Probabilistic Attack Sequence Generation and Execution Based on MITRE ATT&CK for ICS Datasets

2021. 8. 9.

Seungoh Choi, Jeong-Han Yun, and Byung-Gil Min
I | Motivation

II | Background
   • MITRE ATT&CK for ICS

III | Proposed method
   • Overview
   • Attack sequence generator
   • Attack sequence executor

IV | Case study
   • HMM for all ICS Incident
   • HMM for specific ICS Incident

V | Conclusion
Security research in industrial control systems (ICSs)

Constraints

Availability
Actual attack are difficult to reproduce at the ICS operating environment.

Dataset
An abnormal dataset that includes attack-related data, should be provided.

Previous work

HAI Testbed

Ongoing work

Developing a Dataset for all ICS levels

Level 0
Sensor, Pump, Actuator, Breaker

Level 1
DCS, PLC, RTU, IED

Level 2
EWS, HMI, Historian, NTP

Network

Physical

Control Systems

Field Devices

System

Ethernet
Three aspects to develop an abnormal dataset

Reproducibility: An representation that can reproduce abnormal situations

Reality: Adversary tactics and techniques based on real-world observations

Diversity: A model that can reflect more diverse attack sequences

Stochastic Modelling

Represented attack sequence based on adversary tactics and techniques

Analyzed the existing ICS incident reports to determine the probabilities

Generated various attack sequences by the probabilities

Generating attack sequence defined as a series of technique with tactic based on MITRE ATT&CK
## Background

### MITRE ATT&CK for ICS*

<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>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>Block Reporting Message</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>Block Serial COM</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>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>Valid Accounts</td>
<td>Utilize/Change Operating Mode</td>
<td>Serial Connection Enumeration</td>
<td>Monitor Process State</td>
<td>Point &amp; Tag Identification</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>Program Upload</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>Role Identification</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>Screen Capture</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>

* We referred to the initial version of ATT&CK for ICSs, which was extensively edited on 29 April 2021 while working on this paper.
Overview

- **Attack sequence generator**
  - Generating attack sequence with probabilities

- **Attack sequence executor**
  - Applying attack sequence with attack profiles

- **Attack tool**
  - Metasploit with module from Purple Team ATT&CK Automation

- **Attack environment**
  - HAI Testbed

Proposed method (1/7)
**Proposed method (2/7)**

**Attack sequence generator**

- Using Hidden Markov Model (HMM) to generate attack sequence based on MITRE ATT&CK for ICSs
- Assumption
  - The tactic \( (x_t) \) used by the attacker at the current time \( (t) \) is only affected by the tactic \( (x_{t-1}) \) used by the previous time \( (t-1) \). (i.e., Markovian property)
  - The technique \( (y_t) \) observed at the current time \( (t) \) is affected only by the tactic \( (x_t) \) at the current time \( (t) \).
Proposed method (3/7)

Attack sequence generator

- **HMM configuration**
  1. *Hidden states* \((S)\)
     - Tactics from MITRE ATT&CK
  2. *Observations* \((O)\)
     - Techniques from MITRE ATT&CK

- **HMM parameters**
  1. *Initial state probability* \((\pi)\)
     - Probability of starting at each tactic
  2. *Transition probability* \((T)\)
     - Probability of transition between each tactic
  3. *Emission probability* \((E)\)
     - Probability of the occurrence of the technique observed in each tactic
## Proposed method (4/7)

### Attack sequence generator
- HMM parameters calculation

### Table 1: Related materials of ICS incidents

<table>
<thead>
<tr>
<th>Type</th>
<th>Name (Incident)</th>
<th>Materials</th>
</tr>
</thead>
<tbody>
<tr>
<td>Malware</td>
<td>Stuxnet (Iran nuclear facilities)</td>
<td>[11, 16]</td>
</tr>
<tr>
<td></td>
<td>BlackEnergy3, Indoroyer (Ukraine power grid)</td>
<td>[3, 15, 18, 29]</td>
</tr>
<tr>
<td></td>
<td>Triton (Saudi Arabia petrochemical plant)</td>
<td>[5, 18]</td>
</tr>
<tr>
<td></td>
<td>Duqu</td>
<td>[30]</td>
</tr>
<tr>
<td></td>
<td>Flame</td>
<td>[25]</td>
</tr>
<tr>
<td></td>
<td>BlackEnergy (KillDisk)</td>
<td>[12]</td>
</tr>
<tr>
<td></td>
<td>ACAD/Medre.A</td>
<td>[10]</td>
</tr>
<tr>
<td></td>
<td>Backdoor.Oldrea (HAVEX)</td>
<td>[18]</td>
</tr>
<tr>
<td></td>
<td>Conficker</td>
<td>[4]</td>
</tr>
<tr>
<td></td>
<td>VPNFilter</td>
<td>[17]</td>
</tr>
<tr>
<td></td>
<td>Bad Rabbit (Ukrainian transportation)</td>
<td>[19]</td>
</tr>
<tr>
<td></td>
<td>LockerGoga (Norway aluminum company)</td>
<td>[1, 26]</td>
</tr>
<tr>
<td></td>
<td>NotPetya (Ukrainian organizations)</td>
<td>[32]</td>
</tr>
<tr>
<td></td>
<td>Ryuk</td>
<td>[13, 26]</td>
</tr>
<tr>
<td></td>
<td>WannaCry</td>
<td>[14, 26]</td>
</tr>
<tr>
<td>PoC</td>
<td>PLC-Blaster (Worm that runs on Siemens S7 PLC)</td>
<td>[27]</td>
</tr>
<tr>
<td></td>
<td>SoftPLC</td>
<td>[33]</td>
</tr>
</tbody>
</table>
Attack sequence generator

- HMM parameters setup
Attack sequence generator

- Transition within attack sequence
  - Self transition
    - Multiple techniques can be used within the same tactic.
    - The same technique can be retried.
  - Terminus transition
    - When reaching final state "Impact", single attack sequence considered complete.

---

Initial Access → Execution → Persistence → ... → Impact

Self transition

Terminus transition
**Proposed method (7/7)**

**Attack sequence executor**

- **(Attack profile)** information required to execute each technique constituting the attack sequence
  - Attacker and victim information on executing the attack technique
  - Time information to sequentially perform attack sequence according to the timeline
  - Various options such as commands and file paths to be used

![Attack sequence diagram](image)

**Execution tool**

- Using Metasploit with post module from the Purple Team ATT&CK Automaiton
- Currently developing an the automation tool to facilitate attack reproduction
HMM for all ICS incidents

- HMM configuration
  - (Input) State and observation graph with the HMM parameters ($\pi$, $T$, $E$) for all Incidents attack sequence
  - (output) Attack sequence generated by the HMM for all ICS Incidents
    - Note that we limited the number of transition as 20 to compare with attack sequences.
    - Examples of generated attack sequence
      1. Attack sequence where reached final state
         
         ![Attack sequence diagram](image)
      2. Attack sequence where not reached final state
         
         ![Attack sequence diagram](image)
**HMM for specific ICS incident**

**HMM configuration**

- (Input) State and observation graph with the HMM parameters for TRITON malware attack sequence

- (Output) Triton-like attack sequence
Conclusion

Attack Sequence Generation and Execution

- **Attack sequence generation**
  - **Probability issues**
    - The probabilities are likely not a representative for all adversaries.
    - The propabilities cannot be automatically obtained to evolve for attack patterns.

- **Discussion**
  - **Target of attack execution**
    - We did not aim to attack the same devices that were subjected to every real ICS attack.
    - It was limited to the HAI testbed.

---

Development of a dataset of which all levels of the HAI testbed are covered with:

1) Using the proposed method to generate attack sequence for an abnormal data
2) then implement and test to execute at the HAI testbed