Public and Private, Common Flaws in ICS Network Protocols

Mars Cheng and Selmon Yang

Cyber Threat Researcher and Staff Engineer, TXOne Networks
WHO WE ARE

A Joint venture company of Trend Micro Inc. and Moxa Inc.

30 years+ Cybersecurity Threat Intelligence
30 years+ OT Network Expertise

To accelerate the industrial world to secure automation and data exchange
Who we are?

Mars Cheng
Cyber Threat Researcher
ICS/SCADA Security Research
Threat Hunting
Web, App, IoT, ICS/SCADA Penetration Testing
Applied Cryptography

Selmon Yang
Staff Engineer
IT/SCADA Protocol Parsing
Linux Kernel Programming
Honeypot Deployment & Optimization
Outline

- ICS Architecture and Attack Vectors
- Public and Private: ICS Protocols
- Common Flaws in ICS Protocols
- How to Work Against ICS Network Protocol Attacks
ICS Architecture and Attack Vectors
Remote maintenance
Lateral / longitudinal movement devices
Multiple Sites

Information Technology (IT)
Operational Technology (OT)
Common ICS Architecture

- Primary Historian
- Data Acquisition Server
- Database Server
- Configuration Server
- Engineering Workstations
- Remote Network Router
- HMI
- Industrial Wireless
- Field Controller
- Field Devices
- Safe System
- Field Device Network
ICS-Related Vulnerabilities Information

[2020-07-13] CVSS2.0 Statistics

- High: 39%
- Medium: 51%
- Low: 7%
- Other: 3%


- Critical: 18%
- High: 34%
- Medium: 17%
- Other: 30%
- Low: 1%
## ICS ATT&CK Matrix - Stuxnet

<table>
<thead>
<tr>
<th>Initial Access</th>
<th>Execution</th>
<th>Persistence</th>
<th>Evasion</th>
<th>Discovery</th>
<th>Lateral Movement</th>
<th>Collection</th>
<th>Command and Control</th>
<th>Inhibit Response Function</th>
<th>Impair Process Control</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Historian Compromise</td>
<td>Change Program State</td>
<td>Hooking</td>
<td>Exploitation for Evasion</td>
<td>Control Device Identification</td>
<td>Default Credentials</td>
<td>Automated Collection</td>
<td>Commonly Used Port</td>
<td>Activate Firmware Update Mode</td>
<td>Brute Force I/O</td>
<td>Damage to Property</td>
</tr>
<tr>
<td>Drive-by Compromise</td>
<td>Command-Line Interface</td>
<td>Module Firmware</td>
<td>Indicator Removal on Host</td>
<td>I/O Module Discovery</td>
<td>Exploitation of Remote Services</td>
<td>Data from Information Repositories</td>
<td>Connection Proxy</td>
<td>Alarm Suppression</td>
<td>Change Program State</td>
<td>Denial of Control</td>
</tr>
<tr>
<td>Engineering Workstation</td>
<td>Execution through API</td>
<td>Program Download</td>
<td>Masquerading</td>
<td>Network Connection Enumeration</td>
<td>External Remote Services</td>
<td>Detect Operating Mode</td>
<td>Standard Application Layer Protocol</td>
<td>Block Command Message</td>
<td>Masquerading</td>
<td>Denial of View</td>
</tr>
<tr>
<td>Exploit Public-Facing Application</td>
<td>Graphical User Interface</td>
<td>Project File Infection</td>
<td>Rogue Master Device</td>
<td>Network Service Scanning</td>
<td>Program Organization Units</td>
<td>Detect Program State</td>
<td></td>
<td>Block Reporting Message</td>
<td>Modify Control Logic</td>
<td>Loss of Availability</td>
</tr>
<tr>
<td>External Remote Services</td>
<td>Man in the Middle</td>
<td>System Firmware</td>
<td>Rootkit</td>
<td>Network Sniffing</td>
<td>Remote File Copy</td>
<td>I/O Image</td>
<td></td>
<td>Block Serial Comm Port</td>
<td>Modify Parameter</td>
<td>Loss of Control</td>
</tr>
<tr>
<td>Internet Accessible Device</td>
<td>Program Organization Units</td>
<td>Valid Accounts</td>
<td>Spooft Reporting Message</td>
<td>Remote System Discovery</td>
<td>Valid Accounts</td>
<td>Location Identification</td>
<td></td>
<td>Data Destruction</td>
<td>Module Firmware</td>
<td>Loss of Productivity and Revenue</td>
</tr>
<tr>
<td>Replication Through Removable Media</td>
<td>Project File Infection</td>
<td>Utilize/Change Operating Mode</td>
<td>Serial Connection Enumeration</td>
<td>Monitor Process State</td>
<td>Point &amp; Tag Identification</td>
<td>Program Upload</td>
<td></td>
<td>Denial of Service</td>
<td>Program Download</td>
<td>Loss of Safety</td>
</tr>
<tr>
<td>Spear phishing Attachment</td>
<td>Scripting</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Role Identification</td>
<td></td>
<td>Device Restart/Shutdown</td>
<td>Rogue Master Device</td>
<td>Loss of View</td>
</tr>
<tr>
<td>Supply Chain Compromise</td>
<td>User Execution</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Screen Capture</td>
<td></td>
<td>Manipulate I/O Image</td>
<td>Service Stop</td>
<td>Manipulation of Control</td>
</tr>
<tr>
<td>Wireless Compromise</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Modify Alarm Settings</td>
<td>Spooft Reporting Message</td>
<td>Manipulation of View</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Modify Control Logic</td>
<td>Unauthorized Command Message</td>
<td>Theft of Operational Information</td>
</tr>
</tbody>
</table>

**11 Tactics**

**81 Techniques**
<table>
<thead>
<tr>
<th>Initial Access</th>
<th>Execution</th>
<th>Persistence</th>
<th>Evasion</th>
<th>Discovery</th>
<th>Lateral Movement</th>
<th>Collection</th>
<th>Command and Control</th>
<th>Inhibit Response Function</th>
<th>Impair Process Control</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Historian Compromise</td>
<td>Change Program State</td>
<td>Hooking</td>
<td>Exploitation for Evasion</td>
<td>Control Device Identification</td>
<td>Default Credentials</td>
<td>Automated Collection</td>
<td>Commonly Used Port</td>
<td>Activate Firmware Update Mode</td>
<td>Brute Force I/O</td>
<td>Damage to Property</td>
</tr>
<tr>
<td>Drive-by Compromise</td>
<td>Command-Line Interface</td>
<td>Module Firmware</td>
<td>Indicator Removal on Host</td>
<td>I/O Module Discovery</td>
<td>Exploitation of Remote Services</td>
<td>Data from Information Repositories</td>
<td>Connection Proxy</td>
<td>Alarm Suppression</td>
<td>Change Program State</td>
<td>Denial of Control</td>
</tr>
<tr>
<td>Engineering Workstation</td>
<td>Execution through API</td>
<td>Program Download</td>
<td>Masquerading</td>
<td>Network Connection Enumeration</td>
<td>External Remote Services</td>
<td>Detect Operating Mode</td>
<td>Standard Application Layer Protocol</td>
<td>Block Command Message</td>
<td>Masquerading</td>
<td>Denial of View</td>
</tr>
<tr>
<td>Compromise</td>
<td>Exploit Public-Facing Application</td>
<td>Graphical User Interface</td>
<td>Project File Infection</td>
<td>Rogue Master Device</td>
<td>Network Service Scanning</td>
<td>Program Organization Units</td>
<td>Detect Program State</td>
<td>Block Reporting Message</td>
<td>Modify Control Logic</td>
<td>Loss of Availability</td>
</tr>
<tr>
<td>External Remote Services</td>
<td>Man in the Middle</td>
<td>System Firmware</td>
<td>Rootkit</td>
<td>Network Sniffing</td>
<td>Remote File Copy</td>
<td>I/O Image</td>
<td>Block Serial COM</td>
<td>Modify Parameter</td>
<td>Loss of Control</td>
<td></td>
</tr>
<tr>
<td>Internet Accessible Device</td>
<td>Program Organization Units</td>
<td>Valid Accounts</td>
<td>Spoof Reporting Message</td>
<td>Remote System Discovery</td>
<td>Valid Accounts</td>
<td>Location Identification</td>
<td>Data Destruction</td>
<td>Module Firmware</td>
<td>Loss of Productivity and Revenue</td>
<td></td>
</tr>
<tr>
<td>Replication Through Removable Media</td>
<td>Project File Infection</td>
<td>Utilize/Change Operating Mode</td>
<td>Serial Connection Enumeration</td>
<td>Monitor Process State</td>
<td>Point &amp; Tag Identification</td>
<td>Program Upload</td>
<td>Denial of Service</td>
<td>Program Download</td>
<td>Loss of Safety</td>
<td></td>
</tr>
<tr>
<td>Spear phishing Attachment</td>
<td>Scripting</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Role Identification</td>
<td>Device Restart/Shutdown</td>
<td>Rogue Master Device</td>
<td>Loss of View</td>
<td></td>
</tr>
<tr>
<td>Supply Chain Compromise</td>
<td>User Execution</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Screen Capture</td>
<td>Manipulate I/O Image</td>
<td>Service Stop</td>
<td>Manipulation of Control</td>
<td></td>
</tr>
<tr>
<td>Wireless Compromise</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Modify Alarm Settings</td>
<td>Spoof Reporting Message</td>
<td>Manipulation of View</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Modify Control Logic</td>
<td>Unauthorized Command Message</td>
<td>Theft of Operational Information</td>
<td></td>
</tr>
</tbody>
</table>

11 Tactics
81 Techniques
<table>
<thead>
<tr>
<th>Initial Access</th>
<th>Execution</th>
<th>Persistence</th>
<th>Evasion</th>
<th>Discovery</th>
<th>Lateral Movement</th>
<th>Collection</th>
<th>Command and Control</th>
<th>Inhibit Response Function</th>
<th>Impair Process Control</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Historian Compromise</td>
<td>Change Program State</td>
<td>Hooking</td>
<td>Exploitation for Evasion</td>
<td>Control Device Identification</td>
<td>Default Credentials</td>
<td>Automated Collection</td>
<td>Commonly Used Port</td>
<td>Activate Firmware Update Mode</td>
<td>Brute Force I/O</td>
<td>Damage to Property</td>
</tr>
<tr>
<td>Drive-by Compromise</td>
<td>Command-Line Interface</td>
<td>Module Firmware</td>
<td>Indicator Removal on Host</td>
<td>I/O Module Discovery</td>
<td>Exploitation of Remote Services</td>
<td>Data from Information Repositories</td>
<td>Connection Proxy</td>
<td>Alarm Suppression</td>
<td>Change Program State</td>
<td>Denial of Control</td>
</tr>
<tr>
<td>Engineering Workstation Compromise</td>
<td>Execution through API</td>
<td>Program Download</td>
<td>Masquerading</td>
<td>Network Connection Enumeration</td>
<td>External Remote Services</td>
<td>Detect Operating Mode</td>
<td>Standard Application Layer Protocol</td>
<td>Block Command Message</td>
<td>Block Reporting Message</td>
<td>Denial of View</td>
</tr>
<tr>
<td>Exploit Public-Facing Application</td>
<td>Graphical User Interface</td>
<td>Project File</td>
<td>Rogue Master Device</td>
<td>Network Service Scanning</td>
<td>Program Organization Units</td>
<td>Detect Program State</td>
<td>Block Reporting Message</td>
<td>Modify Control Logic</td>
<td>Loss of Availability</td>
<td></td>
</tr>
<tr>
<td>External Remote Services</td>
<td>Man in the Middle</td>
<td>System Firmware</td>
<td>Rootkit</td>
<td>Network Sniffing</td>
<td>Remote File Copy</td>
<td>I/O Image</td>
<td>Block Serial Comm Port</td>
<td>Modify Parameter</td>
<td>Loss of Control</td>
<td></td>
</tr>
<tr>
<td>Internet Accessible Device</td>
<td>Program Organization Units</td>
<td>Valid Accounts</td>
<td>Spoof Reporting Message</td>
<td>Remote System Discovery</td>
<td>Valid Accounts</td>
<td>Location Identification</td>
<td>Data Destruction</td>
<td>Module Firmware</td>
<td>Loss of Productivity and Revenue</td>
<td></td>
</tr>
<tr>
<td>Replication Through Removable Media</td>
<td>Project File</td>
<td>Utilize/Change Operating Mode</td>
<td>Serial Connection Enumeration</td>
<td>Monitor Process State</td>
<td></td>
<td></td>
<td>Denial of Service</td>
<td>Program Download</td>
<td>Loss of Safety</td>
<td></td>
</tr>
<tr>
<td>Spearphishing Attachment</td>
<td>Scripting</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Device Restart/Shutdown</td>
<td>Rogue Master Device</td>
<td>Loss of View</td>
<td></td>
</tr>
<tr>
<td>Supply Chain Compromise</td>
<td>User Execution</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Manipulate I/O Image</td>
<td>Service Stop</td>
<td>Manipulation of Control</td>
<td></td>
</tr>
<tr>
<td>Wireless Compromise</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Modify Alarm Settings</td>
<td>Spoof Reporting Message</td>
<td>Manipulation of View</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Modify Control Logic</td>
<td>Unauthorized Command Message</td>
<td>Theft of Operational Information</td>
<td></td>
</tr>
</tbody>
</table>

**11 Tactics**

**81 Techniques**
ICS/SCADA Security Threat Situation

Vulnerabilities are mostly critical and high risk levels

The number of vulnerability is rising year by year

The security incidents have a huge impact

ICS/SCADA are not secure at all

Critical
ICS Protocols

Process
- Modbus
- SIEMENS
- HART
- MITSUBISHI ELECTRIC
- OMRON

Industrial Control
- OPC
- Power
- BACnet
- Fox

Building
The Communication of ICS Protocols

- Primary Historian
- Data Acquisition Server
- Database Server
- Configuration Server
- Engineering Workstations
- Remote Network Router
- HMI
- Industrial Wireless
- Field Controller
- Field Devices
- Safe System
- Field Device Network
Critical Infrastructure Sectors (Taiwan)
ICS Protocols and Critical Infrastructure Sectors (Singapore)
ICS Protocols and Critical Infrastructure Sectors (Japan)

- Aviation
- Financial
- Airport
- Gas
- Water
- Information and communication
- Medical
- Electric power supply
- Railway
- Chemical
- Credit card
- Government and administrative
- Petroleum
- Logistics
ICS Protocols and Critical Infrastructure Sectors (US)

- Chemical
- Commercial Facilities
- Communications
- Critical Manufacturing

- Emergency Services
- Energy
- Financial Services
- Healthcare and Public Health

- Transportation Systems
- Food and Agriculture
- Defense Industrial Base
- Government Facilities

- Nuclear Reactors, Materials, and Waste
- Dams
- Information Technology
- Water and Wastewater Systems
ICS Protocols and Critical Infrastructure Sectors (US)

- Chemical
- Emergency Services
- Transportation Systems
- Nuclear Reactors, Materials, and Waste
- Commercial Facilities
- Energy
- Food and Agriculture
- Dams
- Communications
- Financial Services
- Defense Industrial Base
- Information Technology
- Critical Manufacturing
- Healthcare and Public Health
- Government Facilities
- Water and Wastewater Systems
Public and Private: ICS Network Protocols
Why Public vs. Private Protocols?

Public
- Modbus
- dnp
- IEC
- EtherNet/IP

Private
- Mitsubishi Electric
- OMRON
- SIEMENS
The Specification of Public Protocols
Modbus/TCP Handshake Process

### M₁. Request

**Modbus =** \( \langle \text{Function Code} | \text{Request Data} \rangle \)

**Modbus/TCP =** \( \langle \text{Transaction ID} | \text{Protocol ID} | \text{Length} | \text{Unit ID} \rangle \)

<table>
<thead>
<tr>
<th>Modbus/TCP</th>
<th>Modbus</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transaction ID</td>
<td>Protocol Identifier</td>
</tr>
<tr>
<td>Length Field</td>
<td>Unit ID</td>
</tr>
<tr>
<td>Function Code</td>
<td>Request Data</td>
</tr>
</tbody>
</table>

### M₂. Response

**Modbus =** \( \langle \text{Function Code} | \text{Response Data} \rangle \)

**Modbus/TCP =** \( \langle \text{Transaction ID} | \text{Protocol ID} | \text{Length} | \text{Unit ID} \rangle \)

<table>
<thead>
<tr>
<th>Modbus/TCP</th>
<th>Modbus</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transaction ID</td>
<td>Protocol Identifier</td>
</tr>
<tr>
<td>Length Field</td>
<td>Unit ID</td>
</tr>
<tr>
<td>Function Code</td>
<td>Response Data</td>
</tr>
</tbody>
</table>
Modbus/TCP Handshake Process

\[ M_1\text{. Request} \rightarrow M_2\text{. Response} \]
EtherNet/IP CIP Handshake Process

<table>
<thead>
<tr>
<th>Command</th>
<th>Length</th>
<th>Session Handle</th>
<th>Status</th>
<th>Max Delay</th>
<th>Sender Context</th>
<th>Options</th>
<th>Command-specific Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>2 bytes</td>
<td>2 bytes</td>
<td>4 bytes</td>
<td>4 bytes</td>
<td>2 bytes</td>
<td>6 bytes</td>
<td>4 bytes</td>
<td>6 bytes</td>
</tr>
</tbody>
</table>
Function Code

- Get Attributes All 0x01
- Set Attributes All 0x02
- Get Attribute List 0x03
- Set Attribute List 0x04
- Start 0x06
- Stop 0x07
EtherNet/IP Traffic
DNP3 Handshake Process

**TCP Connection Established**

- **M₁. TCP SYN**
- **M₂. TCP SYN/ACK**
- **M₃. TCP ACK**

**DNP3 Communication**

- **M₄. DNP3 Request**
- **M₅. DNP3 Response**
- **M₆. ACK**

**DNP3**

- Application Layer = [Control|Function|Internal Indicators|Data Objects]
- Application Chunks = [Length|CRC]
- Pseudo Transport Layer = [Transport Control]
- Data Link Layer = [Start Byte|Length|Control|Destination|Source|CRC]
  - TCP
  - IP
  - Ethernet
DNP3 Handshake Process

- **M₁. TCP SYN**
- **M₂. TCP SYN/ACK**
- **M₃. TCP ACK**
- **M₄. DNP3 Request**
- **M₅. DNP3 Response**
- **M₆. ACK**

DNP3 Response

```
Frame 4: 108 bytes on wire (864 bits), 108 bytes captured (864 bits)
  Ethernet   Internet Protocol Version 4
  Src: 192.168.1.2, Dst: 192.168.1.1
  Transmission Control Protocol,Src Port: 20000, Dst Port: 49278
  Data Link Layer, Len: 43, From: 4, To: 2, FIM, Unconfirmed User Data
  Start Bytes: 0x8064
  Length: 43
  Control: 0x48 (FIM, Unconfirmed User Data)
  Source: 4
  Data Link Header checksum: 0x8097 [correct]
  Data Link Header Checksum Status: Good
  Transport Control: 0x08, Final(FIM, FIM, Sequence 40)
  Data chunks
  [1 DNP 3.0 AL fragment (37 bytes): #4(37)]
  [Application Layer: (FIM, FIM, Sequence 2, Response)]
  [Application Control: 0x02, Final(FIM, FIM, Sequence 2)]
  1....  = First: Set
  1....  = Final: Set
  1....  = Confirm: Not set
  0....  = Unsolicited: Not set
  .... 0108 = Sequence: 2
  Function Code: Response (0x01)
  Internal Indications: 0x0000
  RESPONSE Data Objects
  - Object(s): File Control - File Transport (Obj:7B, Var:85) (0x4680), 1 point
    - Qualifier Field, Prefix: 2-Octet Object Size Prefix, Range: Free-format Qualifier
      185.... = Prefix Code: 2-Octet Object Size Prefix (5)
  - Number of Items: 1
  - Object: Sim 27
    - Size (16-bit): 27
    - File Handle: 0x7346578
    - Range Code: Free-format Qualifier (11)
    - File Block Number: 0x00000000
    - File Last Block: Set
    - File Data: 54689732069732061287465734266696c65
```
DNP3 Handshake Process (Unsolicited responses)

- $M_1$. TCP SYN
- $M_2$. TCP SYN/ACK
- $M_3$. TCP ACK
- $M_4$. DNP3 Unsolicited responses
- $M_5$. DNP3 Confirm
IEC 104 Handshake Process

**M1:** TCP SYN

**M2:** TCP SYN/ACK

**M3:** TCP ACK

**M4:** IEC104 STARTDT Act

**M5:** IEC104 STARTDT Con

**M6:** IEC104 Control/MonitorRequest

**M7:** IEC104 Control/MonitorResponse

Application Protocol Data Unit = APCI + ASDU
IEC 104 Handshake Process

$M_1$. TCP SYN
$M_2$. TCP SYN/ACK
$M_3$. TCP ACK

$M_4$. IEC104 STARTDT Act
$M_5$. IEC104 STARTDT Con

$M_6$. IEC104 Control/MonitorRequest
$M_7$. IEC104 Control/MonitorResponse
Function List

- Process information in monitor direction (21)
  - 0x0a (10) M_ME_TA_1: Measured value, normalized value with time tag
- Process telegrams with long time tag IO (11)
- Process information in control direction (7)
  - 0x2d (45) C_SC_NA_1: Single command
- Command telegrams with long time tag (7)
- System information in monitor direction (1)
- System information in control direction (8)
  - 0x65 (101) C_CI_NA_1: Counter interrogation command
- Parameter in control direction (4)
- File transfer (8)
  - 0x78 (120) F_FR_NA_1: File ready
ORMON FINS Handshake Process

1. **Connection Established**
   - **Request:**
     - **FINS Frame:** \(<\text{Request Command}|\text{Data}\>)
     - **FINS Header:** \(<\text{ICF}|\text{RSV}|\text{GCT}|\text{DNA}|\text{DA1}|\text{DA2}|\text{SNA}|\text{SA1}|\text{SA2}|\text{SID}\>)
     - **FINS/TCP Header:** \(<\text{Magic}|\text{Length}|\text{Command}|\text{Error Code}\)
     - **TCP/UDP:** IP
     - **Ethernet:**

2. **FINS Node Address Exchanged**
   - **Response:**
     - **FINS Frame:** \(<\text{Response Code}|\text{Request Command}|\text{Data}\>)
     - **FINS Header:** \(<\text{ICF}|\text{RSV}|\text{GCT}|\text{DNA}|\text{DA1}|\text{DA2}|\text{SNA}|\text{SA1}|\text{SA2}|\text{SID}\>)
     - **FINS/TCP Header:** \(<\text{Magic}|\text{Length}|\text{Command}|\text{Error Code}\)
     - **TCP/UDP:** IP
     - **Ethernet:**
ORMON FINS Handshake Process

- $M_1$. TCP SYN
- $M_2$. TCP SYN/ACK
- $M_3$. TCP ACK
- $M_4$. FINS Node Address X Sent
- $M_5$. FINS Node Address Y Sent
- $M_6x$. FINS Request
- $M_7x$. FINS Response
- $M_6y$. FINS Request
- $M_7y$. FINS Response
Siemens S7 Handshake Process

TCP 3-Way Connection Set-up
ISO 8073/X.224 COTP Connection — Oriented Transport Protocol
ISO transport services on top of the TCP (TPKT)
TCP
IP
Ethernet

COTP Connection Establishment

Siemens S7 Communication Establishment

Siemens S7 Communication
ISO 8073/X.224 COTP Connection — Oriented Transport Protocol
ISO transport services on top of the TCP (TPKT)
TCP
IP
Ethernet

TCP 4-Way Connection Close

M₁. TCP SYN
M₂. TCP SYN/ACK
M₃. TCP ACK
M₄. CR Connect Request
M₅. CC Connect Confirm
M₆. Setup Communication Request
M₇. Setup Communication Response
M₈. Siemens S7 Request
M₉. Siemens S7 Response
M₁₀. TCP FIN/ACK
M₁₁. TCP ACK
M₁₂. TCP FIN/ACK
M₁₃. TCP ACK

Packet
Siemens S7 Handshake Process

- **M1.** TCP SYN
- **M2.** TCP SYN/ACK
- **M3.** TCP ACK
- **M4.** CR Connect Request
- **M5.** CC Connect Confirm
- **M6.** Setup Communication Request
- **M7.** Setup Communication Response
- **M8.** Siemens S7 Request
- **M9.** Siemens S7 Response
- **M10.** TCP FIN/ACK
- **M11.** TCP ACK
- **M12.** TCP FIN/ACK
- **M13.** TCP ACK

Diagram showing the handshake process between HMI and PLC, with steps M1 to M8 detailed.
Siemens S7 Plus Handshake Process

- $M_1$. TCP SYN
- $M_2$. TCP SYN/ACK
- $M_3$. TCP ACK
- $M_4$. CR Connect Request
- $M_5$. CC Connect Confirm
- $M_6$. 1st S7+ Connection Request
- $M_7$. 1st S7+ Connection Response (with Object ID and Value Array)
- $M_8$. 2nd S7+ Connection Request (with Session ID and KeyBlock)
- $M_9$. 2nd S7+ Connection Response
- $M_{10}$. Siemens S7 Request (with Integrity Part)
- $M_{11}$. Siemens S7 Response

HMI

PLC
Siemens S7 Plus Version

**V1**
- Protocol: S7 Communication Plus
- Version: V5 (V4.1)

**V2**
- Protocol: S7 Communication Plus
- Version: V6 (V4.2)

**V3**
- Integrity part
  - Integrity ID: 10
  - Digest Length: 32
- Packet Digest: 4609653b08b18a54db468e72c320718b17720d92530e2aC
- Trailer: Protocol version-V3
Wireshark can’t analyze MELSEC Traffic
Again, we built a Lua Plugin for MELSEC
Mitsubishi Melsec/TCP Handshake Process

$M_1$. Request

$M_2$. Response

$\{MELSEC = \langle Sub - Header | Access Route | Request Data Length | Timer | Request Data \rangle\$

TCP
IP
Ethernet

$\{MELSEC = \langle Sub - Header | Access Route | Response Data Length | End Code | Response Data \rangle\$

TCP
IP
Ethernet
Mitsubishi Melsec/TCP Handshake Process

M1.Request

M2.Response

M1.Request

M2.Response
Common Flaws in ICS Network Protocols
## Insecure by Design

<table>
<thead>
<tr>
<th>Type</th>
<th>Protocols</th>
<th>Handshake</th>
<th>Authentication</th>
<th>Message Encryption</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public</td>
<td>Modbus/TCP</td>
<td>TCP Connection</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td></td>
<td>DNP3/TCP</td>
<td>TCP Connection</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td></td>
<td>EtherNet/IP/CIP</td>
<td>ENIP Connection based</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td></td>
<td>IEC104</td>
<td>TCP Connection + STARTDT</td>
<td>✗</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Melsec/TCP</td>
<td>TCP Connection</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td></td>
<td>OMRON FINS/TCP</td>
<td>TCP Connection + FINS/TCP session based</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td></td>
<td>S7COMM</td>
<td>TCP Connection + COTP + S7COMM Session</td>
<td>✗</td>
<td>△(when EWS compile PLC program)</td>
</tr>
<tr>
<td>Private</td>
<td>S7COMM Plus</td>
<td>TCP Connection + COTP + S7COMM+ Session</td>
<td>V1</td>
<td>✗</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>V2</td>
<td>✗</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>V3</td>
<td>√ (EWS &lt;-&gt; PLC)</td>
</tr>
</tbody>
</table>
# Attacks on ICS Protocols

<table>
<thead>
<tr>
<th>Type</th>
<th>Protocols</th>
<th>T814 Denial-of-Service</th>
<th>T836 Modify Parameter</th>
<th>T856 Spoof Reporting Message</th>
<th>T843 Program Download</th>
<th>T855 Unauthorized Command Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public</td>
<td>Modbus/TCP</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>?</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>DNP3/TCP</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>?</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>EtherNet/IP/CIP</td>
<td>?</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>IEC104</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>?</td>
<td>✓</td>
</tr>
<tr>
<td>Private</td>
<td>Melsec/TCP</td>
<td>?</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>OMRON FINS/TCP</td>
<td>?</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>S7COMM</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>S7COMM Plus V1</td>
<td>?</td>
<td>✓</td>
<td>?</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>S7COMM Plus V2</td>
<td>?</td>
<td>✓</td>
<td>?</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>S7COMM Plus V3</td>
<td>?</td>
<td>✓</td>
<td>?</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>
# ICS ATT&CK Matrix map to ICS Protocols Attack

<table>
<thead>
<tr>
<th>Initial Access</th>
<th>Execution</th>
<th>Persistence</th>
<th>Evasion</th>
<th>Discovery</th>
<th>Lateral Movement</th>
<th>Collection</th>
<th>Command and Control</th>
<th>Inhibit Response Function</th>
<th>Impair Process Control</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Historian Compromise</td>
<td>Change Program State</td>
<td>Hooking</td>
<td>Exploitation for Evasion</td>
<td>Control Device Identification</td>
<td>Default Credentials</td>
<td>Automated Collection</td>
<td>Commonly Used Port</td>
<td>Activate Firmware Update Mode</td>
<td>Block Command Message</td>
<td>Masquerading Denial of View</td>
</tr>
<tr>
<td>Drive-by Compromise</td>
<td>Command-Line Interface</td>
<td>Module Firmware</td>
<td>Indicator Removal on Host</td>
<td>I/O Module Discovery</td>
<td>Exploitation of Remote Services</td>
<td>Data from Information Repositories</td>
<td>Connection Proxy</td>
<td>Alarm Suppression Change Program State</td>
<td>Denial of Control</td>
<td></td>
</tr>
<tr>
<td>Exploit Public-Facing Application</td>
<td>Graphical User Interface</td>
<td>Project File</td>
<td>Rogue Master Device</td>
<td>Network Service Scanning</td>
<td>Program Organization Units</td>
<td>Detect Program State</td>
<td>Block Reporting Message</td>
<td>Modify Control Logic Loss of Availability</td>
<td></td>
<td></td>
</tr>
<tr>
<td>External Remote Services</td>
<td>Man in the Middle</td>
<td>System Firmware</td>
<td>Rootkit</td>
<td>Network Sniffing</td>
<td>Remote File Copy</td>
<td>I/O Image</td>
<td>Block Serial Comm Port Modify Parameter Loss of Control</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Internet Accessible Device</td>
<td>Program Organization Units</td>
<td>Valid Accounts</td>
<td>Spoofer Reporting Message</td>
<td>Remote System Discovery</td>
<td>Valid Accounts</td>
<td>Location Identification</td>
<td>Denial of Service Program Download Loss of Safety</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Replication Through Removable Media</td>
<td>Project File</td>
<td>Scripting</td>
<td>Utilize/Change Operating Mode</td>
<td>Serial Connection Enumeration</td>
<td>Monitor Process State</td>
<td>Block Reporting Message</td>
<td>Device Restart/Shutdown Rogue Master Device Loss of View</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Spearphishing Attachment</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Manipulate I/O Image Service Stop Manipulation of Control</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Supply Chain Compromise</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Modify Alarm Settings Spoofer Reporting Message Manipulation of View</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Wireless Compromise</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Modify Control Logic Unauthorized Command Message Theft of Operational Information</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### 11 Tactics

### 81 Techniques

- Program Download
- Rootkit
- System Firmware
- Utilize/Change Operating Mode
T836-Modify Parameter with Mitsubishi Melsec
T836-Modify Parameter
T843-Program Download with Mitsubishi Melsoft
T856-Spoof Reporting Message with Modbus/TCP
T855-Unauthorized Command Message with Omron FINS
Common Flaws in ICS Protocols

- No Authentication
- No Authorization
- No Encryption
- Stack Overflow

Impact:
- T880 - Loss of Safety
- T829 - Loss of View
- T827 - Loss of Control
- T826 - Loss of Availability
- T815 - Denial of View
- T813 - Denial of Control
- T832 - Manipulation of View
- T831 - Manipulation of Control
How to Defend Against ICS Network Protocol Attacks
Vulnerable OT Environment

1. **Shadow OT**
   - Unknown devices and unknown connections

2. **Insecure Authentication**
   - Flaws come from design or implementation

3. **Insecure Protocols**
   - Simply unencrypted

4. **Unpatched Devices**
   - Patching is not feasible or available

5. **Insecure 3rd-Party Software**
   - Vulnerable, and might be compromised from supply chain in the beginning
Suggested Strategies from ICS CERT

<table>
<thead>
<tr>
<th>Strategy</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manage authentication</td>
<td>4%</td>
</tr>
<tr>
<td>Implement application whitelisting</td>
<td>38%</td>
</tr>
<tr>
<td>Implement secure remote access</td>
<td>1%</td>
</tr>
<tr>
<td>Monitor and respond</td>
<td>2%</td>
</tr>
<tr>
<td>Configuration/patch mgmt.</td>
<td>29%</td>
</tr>
<tr>
<td>Build a defendable environment</td>
<td>9%</td>
</tr>
<tr>
<td>Reduce your attack surface</td>
<td>17%</td>
</tr>
</tbody>
</table>


Implementing **FIVE** Tactics to prevent 98% incidents
Effective Segmentation, Virtual Patch, Containment

- Divide a big flat L2 network into secured segments
- Virtual Patch (IPS)
  - Containment of malware and worms
  - Shield device vulnerabilities
  - Deeply inspect IT protocols: SMB, RDP, ...
- Industrial-Grade Hardware
Granular Control Over Popular OT Protocols

- Asset and protocol visibility
- Fine-grained access control in different levels
  - Devices
  - Protocols (Modbus, Melsec/SLMP, CC-Link IE, Ethernet/IP, Profinet, S7COMM, HSMS/SECS-II, ...)
  - Control Commands (read, configure, shutdown, ...)
- Greatly lower the possibility of Denial-of-Service attacks by OT trojans
Network Whitelisting Control against Siemens S7 attack