Security Hardening of Industrial Control Systems through Attribute Based Access Control

Shwetha Gowdanakatte, Mahmoud Abdelgawad, and Indrakshi Ray

Ninth Annual Industrial Control System Security (ICSS) Workshop
October 2023
Austin, Texas, USA
Outline

- Introduction
- Background
  - PLC and their Security Vulnerabilities
  - NIST NGAC for PLC
- Attack demonstration
  - Attack Model
  - DoS Attack on the PLC
- Security Hardening
  - ABAC Gateway
  - Testbed
  - Prevention of DoS Attack with ABAC Gateway
- Formal Verification
  - Use Case 1: PLC without ABAC Gateway
  - Use Case 2: PLC with ABAC Gateway
- Formal Analysis
- Conclusion & Future work
Industrial Control Systems (ICS)

- Human Machine Interface (HMI)
- Programmable Logic Controller (PLC)
- Remote Monitoring and Control (RMC)
- Actuators
- Sensors
- Controlled Process

- Set points, parameter, control algorithms, constraints, process data
- Manipulated variable
- Process outputs
- Controlled variables

12/8/23
Background: PLC and their Security Vulnerabilities

- Programmable Logic Controllers
  - Rockwell Compact Logix
    - Engineering Framework: Studio 5000
    - Communication Protocol: Common Industrial Protocol (CIP)
  - Siemens S7-1500
    - Engineering Framework: Totally Integrated Automation (TIA) portal
    - Communication Protocol: S7-P3

- Recent Vulnerabilities
  - CVE-2021-1392: Obtain a CIP password and add an authorized admin user
  - CVE-2021-22681: Bypass authentication to impersonate Studio 5000
  - CVE-2016-9342 and CVE-2021-37185: Crafted TCP packets to the PLC
Attribute-Based Access Control for PLC: Gowdanakatte et al. [1]

Each policy is expressed as a tuple
\(<\{\text{User Attribute}\}, \{\text{Resource Attribute}\}, \{\text{Environmental Attribute}\}, \{\text{operation}\}>\)

**User Attributes**
- Access Level = \{Operator, Engineer, Administrator\}
- Device ID

**Resource (PLC) Attributes**
- Module = \{Software, Firmware, Communication, Memory\}
- Status = \{Stopped, Running, Emergency Stop Active\}
- Operating Mode = \{Program, Test, Error, Remote\}
- Port

**Environmental Attributes**
- User Access Time
- User Access Location

**Example Policy: Communication Setup**
\(<\{(\text{User.AccessLevel} \in \{\text{Operator, Engineer, Administrator}\}), (\text{User.Device} = \text{"Equip 21L OrgABC"}), (\text{PLC.OperatingMode} = \text{Remote})\}, (\text{Env. Access Time} = 700 - 16:00EST), (\text{Env. Access Loc} = \text{OrgABC.local"})\}, \{\text{CommSetup}\}>\)
Phase-1: Man-in-the-Middle (MITM) Attack

- Establish communication
- Process communication
- Intercept and capture packets
- Extract firmware version
- Create Crafted TCP packets

Engineering Workstation → Attacker
Attacker → PLC

12/8/23
Phase-2: Denial of Service (DoS) Attack

- **Init Comm.: PLC IP+Port 102**
  - Challenge question
  - Challenge response
  - Session OK
  - Crafted TCP Packets
- **Init Comm.: PLC IP+ port 102**
  - Challenge question
  - Challenge response
  - Session OK
  - Crafted TCP Packets
# Attack Demonstration

- **Attack Setup**

![Network Diagram](image)

## Phase 1: Man-in-the-Middle Attack

### Code for requesting status

```
0000  b8 27 eb ab 9f 2c b8 27 eb c6 86 fa 08 00 45 00 .....
0010  00 72 cb e2 40 00 40 06 d5 d9 de a8 0b 0c 0a 8a ..r.@
0020  00 2d 0d 24 af 12 49 01 00 39 62 65 76 0a 08 18 ..$..I..9be.K
0030  01 f9 fc e4 00 01 01 08 05 6c 13 f1 03 09 b9 ...........R.
0040  65 3b 6f 00 26 00 01 00 09 00 00 00 00 00 5f 70 e;j;&
0050  79 63 6f 66 0d 6d 6f 00 00 00 00 00 00 00 00 00 ycomm....
0060  02 00 00 00 00 00 00 b2 00 16 00 52 02 20 06 24 01 ...........R.
0070  0a 05 08 08 03 20 01 24 01 30 05 01 01 01 01
```

---

**Timeout:** 10

- **Item Count:** 2

**Common Industrial Protocol**

- **Service:** Unconnected Send (Request)
  
  0...7 = Request/Response: Request (0x8)
  
  101 0010 = Service: Unconnected Send (0x52)

- **Command Specific Data**
  
  0...7 = Priority: 0
  
  1010 = Tick time: 10

- **Time-out ticks:** 5

- **Actual Time Out:** 5120ms

- **Message Request Size:** 8

**Message Request**

- **Service:** Get Attribute Single (Request)

  **Request Path Size:** 3 (words)

  - **Path Segment:** 0x20 (0-Bit Class Segment)
  
  - **Path Segment:** 0x24 (8-Bit Instance Segment)
  
  - **Path Segment:** 0x30 (8-Bit Attribute Segment)

  Get Attribute Single (Request)
Phase 2: DoS Attack

- Recoverable major fault on the PLC
- Stopping the running process
- Unavailability of PLC for further online requests
- Caused DoS attack

Resolution

- Manual restarting of the PLC through a power cycle
- Clear major fault
NGAC-ABAC Implementation on Raspberry Pi3

- Python Vakt library
- Example Policy

```python
actions=[Eq('CommSetup')],
subjects=[{'User.AccessLevel': In('Operator', 'Engineer', 'Administrator'),
 'User.Device': Eq("Equip21L0rgABC")},
context={
    'Env.AccessTime': And(GreaterOrEqual(7.00), LessOrEqual(16.00)),
    'Env.AccessLoc': Eq("OrgABC.local"),
    'PLC.OperatingMode': Eq('Remote')}],
resources=[Eq('PLC')],
effect=vakt.ALLOW_ACCESS
```
Crafted TCP Packet

Device ID of Engineering Workstation: ‘velpi’

Allowed device ID for establishing the communication with Compact Logix: ‘Equip21LOrgABC’

Communication Request Packet
Policy Verification for ‘Register Session’ Request

DoS attack prevented based on invalid device ID
Verification: PLC Operates without ABAC Gateway

• **CPN Block Diagram**

• **Three CPNs:**
  - User, Network, and PLC

1. User sends a request packet to initialize communication with PLC
2. The PLC receives the request and replies with a challenge question
3. The user sends the challenge response.
4. The PLC confirms that the session is OK to be established.
5. The user sends a command to PLC to be executed.
6. The PLC executes the command and confirms the user with PLC status
Verification: PLC Operates without ABAC Gateway

CPN Demo: TCP Packets traveling between User and PLC through Network
### Verification: PLC Operates without ABAC Gateway

**Testcases:** CPN Tokens demonstrate legal access (first 3 tokens) and attacks (last 2 tokens)

<table>
<thead>
<tr>
<th>TC#</th>
<th>Description</th>
<th>Input (Token)</th>
<th>Expected Output</th>
<th>Actual Output</th>
<th>Testcase Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>ADMIN: A legal user listed in DAC-ACL and has privilege to setup PLC communication</td>
<td>{IP = &quot;10.255.10.7&quot;, dstIPAddr = &quot;129.10.1.3&quot;}, TCP = {srcPort = &quot;5357&quot;, dstPort = &quot;44818&quot;, CIP = &quot;Command = Comm.Setup, SessionHandle = &quot;established&quot;.&quot;}</td>
<td>PLC Status Running</td>
<td>PLC Status Running</td>
<td>Passed</td>
</tr>
<tr>
<td>2</td>
<td>ADMIN: A legal user listed in DAC-ACL privilege to stop PLC communication</td>
<td>{IP = &quot;10.255.10.7&quot;, dstIPAddr = &quot;129.10.1.3&quot;}, TCP = {srcPort = &quot;5357&quot;, dstPort = &quot;44818&quot;, CIP = &quot;Command = Comm.Stop, SessionHandle = &quot;established&quot;.&quot;}</td>
<td>PLC Status Stopped</td>
<td>PLC Status Stopped</td>
<td>Passed</td>
</tr>
<tr>
<td>3</td>
<td>USER: A legal user listed in DAC-ACL but does not have privilege to stop PLC communication</td>
<td>{IP = &quot;10.255.10.23&quot;, dstIPAddr = &quot;129.10.1.3&quot;}, TCP = {srcPort = &quot;5357&quot;, dstPort = &quot;44818&quot;, CIP = &quot;Command = Comm.Stop, SessionHandle = &quot;established&quot;.&quot;}</td>
<td>PLC Status Stopped</td>
<td>TCP Packet Rejected</td>
<td>Failed</td>
</tr>
<tr>
<td>4</td>
<td>ATTACKER-1: An attacker impersonates USER to stop PLC communication</td>
<td>{IP = &quot;13.255.255.1&quot;, dstIPAddr = &quot;129.10.1.3&quot;}, TCP = {srcPort = &quot;5357&quot;, dstPort = &quot;44818&quot;, CIP = &quot;Command = Comm.Stop, SessionHandle = &quot;established&quot;.&quot;}</td>
<td>PLC Status Stopped</td>
<td>TCP Packet Rejected</td>
<td>Failed</td>
</tr>
<tr>
<td>5</td>
<td>ATTACKER-2: An attacker impersonates ADMIN to setup PLC communication</td>
<td>{IP = &quot;13.255.255.3&quot;, dstIPAddr = &quot;129.10.1.3&quot;}, TCP = {srcPort = &quot;5357&quot;, dstPort = &quot;44818&quot;, CIP = &quot;Command = Comm.Setup, SessionHandle = &quot;established&quot;.&quot;}</td>
<td>PLC Status Stopped</td>
<td>PLC Status Stopped</td>
<td>Passed</td>
</tr>
</tbody>
</table>

- **TC#4:** ATTACKER-1 impersonates USER and obtained the same access discretion, but DAC blocked its TCP request packet. (Testcase failed)
- **TC#5:** ATTACKER-2 impersonates ADMIN, gained its discretion, and stopped the PLC. (Testcase passed)
Verification: PLC Operates with ABAC Gateway

- **CPN Block Diagram**: Four CPNs (User, Network, ABAC Gateway, and PLC)
- **ABAC Gateway**: contains three sub CPN blocks: Authentication Module, Comm. Handler, and Access Control Module (NGAC)
- Any TCP Packet sent from User to PLC must go through the ABAC Gateway
Verification: PLC Operates with ABAC Gateway

CPN Demo: TCP Packets traveling between User and PLC through Network and ABAC Gateway
Verification: PLC Operates with ABAC Gateway

Testcases: CPN Tokens demonstrate legal access (first 3 tokens) and attacks (last 3 tokens)

- TC#6: ATTACKER-2 impersonates ADMIN, sends setup command, but it is denied by the ABAC Gateway. (Testcase failed)
Formal Analysis

State-Space Analysis for Use Case 1

- State Space - Total number of states and transitions during the communication between the user and the PLC
- Strongly Connected Graphs (SCC) - Verifies the correctness of the model
- Dead State – Represent the state at which the communication is terminated between the user and the PLC

<table>
<thead>
<tr>
<th>State Space</th>
<th>SCC Graph</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>#State 1820</td>
<td>#Transition 5733</td>
<td>#State 1820</td>
</tr>
<tr>
<td>Home State [1653]</td>
<td>Dead State [1378,1745]</td>
<td></td>
</tr>
</tbody>
</table>

State-Space Analysis for Use Case 2

<table>
<thead>
<tr>
<th>State Space</th>
<th>SCC Graph</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>#State 4876</td>
<td>#Transition 18057</td>
<td>#State 4876</td>
</tr>
<tr>
<td>Home State [683]</td>
<td>[722,723,3156,3157,3158,3159,3160,3161,3162,3163,3164,3165,3166,3167]</td>
<td></td>
</tr>
</tbody>
</table>
Conclusion

- It may be impossible to patch all the vulnerabilities of ICS.
- The solution is to protect against authentication vulnerabilities in PLC.
- We developed NIST NGAC Attribute-Based Access Control for PLC protection.
- We built a testbed to demonstrate the ABAC Gateway.
- Formal Verification is executed to verify the PLC system in Use Cases:
  1) PLC operates without ABAC Gateway
  2) PLC operates with ABAC Gateway
- Result shows ABAC Gateway effectively hardens the PLC security.
Future Work

• Currently, we are investigating the use of NIST NGAC for the security hardening of other devices in an ICS environment.

• Next, we will analyze the latency, performance, and throughput of the ICS due to the incorporation of the ABAC module
• NSF
• NIST
• Cyber Risk Research
• Statnett
• AMI
• ARL
• New Push
Thank you!

Questions?