Attack Graph Driven Cyber-Physical System (CPS) Resilience Assessment

Sumit Purohit, PhD

Sumit.Purohit@pnnl.gov
• Cyber Physical System (CPS) such as microgrid has large input space (elements, measurements, users) with discrete (cyber) and continuous (physical) measurements across multiple layers

• Multimodalities and complex interdependencies in cyber-physical systems (CPSs) give rise to emergent of behaviors under adverse conditions that are difficult to observe and characterize in real-world or demonstrated normal conditions.

• Develop methodologies to perform cyber security experimentation

• Experimentation of contingencies with edge cases is critical to identify resilient Cyber-Physical System (CPS) control strategies
  - Existing security assessment approaches, such as penetration testing and red teaming
    ✓ Rely on subject matter experts’ experience and forensic
    ✓ Analysis of historical events to perform realistic assessment
  - State-space explosion may lead to computational costs that can delay access to critical decision support inputs

• Hybrid attack graphs (HAGs) can be used for resilience assessment
Ongoing research

- To develop data-driven and physics informed novel theory and algorithms to generate hybrid attack graphs for cyber-physical system (CPS) resilience experimentation at desired scale and speed.

S&T Challenges

- How to characterize hybrid CPS dynamics across scale with sparse data?
- How can the hybrid dynamics be leveraged to generate credible course-of-action HAGs?
- How to perform dimension reduction of HAGs for edge test case experimentation?

- One of the first cyber espionage campaign that targeted oil, energy, and petrochemical companies, along with individuals and executives in Kazakhstan, Taiwan, Greece, and the United States
- Threat actors searched for information related to oil and gas field production systems, financials, and collected data from SCADA systems
MITRE ATT&CK

Globally-accessible knowledge base of adversary tactics and techniques based on real-world observations.

<table>
<thead>
<tr>
<th>Initial Access</th>
<th>Execution</th>
<th>Persistence</th>
<th>Privilege Escalation</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>12 techniques</td>
<td>9 techniques</td>
<td>6 techniques</td>
<td>2 techniques</td>
<td>6 techniques</td>
<td>5 techniques</td>
<td>7 techniques</td>
<td>10 techniques</td>
<td>3 techniques</td>
<td>13 techniques</td>
<td>5 techniques</td>
<td>12 techniques</td>
</tr>
<tr>
<td>Drive-by Compromise</td>
<td>Change Operating Mode</td>
<td>Hardcoded Credentials</td>
<td>Exploitation for Privilege Escalation Hooking</td>
<td>Change Operating Mode</td>
<td>Network Connection Enumeration</td>
<td>Default Credentials</td>
<td>Adversary-in-the-Middle</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>Exploit Public-Facing Application</td>
<td>Command-Line Interface</td>
<td>Modify Program Module Firmware</td>
<td>Exploitation for Evasion</td>
<td>Network Sniffing</td>
<td>Adversary-in-the-Middle</td>
<td>Commonly Used Port</td>
<td>Brute Force I/O</td>
<td>Modify Parameter</td>
<td>Denial of Control</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Exploitation of Remote Services</td>
<td>Execution through API</td>
<td>Module Firmware</td>
<td>Indicator Removal on Host Masquerading</td>
<td>Remote System Discovery</td>
<td>Automated Collection</td>
<td>Adversary-in-the-Middle</td>
<td>Brute Force I/O</td>
<td>Module Firmware</td>
<td>Denial of View</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Internet Accessible Device</td>
<td>Hooking</td>
<td>Valid Accounts</td>
<td>Spoof Reporting Message</td>
<td>Wireless Sniffing</td>
<td>Detect Operating Mode</td>
<td>Block Command Message</td>
<td>Brute Force I/O</td>
<td>Unauthorized Command Message</td>
<td>Loss of Control</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Remote Services Replication Through Removable Media</td>
<td>Modify Controller Tasking</td>
<td>Native API</td>
<td>Rootkit</td>
<td>Program Upload</td>
<td>I/O Image</td>
<td>Block Reporting Message</td>
<td>Brute Force I/O</td>
<td>Theft of Operational Information</td>
<td>Loss of Productivity and Revenue</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rogue Master Spearphishing Attachment</td>
<td>Scripting</td>
<td>Scripting</td>
<td>Rootkit</td>
<td>Screen Capture</td>
<td>Monitor Process State</td>
<td>Block Serial COM</td>
<td>Brute Force I/O</td>
<td>Theft of Operational Information</td>
<td>Loss of Protection</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Supply Chain Compromise</td>
<td>User Execution</td>
<td>User Execution</td>
<td>Rootkit</td>
<td>Wireless Sniffing</td>
<td>Point &amp; Tag Identification</td>
<td>Data Destruction</td>
<td>Brute Force I/O</td>
<td>Theft of Operational Information</td>
<td>Loss of Safety</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Transient Cyber Asset Wireless</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Baseline Attack Sequences from Real-World Incidents

Motivation

✓ Historical CPS attacks represented as HAG can serve as ground-truth for adversary modeling

43 Real Incidents from MITRE ICS
Cybersecurity knowledge alignment

- To identify and synthesize credible attack sequences from historical data and MITRE ATT&CK tactics, ICS kill chain, and NIST NSCORE.
  - Bootstrap from attack taxonomies and observed real-world attacks to generate initial base attack sequences

**Attack Tactic → Technique → Attack Pattern → Weakness → Vulnerability → CPS components**

**MITRE ATT&CK Framework → CAPEC → CWE → CVE → CPS components**

**MITRE ATT&CK** (Adversarial Tactics, Techniques, and Common Knowledge):
- Provides contextual understanding of malicious activities and will be used to generalized about attacker behavior

**CAPEC** (Common Attack Pattern Enumeration and Classification):
- List common exploits adversaries use in applications and other cyber-enabled capabilities
- Associated with Common Weakness Enumeration (**CWE**)

**Common Vulnerabilities and Exposures (**CVE**)**
Finding attack actions (ATT&CK techniques and CAPECs) against the given component based on historical incident (i.e., STIX) reports.
Attack Sequence Generation

- High-level attack scenarios or objectives can be obtained from threat-incident reports (e.g., MITRE ATT&CK repositories) and risk scenarios (e.g., EHFS failure scenarios)
- Attack sequences illustrated with target assets/devices of a network
Developing NLP models for automated mapping among attack objectives (e.g., MITRE Tactic/Technique), attack patterns (e.g., CAPEC), and CWE.

The exploitability of a CWE depends on the severity of its existing vulnerabilities.

Exploitability (i.e., success likelihood) of a CWE, $w_j$:

$$p(w_j) = \begin{cases} 0 & V_j = \emptyset \\ 1 - \prod_{v \in V_j} (1 - e(v)) & Otherwise \end{cases}$$
Accomplishment: Cyber Attack Generation (CAGen)

CPS Characterization Using Simulation Environment

Constance High Performance Computing Environment

IEEE 123 Feeder

Control Library

- Baseline control
- Adaptive Resilient Control (e.g., ALRT control)

Closed-loop control simulation

Library of Attack Scenarios

- Setpoint manipulations**
- Generator/Inverter faults
- Loss of load
- Islanding

Attack impact metrics

Frequency perturbation on opening a generator switch

Motivation

✓ Fundamental to understand underlying dynamics of CPS
✓ Validate adversary model and its impact on CPS
✓ Low-fidelity simulations to have an agile methodology
✓ Simulation setup and data generation for initial set of attack scenarios

Adversarial-data generation pipeline for different attack scenarios
CPS Characterization Using NS3

Motivation

✓ Simulate communication layer with different network topologies, protocols, and control parameters
✓ Complements Physical layer
✓ Interplay between physical and communication components is key for a CPS experimentation
✓ Discrete state transition vs. continuous measurements
✓ Develop a community of system modelers developing scenarios

✓ Implemented LTE network, Packet Data Network Gateway (PGW), and topology to represent control center and substations within NS3
✓ User equipment as router
✓ Implemented DNP3 protocol to send power data from devices to control center
✓ Helics integration to send updated/adversary’s measurement from control center to devices.
✓ Man in the middle (MIM) and Dynamic packet rerouting scenario within NS3
Domain-aware Sampling for HAGs

- Given combinatorial explosion of possible attack sequences, there is a need to explore dimensionality reduction and sampling approaches.

- Targeted Scenarios:
  - List top X attack sequences that exploit Y vulnerabilities starting from a set of initial security states $S_{in}$ and ending at security states $S_{out}$.
  - List the vulnerability that has the largest number of potential attack sequences (paths) for a given CPS.

- Identify optimal HAG representation for scalable sampling.

- Extend Graph-theoretic sampling approaches for HAG.
  - Shortest Path length
  - # Shortest Paths
  - Node reachability
**Condition-based Graph**

**Vulnerability-based Graph**

---

**Worst-Case Growth of Attack Graph Representations**

<table>
<thead>
<tr>
<th>Representation</th>
<th>Nodes</th>
<th>Edges</th>
</tr>
</thead>
<tbody>
<tr>
<td>Condition</td>
<td>$hc$</td>
<td>$h^2vc^2$</td>
</tr>
<tr>
<td>Exploit</td>
<td>$h^2v$</td>
<td>$h^3v^2c$</td>
</tr>
<tr>
<td>Vulnerability</td>
<td>$hv$</td>
<td>$h^2v^2c$</td>
</tr>
<tr>
<td>Condition/Exploit</td>
<td>$hc+h^2v$</td>
<td>$2h^2vc$</td>
</tr>
<tr>
<td>Condition/Vulnerability</td>
<td>$hc+hv$</td>
<td>$h^2vc+hvc$</td>
</tr>
</tbody>
</table>

• Domain-aware sampling for CPSs
• Sampling approach to maximize “coverage” of a security policy that exist in the CPS
• Given a CPS and a targeted impact, generate graph-walks that lead to maximum number of weaknesses (or vulnerabilities) in the sampled graph
• Algorithm implanted in python that produce sampled graph with additional metrics
  ▪ Configured to used out-of-box graph metric-based sampling
Attack graph sampling: Sampling Strategies for Hybrid Attack Graphs (HAGs)

**Motivation**
- Given combinatorial explosion of possible attack sequences, there is a need to explore dimensionality reduction and sampling approaches

**Accomplishments**
- Developed prototype for domain-aware intelligent sampling based on “coverage” of weaknesses observed in HAG
- Node-based sampling to create small subgraph with complete coverage of a property required to execute the attack sequence: Weaknesses (CWE)
- Initial and impact states in the attack graph
Impact

• Publications:
  ▪ **Cyber Attack Sequences Generation for Electric Power Grid** A Dutta, S Purohit, A Bhattacharya, O Bel 10th Workshop on Modelling and Simulation of Cyber-Physical Energy Systems (MSCPES 2022)
  ▪ Community outreach
  ▪ Parallel Computing Special Issue: “Scalable Graph Neural Networks: Theory & Practice”
    ✓ Guest Editor: Sumit Purohit

• Containerized software pipelines and standalone tool development:
  ▪ Cyber knowledge extraction, attack sequence generation, and sampling

• DOE College Internship
• Inviting Collaboration
Thank you