Network Security Monitoring in Critical Infrastructure

Martin Scheu
23. June 2022
ntopConf '22
Agenda

What is Industrial Communication about

How to get started

Monitoring Examples
Industrial Communication
Environment

Industrial Control

Full pcap

- Current: 125, Unit: A

512 Mbit/s ≈ 5 TB/day

Flows

<table>
<thead>
<tr>
<th>IP.Src</th>
<th>Src.Port</th>
<th>IP.Dst</th>
<th>Dst.Port</th>
<th>Proto</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.16.2.11</td>
<td>58336</td>
<td>172.16.2.1</td>
<td>53</td>
<td>DNS</td>
</tr>
<tr>
<td>172.16.2.1</td>
<td>45771</td>
<td>9.9.9.9</td>
<td>53</td>
<td>DNS</td>
</tr>
</tbody>
</table>
Connectivity Evolution I
Connectivity Evolution II
Industrial Protocol Characteristics

Data exchange Flow

Connection check / Keep a live Flows

| Frame | Ethernet | IP | TCP/UDP | Current: 125, Unit: A |

Source symbols: https://openclipart.org
# Protocols

## 2 - wire

- CAN
- HART
- IEC 60870
- IO-Link
- Modbus
- PROFIBUS

## Ethernet based

<table>
<thead>
<tr>
<th>Layer</th>
<th>PROFINET</th>
<th>OPC UA</th>
<th>IEC 60870-5-104</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application - 7</td>
<td>IO</td>
<td>RPC</td>
<td>CBA</td>
</tr>
<tr>
<td>Presentation - 6</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Session - 5</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Transport - 4</td>
<td></td>
<td>UDP</td>
<td>TCP</td>
</tr>
<tr>
<td>Network - 3</td>
<td></td>
<td>IP</td>
<td>IP</td>
</tr>
<tr>
<td>Data Link - 2</td>
<td></td>
<td>C/C</td>
<td>C/C</td>
</tr>
<tr>
<td>Physical - 1</td>
<td></td>
<td>Eth</td>
<td>Eth</td>
</tr>
</tbody>
</table>

## Safety

- ProfiSAFE
- IO-Link Safety
- CIP Safety

Implemented as “black channel” on top of a Protocol

---

**TSN**: Time sensitive network
OT Malware

- Stuxnet (2010)
- Havex (2013)
- BlackEnergy (2014)
- Industroyer (2016)
- Triton/Trisys (2017)
- Industroyer2 (2022 April)
- Incontroller/Pipedream (2022 April)
Industrial Network Security Monitoring
Why?
Engineering bow-tie

Source: #S4x20, Shiny Object Syndrome, Rebekah Mohr
Commercial Products

- Asset discovery
- Asset management
- Network monitoring
- Anomaly detection
- Vulnerability management
- Threat intelligence feed
- Version control of user software, e.g. PLC program
## Open-source

<table>
<thead>
<tr>
<th>IEC 104</th>
<th>Script language</th>
<th>Ease of use</th>
<th>Resource requirements</th>
<th>Setup and installation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Malcolm</td>
<td>no</td>
<td>zeek script</td>
<td>-</td>
<td>huge</td>
</tr>
<tr>
<td>ntopen</td>
<td>yes</td>
<td>Lua</td>
<td>+</td>
<td>minimal</td>
</tr>
<tr>
<td>Suricata</td>
<td>no</td>
<td>Lua</td>
<td>-</td>
<td>minimal</td>
</tr>
<tr>
<td>Snort</td>
<td>yes</td>
<td>snort rules</td>
<td>-</td>
<td>minimal</td>
</tr>
<tr>
<td>SoS</td>
<td>no</td>
<td>n/a</td>
<td>+</td>
<td>depends</td>
</tr>
<tr>
<td>zeek</td>
<td>PoC available</td>
<td>zeek script</td>
<td>-</td>
<td>minimal</td>
</tr>
</tbody>
</table>
Toolitis
Where to start
Choose a tool

One GUI for Alerts and Configuration.

Easy to use for not-field experts.

Use of Risk score for flows and hosts.

ntopng
Choose a Use Case - Playbook
General Use Cases

- Unusual or exceptional activities in a network
- Connection of a new device, disconnection of a device
- Rogue DHCP, DNS, SMTP or NTP server
- Data packets from an unknown device
- Data transmission between devices that have not previously communicated
- Data transmission via a protocol/port that has not been used before
- Data transmission via an unusual protocol or one not intended for the purpose at hand
- Events that occur at unusual times
- Use of unexpected addresses (public IP addresses, etc.)
- Generally noteworthy events such as address or port scans
- Changes in network quality, including high broadband usage, increased round-trip times and smaller TCP window sizes

Source: allianz-fuer-cybersicherheit.de
ICS Use Cases

- Unusual error messages
- Unsupported function calls
- Function calls that have not been used before
- Flawed data packets
- Unknown function codes
- Abnormal protocol behaviour
- Unexpected transition from one protocol to another
- Values outside of defined ranges
- Changes in frequency / periodicity
- Changes in cycle times
- Changing variance within certain periods of time

Source: allianz-fuer-cybersicherheit.de
Place the Sensor
Best practice

Select Use Cases together with OT Colleagues.

Besides the use case, define the alerting and playbook as well.

Have regular “Monitoring” meetings.
Examples
### Example II - GEO Fence on Firewalls

<table>
<thead>
<tr>
<th>Date/Time</th>
<th>Score</th>
<th>Application</th>
<th>Alert</th>
<th>Flow</th>
<th>De</th>
</tr>
</thead>
<tbody>
<tr>
<td>09/11/2021 10:13:26</td>
<td>200</td>
<td>TCP:HTTP</td>
<td>Blacklisted Flow</td>
<td>45.134.144.42@3654:44588</td>
<td></td>
</tr>
</tbody>
</table>

**Other Issues** Remote to Local Insecure Protocol [Score: 100] [Predominant Traffic: Srv → Cli]

---

**v4.whois.cymru.com**

The server returned 2 line(s).

<table>
<thead>
<tr>
<th>AS</th>
<th>IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>49870</td>
<td>45.134.144.42</td>
</tr>
</tbody>
</table>

### Detection Details

<table>
<thead>
<tr>
<th>DETECTION</th>
<th>DETAILS</th>
<th>RELATIONS</th>
<th>COMMUNITY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certego</td>
<td>Malicious</td>
<td>Comodo Valkyrie Verdict</td>
<td>Malicious</td>
</tr>
<tr>
<td>CRDF</td>
<td>Malicious</td>
<td>CyRadar</td>
<td>Malicious</td>
</tr>
<tr>
<td>GreenSnow</td>
<td>Malicious</td>
<td>IPharm</td>
<td>Malicious</td>
</tr>
<tr>
<td>Spamhaus</td>
<td>Malicious</td>
<td>Abusix</td>
<td>Clean</td>
</tr>
</tbody>
</table>

© 2022 Martin Scheu | 26
Example III - IEC 60870-5-104

**Multiple APDUs**

<table>
<thead>
<tr>
<th>Application</th>
<th>Protocol</th>
<th>VLAN</th>
<th>Client</th>
<th>Server</th>
<th>Actual Thpt</th>
<th>Total Bytes</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>IEC60870👍</td>
<td>TCP</td>
<td>21</td>
<td>:2404</td>
<td>44404</td>
<td>0 bps  —</td>
<td>100.48 KB</td>
<td>← S, RX 21582</td>
</tr>
<tr>
<td>IEC60870👍</td>
<td>TCP</td>
<td>21</td>
<td>:2404</td>
<td>59749</td>
<td>0 bps  —</td>
<td>53.31 KB</td>
<td>→ I, RX 65, TX 28985</td>
</tr>
<tr>
<td>IEC60870👍</td>
<td>TCP</td>
<td>21</td>
<td>:58463</td>
<td>2404</td>
<td>0 bps  —</td>
<td>8.44 KB</td>
<td>← S, RX 14</td>
</tr>
<tr>
<td>IEC60870👍</td>
<td>TCP</td>
<td>21</td>
<td>:54827</td>
<td>2404</td>
<td>0 bps  —</td>
<td>12.1 KB</td>
<td>→ U (TESTFR con)</td>
</tr>
</tbody>
</table>

**Multiple IOA’s**

- Type Identification
  - Number of Objects
  - Cause of transmission (CoT)
- Originator Address (ORG)
- ASDU address fields
  - Information object address fields (IOA) #1
  - Object information #1
  - Information object address fields (IOA) #2
  - Object information #2
  - Information object address fields (IOA) #n
  - Object information #n
Example III - IEC 60870-5-104

<table>
<thead>
<tr>
<th>Alarm Typ</th>
<th>Score</th>
<th>Applikation</th>
<th>Beschreibung</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Invalid IEC Transition</td>
<td>50</td>
<td>IEC60870</td>
<td>Invalid transition detected [M_ME_NB_1 (11) -&gt; C_CS_NA_1 (103)] [Flow: Lokaler Host:2404 ↔ Lokaler Host:22525] [TCP] [Applikation: IEC60870] [Info: IEC60870]</td>
<td></td>
</tr>
</tbody>
</table>

Type ID Transitions

- **M_ME_TF_1 (36) ⇔ M_ME_TF_1 (36)**: 98.651 %
- **M_IT_TB_1 (37) ⇔ M_IT_TB_1 (37)**: 1.000 %
- **M_ME_TF_1 (36) → M_IT_TB_1 (37)**: 0.116 %
- **M_IT_TB_1 (37) → M_ME_TF_1 (36)**: 0.116 %
- **C_CS_NA_1 (103) → M_ME_TF_1 (36)**: 0.047 %
- **M_ME_TF_1 (36) → C_CS_NA_1 (103)**: 0.047 %
- **C_CS_NA_1 (103) ⇔ C_CS_NA_1 (103)**: 0.023 %

Type I-S Ack Latency (Average / Std Dev)

- **0.160 ms (0.474 msec)**

Messages Breakdown

- **83.9%**
- **16.1%**

Messages Lost / Retransmissions

- **0**, 18 / 1 Retransmitted

Transitions

- **M_ to M_**: > 1000, 0
- **M_ to C_ or C_ to M_**: > 0 && < 10, 0
- **C_ to C_**: 0, > 10
Example IV - Clear Text Passwords
Example V - Malware Traffic

Score as Attacker: 12,305
Score as Victim: 5

Top Hosts
- desktop-kkitb6q (98.6%)
- 94.158.245.52 (44.6%)
- 10.9.10.9 (12.2%)

Top Alerts
- Missing TLS SNI (29.7%)
- Too Long TLS Certificate... (23.0%)
- TLS Certificate Self-sig... (16.2%)

<table>
<thead>
<tr>
<th>Date/Time</th>
<th>Score</th>
<th>Application</th>
<th>Alert</th>
<th>Flow</th>
</tr>
</thead>
<tbody>
<tr>
<td>16:37:25</td>
<td>250</td>
<td>TCP:HTTP</td>
<td>Binary Application Trans...</td>
<td>desktop-kkitb6q:58131</td>
</tr>
</tbody>
</table>

Description: Detected binary application transfer [simpsonsavings.com/bmdff/BhoHsCtZ/MLdmpfjaX/5uFG3Dz7yt/date1?BN...](simpsonsavings.com/bmdff/BhoHsCtZ/MLdmpfjaX/5uFG3Dz7yt/date1?BN...?) [Score: 250] [Method: GET] [Return Code: 200] [URL: simpsonsavings.com/bmdff/BhoHsCtZ/MLdmpfjaX/5uFG3Dz7yt] [Other Issues]

Other Issues
- TLS Certificate Self-signed

<table>
<thead>
<tr>
<th>Date/Time</th>
<th>Score</th>
<th>Application</th>
<th>Alert</th>
<th>Flow</th>
</tr>
</thead>
</table>

Description: TLS Certificate Self-signed [Other Issues: Missing TLS SNI](Missing TLS SNI) [Score: 100] [Main Direction: Cli → Svr] [Possibly Client Malicious JA3 Signature] [Score: 100] [Main Direction: Cli → Svr] [TLS not carrying HTTPS](TLS not carrying HTTPS) [Score: 100] [Main Direction: Cli → Svr]

Source sample: https://www.malware-traffic-analysis.net/2021/09/10/index.html
LOOKS LIKE LOT OF WORK
Thank you!

martin.scheu@switch.ch

martin-scheu

@martin_scheu