Sensor and Process Fingerprinting in Industrial Control Systems

Martín Ochoa  
*Cyxtera Technologies*

Mujeeb Chuadhry  
*Singapore University of Technology and Design*
Bio

Martín:

• Head of Research, Cyxtera TFP
• Previously Assistant Professor in Bogotá and SUTD, Singapore.
• Ph.D. in CS, background in Math and Systems Engineering.
• Interested in software and systems security applications to ICS, IoT.

Mujeeb:

• Ph.D. student at SUTD in Singapore.
• Thesis on sensor fingerprinting in ICS.
• Background in Electronic Engineering.
ICS Security is important
**Software**

**Hacker jailed for revenge sewage attacks**

Job rejection caused a bit of a stink

By Tony Smith 31 Oct 2001 at 15:55

An Australian man was today sent to prison for two years after he was found guilty of hacking into the Maroochy Shire, Queensland computerised waste management system and caused millions of litres of raw sewage to spill out into local parks, rivers and even the grounds of a Hyatt Regency hotel.

"Marine life died, the creek water turned black and the stench was unbearable for residents," said Janelle Bryant of the Australian Environmental Protection Agency.
Noise is bad...

https://giphy.com/gifs/quiet-minimal-white-noise-vxcsu6bl20dm0
Noise is good!

What kind of noise?

Measured values

<table>
<thead>
<tr>
<th>Timestamp</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>30.541212341</td>
</tr>
<tr>
<td>1</td>
<td>30.481231303</td>
</tr>
<tr>
<td>2</td>
<td>30.521231290</td>
</tr>
<tr>
<td>3</td>
<td>30.342305190</td>
</tr>
<tr>
<td>4</td>
<td>30.560392148</td>
</tr>
<tr>
<td>5</td>
<td>30.531091240</td>
</tr>
<tr>
<td>6</td>
<td>30.494756191</td>
</tr>
</tbody>
</table>

Wall 30 cm
Talk outline

1. An ICS testbed (SWaT)
2. Cyber/Physical attacks on SWaT
3. How to detect attacks?
4. How to detect attacks using sensor and process noise?
5. Discussion
Secure Water Treatment Testbed (SWaT)

- Water treatment testbed for security research since 2015.
- 6 stages of processing (including UV, chemical treatment)

https://itrust.sutd.edu.sg/itrust-labs-home/itrust-labs_swat/
Network overview

ISA-99 Levels

Level 3
- Laptop PC
- SCADA Workstation
- SCADA Server

Zone D: Plant Network

Zone C: DMZ
- Remote operator console
- Smart device

Security level
- Highest
- Zone A
- Zone B
- Zone C
- Lowest
- Zone D

Level 2
- Operator console HMI
- Engineering Workstation

Zone B: Control System

Level 1
- PLC1
- PLC2
- PLC3
- PLC4
- PLC5
- PLC6

Level 0
- Zone A
- S
- A

Zone A: SIS

L0

L1
IF WE PROTECT THE PERIMETER

THAT'D BE GREAT
Thanks! Questions?

https://looneytunes.fandom.com/wiki/That%27s_all_Folks
Why we need defense in depth in ICS

- Multiple advanced attack vectors that challenge traditional IT security views.
  - Insider threats
  - Insecure Updates
  - Supply chain attacks
  - Lack of authentication in L1 and L0! (field network/protocols)

Why have supply chain partners proven to be the weakest links in cyberattacks

A South African IT manager, supply chains under siege

"Why have supply chain partners proven to be the weakest links in cyberattacks?"

How to control a water tank?

Valve (inflow)

Sensor

HH

LL

Remote I/O

Pump (outflow)

PLC
How to control a water tank?

Valve (inflow) -> Sensor (LL) -> Remote I/O -> Pump (outflow)
Attacks?
Authentication?
Attacker model

**ATTACK FROM TRANSMITTER**

HART transmitter reference design ;-)  

DAC with s/r up to 100kHz 
(smooth sine wave at ~ 5kHz)

- **Physical:**
  - Can replace sensors (hardware)
  - Can manipulate analog/smart signal

- **Cyber:**
  - Any kind of Man-in-the-middle at L0 and L1 networks.
  - Otherwise spoof sensor values (i.e. SCADA)

(hardware)

- Can manipulate analog/smart signal

[Bolshev et al. BH Asia 16]  

[Urbina et al. CCS 16]  

[Krotofil et al. HITB 15]
("Shameless") attack

Sensor and Process Fingerprinting in ICS
Data spoofing attacks

RED OR BLUE

WHAT'S THE SENSOR VALUE?

limgflip.com
Video of data spoofing attack
Defenses?
How to raise the bar against attacks?

• Use cryptographic primitives to authenticate data?
  • Cumbersome in legacy systems.
    • Computational resources are limited.
    • Not supported by industrial protocols.
  • Doesn't entirely solve the problem.
    • Analog data could already be malicious.
    • Cryptographic keys can be stolen.
Authentication?

- Sensor data could already be malicious before authenticating.
- Keys can be stolen.
• Idea: a mathematical model of the process gives a "prediction" of future plant states.
  • If observation does not match the prediction, raise an alarm.
"Shameless" attack detection

Sensor and Process Fingerprinting in ICS

Prediction based on last observed value
Stealthy attacks

https://www.cinemaspartan.com/somewhere-oliver-stone-is-frowning-tropic-thunder/
• Small deviations have a cumulative effect.

• Can bypass model-based countermeasures.
• Idea: detect violations of laws of physics, i.e. pressure as a function of a water tank level. [Adepu et al. IFIP SEC 16]

• Shortcomings: hard to produce exhaustive invariant list for a system.
Noise!
• Can we use sensor noise to fingerprint sensor values and address shortcomings of previous defenses?

• Can we distinguish sensors of same type and brand?
Our sensors

$1500 - $3000
Noise in different sensors

Ultrasonic Level Sensor (SWaT)

Electromagnetic Flow Sensor (SWaT)

Pressure Sensor (SWaT)

Pressure Sensor (WADI)

Electromagnetic Flow Sensor (WADI)

Radar Level Sensor (WADI)
• Water level not changing.
• Stable behavior in two runs.
• Cannot really distinguish Sensor 1 from Sensor 2 visually but...
### Feature Description

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mean</td>
<td>$\bar{x} = \frac{1}{N} \sum_{i=1}^{N} x_i$</td>
</tr>
<tr>
<td>Std-Dev</td>
<td>$\sigma = \sqrt{\frac{1}{N-1} \sum_{i=1}^{N} (x_i - \bar{x})^2}$</td>
</tr>
<tr>
<td>Mean Avg. Dev</td>
<td>$D_{\bar{x}} = \frac{1}{N} \sum_{i=1}^{N}</td>
</tr>
<tr>
<td>Skewness</td>
<td>$\gamma = \frac{1}{N} \sum_{i=1}^{N} \left( \frac{x_i - \bar{x}}{\sigma} \right)^3$</td>
</tr>
<tr>
<td>Kurtosis</td>
<td>$\beta = \frac{1}{N} \sum_{i=1}^{N} \left( \frac{x_i - \bar{x}}{\sigma} \right)^4 - 3$</td>
</tr>
<tr>
<td>Spec. Std-Dev</td>
<td>$\sigma_s = \sqrt{\frac{\sum_{i=1}^{N}(y_f(i))^2 + y_m(i)}{\sum_{i=1}^{N} y_m(i)}}$</td>
</tr>
<tr>
<td>Spec. Centroid</td>
<td>$C_s = \frac{\sum_{i=1}^{N}(y_f(i)) y_m(i)}{\sum_{i=1}^{N} y_m(i)}$</td>
</tr>
<tr>
<td>DC Component</td>
<td>$y_m(0)$</td>
</tr>
</tbody>
</table>

[Ahmed et al. ArxiV 17]
Supervised Machine Learning can help distinguishing between the noise of different sensors!

[Ahmed et al. Arxiv 17, AsiaCCS 18]
Towards authentication

Can we distinguish data belonging to Sensor 1 from other sensors?

Sensor 1

Sensor 2
• Want to build a binary classifier (authentic/not authentic) to act as an authenticity verifier.
• Fingerprint check!

Trained with lots of data belonging to Sensor 1 and all other sensors in the plant!
Towards authentication

- Chunks of observations from other sensors, even for similar values, brand, type etc. should not pass!
• An attacker using a constant value (no-noise) is easy to detect.
Does it work?

Check: Count how many samples in the Testing set are correctly classified after training with the Training set.
Does it work?

- Chunk size of about 2 minutes works best (120 samples).
- Tested on up to 60 sensors of the same class (cheap sensors).
- 99% accuracy in authentication test. [Ahmed et al. Arxiv 17, AsiaCCS 18]
- Fingerprints are still valid after 4 years at least.
- Tested in room temperature (20 to 35 °C)

Note that this works when physical quantity is constant!
Attacks detected?

- "Shameless" attacks:
  - Abrupt jumps can be detected by Model-Based countermeasures.
  - "Flat" noise injections can be detected by noise patterns (even stealthy).

- Malicious sensors (hardware) can be detected.
  - Like [Bolshev et al. BH Asia 16]

- What about stealthy attacks that also try to inject coherent noise against a dynamic system?
• In practice we have a combination of sensor plus process noise, i.e. water moving generates a certain characteristic "noise".

• I.e. even if sensor is perfect (no noise) measurement is "noisy".
Residual = Observation - Prediction
Detecting flat noise
Noise vs. Stealthy attacks

[Ahmed et al. ACSAC 18]
Video of attack detection
Does it work?

Check: Same as before, note that we are now training and testing against the residual!
Does it work?

- Chunk size of about 2 minutes (120 samples) works best (again).

- Tested on up to 18 sensors and respective process on SWaT.

- 96% accuracy in authentication test.
  
  [Ahmed et al. ACSAC 18]

- Considered several "stealthy" strategies.
  - But CPS are different! [Krotofil et al. HITB 15]
Architecture

Sensor Auth. Checker

Zone D: Plant Network
- Laptop PC
- SCADA Workstation
- SCADA Server

Zone C: DMZ
- Remote operator console
- Smart device

Zone B: Control System
- Operator console HMI
- Engineering Workstation

Security level:
- Highest
- Zone A
- Zone B
- Zone C
- Zone D

ISA-99 Levels:
- Level 3
- Level 2
- Level 1
- Level 0

L0

L1
Summary

• We have shown empirical evidence of existence of sensor fingerprint in real-world ICS.
  • Over 10 sensor types, up to 60 sensors for each type.

• We have shown how this fingerprint, together with a process fingerprint, can help in authenticating sensor readings.
  • High detection/authentication accuracy (96%-99%).
• On the other hand, this is just the beginning!

• What if threat actor has an entire research institute at their disposal?
Next steps?

- A lack of model makes things challenging, under advanced attacks.

- Case of super powerful attacker (Ironman + PhD)

  - We have ideas on how to deal with this using a challenge-response protocol
    [Ahmed et al, ArxiV 17]
  
  [Krotofil et al. HITB 15]
• In most real-world ICS sensor data is not authenticated at L0 and/or L1 levels.

• Sensor noise can be useful to authenticate sensors without using cryptography.

• Process + Sensor noise results in a more robust fingerprint.

Thanks!

martin.ochoa@cyxtera.com  chuadhry@mymail.sutd.edu.sg


• **[Bolshev et al. BH Asia 16]** A. Bolshev and M. Krotofil *Never trust your inputs: causing 'catastrophic physical consequences' from the sensor (or how to fool ADC)*. Black Hat Asia 2016.
