Author : Muhammad Mardiansyah

LAPORAN ANALISIS KEAMANAN SIBER SCADA - SISTEM KONVEYOR

---

1. Pendahuluan

Dalam simulasi ini, penulis membangun sistem kontrol conveyor sederhana dengan tujuan menguji komunikasi antar perangkat dalam sistem SCADA (Supervisory Control and Data Acquisition) berbasis Modbus TCP. Selain dari sisi fungsi, fokus utama dari eksperimen ini adalah menganalisis aspek keamanan siber dari komunikasi antar perangkat di jaringan industri.

---

2. Rancangan Sistem

Pada proyek ini, sistem otomasi yang disimulasikan terdiri dari:

- Satu unit konveyor dengan panjang 4 meter.
- Sebuah tombol Start (Push Button).
- Sebuah tombol Stop.
- Variabel Motor untuk menjalankan dan menghentikan konveyor.

Desain tersebut diimplementasikan pada platform Factory I/O dengan konfigurasi sebagai Modbus TCP Server, yang berperan sebagai antarmuka fisik (I/O) dari sistem

---

3. Analisis Keamanan

3.1 Komunikasi Modbus Tanpa Enkripsi

Modbus TCP, sebagai protokol industri yang umum digunakan, tidak memiliki fitur enkripsi maupun autentikasi. Hasil tangkapan paket menunjukkan bahwa seluruh data, termasuk register input dan output, dapat dilihat dalam bentuk plaintext. Hal ini mengindikasikan potensi besar terhadap:

- Man-in-the-Middle (MitM) : Pihak ketiga bisa menyadap dan memodifikasi perintah atau data yang dikirim.

- Reconnaissance : Penyerang dapat dengan mudah mengidentifikasi alamat register dan struktur kontrol.

3.2. Register Berhasil Diidentifikasi Melalui hasil tangkapan paket dan antarmuka web monitoring, ditemukan data berikut:

Nama Variabel	Jenis	Alamat	Nilai
Start	Bool	%IX100.0	FALSE
Stop	Bool	%IX100.1	TRUE
Motor	Bool	%QX100.0	FALSE

Wireshark berhasil mengcapture jaringan dimana kondisi alat dalam posisi berhenti karena kondisi variabel dalam posisi stop.

3.3. HTTP Monitoring Interface Tanpa Keamanan Ditemukan komunikasi HTTP berikut:

Berdasarkan tangkapan tersebut:

- Komunikasi dilakukan melalui HTTP (port 8080) tanpa TLS/SSL, sehingga isi komunikasi dapat dibaca langsung.
- Cookie session terlihat dalam bentuk plaintext, berisiko diretas melalui session hijacking.
- Antarmuka web memuat seluruh status variabel dan kontrolnya, yang dapat dimanipulasi tanpa autentikasi tambahan.
- Server menggunakan Werkzeug (Python) sebagai backend, yang sering digunakan dalam pengembangan dan bukan untuk produksi.

4. Potensi Serangan

4.1 Protokol Modbus TCP.

- Tidak ada enkripsi : Data transmisi dalam plaintext.
- Tidak ada autentikasi : Tidak ada verifikasi identitas client/server.
- Tidak ada authorization : Semua client dapat mengakses semua fungsi.
- Vulnerable terhadap Man-in-the-Middle attacks.

4.2 OpenPLC Runtime

- Default credentials : Kemungkinan penggunaan username/password default.
- Web interface tidak terenkripsi : HTTP instead of HTTPS.
- Tidak ada session management yang kuat.
- Potential buffer overflow vulnerabilities.

4.3 Network Infrastructure

- Unprotected network : Tidak ada segmentasi jaringan.
- Tidak ada firewall : Traffic tidak difilter.
- Monitoring dapat dieksploitasi : Wireshark menunjukkan semua komunikasi terlihat.

5. Analisis Vulnerability dari Wireshark

Berdasarkan hasil monitoring, teridentifikasi:

GET /monitor-update?mb_port=502 HTTP/1.1
Host: localhost:8080

5.1 Temuan Keamanan:

- Unencrypted HTTP : Semua data status dikirim dalam plaintext
- Session cookies : Menggunakan session management sederhana
- No HTTPS : Tidak ada enkripsi transport layer
- Predictable endpoints : URL pattern mudah ditebak
- No rate limiting : Tidak ada pembatasan request

6. Model Serangan

6.1 Potensi serangan

- Network Sniffing : Attacker dapat monitor semua komunikasi
- Unauthorized Control : Akses tidak sah ke kontrol motor
- Denial of Service : Flooding Modbus requests
- Data Manipulation : Mengubah status button/motor
- Privilege Escalation : Akses ke fungsi admin
- Lateral Movement : Akses ke sistem lain dalam jaringan

6.2 Dampak Berdasarkan CIA TRIAD

- Confidentiality : HIGH - Status operasional terekspos
- Integrity : CRITICAL - Kontrol motor dapat dimanipulasi
- Availability : HIGH - Sistem dapat di-shutdown
- Safety : CRITICAL - Risiko kecelakaan industri

7. MITIGASI SERANGAN PADA SISTEM SCADA / PLC / MODBUS TCP

7.1. Network Sniffing

- Deskripsi: Attacker dapat memonitor semua komunikasi, termasuk Modbus TCP dan cookie dari HMI berbasis web.
- Pencegahan:
- Gunakan VPN atau tunneling terenkripsi (TLS, SSH)
- Lakukan segregasi jaringan (VLAN / segmentasi fisik antara OT dan IT)
- Aktifkan switch port security untuk mencegah sniffing

7.2. Unauthorized Control

- Deskripsi: Attacker mengirim perintah langsung ke PLC tanpa otorisasi.
- Pencegahan:
- Pasang firewall ICS-aware yang hanya mengizinkan IP tertentu
- Gunakan Modbus Gateway dengan otentikasi dan whitelisting
- Terapkan Role-Based Access Control (RBAC) pada sistem SCADA

7.3. Denial of Service (DoS)

- Deskripsi: Flooding request Modbus untuk membebani PLC atau SCADA
- Pencegahan:
- Gunakan rate limiting dan timeout
- Gunakan IDS/IPS khusus ICS seperti Snort (dengan Modbus rules) atau Zeek
- Gunakan perangkat PLC yang mendukung proteksi DoS

7.4. Data Manipulation

- Deskripsi: Attacker mengubah status register, tombol, atau aktuator.
- Pencegahan:
- Validasi semua input di sisi PLC dan SCADA
- Log setiap perubahan register dan coil
- Batasi penulisan hanya dari IP tertentu (whitelist)

7.5. Privilege Escalation

- Deskripsi: User biasa mendapatkan akses admin (biasanya melalui cookie atau eksploitasi celah otorisasi).
- Pencegahan:
- Jangan menyimpan peran di cookie tanpa enkripsi dan signing
- Terapkan Least Privilege Access
- Gunakan Multi-Factor Authentication (MFA)

7.6. Lateral Movement

- Deskripsi: Penyerang berpindah dari satu sistem ke sistem lain dalam jaringan OT.
- Pencegahan:
- Segmentasikan jaringan SCADA, PLC, dan IT (network zoning)
- Terapkan prinsip Zero Trust Network (setiap koneksi diverifikasi)
- Gunakan IDS dan sistem monitoring jaringan (SIEM)

8. Kesimpulan

Sistem conveyor berhasil diimplementasikan dengan fungsi operasional yang baik, namun memiliki risiko keamanan yang signifikan. Analisis cybersecurity menunjukkan:

Kelemahan Utama:

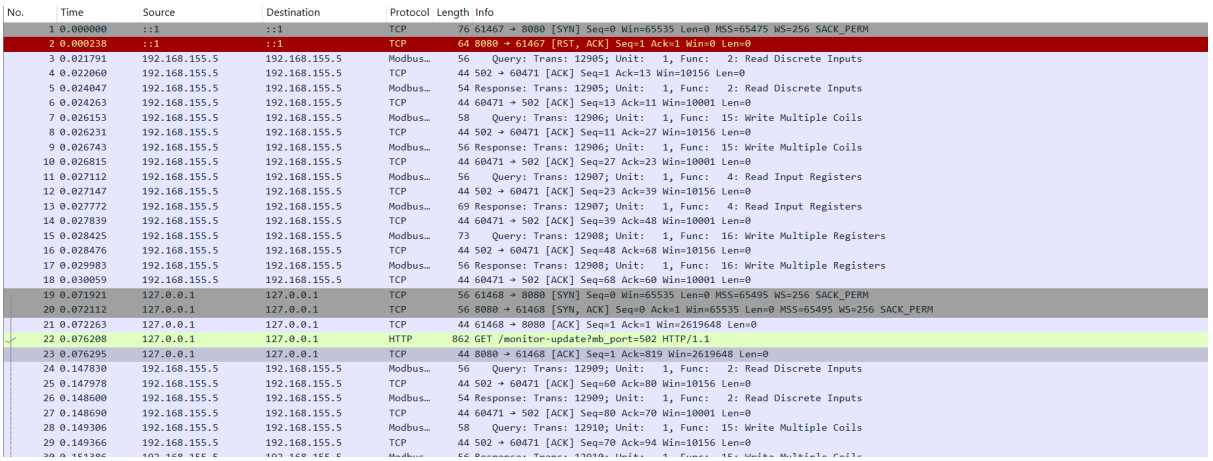
- Tidak ada enkripsi komunikasi
- Tidak ada autentikasi yang kuat
- Network tidak tersegmentasi
- Monitoring menunjukkan semua data terekspos

Dampak Potensial:

- Unauthorized control terhadap sistem industri
- Data breach operasional
- Sabotase atau kerusakan peralatan
- Risiko keselamatan operator

---

8. Dokumentasi Tambahan



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	::1	::1	TCP	76	61467 → 8080 [SYN] Seq=0 Win=65535 Len=0 MSS=65475 WS=256 SACK_PERM
2	0.000238	::1	::1	TCP	64	8080 → 61467 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
3	0.021791	192.168.155.5	192.168.155.5	Modbus…	56	Query: Trans: 12905; Unit: 1, Func: 2: Read Discrete Inputs
4	0.022060	192.168.155.5	192.168.155.5	TCP	44	502 → 60471 [ACK] Seq=1 Ack=13 Win=10156 Len=0
5	0.024047	192.168.155.5	192.168.155.5	Modbus…	54	Response: Trans: 12905; Unit: 1, Func: 2: Read Discrete Inputs
6	0.024263	192.168.155.5	192.168.155.5	TCP	44	60471 → 502 [ACK] Seq=13 Ack=11 Win=10001 Len=0
7	0.026153	192.168.155.5	192.168.155.5	Modbus…	58	Query: Trans: 12906; Unit: 1, Func: 15: Write Multiple Coils
8	0.026231	192.168.155.5	192.168.155.5	TCP	44	502 → 60471 [ACK] Seq=11 Ack=27 Win=10156 Len=0
9	0.026743	192.168.155.5	192.168.155.5	Modbus…	56	Response: Trans: 12906; Unit: 1, Func: 15: Write Multiple Coils
10	0.026815	192.168.155.5	192.168.155.5	TCP	44	60471 → 502 [ACK] Seq=27 Ack=23 Win=10001 Len=0
11	0.027112	192.168.155.5	192.168.155.5	Modbus…	56	Query: Trans: 12907; Unit: 1, Func: 4: Read Input Registers
12	0.027147	192.168.155.5	192.168.155.5	TCP	44	502 → 60471 [ACK] Seq=23 Ack=39 Win=10156 Len=0
13	0.027772	192.168.155.5	192.168.155.5	Modbus…	69	Response: Trans: 12907; Unit: 1, Func: 4: Read Input Registers
14	0.027839	192.168.155.5	192.168.155.5	TCP	44	60471 → 502 [ACK] Seq=39 Ack=48 Win=10001 Len=0
15	0.028425	192.168.155.5	192.168.155.5	Modbus…	73	Query: Trans: 12908; Unit: 1, Func: 16: Write Multiple Registers
16	0.028476	192.168.155.5	192.168.155.5	TCP	44	502 → 60471 [ACK] Seq=48 Ack=68 Win=10156 Len=0
17	0.029983	192.168.155.5	192.168.155.5	Modbus…	56	Response: Trans: 12908; Unit: 1, Func: 16: Write Multiple Registers
18	0.030059	192.168.155.5	192.168.155.5	TCP	44	60471 → 502 [ACK] Seq=68 Ack=60 Win=10001 Len=0
19	0.071921	127.0.0.1	127.0.0.1	TCP	56	61468 → 8080 [SYN] Seq=0 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM
20	0.072112	127.0.0.1	127.0.0.1	TCP	56	8080 → 61468 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM
21	0.072263	127.0.0.1	127.0.0.1	TCP	44	61468 → 8080 [ACK] Seq=1 Ack=1 Win=2619648 Len=0
22	0.076208	127.0.0.1	127.0.0.1	HTTP	862	GET /monitor-update?mb_port=502 HTTP/1.1
23	0.076295	127.0.0.1	127.0.0.1	TCP	44	8080 → 61468 [ACK] Seq=1 Ack=819 Win=2619648 Len=0
24	0.147830	192.168.155.5	192.168.155.5	Modbus…	56	Query: Trans: 12909; Unit: 1, Func: 2: Read Discrete Inputs
25	0.147978	192.168.155.5	192.168.155.5	TCP	44	502 → 60471 [ACK] Seq=60 Ack=80 Win=10156 Len=0
26	0.148600	192.168.155.5	192.168.155.5	Modbus…	54	Response: Trans: 12909; Unit: 1, Func: 2: Read Discrete Inputs
27	0.148690	192.168.155.5	192.168.155.5	TCP	44	60471 → 502 [ACK] Seq=80 Ack=70 Win=10001 Len=0
28	0.149306	192.168.155.5	192.168.155.5	Modbus…	58	Query: Trans: 12910; Unit: 1, Func: 15: Write Multiple Coils
29	0.149366	192.168.155.5	192.168.155.5	TCP	44	502 → 60471 [ACK] Seq=70 Ack=94 Win=10156 Len=0

```
Frame 22: 862 bytes on wire (6896 bits), 862 bytes captured (6896 bits)
    Encapsulation type: NULL/Loopback (15)
    Arrival Time: Jul  6, 2025 09:57:24.019419000 SE Asia Standard Time
    UTC Arrival Time: Jul  6, 2025 02:57:24.019419000 UTC
    Epoch Arrival Time: 1751770644.019419000
    [Time shift for this packet: 0.000000000 seconds]
    [Time delta from previous captured frame: 0.003945000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 0.076208000 seconds]
    Frame Number: 22
    Frame Length: 862 bytes (6896 bits)
    Capture Length: 862 bytes (6896 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: null:ip:tcp:http]
    [Coloring Rule Name: HTTP]
    [Coloring Rule String: http || tcp.port == 80 || http2]
```

```
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 128
Protocol: TCP (6)
Header Checksum: 0x0000 [validation disabled]
[Header checksum status: Unverified]
Source Address: 127.0.0.1
Destination Address: 127.0.0.1
[Stream index: 1]
```

```
Transmission Control Protocol, Src Port: 61468, Dst Port: 8080, Seq: 1, Ack: 1, Len: 818
    Source Port: 61468
    Destination Port: 8080
    [Stream index: 2]
    [Stream Packet Number: 4]
```

Wireshark · Follow TCP Stream (tcp.stream eq 2) · capture.pcap

```
Host: localhost:8080
Connection: keep-alive
sec-ch-ua-platform: "Windows"
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/138.0.0.0 Safari/537.36
sec-ch-ua: "Not)A;Brand";v="8", "Chromium";v="138", "Google Chrome";v="138"
sec-ch-ua-mobile: ?0
Accept: */*
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://localhost:8080/monitoring
Accept-Encoding: gzip, deflate, br, zstd
Accept-Language: en-US,en;q=0.9,id;q=0.8,ms;q=0.7
Cookie: session=.eJw9zk0KwjAQBtC7ZO0i_5npZUo68w0KWktaV-LdLQge4MF7u9kG9qubjvHCxc03dZOTGIMyUDj1ZrGQcEZCUDNWKT1wsxK7typNFTFpIJ8XqUQIXLoQegu
JSoukAHPzmtjApzSIr0YavU8L-SgZhp7I8lI9cqshkzsjG8ajr1iPf-21Y_x-zw3rdhf3-QIVlzlM.aGnmEw.JdFvE4QReSLC-t9KSEnO5XBim7w


HTTP/1.1 200 OK
Server: Werkzeug/2.3.7 Python/3.12.11
Date: Sun, 06 Jul 2025 02:57:24 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 1296
Vary: Cookie
Set-Cookie: session=.eJw9zk0KwjAQBtC7ZO0i_5npZUo68w0KWktaV-LdLQge4MF7u9kG9qubjvHCxc03dZOTGIMyUDj1ZrGQcEZCUDNWKT1wsxK7typNFTFpIJ8XqUQIXLo
QeguJSoukAHPzmtjApzSIr0YavU8L-SgZhp7I8lI9cqshkzsjG8ajr1iPf-21Y_x-zw3rdhf3-QIVlzlM.aGnmFA.WrIsBEhb-C8buQ6flWplak42XRc; Expires=Sun, 06 Ju
l 2025 03:02:24 GMT; HttpOnly; Path=/
Connection: close


                        <table>
                            <col width="50"><col width="10"><col width="10"><col width="10"><col width="100">
                            <tr style='background-color: white'>
                                <th>Point Name</th><th>Type</th><th>Location</th><th>Write</th><th>Value</th>
                            </tr><tr style="height:60px"><td>Start</td><td>BOOL</td><td>%IX100.0</td><td></td><td valign="middle"><img s
rc="/static/bool_false.png" alt="bool_false" style="width:40px;height:40px;vertical-align:middle; margin-right:10px">FALSE</td></tr><tr
style="height:60px"><td>Stop</td><td>BOOL</td><td>%IX100.1</td><td></td><td valign="middle"><img src="/static/bool_true.png" alt="bool_t
rue" style="width:40px;height:40px;vertical-align:middle; margin-right:10px">TRUE</td></tr><tr style="height:60px"><td>Motor</td><td>BOO
L</td><td>%QX100.0</td><td><button class="write-button true" onclick="fetch('/point-write?value=1&address=%QX100.0')">true</button><butt
on class="write-button false" onclick="fetch('/point-write?value=0&address=%QX100.0')">false</button></td><td valign="middle"><img src="
/static/bool_false.png" alt="bool_false" style="width:40px;height:40px;vertical-align:middle; margin-right:10px">FALSE</td></tr>
                        </table>
```