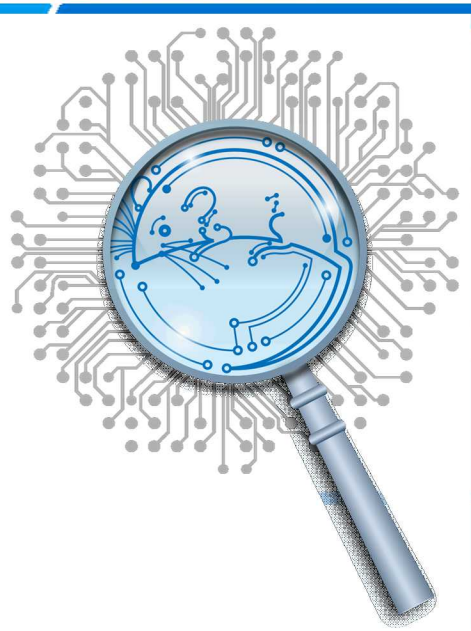
SAND2020-1859C

LDRD
Laboratory Directed Research and Development



Rigorous Cyber Experimentation Security of Cyber Physical Systems

Ali Pinar (apinar@sandia.gov)

Sandia National Laboratories

Livermore, CA

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia LLC, a wholly owned subsidiary of Honeywell International Inc. for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

What is the return on investment for cyber security?

Credit: Staff Sergeant Jason Gamble, United States Air Force

evidence

Without ~~data~~,
you are just another person with an opinion.

W. Edwards Deming

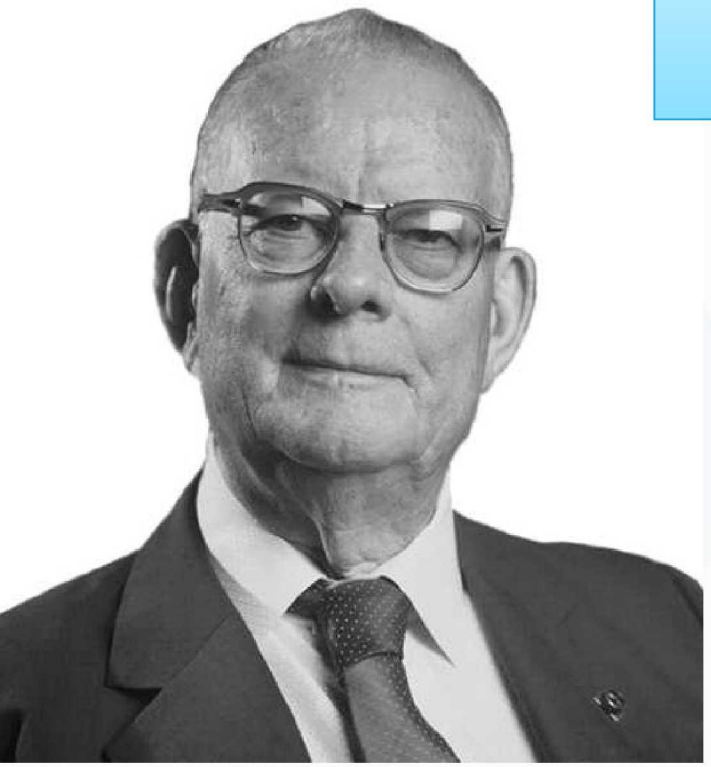


Image Source: census.gov

Bringing Rigor into Cyber Experimentation: The Plan in a Nutshell

SECURE: Science and Engineering of Cyber security through Uncertainty quantification and Rigorous Experimentation

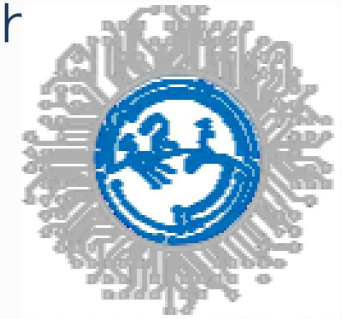
The Goal: Bring rigor into cyber experimentation

The Idea: Follow the principles of Computational Science and Engineering (CSE)

The Challenge: Cyber systems are different than those in traditional CSE applications.

The Three Thrusts:

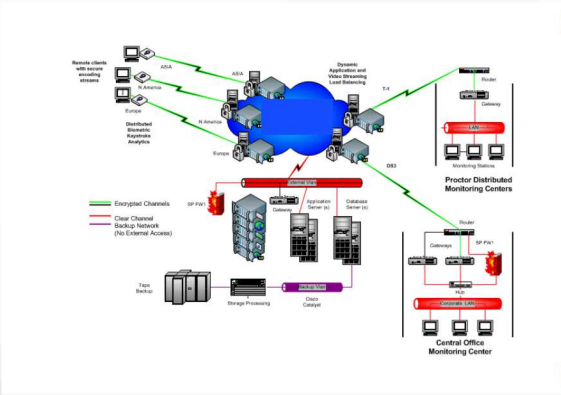
- Predict Answer "What if questions" at scale, with confidence.
- Assess confidence in predictions; characterize and propagate uncertainties
- Make robust decisions under uncertainty and under advanced threat conditions

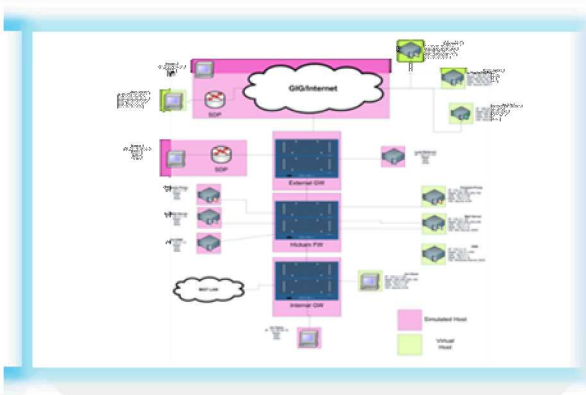


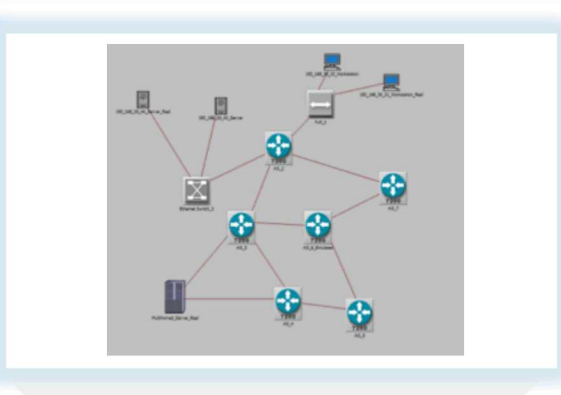
Uncertainty Quantification

Adversarial Optimization

Cyber experimentation approaches







ACTUAL SYSTEM | **VIRTUALIZED TESTBED** | **SIMULATION TESTBED**

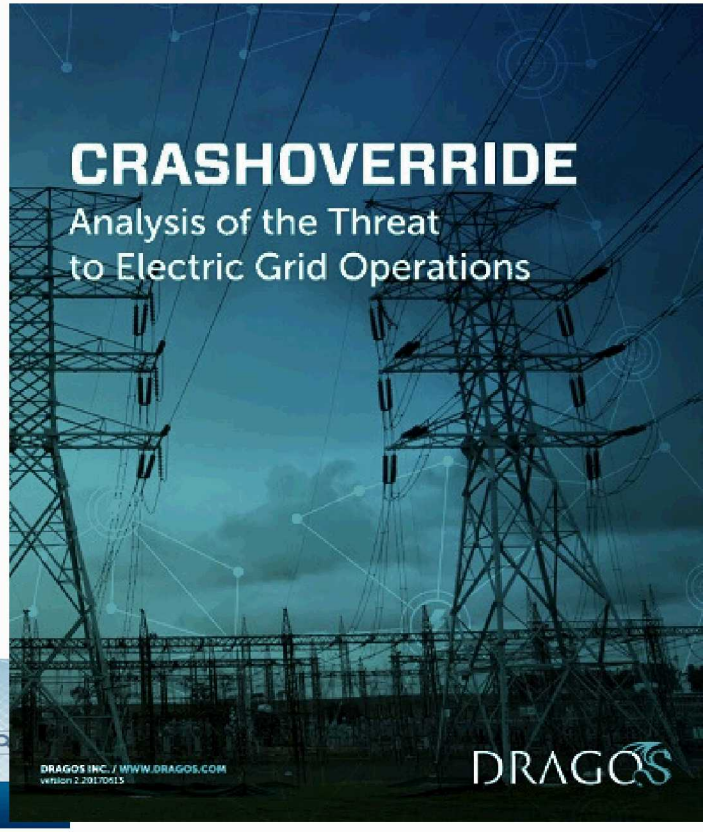
Interoperability in a single experiment

LIVE ← Increase Realism — Decrease Cost, Decrease Time → SIMULATED

REAL HARDWARE REAL SOFTWARE	ABSTRACT HARDWARE REAL SOFTWARE	ABSTRACT HARDWARE ABSTRACT SOFTWARE

Threat is Real

- The Electric power grid is a cyber-physical system that is becoming increasingly information dependent.
- The 2015 Ukranian power grid attack showed the potential effects of a cyber attack on a critical infrastructure.



US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

HOME | ABOUT US | CAREERS | PUBLICATIONS | ALERTS AND TIPS | RELATED RESOURCES | C³ VP

Alert (TA17-163A)
CrashOverride Malware

More Alerts

Original release date: June 12, 2017 | Last revised: July 27, 2017

Print | Tweet | Send | Share

Systems Affected

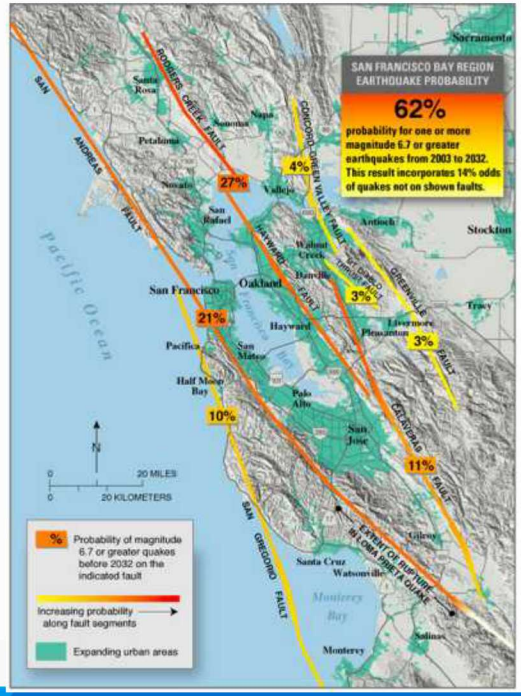
Industrial Control Systems

Overview

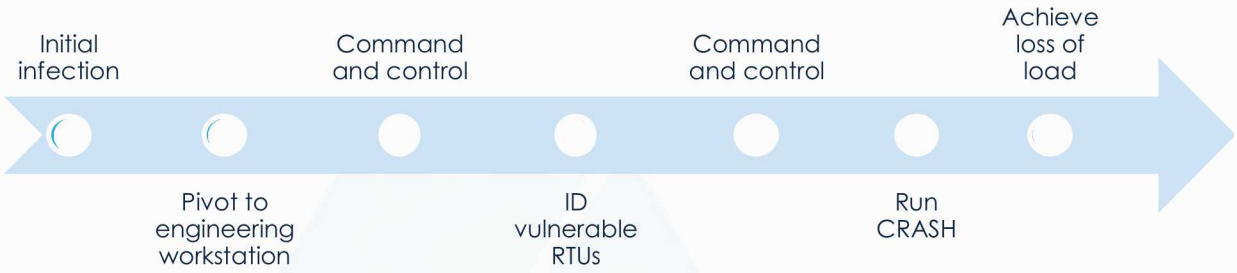
The National Cybersecurity and Communications Integration Center (NCCIC) is aware of public reports from ESET and Dragos outlining a new, highly capable Industrial Controls Systems (ICS) attack platform that was reportedly used in 2016 against critical infrastructure in Ukraine. As reported by ESET and Dragos, the CrashOverride malware is an extensible platform that could be used to target critical infrastructure sectors. NCCIC is working with its partners to validate the ESET and Dragos analysis, and develop a better understanding of the risk this new malware poses to U.S. critical infrastructure.

Cyber-aware resilience and Consequence-aware cyber defense

- Cyber attacks lead to correlated physical failures.
  - What is a cyber fault line?
- How do we prioritize our defenses?
- How effective are our defenses?
  - Is one solution quantifiable better than another?
- How do we improve cyber-systems for better resilience?
- How do we operate on physical systems in a cyber threat-informed way?



Focus on One step of the Kill Chain

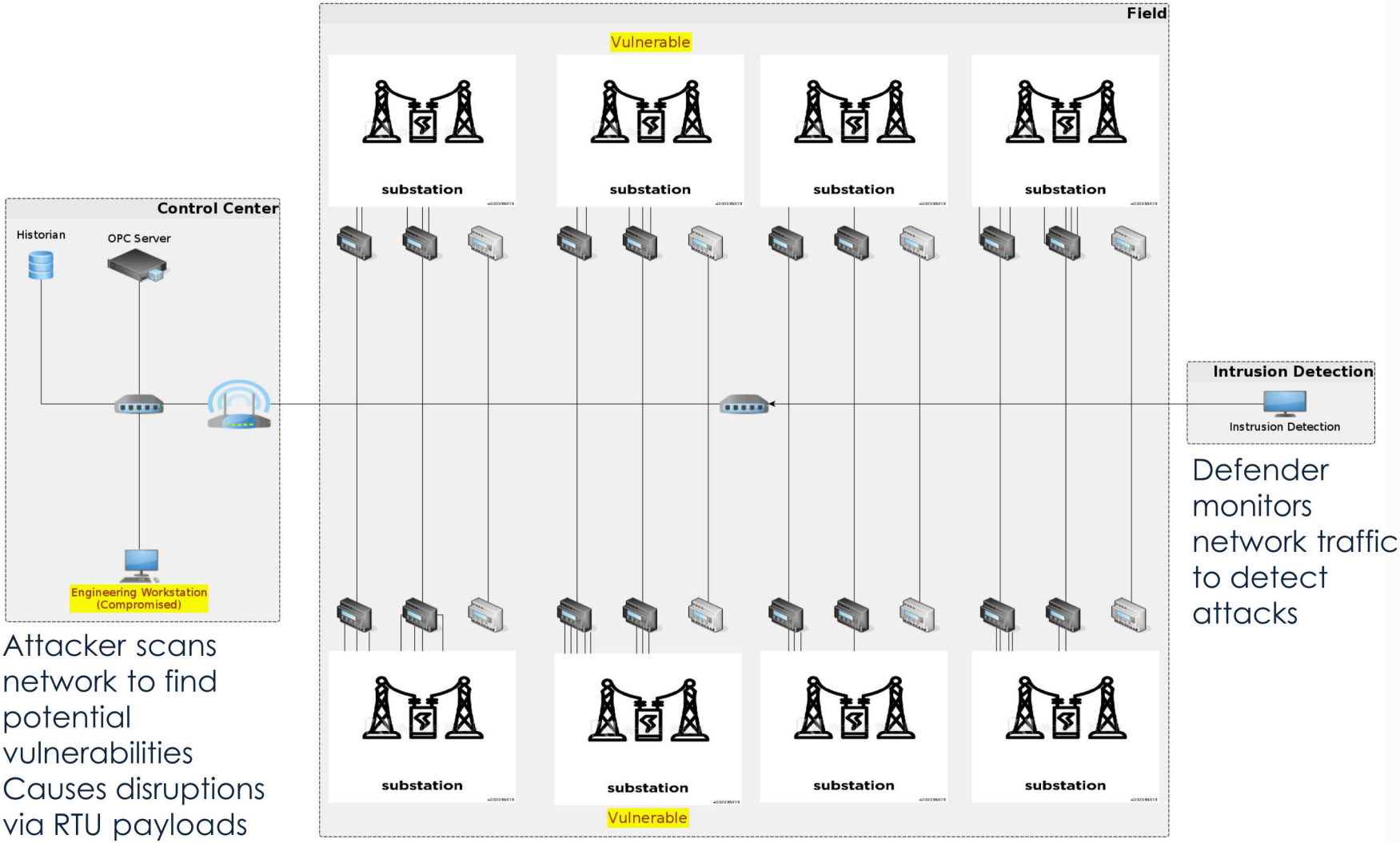


1. Deliver email
2. Follow link
3. Execute
4. Obtain IP of engineering workstation
5. Command/control
6. Pivot to engineering workstation
7. Scan for RTUs
8. Ready for attack

- Key Simplifications
  - Analyzed 1 step of kill chain (ID vulnerable RTUs)
  - Considered relatively small system
    - 8 RTUs total
  - Assumed attacker has prior knowledge of RTUs
  - Metric of interest: load shed in the power system
- Current Work: Command and Control

Scenario – Cyber
Notional SCADA/ICS Network

8 substations, 24 remote terminal units (RTUs)

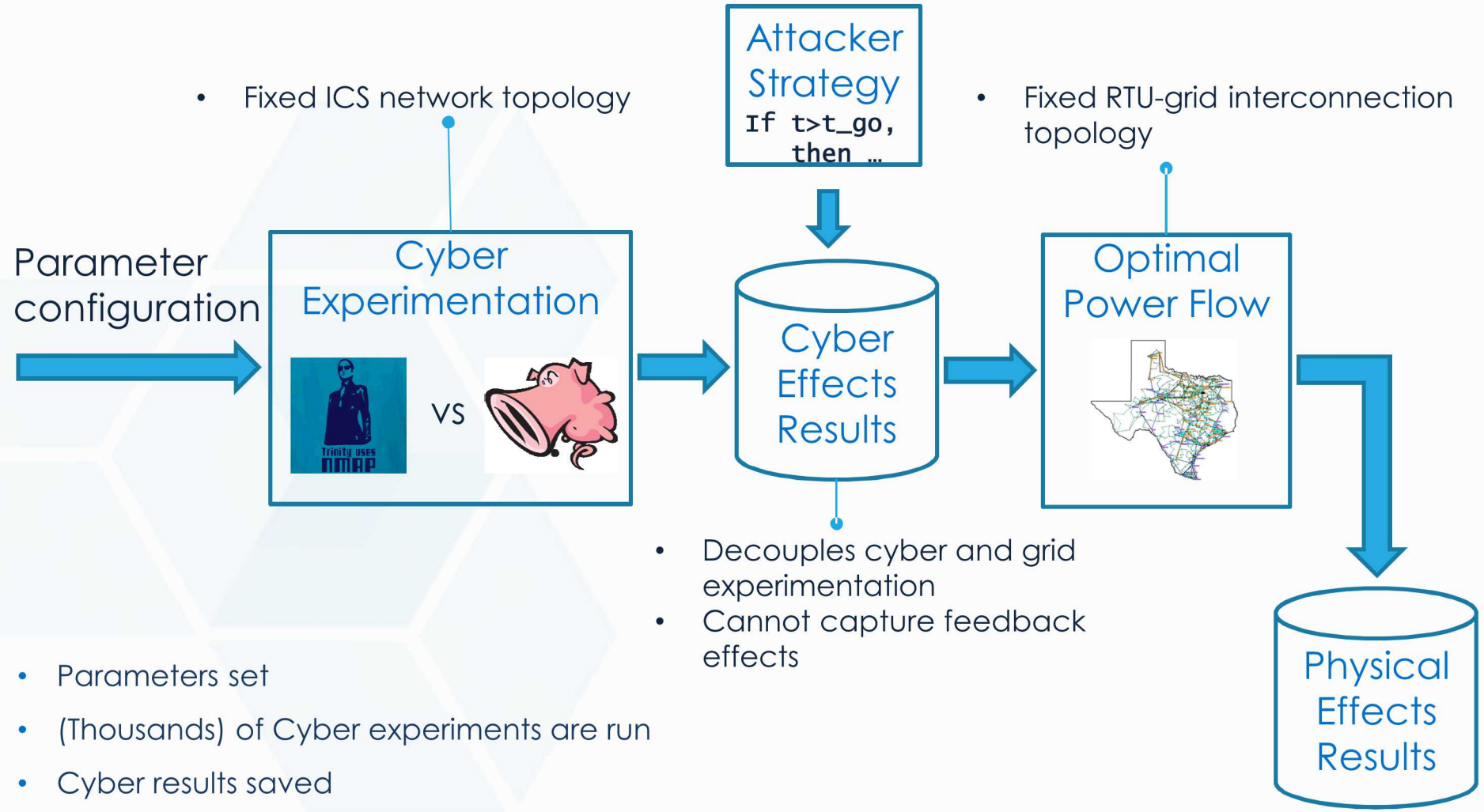


- Attacker scans network to find potential vulnerabilities
- Causes disruptions via RTU payloads

Defender monitors network traffic to detect attacks

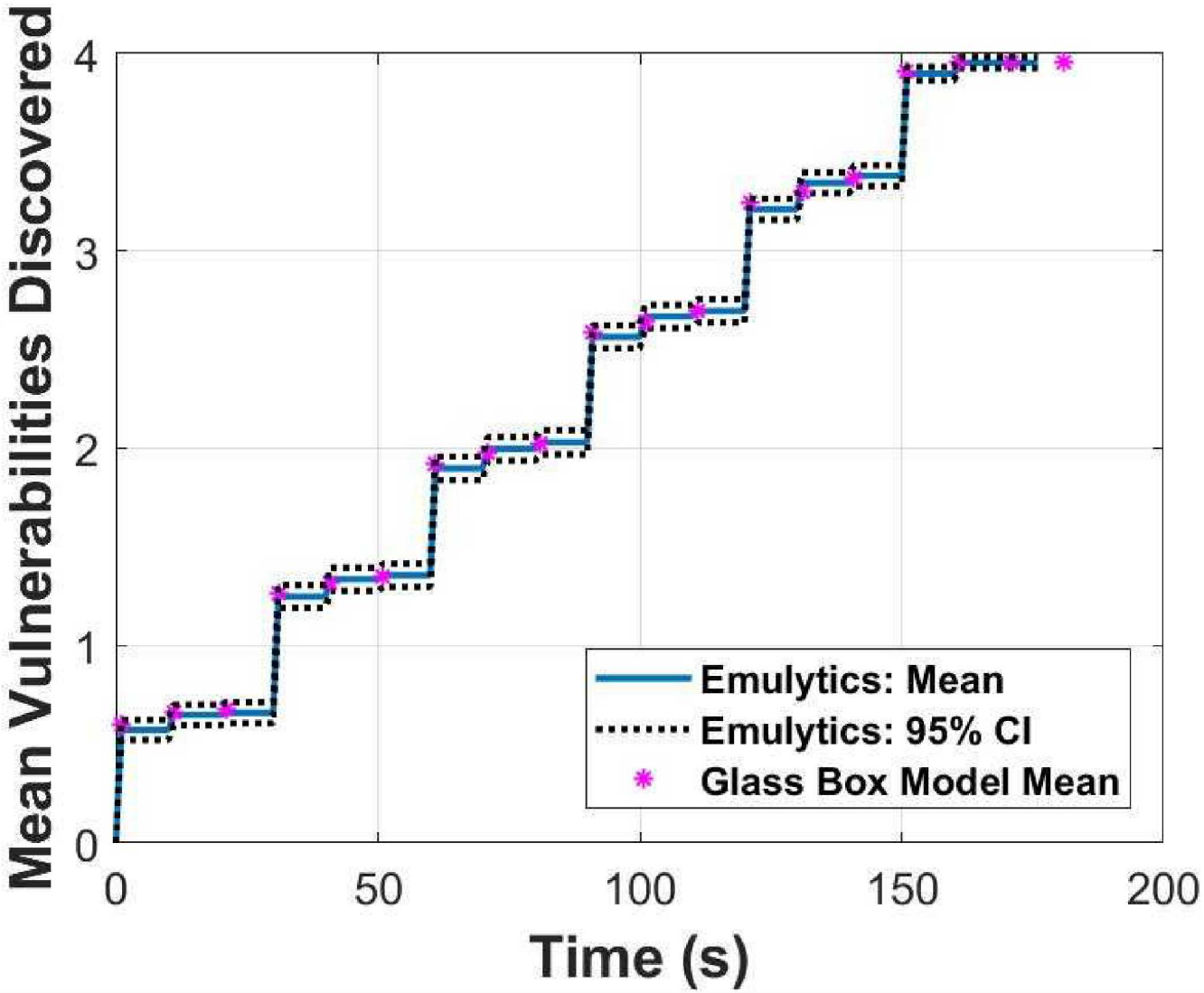
Vulnerable RTUs not firewalled for maintenance

Experimental Workflow

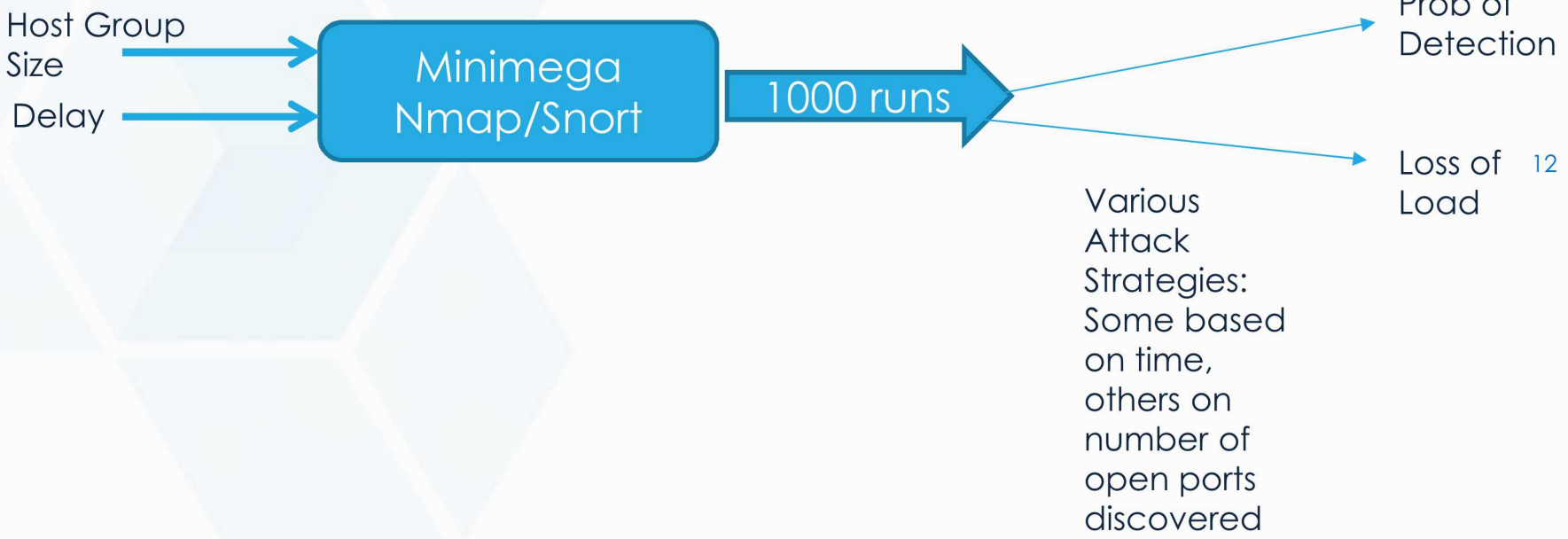


- Parameters set
- (Thousands) of Cyber experiments are run
- Cyber results saved
- Cyber results are translated to inputs to optimal power flow (OPF) tools
- OPF tools generate physical effects results

Results: Vulnerability Identification

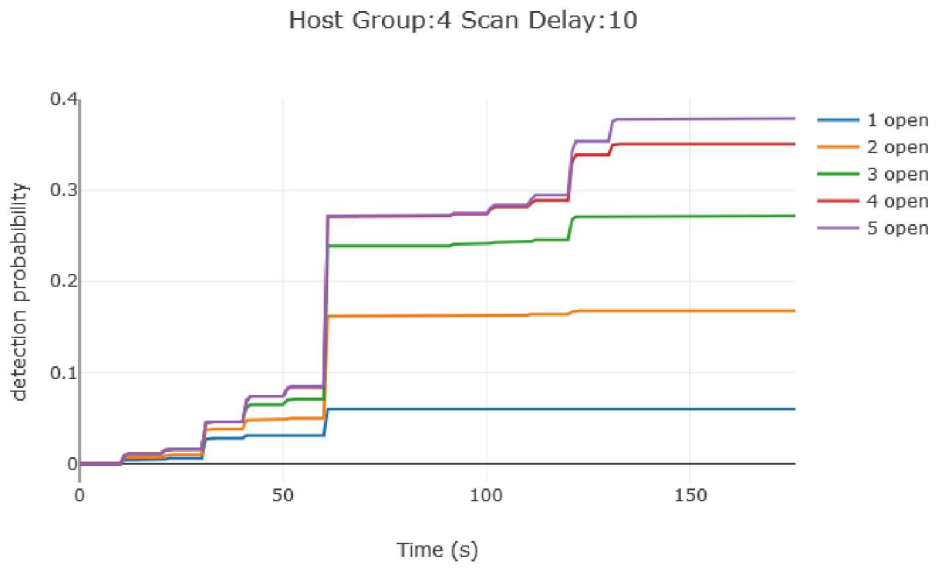


Treatment of uncertainty in scanning

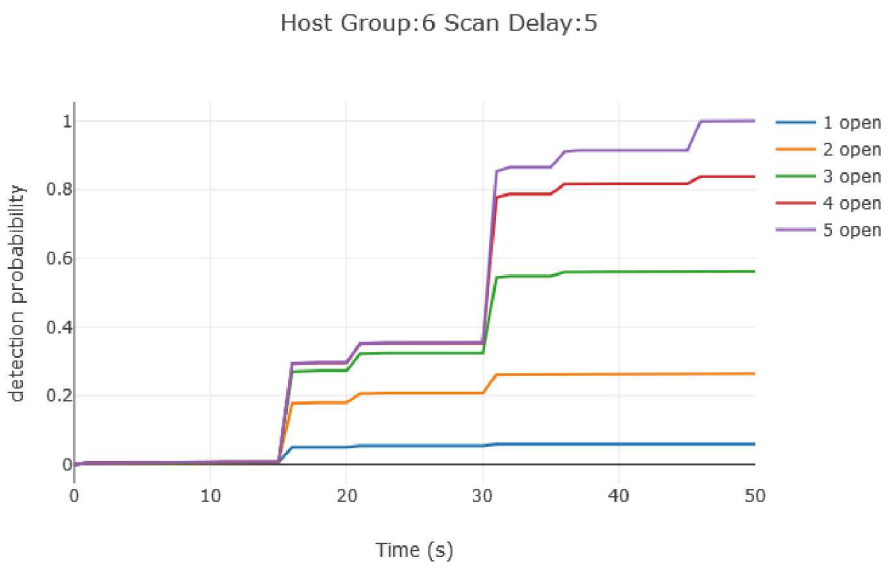


Results: Comparing two versions of attacks

4 probes, Delay 10 sec



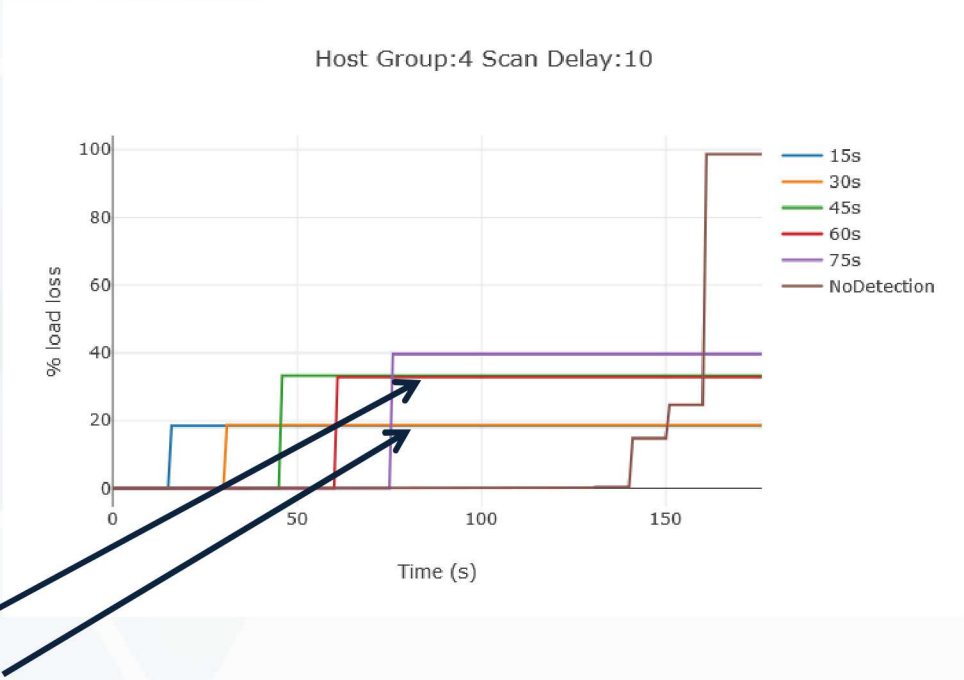
6 probes, Delay 5 sec



- Detection occurs much earlier when attacker runs 6 probes every 5 seconds.
- Attacker has significant probability of NOT being detected in the 4 probe, 10 second delay case.

Results: Comparing two versions of attacks

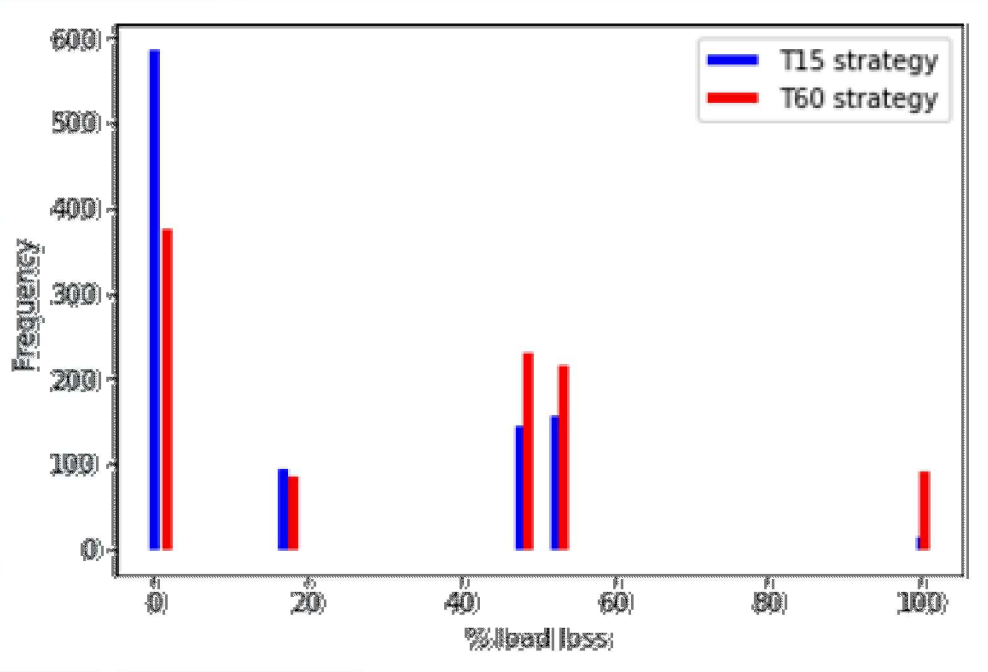
4 probes, Delay 10 sec
Wait for a specified time



Next page will compare these strategies at 80 seconds.
T15 strategy: mean load loss of 18.4%
T60 strategy: mean load loss of 32.8%

Results: Zoom in on 4 probes, delay 10

- Comparing a T15 strategy vs. a T60 strategy at 80 seconds

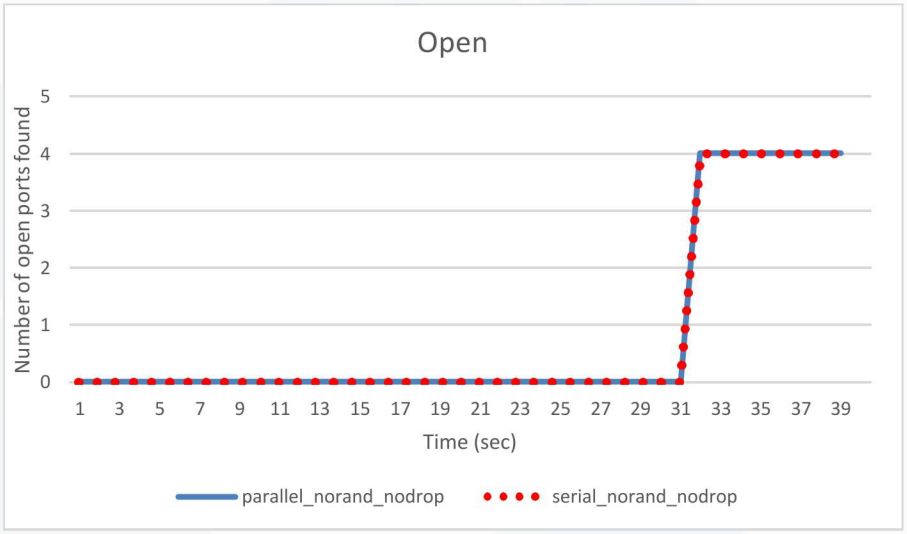


T15 strategy: mean load loss of 18.4%
T60 strategy: mean load loss of 32.8%

- T-test comparison for equality of mean load loss at 80 seconds using these two strategies shows that they are statistically significantly different.
- **If you only look at the mean, you don't see the differences in the distribution**

Reproducibility of Experiments

We did verify that **we get the SAME exact results across all 1000 realizations** for both serial and parallel when we have no probability of dropping a packet and a fixed port order for scanning.



These are consistent with our understanding of the protocol and the fastest the topology can be scanned.

Dealing with discrete high dimensional spaces

- There is a rich literature on uncertainty quantification for continuous, low-dimensional spaces.
- Our problems are discrete and high-dimensional.
- We have an all-hands on deck approach:
  - Better models for discrete spaces
    - PCEs based on discrete polynomials:
  - Dimensionality Reduction
    - Models for the full system. What corresponds to PCA in this space?
    - Reduced set of representatives/observables in the system based on functionality
  - Multi-fidelity Models
    - Monte Carlo should be a part of the toolset.
    - Can we reduce the time for each sample by lower-fidelity models without compromising accuracy?

Dealing with high dimensionality

- **Multifidelity approach**
  - Take a large number of low fidelity runs and a small number of high fidelity runs to achieve statistics on high fidelity responses
    - Low fidelity runs are assumed to have bias
  - Relies on variance reduction: must have correlation between the low and high fidelity model

Fidelity definition

- `minimega` – HF: 100 Requests (average over 10 repetitions)
- `ns3` – LF: 10 Requests (`Delay` $50ms$)
- `ns3` – LF*: 1 Requests (`Delay` $5ms$)

	$\mathcal{C}$
HF	1
LF	0.016
LF*	0.002

TABLE: Normalized Cost

We assume **serial execution for the low-fidelity model**, however we might easily increase the efficiency of LF (`ns3`) by running multiple concurrent evaluations

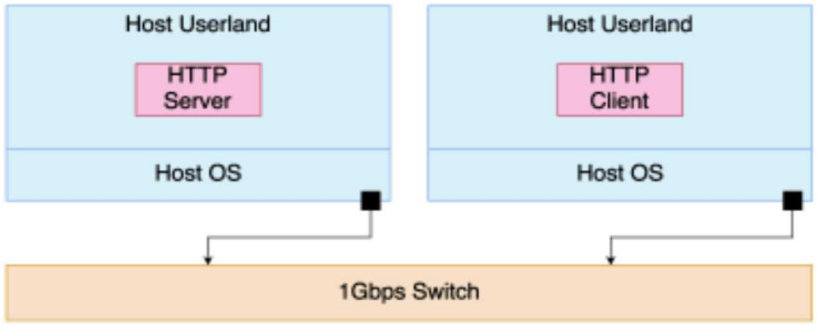


FIGURE: Network Configuration

Multi-fidelity modeling results – variance reduction

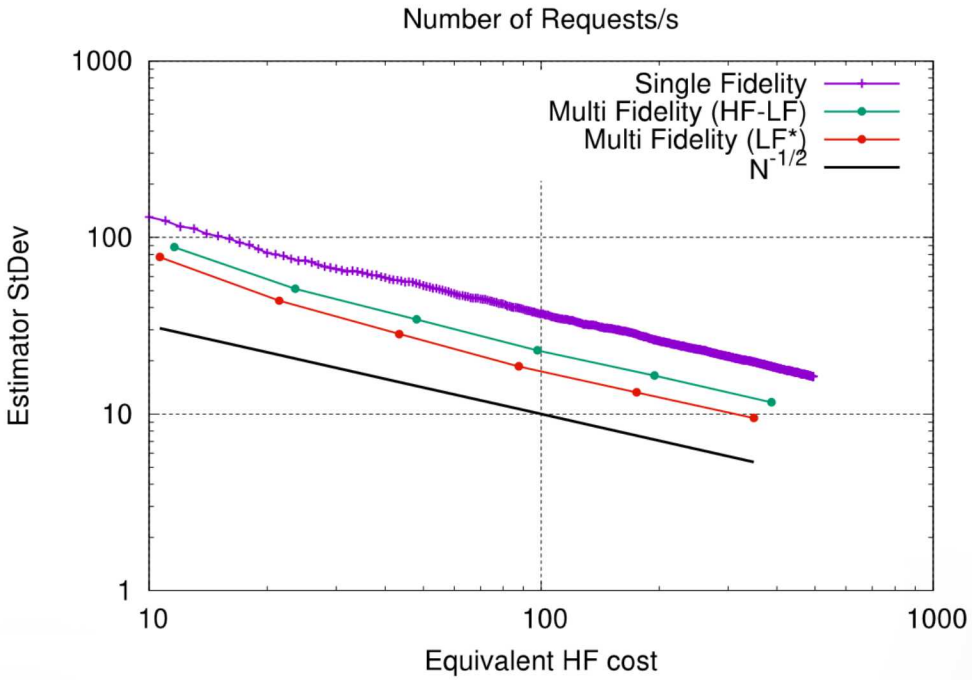


FIGURE: Exp. Value StDev

- The **variance reduction** we obtain w.r.t. MC is

$$\mathbb{V}ar\left(\tilde{Q}\left(\underline{\alpha}^{ACV}\right)\right) = \mathbb{V}ar\left(\hat{Q}\right)\left(1 - \frac{\mathbf{r_1} - 1}{\mathbf{r_1}}\rho_1^2\right)$$

- The **number of low-fidelity simulations** is $N_{LF} = N \times r_1$ where

$$r_1 = \sqrt{\frac{\mathcal{C}_{HF}}{\mathcal{C}_{LF}}\frac{\rho_1^2}{1-\rho_1^2}}$$

- For each HF simulation we need to spend an **extra cost** in LF simulations

$$\text{Eq.Cost}: \quad \mathcal{C}_{tot} = N\left(1 + \mathbf{r_1}\frac{\mathcal{C}_{\mathbf{LF}}}{\mathcal{C}_{\mathbf{HF}}}\right)$$

- For this case

	ρ_1	r_1	$r_1\mathcal{C}_{LF}/\mathcal{C}_{HF}$
LF	0.86	4.69	0.075
LF*	0.90	10.83	0.022

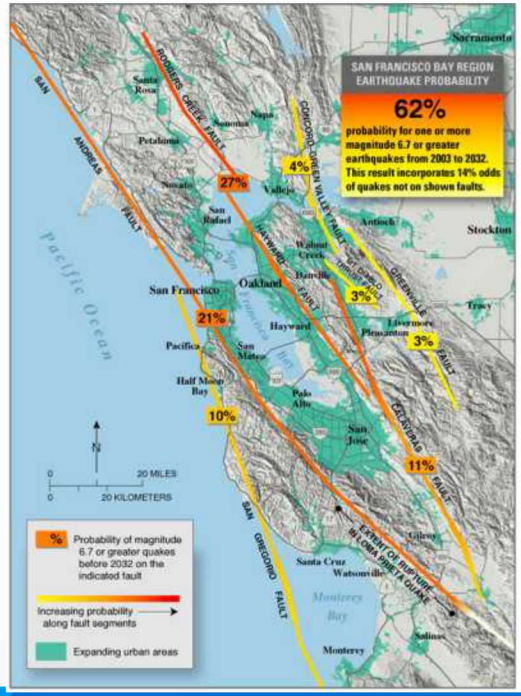
Example (for LF*)

- Number of **HF runs**: $N = 500$
- Number of **LF* runs**: $r_1 \times N = 5415$
- Equivalent **LF cost**: $r_1 \times N \times \frac{\mathcal{C}_{LF}}{\mathcal{C}_{HF}} = 11$
- **Total** estimator **cost** (HF + LF*): $\mathcal{C}_{tot} = 500 + 11 = 511$
- **Variance reduction**: $\left(1 - \frac{r_1 - 1}{r_1}\rho_1^2\right) = 0.23$

More than 70% variance reduction is obtained by adding **only an equivalent cost of 11 HF runs.**

Decision Making: Cyber-aware resilience and Consequence-aware cyber defense

- Cyber attacks lead to correlated physical failures.
  - What is a cyber fault line?
- How do we prioritize our defenses?
- How effective are our defenses?
  - Is one solution quantifiable better than another?
- How do we improve cyber-systems for better resilience?
- How do we operate on physical systems in a cyber threat-informed way?



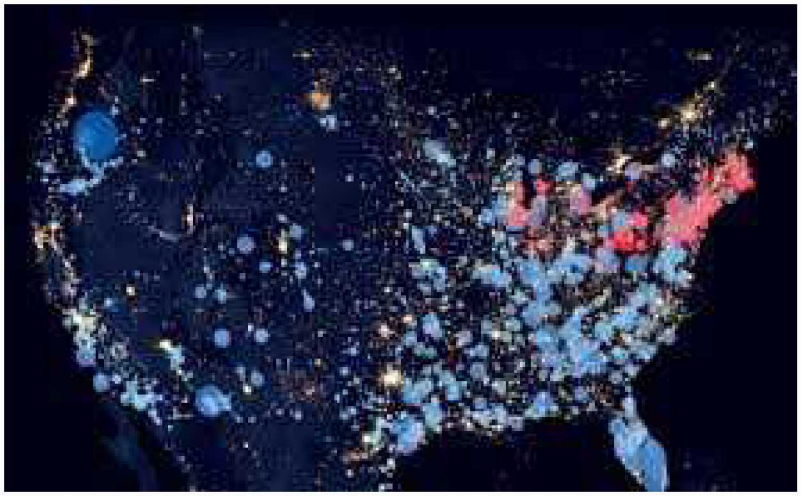
SECURE Optimization Research Challenge

Problem: Decision-makers need to protect power grids against informed, adaptive, malicious adversaries attacking their cyber networks

Decision-makers need to:

- Account for likely adversarial behaviors/responses
- Plan response strategies
- Discover effective investment options

Challenge: There are **exponentially** many adversarial behaviors, response strategies, and investment options



PAO – A Python Library for Adversarial Optimization

IDEA: Extend Pyomo to model bilevel optimization problems that explicitly include both defender and attacker decisions

Pyomo: An Optimization Modeling Tool Built in Python

- Diverse modeling capabilities
  - Disjunctive programs, stochastic programs, dynamic optimization problems, etc.
- Can express modular, hierarchical model structure
- Automatic model transformations

INFORMS Computing Society Prize - 2019

Example: Linear Bilevel Programs

- Hard problems (NP-hard)
- No general-purpose commercial solvers for discrete lower level decisions

$$
\begin{aligned}
\min_{x \geq 0} \quad & c_1^T x + d_1^T y \\
\text{s.t.} \quad & A_1 x + B_1 y \leq b_1 \\
& \min_{y \geq 0} \quad c_2^T x + d_2^T y \\
& \qquad\qquad A_2 x + B_2 y \leq b_2
\end{aligned}
$$

- **Upper level problem**
- **Lower level problem**

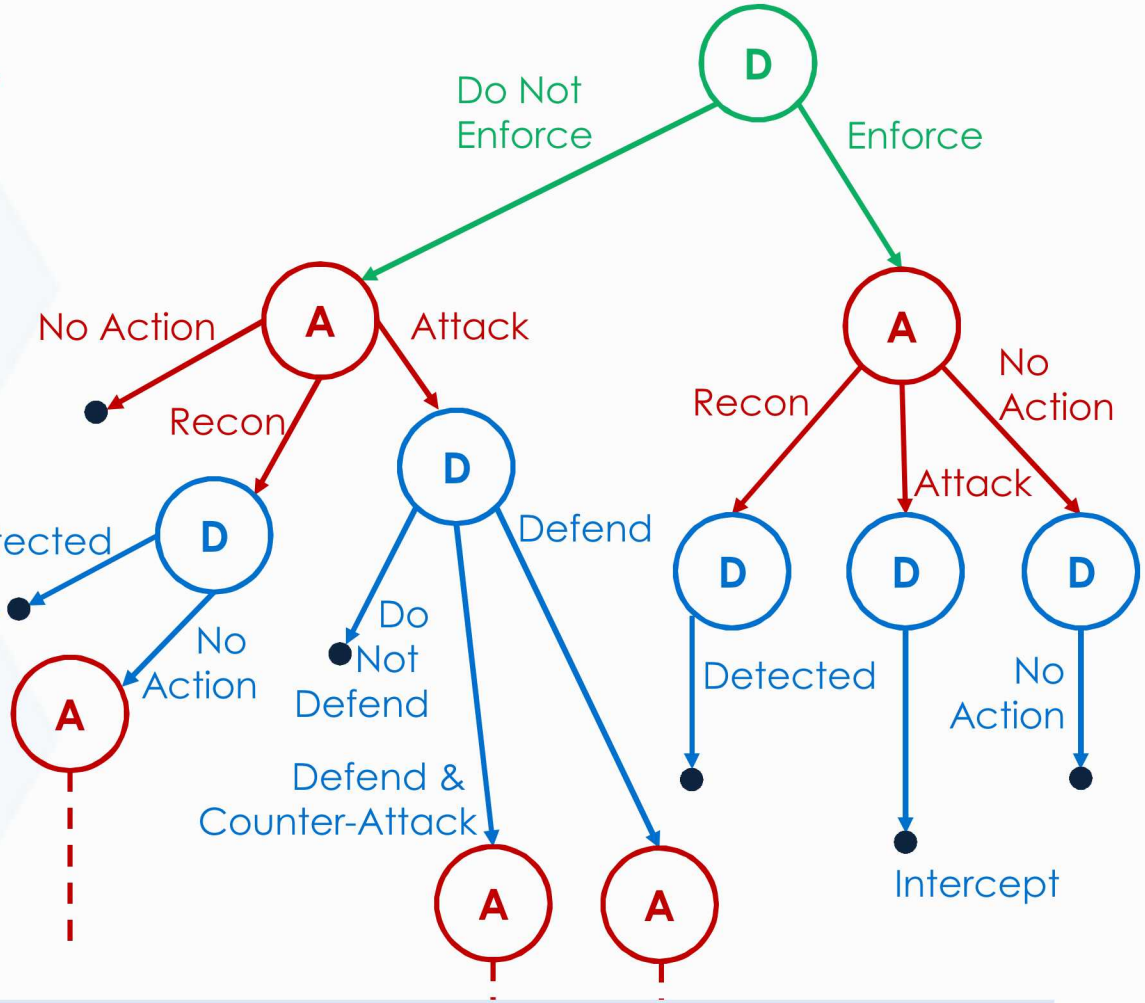
Defending Against: Empowered adversaries

Stackelberg Game:

Defender: An entity operates a cyber-enabled infrastructure and takes certain measures to defend it.

Attacker: A cyber adversary attacks the entity to cause service disruption and physical damage.

Defender: An entity operates a cyber-enabled infrastructure and takes certain measures to defend it.



New software (soon) available: Python Adversarial Optimization (PAO)

Cyber-Aware Operations: Attack by a sophisticated adversary

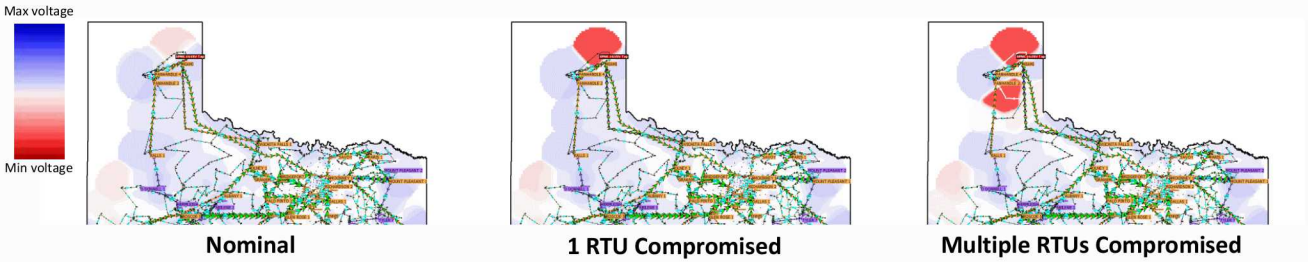
Which RTUs should be hardened in order to minimize power grid effects (measured in megawatts load unserved) from a CRASHOVERRIDE attack?

Nominal Operations:
- Total Load: **320.81 MW**
- No Security Violations

Attack Budget of 1 RTU:
- RTU-4 Compromised
- Total Load Shed: **237.97 MW (75%)**
- Voltage Security Violations

Attack Budget of 2 RTUs:
- RTU-4 and RTU-7 Compromised
- Total Load Shed: **298.81 MW (93%)**
- Increased Voltage Security Violations

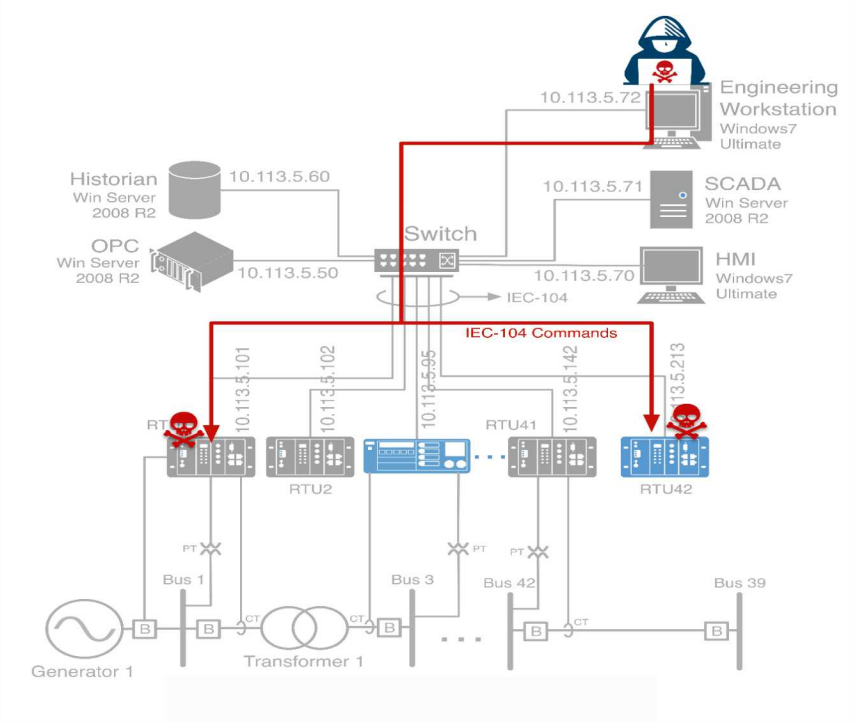
Attack Budget of 3 RTUs:
- RTU-4, RTU-7 and RTU-8 Compromised
- Total Load Shed: **320.81 MW (100%)**
- Severe Voltage Security Violations



- DAKOTA performed a sensitivity analysis on the power grid topology configured in SCEPTRE
- Adversarial Optimization identified worst-case outcomes for increasing attacker budgets (instead of full enumeration of all possible events)
- The exercise indicated inconsistency between SCEPTRE and the Optimization, enabling an improved representation of the exemplar model

Consequence-Aware Cyber Defense

- Network Design
  - How do we avoid placing critical resources away from each other on the cyber network
  - Avoid dependent components placing on the same cyber fault line
  - Burden on system operators
  - Our goal is to <u>quantify return on investment</u>



- Sensor Placement:
  - How do we prioritize cyber defenses to limit physical damage
  - Increases operational costs
  - How do we <u>quantify the return on investment?</u>

Conclusions

- Cyber experimentation is a crucial tool for cyber security.
- Emulation (abstract hardware/real software) provides predictive capability.
- Prediction should be support with confidence bounds to be used for high-consequence decisions.
- We need the ability to identify extreme events in systems.
- We face algorithmic challenges in
  - Dimension reduction for discontinuous systems
  - Ability to sample high-dimensional, categorical spaces
  - V&V for discrete systems
  - Threat Characterization
  - Glass-box models for cyber systems
  - Scalable solvers for design/interdiction problems
  - Scalable solvers stochastic design/interdiction problems
- We welcome collaborations