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

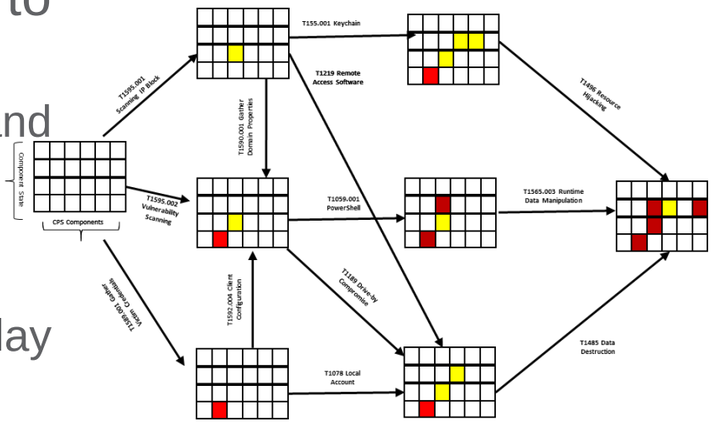
Sumit Purohit, PhD

Sumit.Purohit@pnnl.gov

PNNL is operated by Battelle for the U.S. Department of Energy

Motivation

- 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



Baseline HAG Formulation

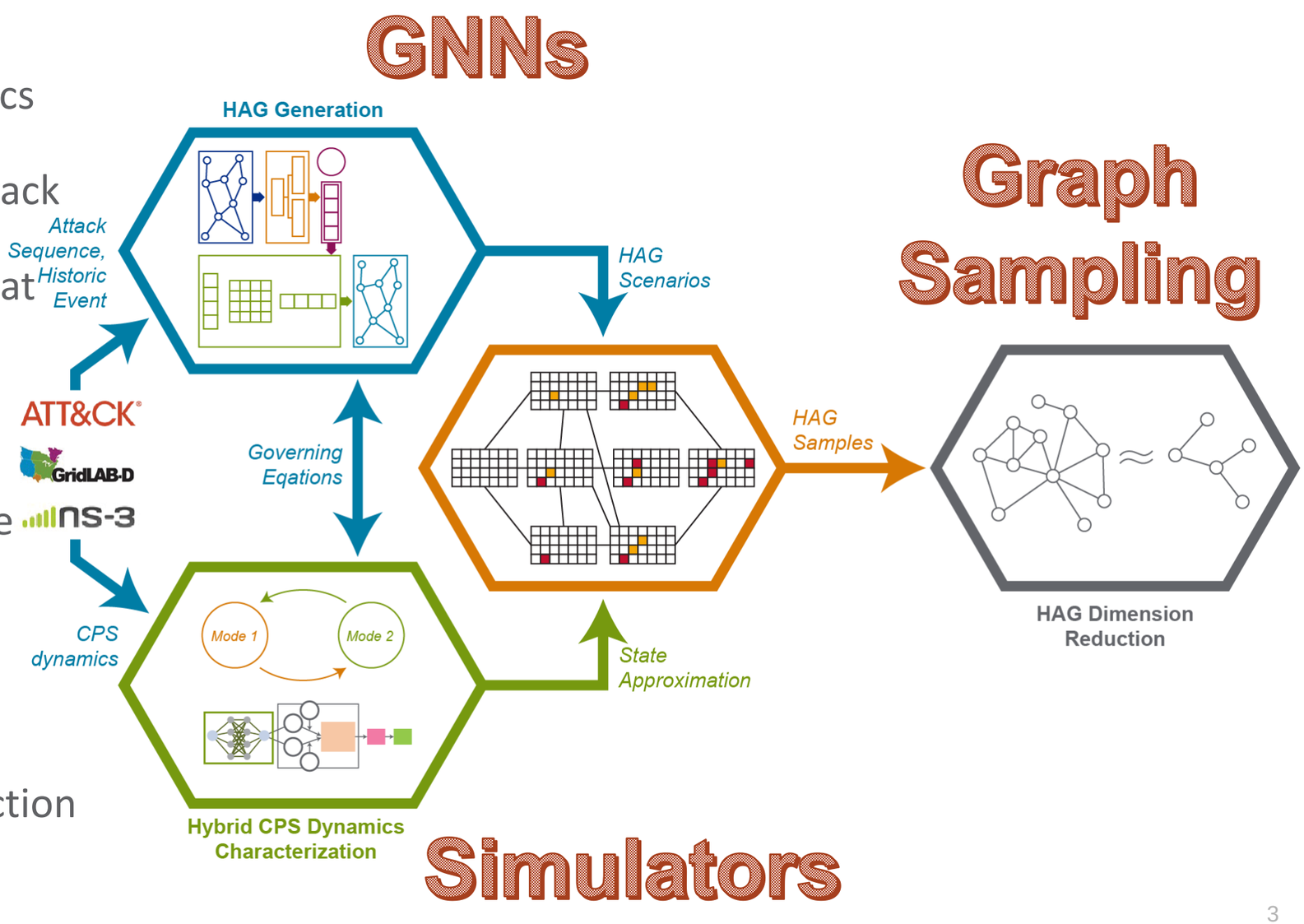
Efficient Hybrid Attack Graph (HAG) Generation

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.

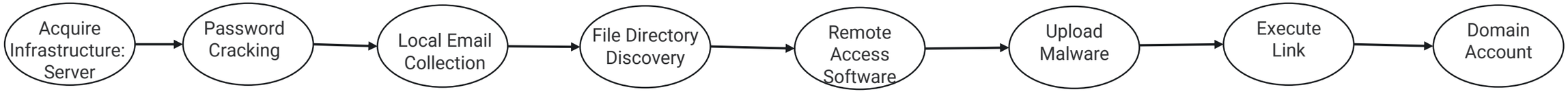
S&T Challenges

- 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?



Cyber Attack Example: Night Dragon (2006)

- 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.

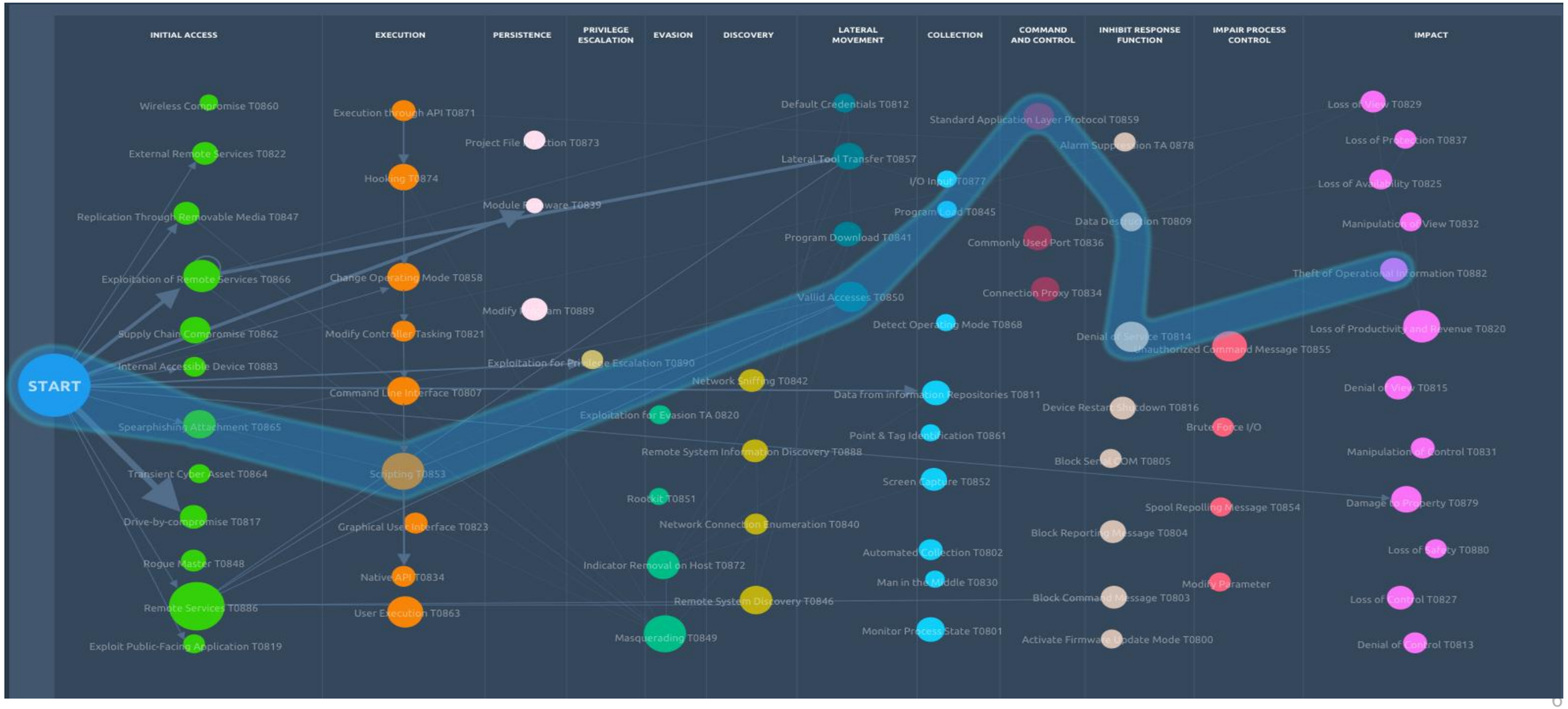
Initial Access	Execution	Persistence	Privilege Escalation	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact
12 techniques	9 techniques	6 techniques	2 techniques	6 techniques	5 techniques	7 techniques	10 techniques	3 techniques	13 techniques	5 techniques	12 techniques
Drive-by Compromise	Change Operating Mode	Hardcoded Credentials	Exploitation for Privilege Escalation	Change Operating Mode	Network Connection Enumeration	Default Credentials	Adversary-in-the-Middle	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Exploit Public-Facing Application	Command-Line Interface	Modify Program	Hooking	Exploitation for Evasion	Network Sniffing	Exploitation of Remote Services	Automated Collection	Connection Proxy	Alarm Suppression	Modify Parameter	Denial of Control
Exploitation of Remote Services	Execution through API	Module Firmware		Indicator Removal on Host	Remote System Discovery	Hardcoded Credentials	Data from Information Repositories	Standard Application Layer Protocol	Block Command Message	Module Firmware	Denial of View
External Remote Services	Graphical User Interface	Project File Infection		Masquerading	Remote System Information Discovery	Lateral Tool Transfer	Detect Operating Mode		Block Reporting Message	Spoof Reporting Message	Loss of Availability
Internet Accessible Device	Hooking	System Firmware		Rootkit	Wireless Sniffing	Program Download	I/O Image		Block Serial COM	Unauthorized Command Message	Loss of Control
Remote Services	Modify Controller Tasking	Valid Accounts		Spoof Reporting Message		Remote Services	Monitor Process State		Data Destruction		Loss of Productivity and Revenue
Replication Through Removable Media	Native API					Valid Accounts	Point & Tag Identification		Denial of Service		Loss of Protection
Rogue Master	Scripting						Program Upload		Device Restart/Shutdown		Loss of Safety
Spearphishing Attachment	User Execution						Screen Capture		Manipulate I/O Image		Loss of View
Supply Chain Compromise							Wireless Sniffing		Modify Alarm Settings		Manipulation of Control
Transient Cyber Asset									Rootkit		Manipulation of View
Wireless									Service Stop		Theft of Operational Information
									System Firmware		

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

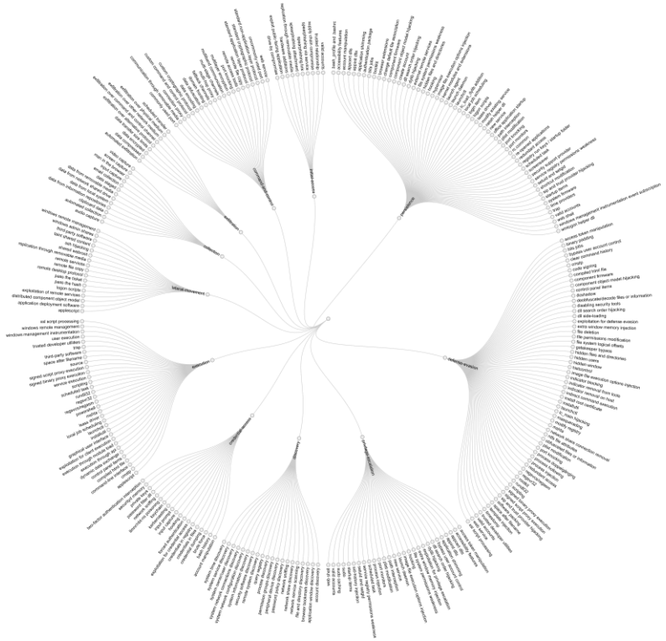
MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge):

- Provides contextual understanding of malicious activities and will be used to generalized about attacker behavior

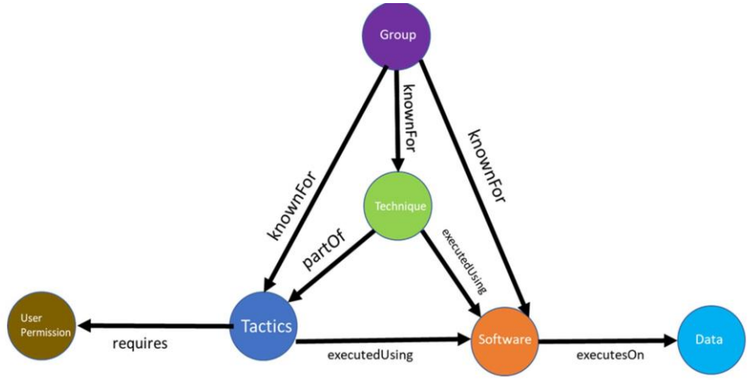
CAPEC (Common Attack Pattern Enumeration and Classification):

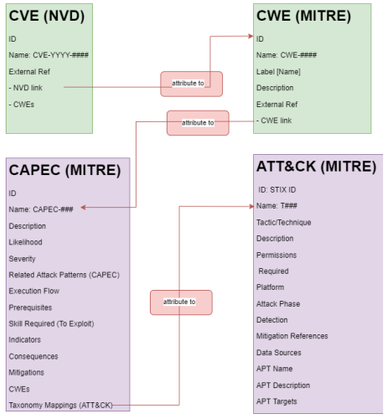
- List common exploits adversaries use in applications and other cyber-enabled capabilities
- Associated with Common Weakness Enumeration (**CWE**)

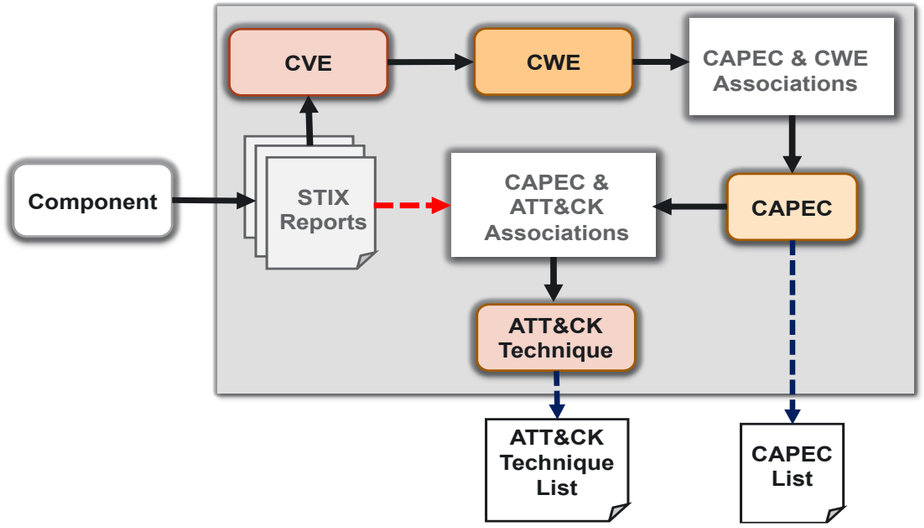
Common Vulnerabilities and Exposures (CVE)

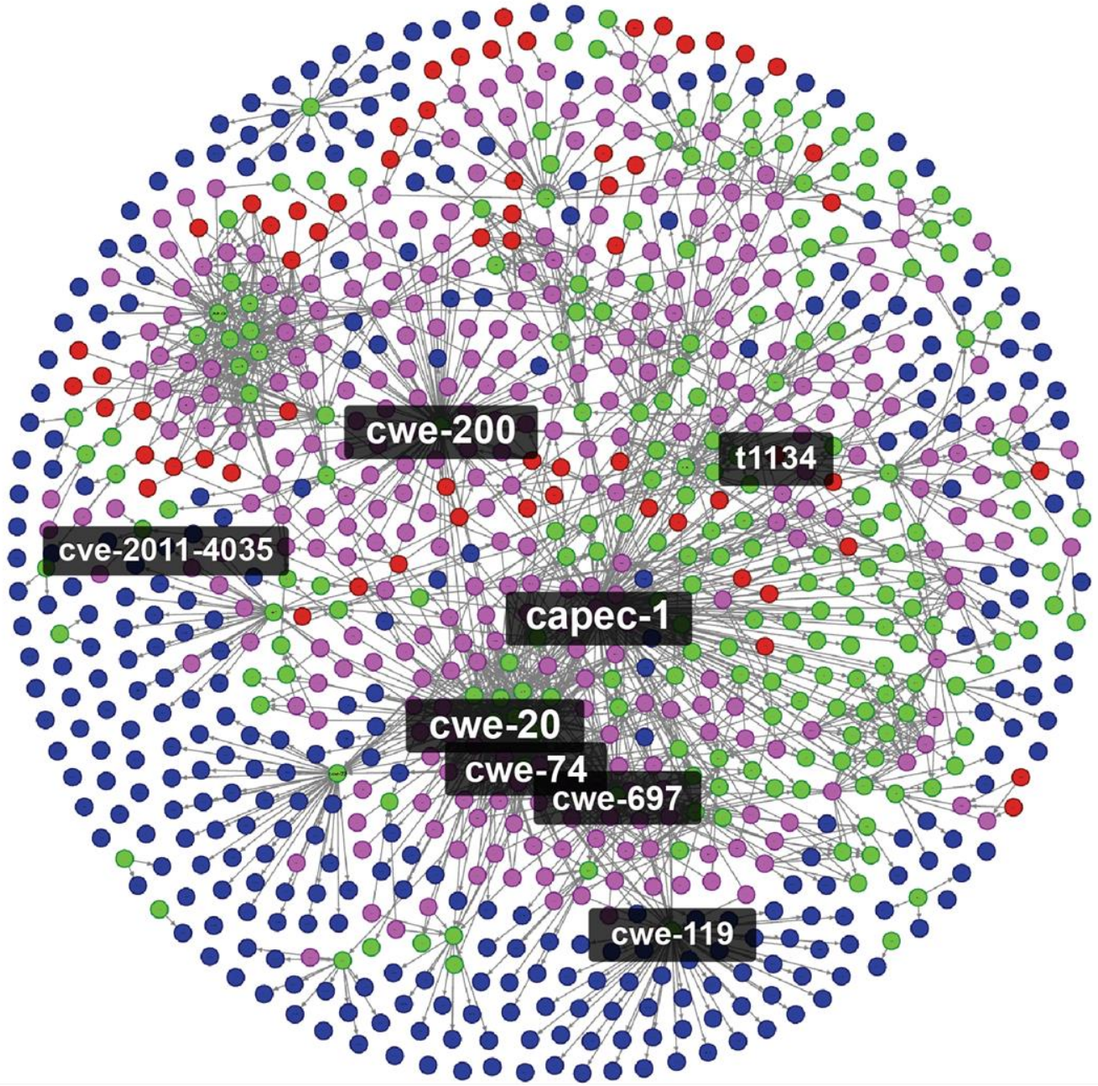


Automated extraction of attack component associations





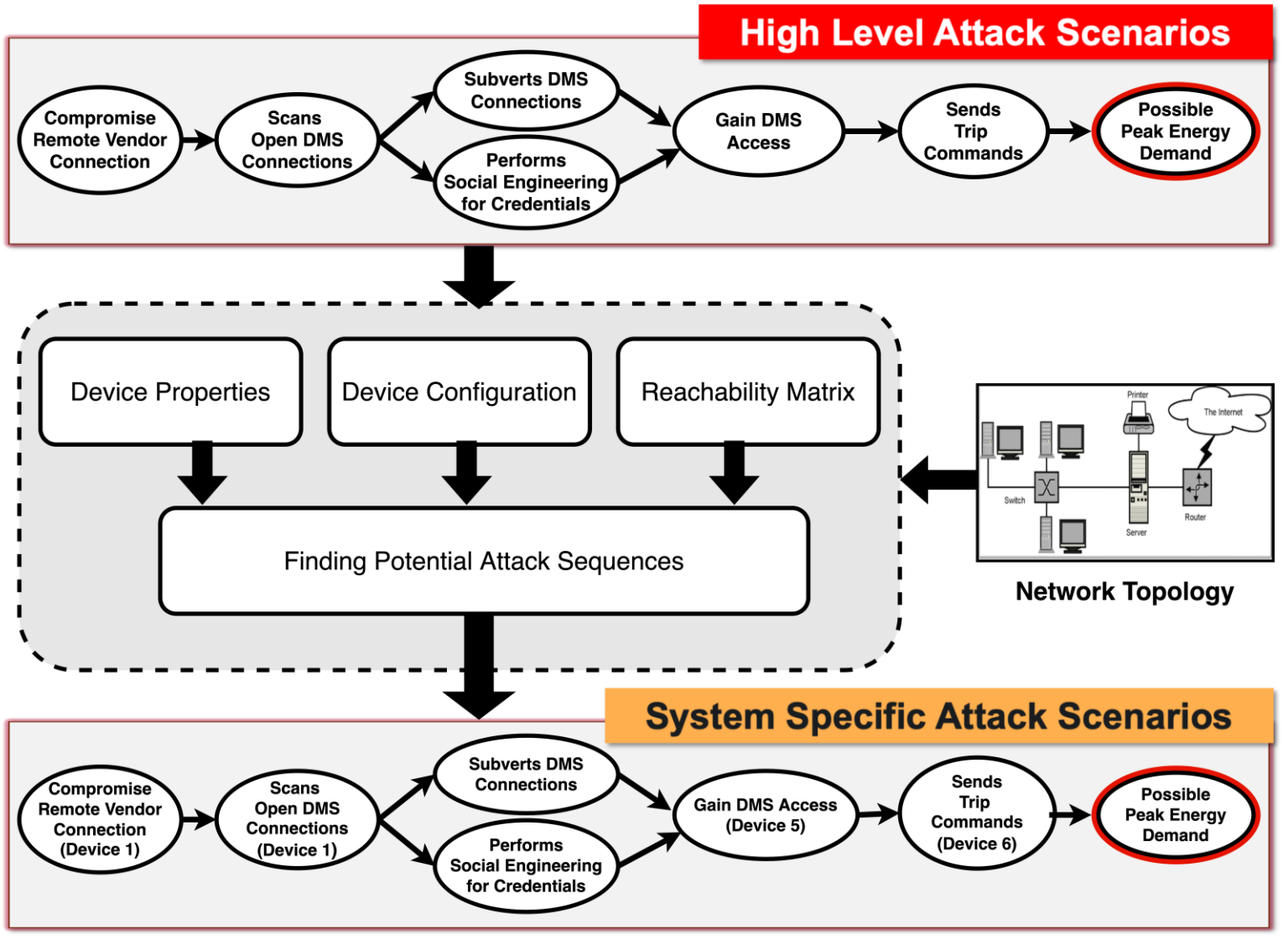




*Finding **attack actions** (ATT&CK techniques and CAPECs) against the **given component** based on historical incident (i.e., STIX) reports*

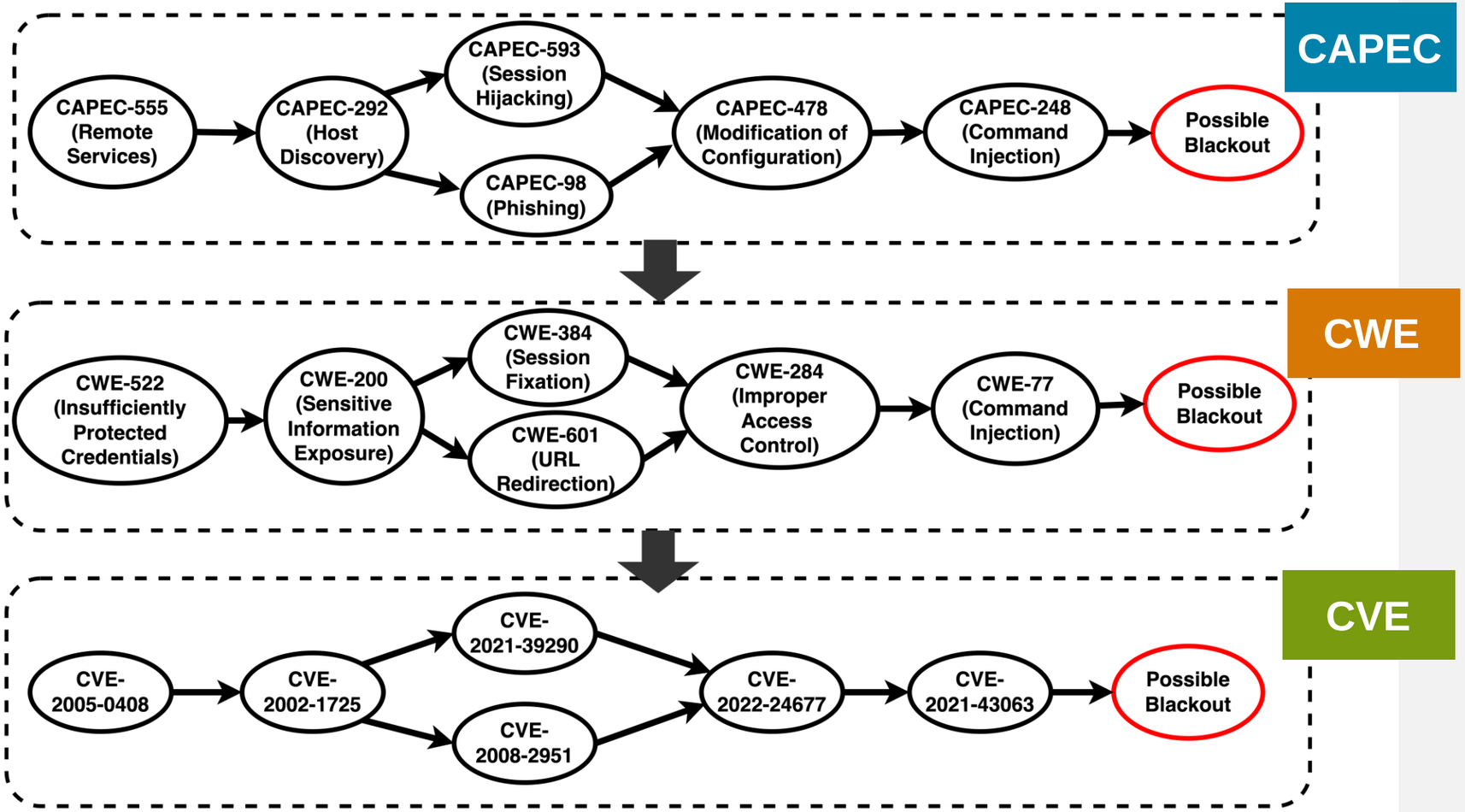
Mapping based on STIX reports on SCADA, sensors, and database

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

Attack Sequence Generation



CAPEC

Developing NLP models for automated mapping among attack objectives (e.g., MITRE Tactic/Technique), attack patterns (e.g., CAPEC), and CWE.

CWE

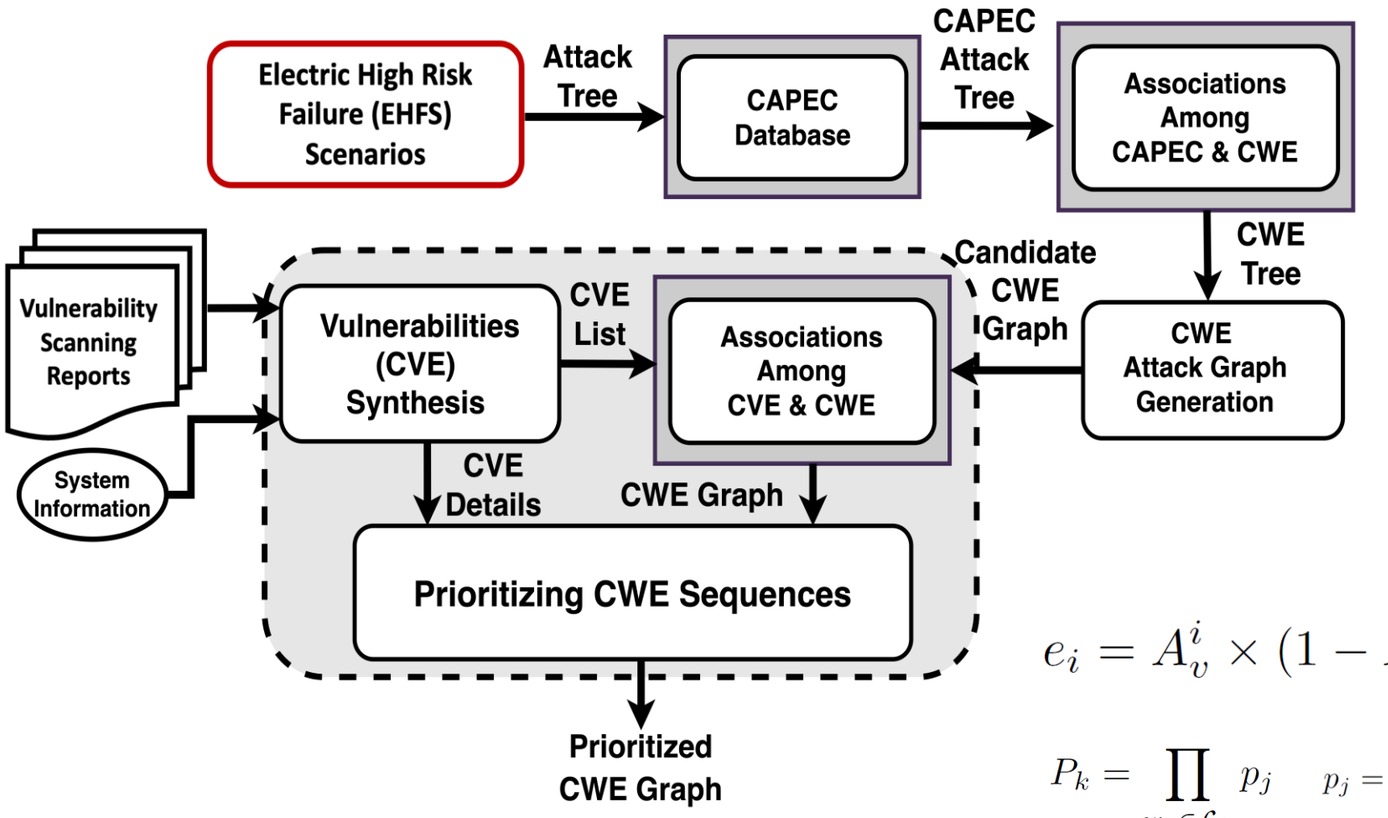
The exploitability of a CWE depends on the severity of its existing vulnerabilities.

CVE

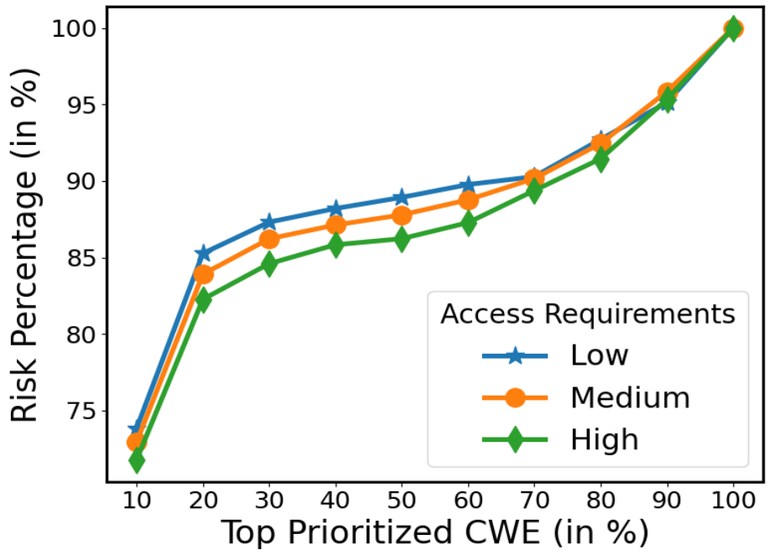
Exploitability (i.e., success likelihood) of a CWE, w_j:

$$p(w_j) = \begin{cases} 0 & V_j = \emptyset \\ 1 - \prod_{v \in V_j}(1 - e(v)) & Otherwise \end{cases}$$

Accomplishment: Cyber Attack Generation (CAGen)



CAGen Architecture



Identifying High Risk CWEs

$$e_i = A_v^i \times (1 - A_c^i) \times (1 - U_i^i)$$

$$P_k = \prod_{w_j \in \mathcal{L}_k} p_j \qquad p_j = \begin{cases} 0, & V_j = \emptyset \\ 1 - \prod_{v_i \in V_j}(1 - e_i), & otherwise \end{cases}$$

$$R_x = \frac{R(W) - R(W - X)}{R(W)}$$

$$R(W) = (1 - \prod_{k \in \mathcal{L}}(1 - P_l)) \times I_m$$

Ashutosh Dutta, Sumit Purohit, Arnab Bhattacharya, Oceane Bel. Cyber Attack Sequences Generation for Electric Power Grid. *10th Workshop on Modelling and Simulation of Cyber-Physical Energy Systems (MSCPES 2022).*

CPS Characterization Using Simulation Environment

Pacific Northwest NATIONAL LABORATORY

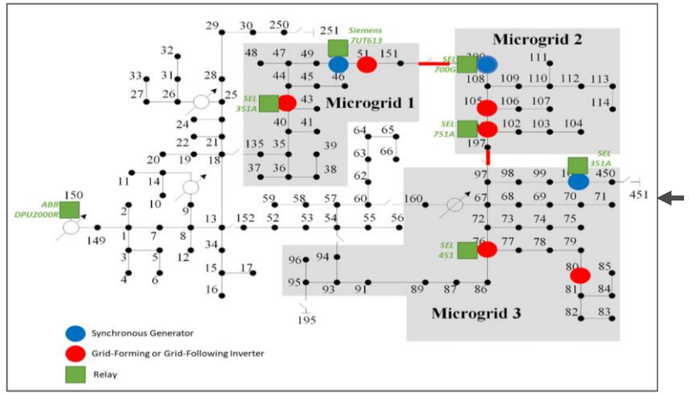
RD2C Data-driven Predictive Understanding Multi-scale Resilient Control

PNNL

Constance High Performance Computing Environment

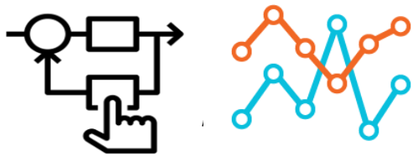
GridLAB-D

IEEE 123 Feeder



Closed-loop control simulation

Control Library



Baseline control

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

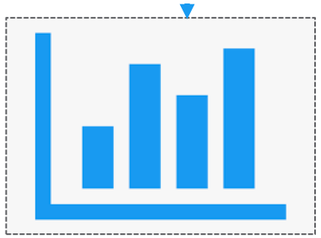
*Setpoint manipulations***

Generator/Inverter faults

Loss of load

Islanding

Library of Attack Scenarios



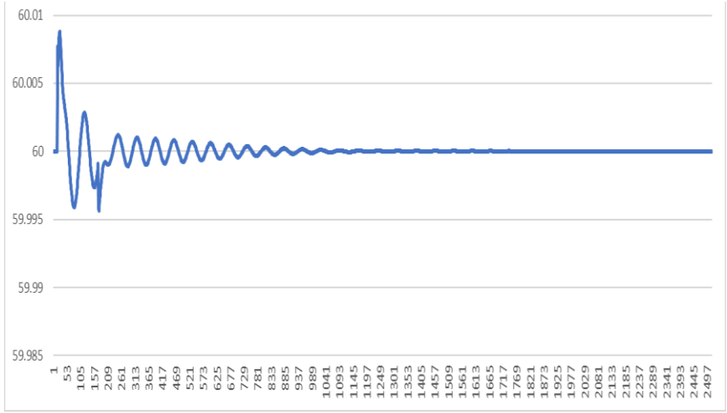
Attack impact metrics)

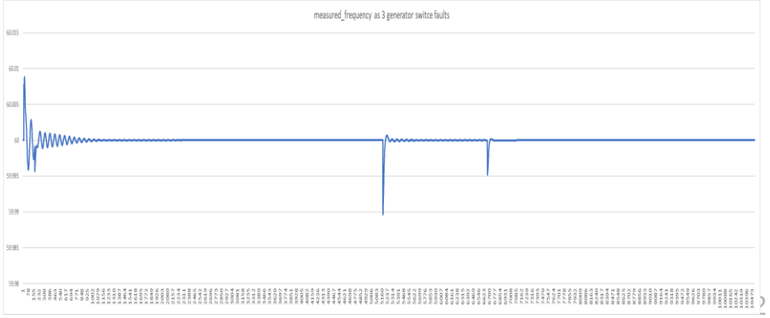
Adversarial-data generation pipeline for different attack scenarios

Motivation

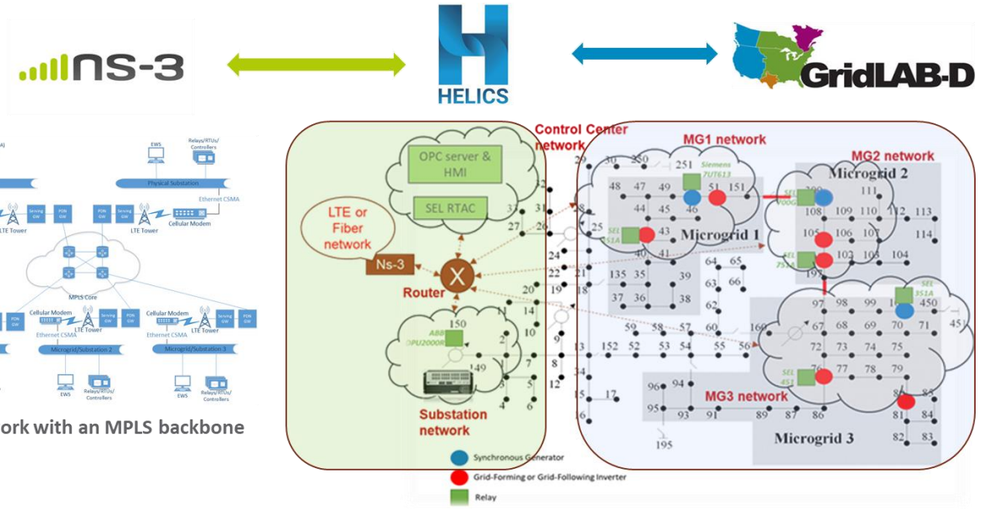
- ✓ Fundamental to understand underlying dynamics of CPS
- ✓ Validate adversary model and its impact on CPS
- ✓ Low-fidelity simulations to have an agile methodology
- ✓ Simulation setup and data generation for initial set of attack scenarios

Frequency perturbation on opening a generator switch



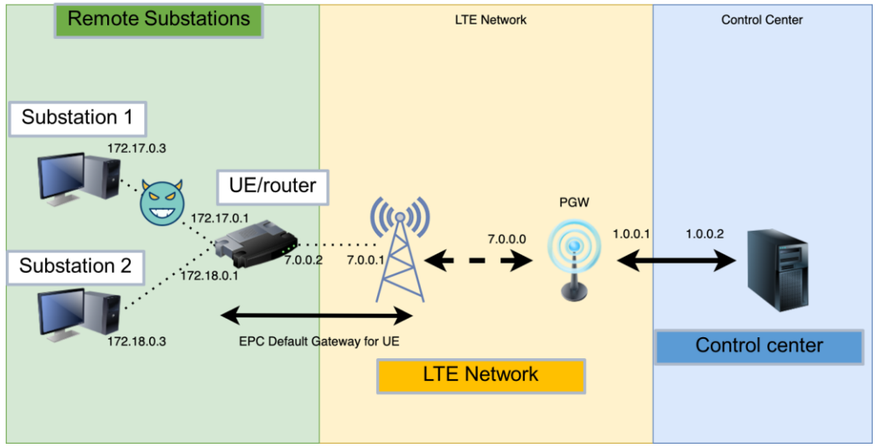


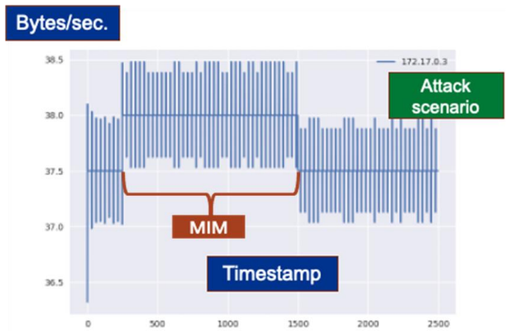
CPS Characterization Using NS3



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



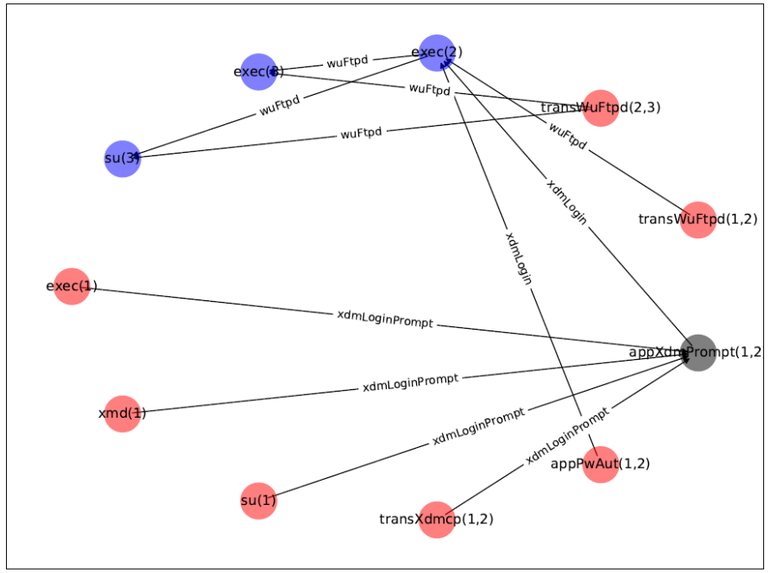


- ✓ Implemented LTE network, Packet Data Network Gateway (PGW), and topology to represent control center and substations within NS3
  - ✓ User equipment as router
- ✓ Implemented DNP3 protocol to send power data from devices to control center
  - ✓ Helics integration to send updated/adversary's measurement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

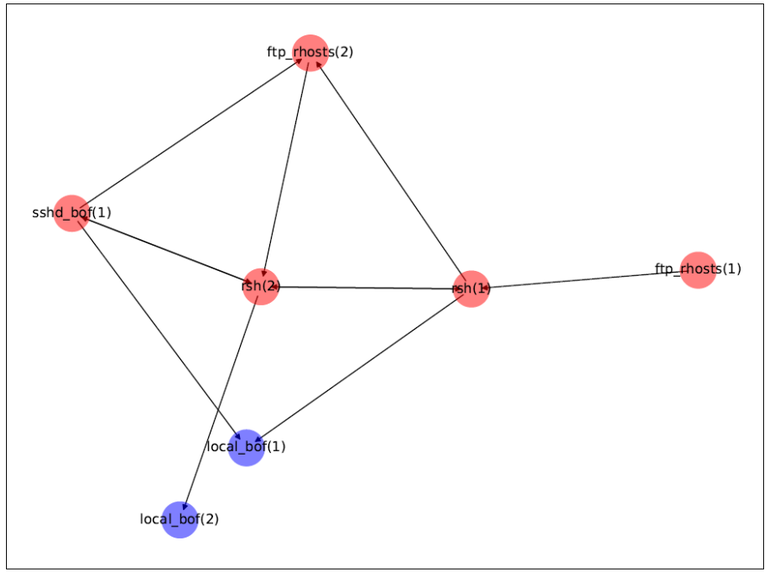
Domain-aware Sampling for HAGs

- 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

HAG representations



Condition-based Graph



Vulnerability-based Graph

WORST-CASE GROWTH OF ATTACK GRAPH REPRESENTATIONS

Representation	Nodes	Edges
Condition	hc	h^2vc^2
Exploit	h^2v	h^3v^2c
Vulnerability	hv	h^2v^2c
Condition/Exploit	$hc+h^2v$	$2h^2vc$
Condition/Vulnerability	$hc+hv$	$h^2vc+hvc$

Ref: Mell, Peter, and Richard Harang. "Minimizing attack graph data structures." The Tenth International Conference on Software Engineering Advances. 2015.

Coverage Driven Sampling

- 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

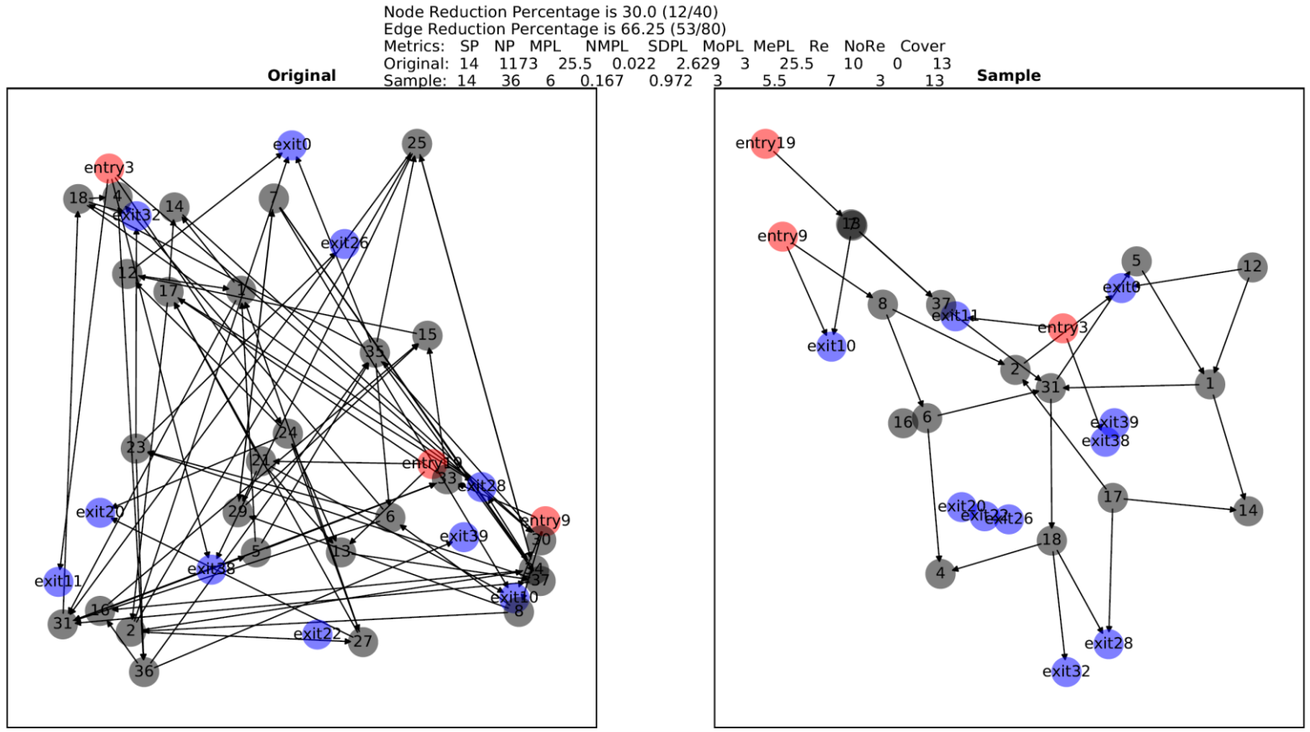
Attack graph sampling: Sampling Strategies for Hybrid Attack Graphs (HAGs)

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)
  - *"Impact-Driven Sampling Strategies for Hybrid Attack Graphs"* International Symposium on Technologies for Homeland Security (IEEE-HST)
  - *"Towards Automatic Mapping of Vulnerabilities to Attack Patterns using Large Language Models"* International Symposium on Technologies for Homeland Security (IEEE-HST)
  - 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