP Address]
- The Pn results in Nmpa to suppress pings when conducting scans to determine if a host is up
- Virtual machines are up and reject pings
- -p to conduct the scan over the whole port range 0-65535
- -v for version detection (although -A already does that)

Nmap-ping Conpot

SPRITZ
Security & Privacy
Research Group

Università
degli Studi
di Padova

- Scanning with the -v and -A flags resulted in no results from the Guardian AST, IPMI, and Kampstrup smart meter
- Pings are rejected
- However, port 22 (ssh) is revealed, an attacker might get suspicious!

TABLE II. NMAP SCANNING (UTILIZING FLAGS –V AND –A)

Honeypot Type	Result	Ports Opened by Conpot
Siemens S7-200	22, 80	80,102, 161, 502, 623, 47808
Guardian AST	N/A	10001
IPMI	N/A	623
Kampstrup Smart Meter	N/A	1025, 50100

Nmap-ping Conpot

SPRITZ
SECURITY & PRIVACY
RESEARCH GROUP

UNIVERSITÀ
DEGLI STUDI
DI PADOVA

- By suppressing pings we get way more results!
- However, most of these ports are not SCADA ports
- E.g., 514 is for system logging ➔ Ubuntu services are still there

TABLE III. NMAP SCANNING (UTILIZING –V, -A, AND -PN FLAGS)

Honeypot Type	**Result**	**Ports Opened by Conpot**
Siemens S7-200	22, 25, 80, 514, 6009, 8443	80,102, 161, 502, 623, 47808
Guardian AST	22, 25, 514, 6004, 10001	10001
IPMI	22	623
Kampstrup Smart Meter	22, 25, 514, 1025, 1068	1025, 50100

Nmap-ping Conpot

SPRITZ Security & Privacy Research Group

Università degli Studi di Padova

- Scanning all ports shows we see open ports in the dynamic range 49152-65536, so questionable

TABLE IV. NMAP SCANNING (UTILIZING –V, –A, –PN, AND -P- FLAGS)

Honeypot Type	Result	Ports Opened by Conpot
Siemens S7-200	22, 80, 102, 502, 514, 2000, 5060, 8008, 8020, 18556	80,102, 161, 502, 623, 47808
Guardian AST	22, 514, 2000, 3826, 5060, 8008, 8020, 10001, 11190, 19116, 36123, 43787, 48191, 63790	10001
IPMI	22, 2000, 5060, 8008, 8020	623
Kampstrup Smart Meter	22, 514, 1025, 2000, 4368, 5060, 8008, 32469, 50100, 52245, 57565	1025, 50100
Vanilla Ubuntu Install	22, 514, 2000, 5060, 8008, 8020, 38051, 38093, 47785	

Shodan

- Engine for detecting everything on the internet
- It works for ICS, databases, network infrastructures
- A lot of crazy info

Shodan

SPRITZ Security & Privacy Research Group
Università degli Studi di Padova

- Shodan is a search engine that lest its users search for various types of servers (webcams, routers, PLCs,..) connected to the internet using a variety of filters
- Mostly collects data on web servers (HTTP/HTTPS 80, 8080, 443, 8443), FTP (port 21), SHH (port 22), SNMP (port 161), ..
- Shodan can help us identify ICS connected to the internet
- However

Shodan

SPRITZ Security & Privacy Research Group

Università degli Studi di Padova

- We also use Shodan data to analyze Conpot to understand which port is open
- Shodan scans the entire IPV4 internet address space and can indicate what can be seen by third party entities

TABLE V. SHODAN SCAN DATA RESULTS

Honeypot Type	**SHODAN Port Scan Results**	**Conpot Ports**
Siemens S7-200	22, 80, 102, 161	80,102, 161, 502, 623, 47808
Guardian AST	10001	10001
IPMI	N/A	623
Kampstrup Smart Meter	N/A	1025, 50100

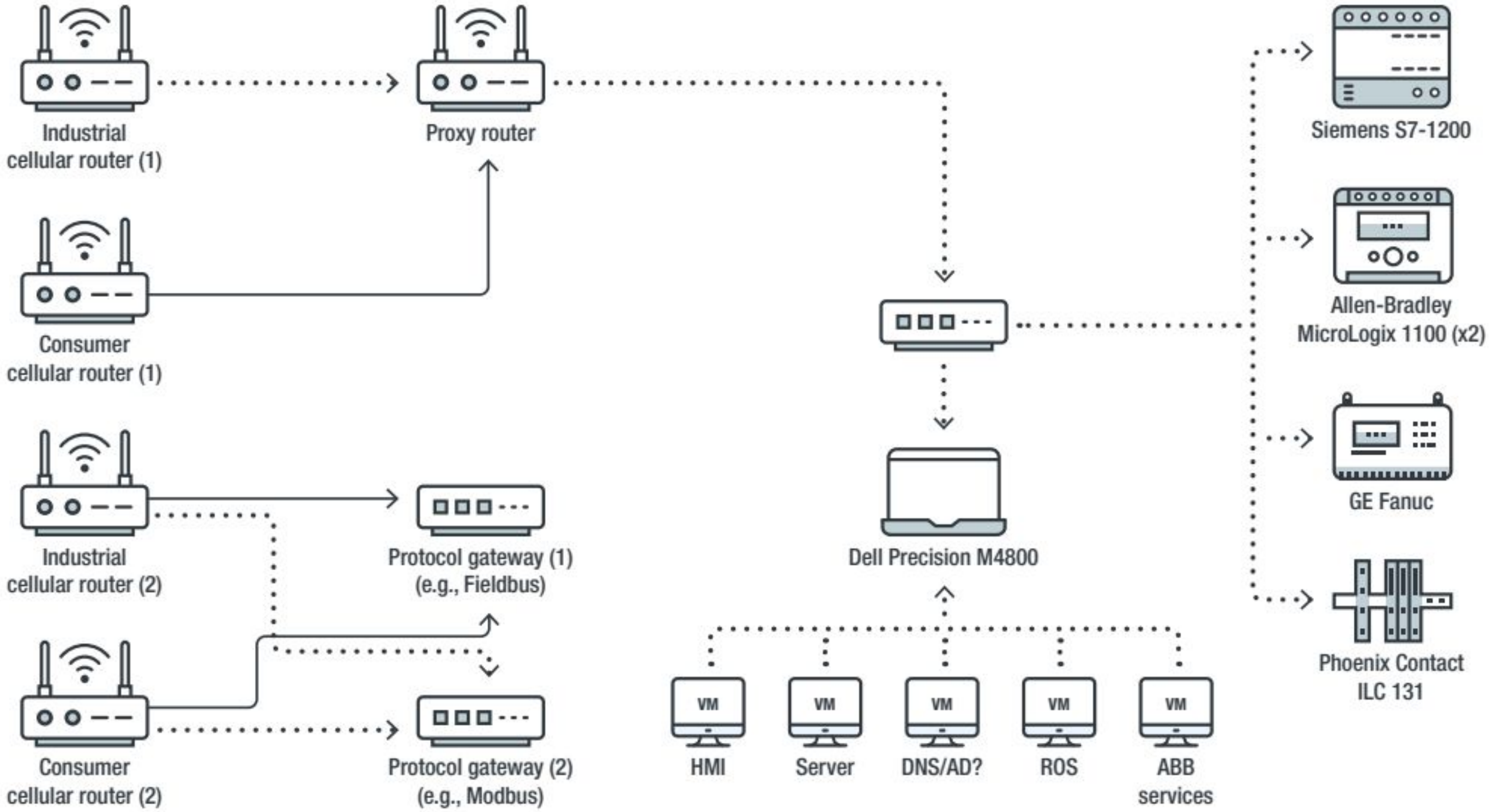
Conpot

- Many Conpot-based honeypots have been developed
  - Additional functions and subfunctions support for S7comm
  - Dynamic HMI for the evaluation of threats to ICS
  - High-fidelity ICS protocol simulations, data capture, and analysis
  - Implementation on real-life resource constrained devices (e.g., Arduino or RaspberryPi)

Realistic Honeypot

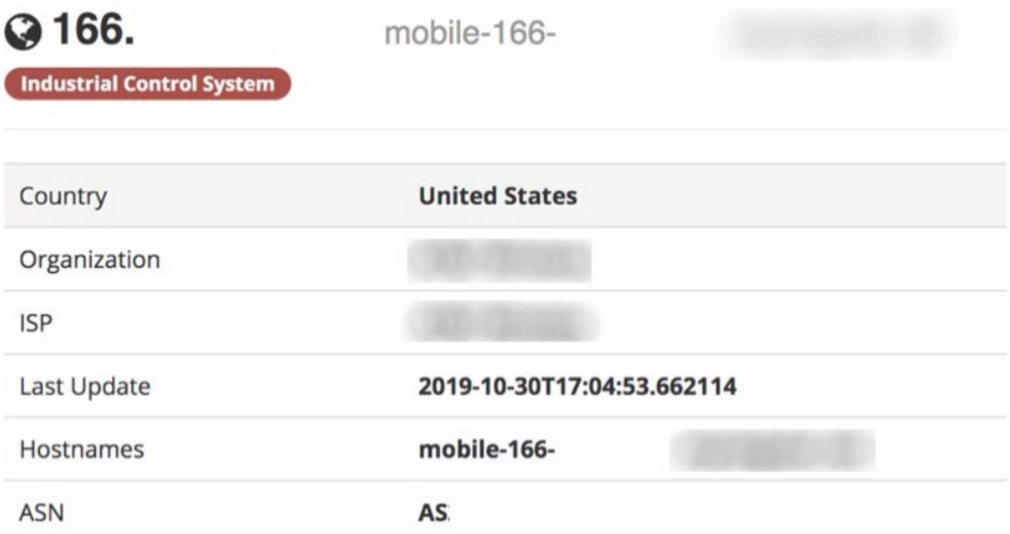
- There have also been realizations of realistic Honeypots, such as the one by Trend Micro
- The goal was to develop a honeypot that appeared so real not even a well-trained control systems engineer would be able to tell it is a fake
- Decide services and ports to expose, keeping them to a minimum number to prevent honeypot to be identified as such
- Made up company history: employee names, working phone numbers, email addresses

Layout Plan


Industrial
cellular router (1)
Proxy router
Consumer
cellular router (1)
Industrial
cellular router (2)
Protocol gateway (1)
(e.g., Fieldbus)
Consumer
cellular router (2)
Protocol gateway (2)
(e.g., Modbus)
Dell Precision M4800
VM
HMI
VM
Server
VM
DNS/AD?
VM
ROS
VM
ABB
services
Siemens S7-1200
Allen-Bradley
MicroLogix 1100 (x2)
GE Fanuc
Phoenix Contact
ILC 131

Undetectable Honeypot

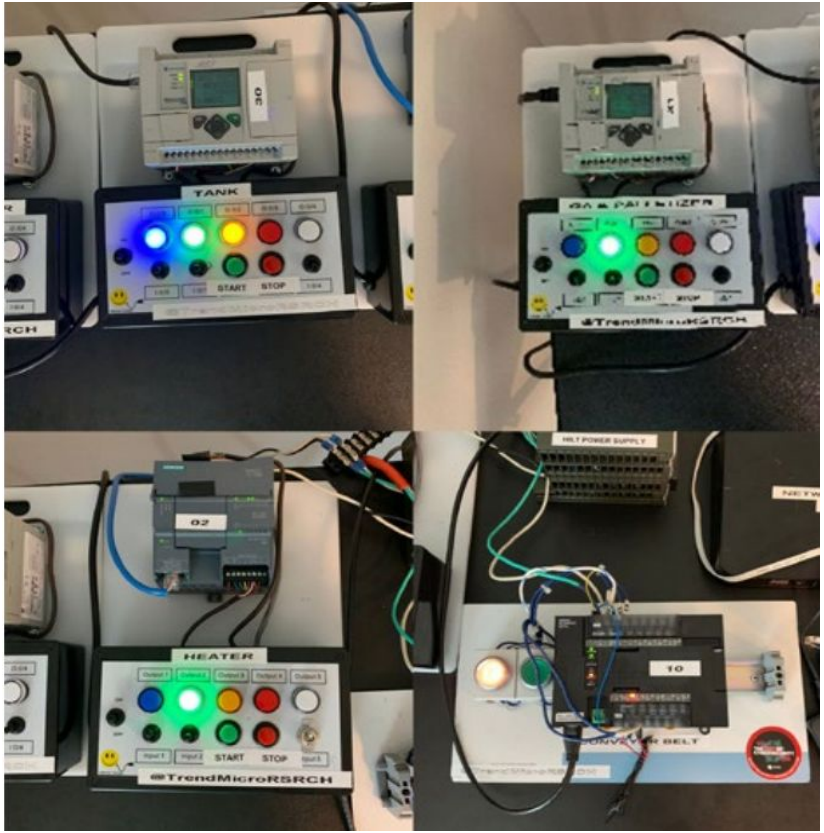
- We want attackers to be able to use Shodan-based -like system to flag our honeypot as such
- To this aim, we can use a real ICS hardware and a mixture of physical hosts and hardened VMs



ICS Hardware

- For PLCs from Siemens s7, Allen-Bradly MicroLogix, Omron CP1L
- Chosen for their popularity in the control system markets from around the world
- Each brand uses different protocols, thus providing more info on possible attacks
- Each PLC is loaded with logic and performed specific tasks together running the facility
- Use of incremental functions through logic to vary the feedback of values

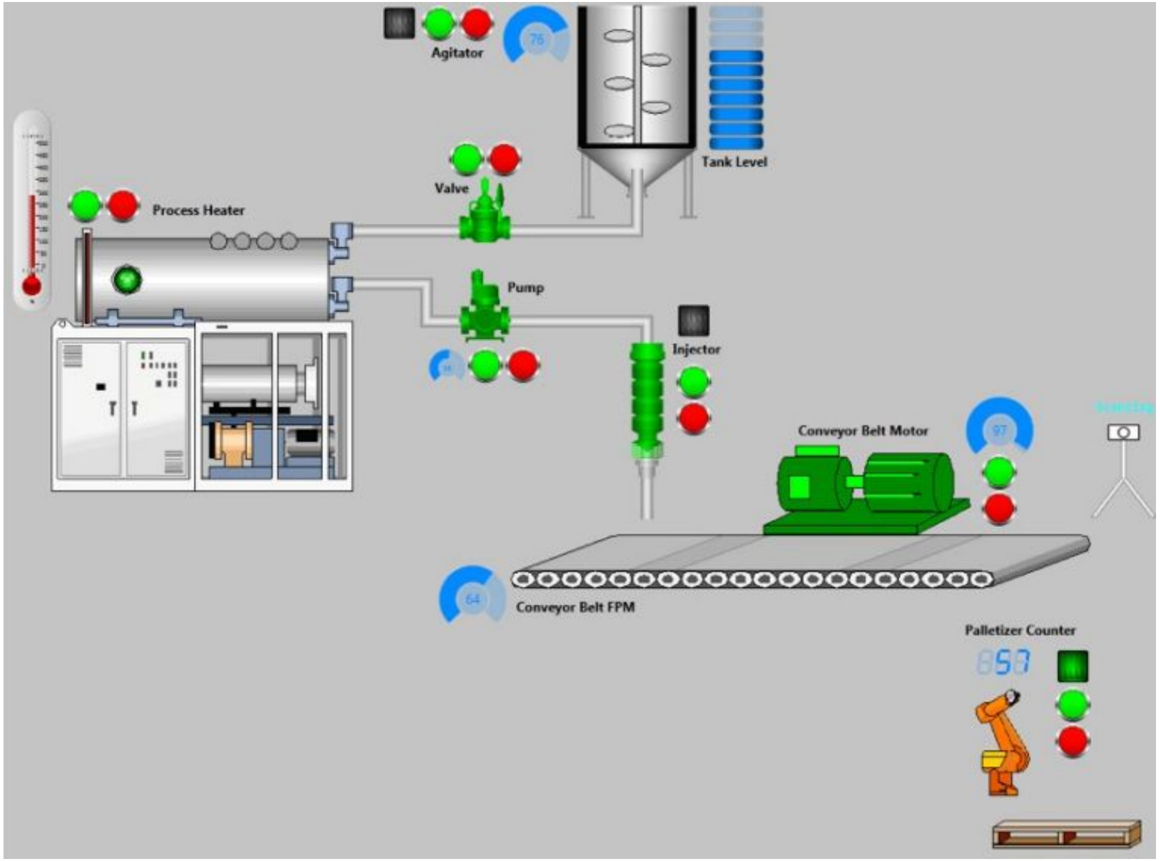
ICS Hardware



Machines and HMIs

- Three VMs and one physical machine
- The three VMs include an HMI to control the factory, a robotic workstation to control a palletizer, and an engineering workstation to program the PLC
- The physical machine is a file server for the factory
- To mimic a realistic manufacturing environment, create an HMI to quickly identify the states of virtual actors
- Expose the HMI through Virtual Network Computing without access control

Machines and HMIs



Robotic Workstation

- Industrial robots are key components of smart manufacturing
- To build a realistic system, we need to include them and their corresponding engineering workstation
- Include robotics workstations that would be used by engineers to graphically write the automation logic
- Install the programming environment on a VM
- The rendered 3D digital twin of the robot is visible by VNC scans

Luring Attackers

- One of the main goal of an honeypot is to be attacked
- Start open specific ports
- No password required for NVC
- A month later, misconfigure VNC to allow remote inputs
- Act like a victim infected by malware and upload items to online antivirus aggregation service including networks diagrams
- Posts on Pastebin

Neural Network-Based Honeypot

- To avoid being detected, an honeypot should be able to reflect changes in the physical process of the ICS
- For instance, the honeypot should send different response messages for the same request at different times
- Neural networks can be used to simulate this process and generate responses that match a particular ICS scenario

Neural Network-Based Honeypot

- Three types of entities:
  - Industrial agent: transmits physical process parameters from ICSs to the server via storage media
  - Server: undertakes honeypot configuration, data storage, and data visualization task. Furthermore, forecasts the physical process data
  - Honeypot node: opens the default port 502 of the Modbus protocol
- The chosen protocol should not be encrypted so that we can easily determine from the protocol specification the definition of each field, data conversion rules, and physical parameter storage locations

System Initialization

SPRITZ Security & Privacy Research Group

Università degli Studi di Padova

- The server receives the physical process parameters (sensors or actuators measurements) generated within a certain period from the industrial agent
- Loads them as input data into the time series forecast model
- These values are converted and stored in the honeypot configuration file together with a timestamp
- Attackers can trigger the transition of the honeypot state by accessing these storage blocks

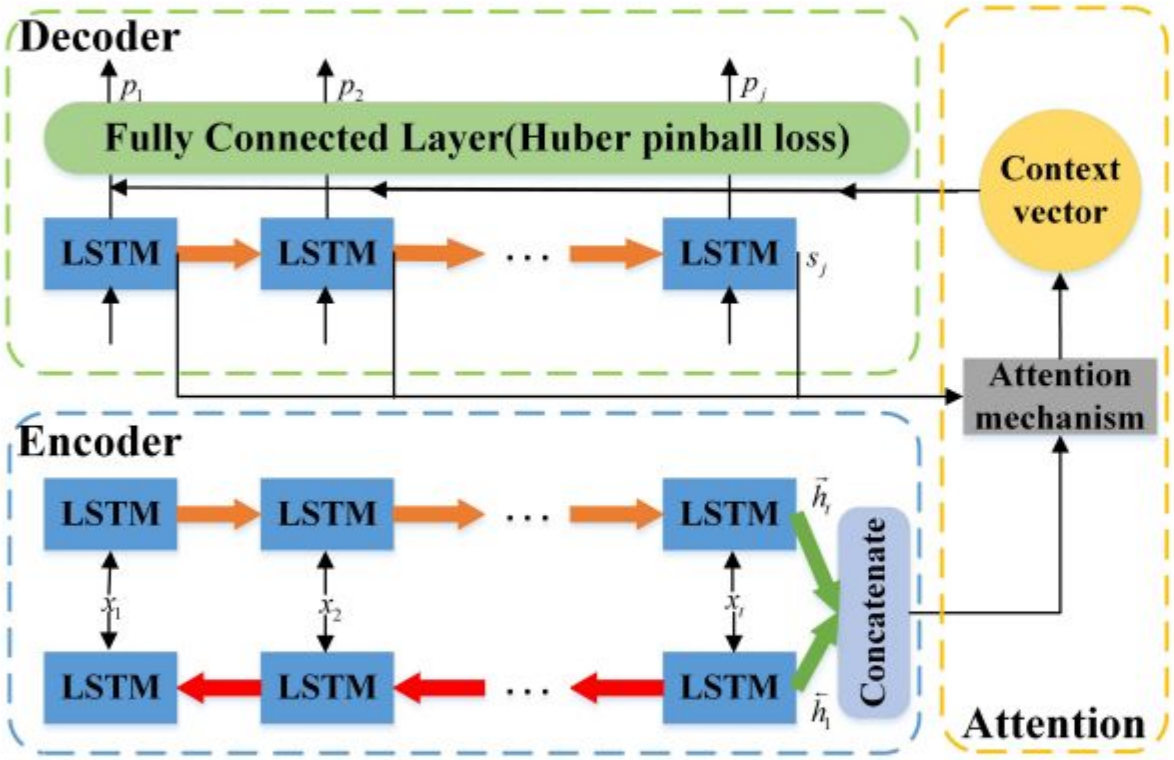
Generate Response Messages

- The honeypot can reply to all request messages using the Modbus protocol
- However, only when the attacker attempts to read or write the storage block will the honeypot response message contain payloads
- For each request message, the honeypot node first locates the timestamp in the storage block configuration file
- The timestamp is given by the difference between the current time and the first arrival time

Malicious Traffic Detection

- The server is in charge of detecting malicious traffic
- First, the server completes the pretraining of the malicious traffic detection model using the attack data obtained by the honeypot
- Every hour, the Tshark on the honeypot node saves the captured malicious traffic as a Pcap file and sends it to the server
- The server will preprocess the traffic data, then feed it into the pretrained model M2 and display the detection result

Sequence Forecast Model



Seq2seq-based model to turn one sequence into another sequence