Pacific Northwest
NATIONAL LABORATORY

Fortify Your Defenses: Strategic Budget Allocation to Enhance Power Grid Cybersecurity

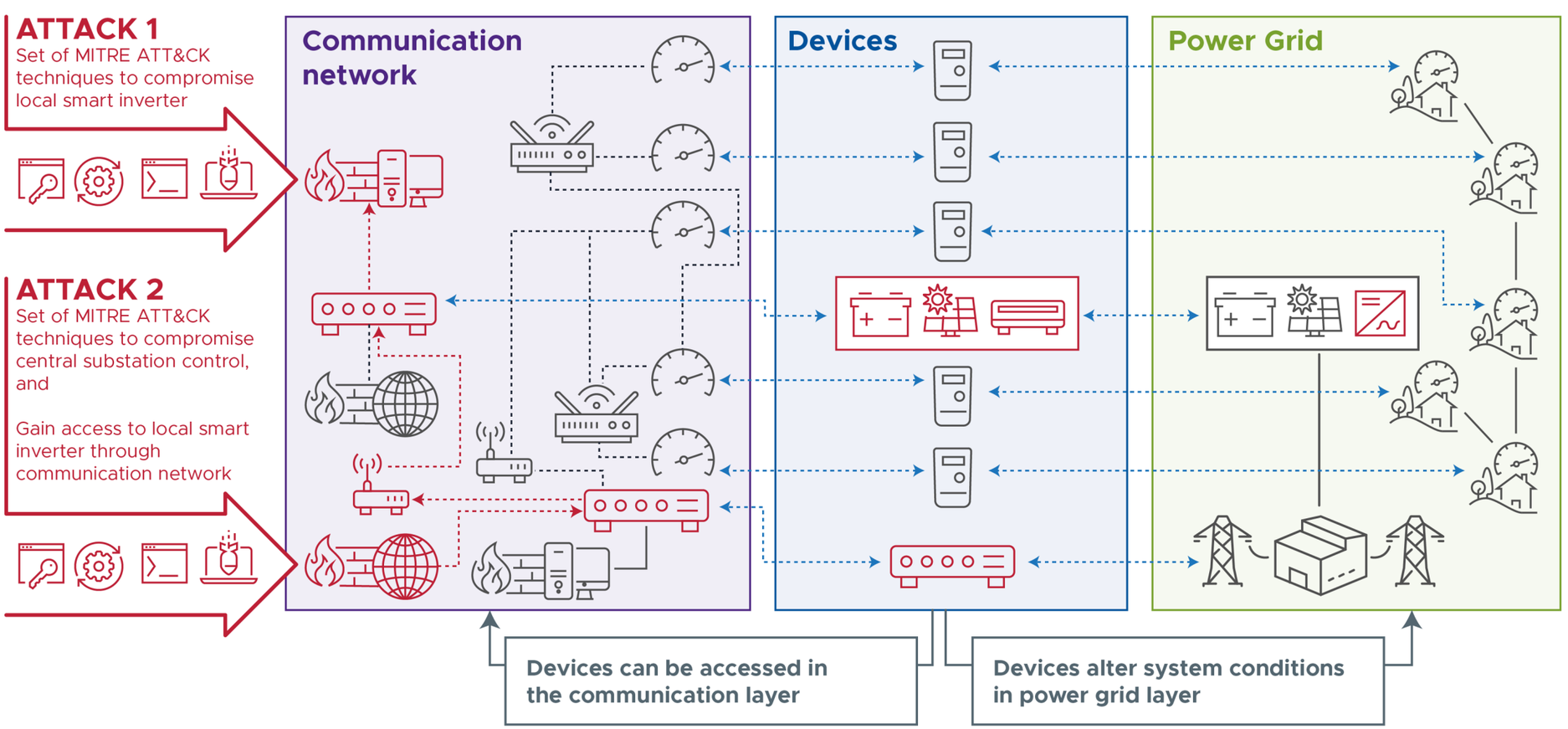
Rounak Meyur
Data Scientist
Data Science and Machine Intelligence

U.S. DEPARTMENT OF ENERGY BATTELLE

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

Motivation

- Developing and implementing patches in a timely manner for individual vulnerabilities is extremely challenging.
- Need a system level solution for long term planning.



MITRE ATT&CK Framework – Tactics, Techniques and Mitigation Measures

- A tactic denotes high level objective of adversary.
- A technique is a method to execute a tactic.
- A mitigation is a remedial measure for a technique.

Analogous example

Tactic
Break into the house

Technique 1
Climb through a window

Technique 2
Break the main door

Mitigation 1
Install a video camera

Mitigation 2
Install door security system

Example from MITRE ATT&CK

Tactic
Command & Control

Technique 1
Use a connection proxy

Technique 2
Use a commonly used port

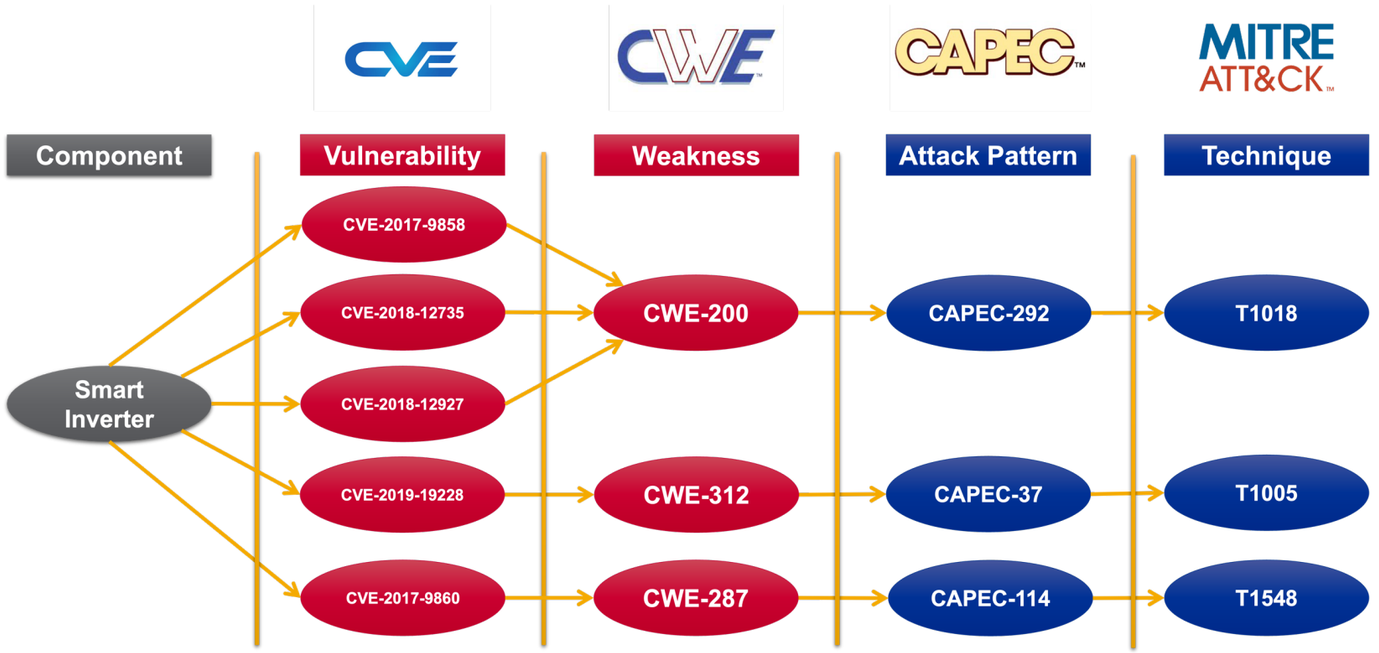
Mitigation 1
Filter network traffic

Mitigation 2
Human user authentication

Cybersecurity Knowledge Graph

List of database:

- Common Vulnerability Enumeration (CVE)
- Common Weakness Enumeration (CWE)
- Common Attack Pattern Enumeration & Classification (CAPEC)
- MITRE Adversarial Tactics, Techniques & Common Knowledge (ATT&CK)

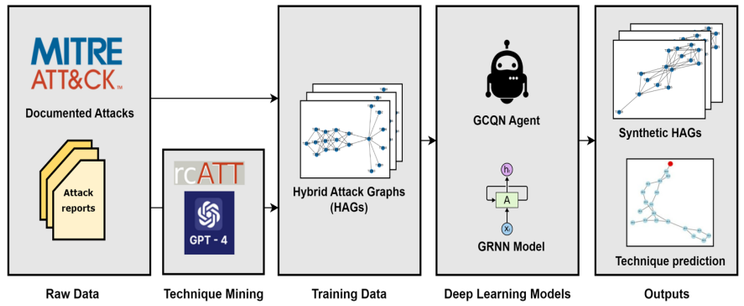


Problem: What are the adversary techniques which can be performed on a component?

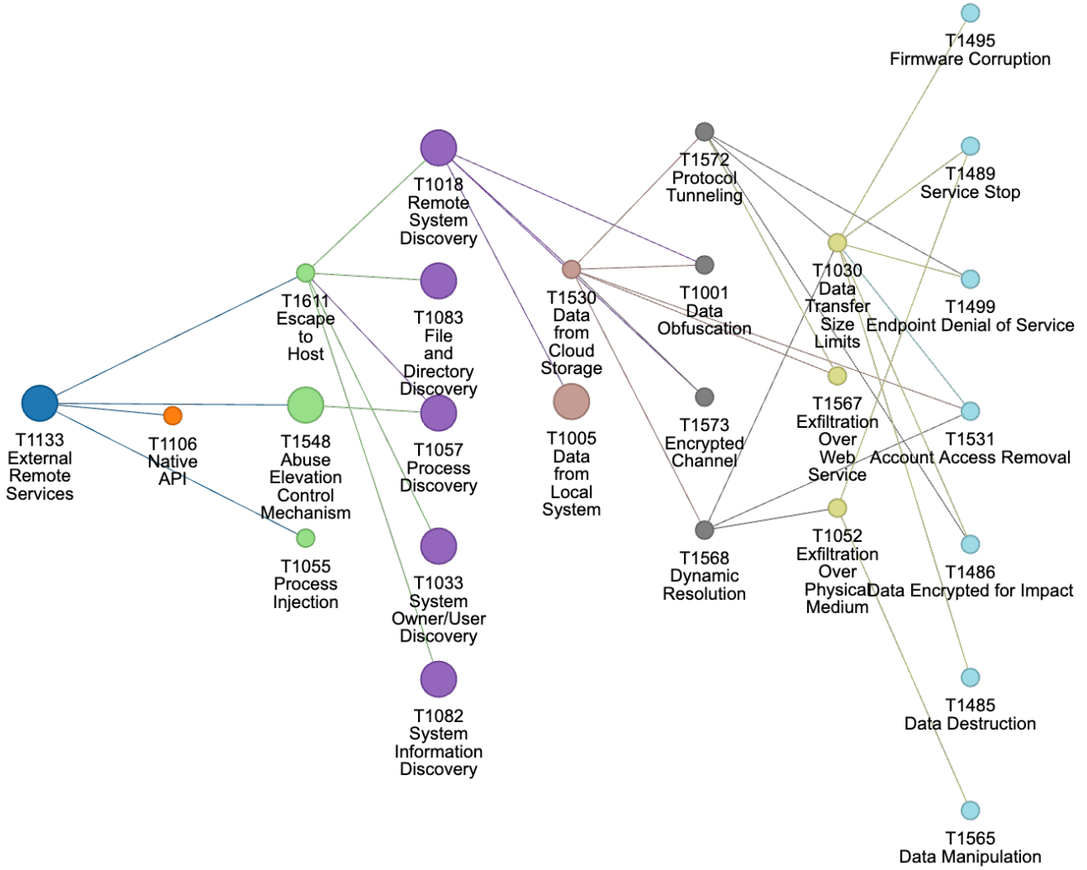
We can use the different database and mappings between them to get a list of probable techniques.

Hybrid Attack Graphs (HAGs)

- **Problem**: What are the attack sequences that can be performed with a given set of techniques?
- **HAG**s are synthetic attack graphs mimicking actual cyber attacks.
- Two sub-problems to generate HAGs:
  - How do we generate the library of sequences given raw data from MITRE ATT&CK Campaigns?
  - Can we guide these sequences to contain a desired attributes?



HAG Generation pipeline



Hybrid Attack Graph for “smart inverter”

S. Donald, R. Meyur, and S. Purohit, “Hybrid Attack Graph Generation with Graph Convolutional Deep-Q Learning,” in IEEE Big Data Conference, The 7th Workshop on Graph Techniques for Adversarial Activity Analytics (GTA³2023), Sorrento, Italy, 2023.

Attack Sequences in HAGs

- Attack sequence consists of a sequence of techniques $\mathfrak{a} := \{t_1, t_2, \ldots t_n\}$.

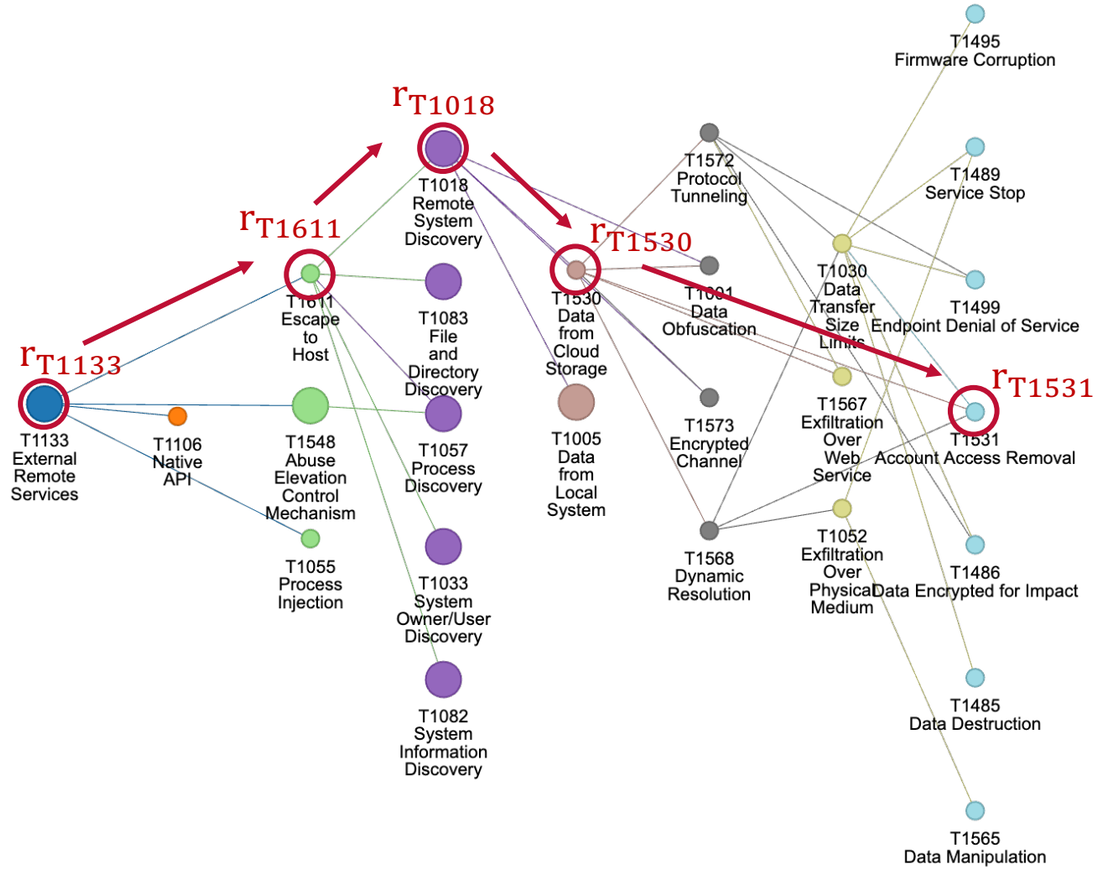
- Success rate of an attack sequence
  - Success rate r_t of a technique t is probability of its successful execution.
  - If success rate of each technique is known, we can compute success rate of attack sequence $\mathfrak{a}$ is

$$\mathbb{Pr}(\mathfrak{a}) = \prod_{t_i \in \mathfrak{a}} r_{t_i}$$

- **Define:** an attack sequence $\mathfrak{a}$ is "highly likely" if

$$\mathbb{Pr}(\mathfrak{a}) \geq \delta$$

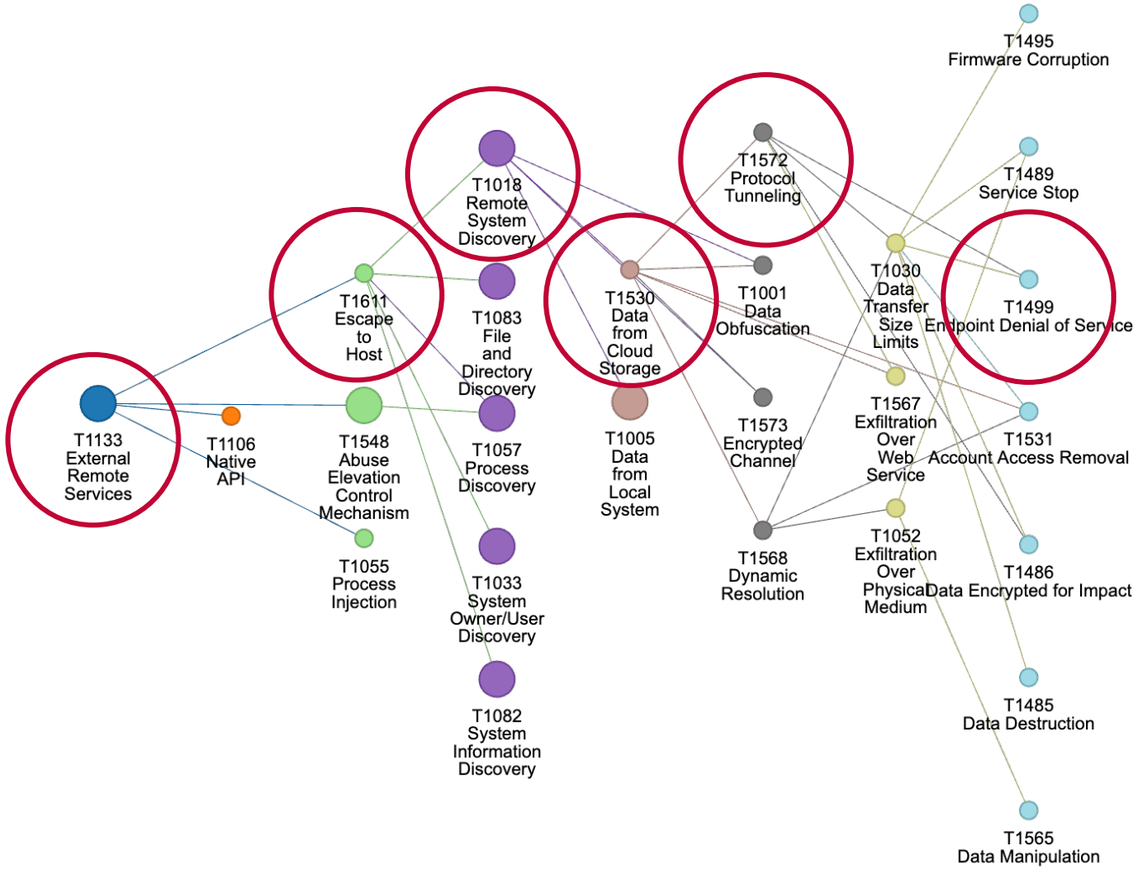
Defender goal: plan mitigation measures to minimize number of highly likely attack sequences.

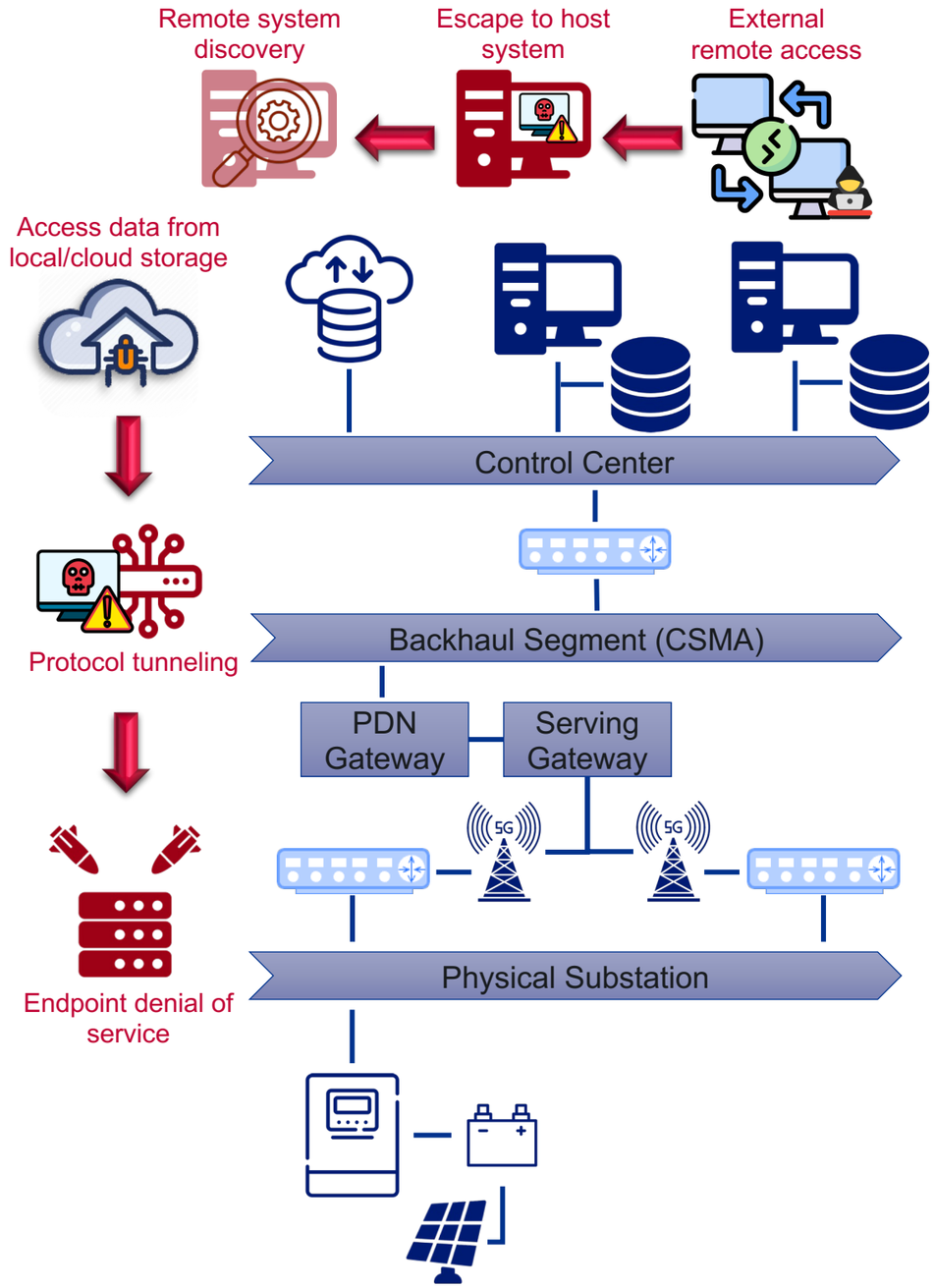


Hybrid Attack Graph for "smart inverter"

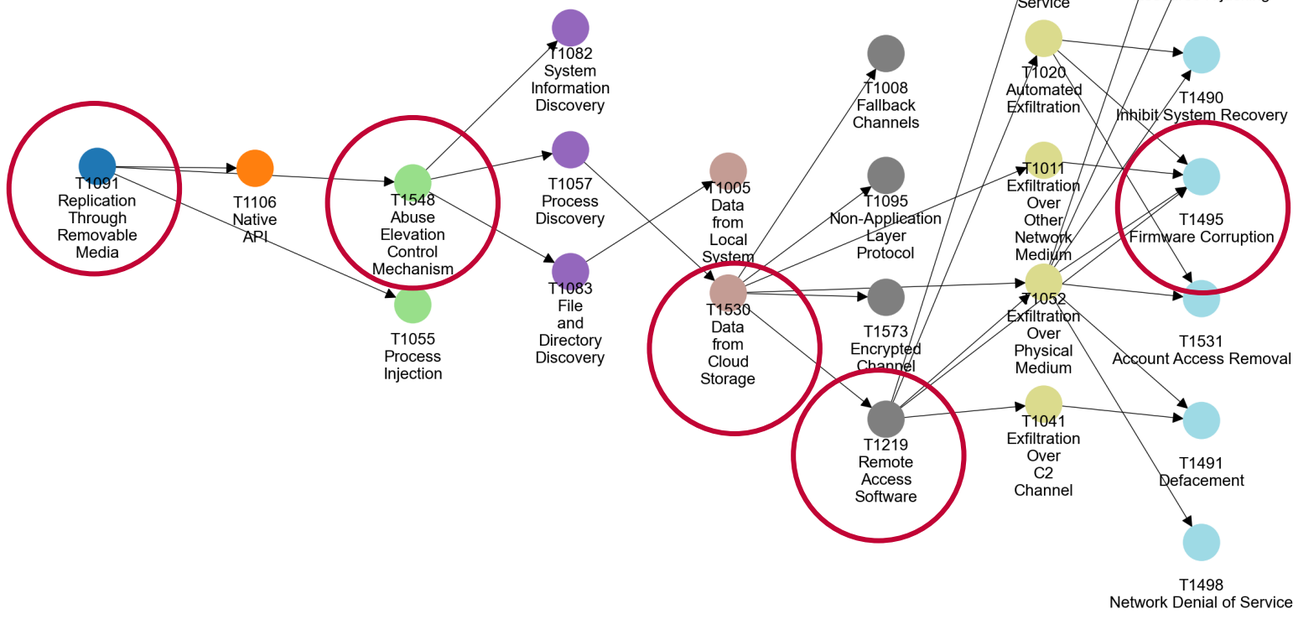
R. Meyur, S. Purohit, and B. K. Webb, "Fortify Your Defenses: Strategic Budget Allocation to Enhance Power Grid Cybersecurity," in The AAAI-24 Workshop on Artificial Intelligence for Cyber Security (AICS), (submitted and under review), Vancouver, Canada, 2024.

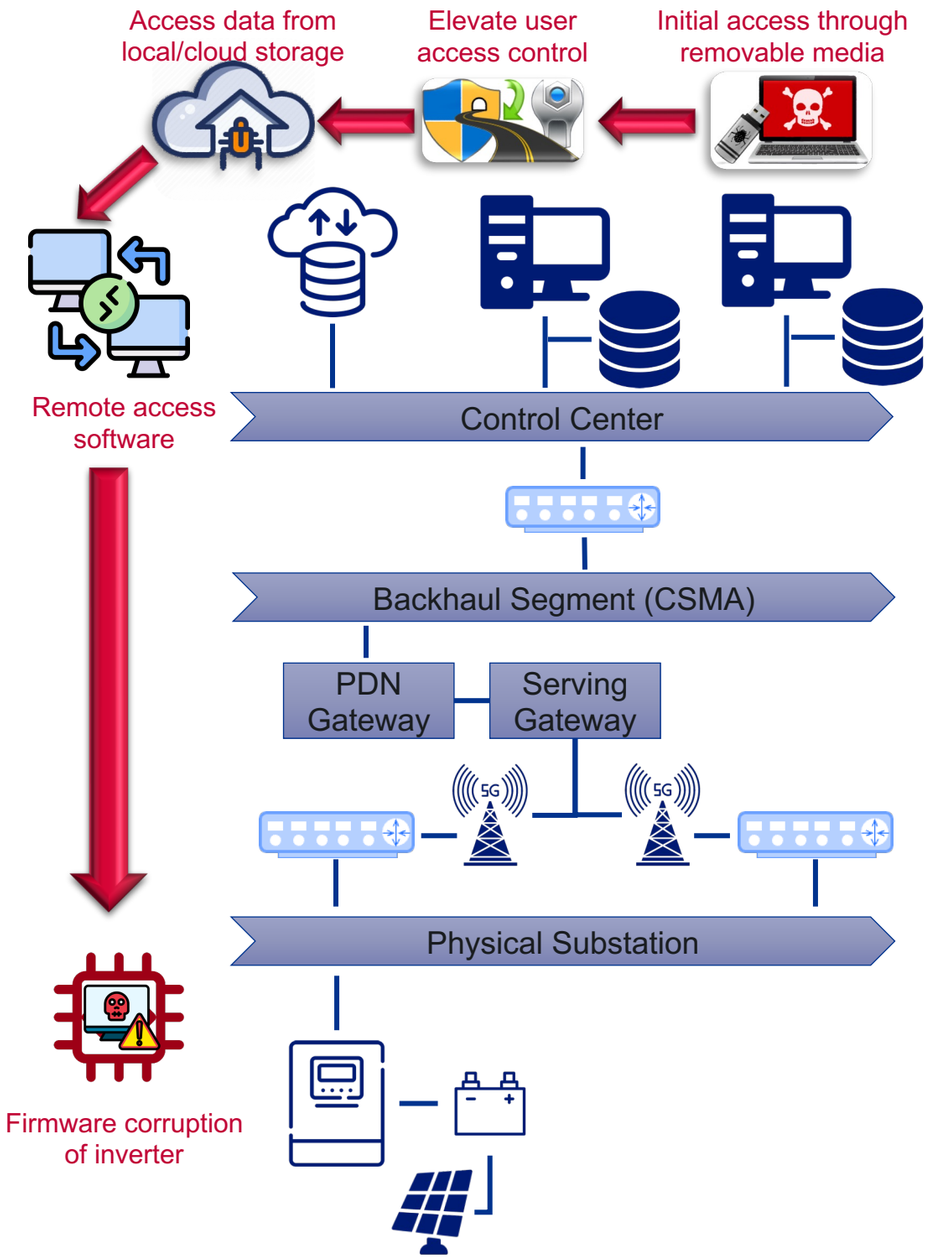
Pacific Northwest
NATIONAL LABORATORY





Pacific Northwest
NATIONAL LABORATORY





Success rate of MITRE ATT&CK Techniques

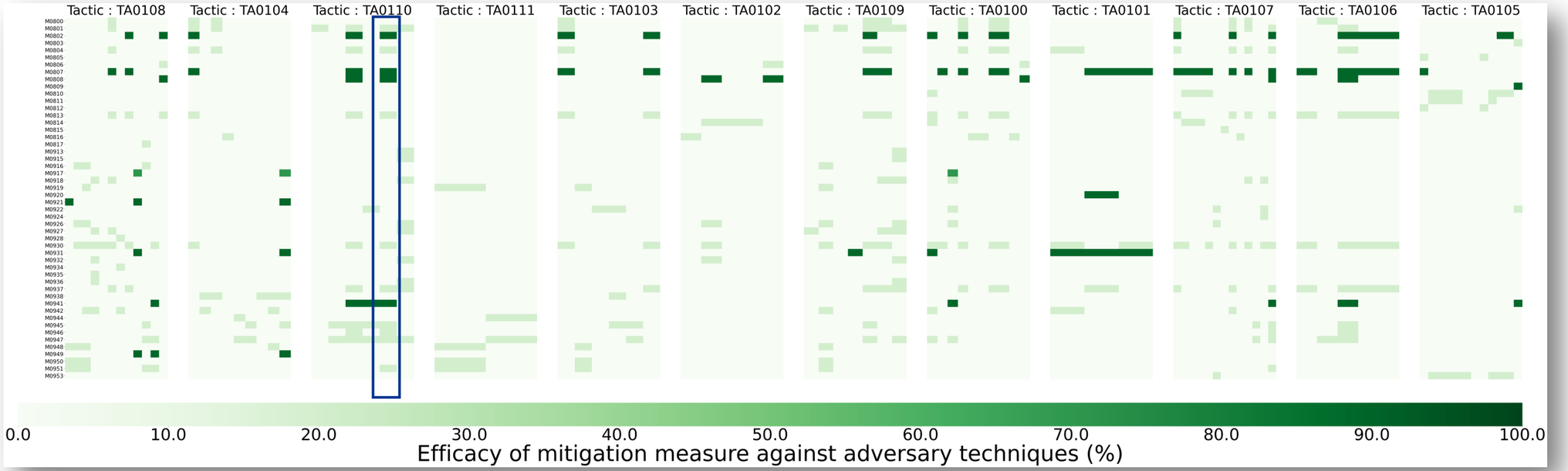
Problem: How can we compute the success rate of each node (technique) in a HAG?

- We use MITRE ATT&CK mitigation to technique relation matrix.
- Rows are mitigations, columns are techniques.
- Matrix entry η_{ij} : efficacy of mitigation i against technique j

- What is success rate of a technique?
  Probability that a technique is not prevented by any mitigation.

- r_j : success rate of technique j

$$r_j = \prod_i (1 - \eta_{ij})$$



R. Meyur, S. Purohit, and B. K. Webb, "Fortify Your Defenses: Strategic Budget Allocation to Enhance Power Grid Cybersecurity," in The AAAI-24 Workshop on Artificial Intelligence for Cyber Security (AICS), (submitted and under review), Vancouver, Canada, 2024.

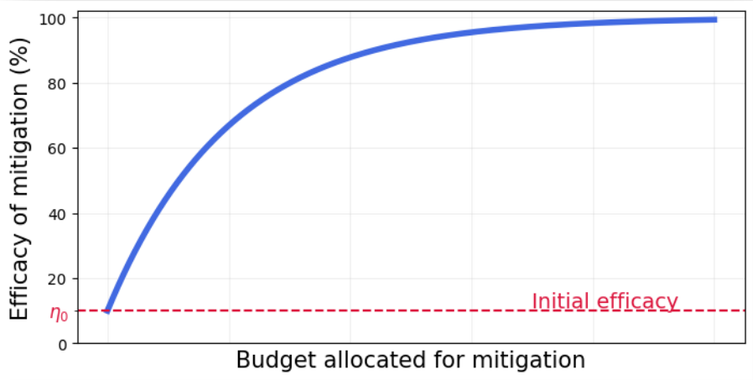
Budget Allocation to improve Mitigation Efficacy

Problems:

- How to evaluate efficacy η_{ij} of a mitigation measure?
- How to estimate cost of a mitigation measure?

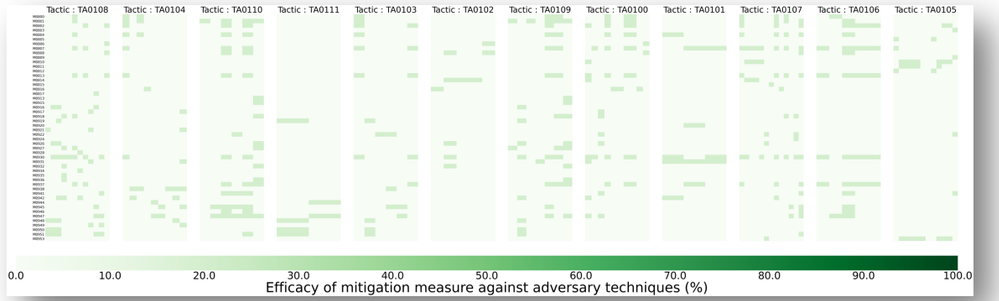
Approach:

- Divide the total budget into different predefined sectors.
- Each sector has a pre-defined set of mitigation measures.
- Budget allocated to a sector improves efficacy of mitigation measures in that sector.

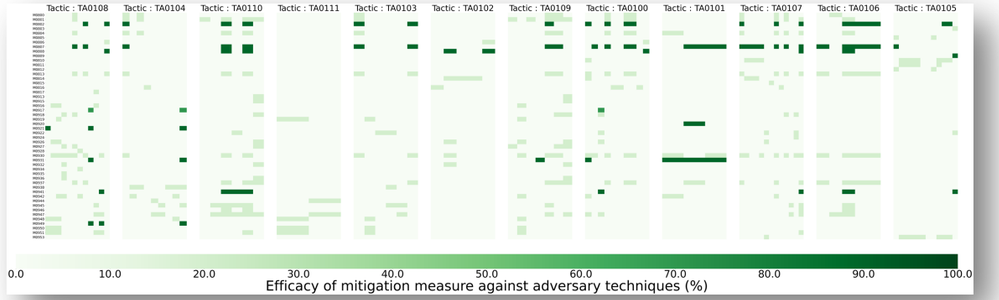


$$\eta_i = 1 - (1 - \eta_0)e^{-\lambda f_i}$$

- η_i: improved efficacy
- f_i: budget allocated
- η_0: initial efficacy
- λ: defender skill level



Entire budget is allocated to “Defense” sector



R. Meyur, S. Purohit, and B. K. Webb, “Fortify Your Defenses: Strategic Budget Allocation to Enhance Power Grid Cybersecurity,” in The AAAI-24 Workshop on Artificial Intelligence for Cyber Security (AICS), (submitted and under review), Vancouver, Canada, 2024.

Optimal Budget Allocation Problem

Goal of the problem:

- divide a limited cybersecurity budget into different pre-defined sectors
- to improve efficacy of mitigation measures
- so that we minimize number of highly likely attack sequences.

Formulate a mixed integer linear problem (MILP)

$$\min \quad \sum_{a \in \mathcal{S}} \mathbb{I}\left[l_a \geq \log(\delta)\right]$$

$$over \quad \{x_i\}_{i=1}^{N_m} \in \{0,1\}, \ \{b_j\}_{j=1}^{N_b} \in [0,1], \ \{f_i\}_{i=1}^{N_m} \in [0,1]$$

$$s.t. \quad l_a = \sum_{t \in a} \sum_{i=1}^{N_m} x_i M_{ik} \left[\log\left(1 - \eta_{i,0}\right) - \lambda f_i\right], \quad \forall a \in \mathcal{S}$$

$$\sum_{j=1}^{N_b} b_j = 1; \qquad f_i = \sum_{j=1}^{N_b} a_{ij} b_j, \quad \forall i = 1, 2, \cdots, N_m$$

Number of highly likely sequences

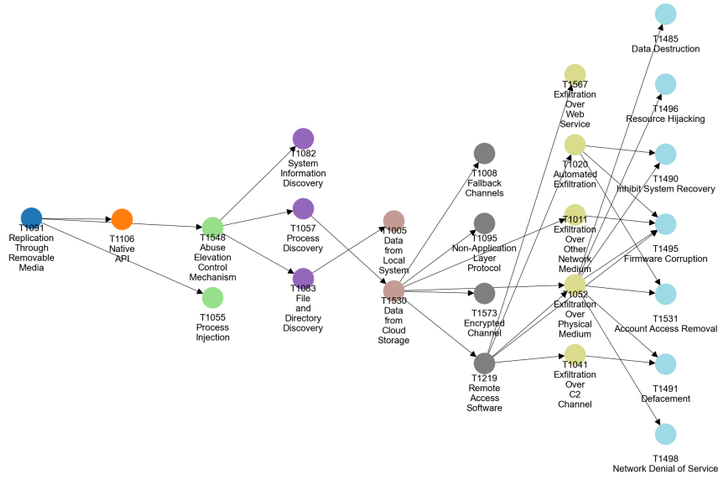
log likelihood of success rate of attack sequence a

Sum of all budget partitions

Fraction of budget allocated to mitigation i

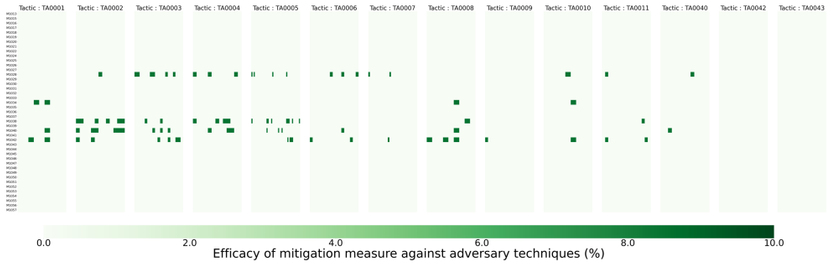
R. Meyur, S. Purohit, and B. K. Webb, "Fortify Your Defenses: Strategic Budget Allocation to Enhance Power Grid Cybersecurity," in The AAAI-24 Workshop on Artificial Intelligence for Cyber Security (AICS), (submitted and under review), Vancouver, Canada, 2024.

Optimal Budget Allocation for a HAG

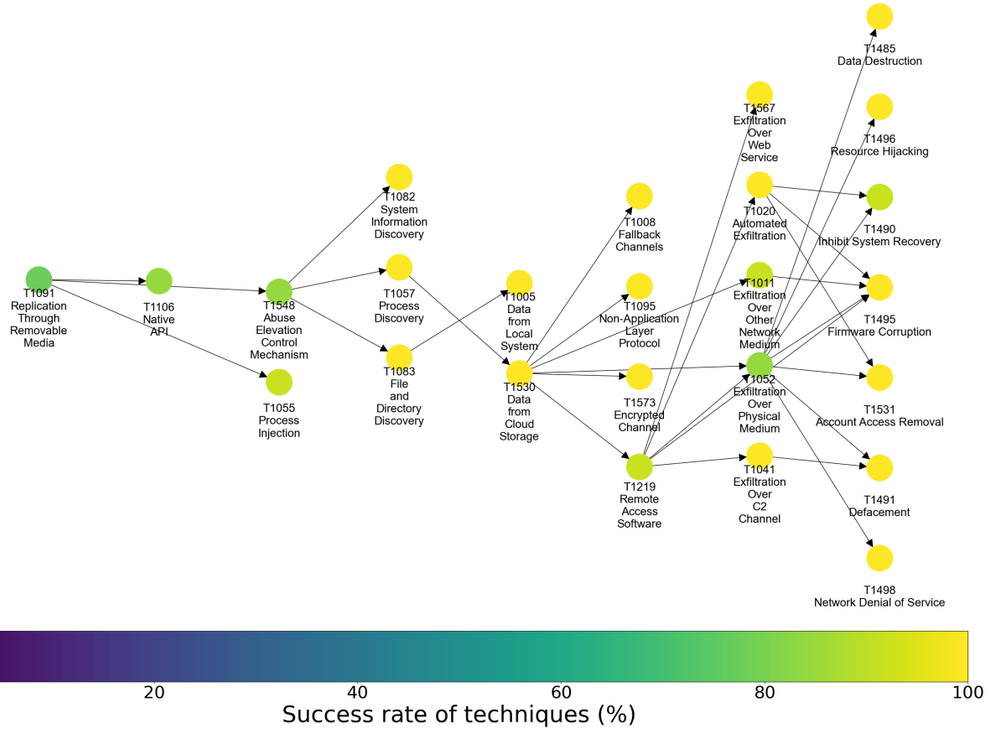


Worst case assumptions:

- no mitigation measures, which implies
- 100% success rate of all techniques.



Optimal mitigation profile



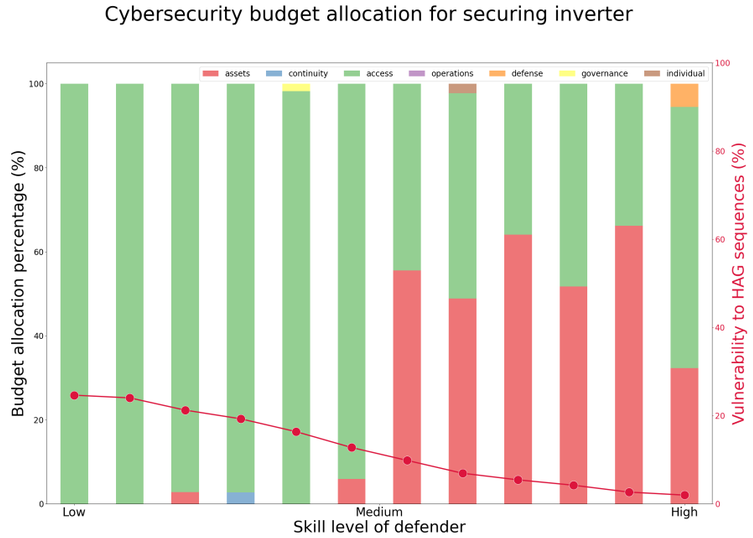
The optimization problem essentially does the following:

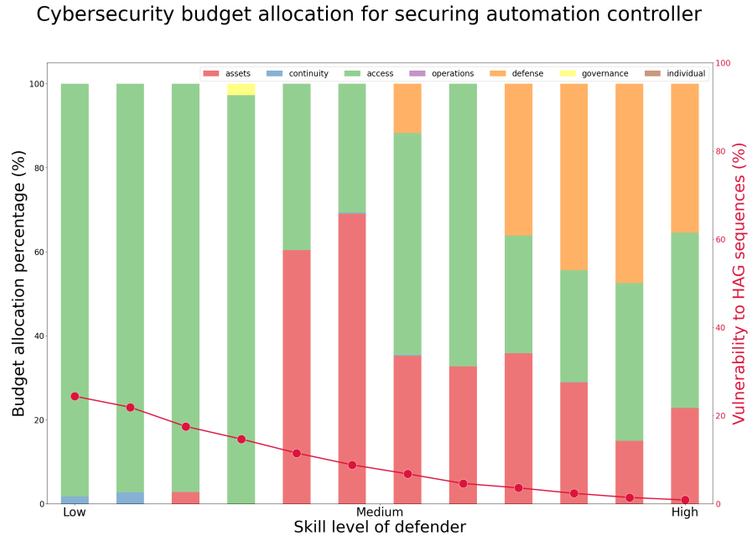
- finds the influential techniques in the HAG, and
- identifies best mitigations to prevent these techniques.

R. Meyur, S. Purohit, and B. K. Webb, "Fortify Your Defenses: Strategic Budget Allocation to Enhance Power Grid Cybersecurity," in The AAAI-24 Workshop on Artificial Intelligence for Cyber Security (AICS), (submitted and under review), Vancouver, Canada, 2024.

Implementing Optimal Budget Allocation

- Implementation
  - HAGs for “smart inverter” and “substation automation controller” are created.
  - Budget partitions for different defender skill level plotted in bar graph.





- Concluding remarks
  - The framework can be used to recommend how to allocate staff budget in an organization to minimize cyber vulnerabilities.
  - An organization can make long term planning to identify budget sectors to focus on in the future years.

R. Meyur, S. Purohit, and B. K. Webb, “Fortify Your Defenses: Strategic Budget Allocation to Enhance Power Grid Cybersecurity,” in The AAAI-24 Workshop on Artificial Intelligence for Cyber Security (AICS), (submitted and under review), Vancouver, Canada, 2024.

Future Work

- Future works
  - Include software/hardware tools budget along with staff budget and improve on the expression for efficacy improvement.

$$\eta_i = 1 - (1 - \eta_0)e^{-\lambda f_i}$$

  - Generate HAGs covering an entire cyber-physical system.

- Acknowledgments

  - The research is part of the Resilience Through Data Driven Intelligently Designed Control (RD2C) Initiative, which is conducted under the Laboratory Directed Research and Development (LDRD) Program.
  - Thanks to the team members
    - Sumit Purohit
    - Braden K. Webb
    - Sam Donald

R. Meyur, S. Purohit, and B. K. Webb, "Fortify Your Defenses: Strategic Budget Allocation to Enhance Power Grid Cybersecurity," in The AAAI-24 Workshop on Artificial Intelligence for Cyber Security (AICS), (submitted and under review), Vancouver, Canada, 2024.

Pacific Northwest
NATIONAL LABORATORY

Thank you