SAND2019-12760C

Cyber Threat Modeling And Validation

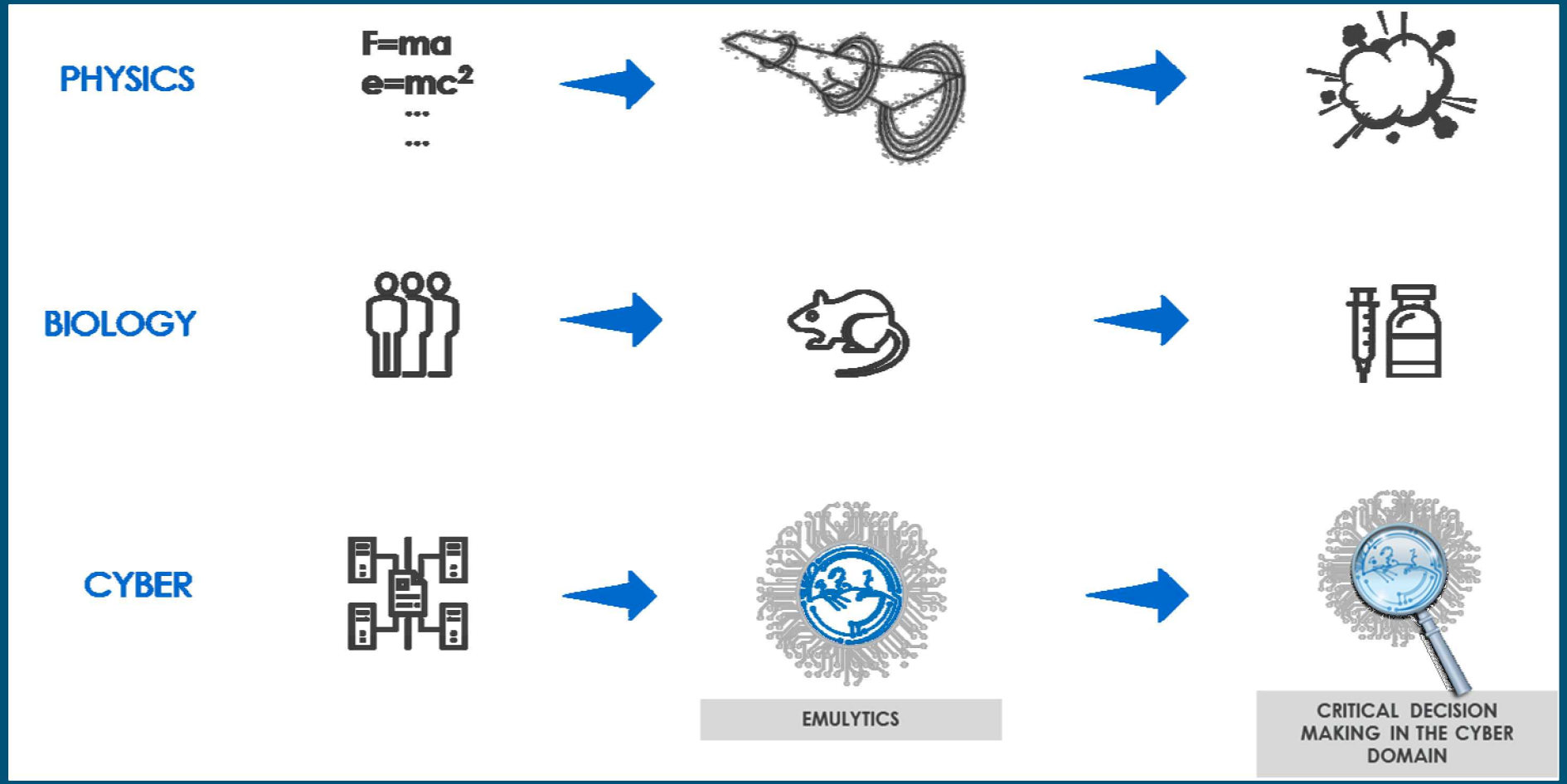
PRESENTED BY
Eric Vugrin, Gerardo Cruz, Christian Reedy,
Alexander Outkin, Vincent Urias, Thomas Tarman
Sandia National Laboratories

2019 Annual INFORMS Meeting
Seattle, WA
October 22, 2019

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & 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.

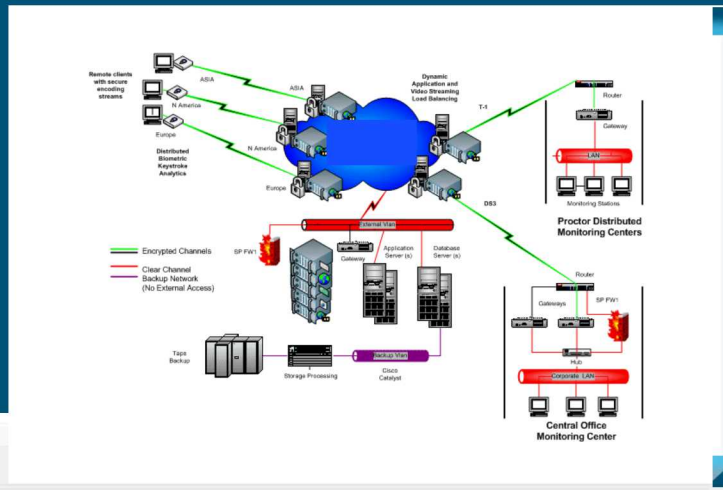
SAND2019-#####

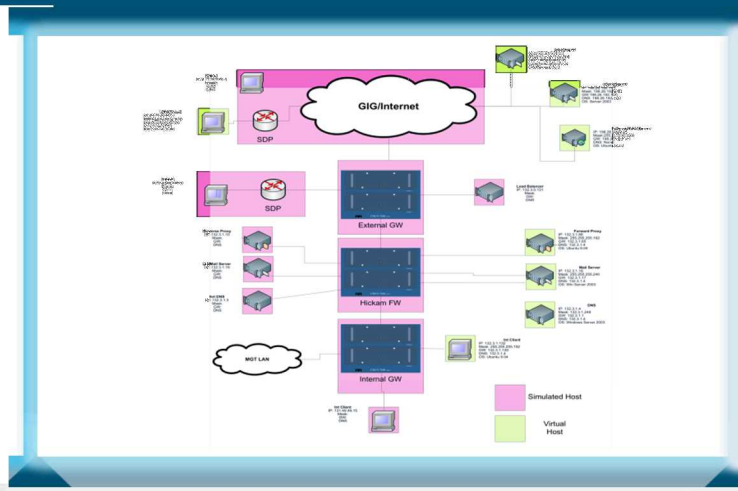
SECURE: Science & Engineering of Cybersecurity by Uncertainty quantification and Rigorous Experimentation

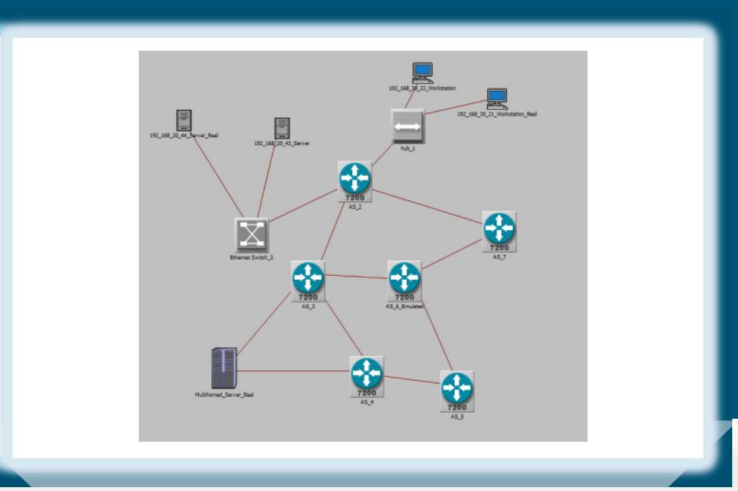


SECURE Goal: develop theory and tools to guide design, efficient execution, and analysis of cyber experiments

Emulation + Analytics = Emulytics







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

SECURE is integrating the mathematics of uncertainty quantification with Emulytics to improve cyber experimentation.

Threat Modelling

"Cyber Security does not exist in the absence of an adversary" (V. Urias)

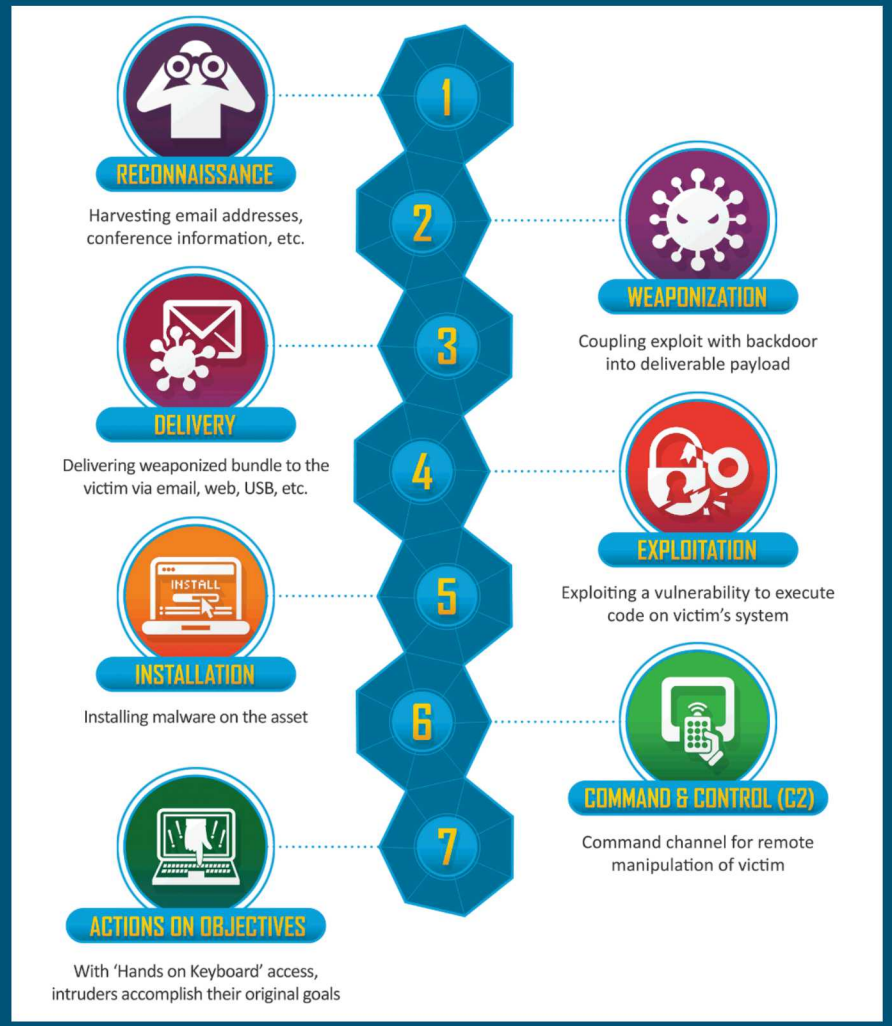
- Good cyber models require credible threat representations

Cyber threats can be complex, multi-step, adaptive

Threat models need to consider

- Attacker and defender goals
- Tools and Capabilities
- Strategies

Objective: develop and validate credible threat models for use in cybersecurity analyses



Lockheed Martin Cyber Kill Chain

https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

Threat Modelling

"Cyber Security does not exist in the absence of an adversary" (V. Urias)

- Good cyber models require credible threat representations

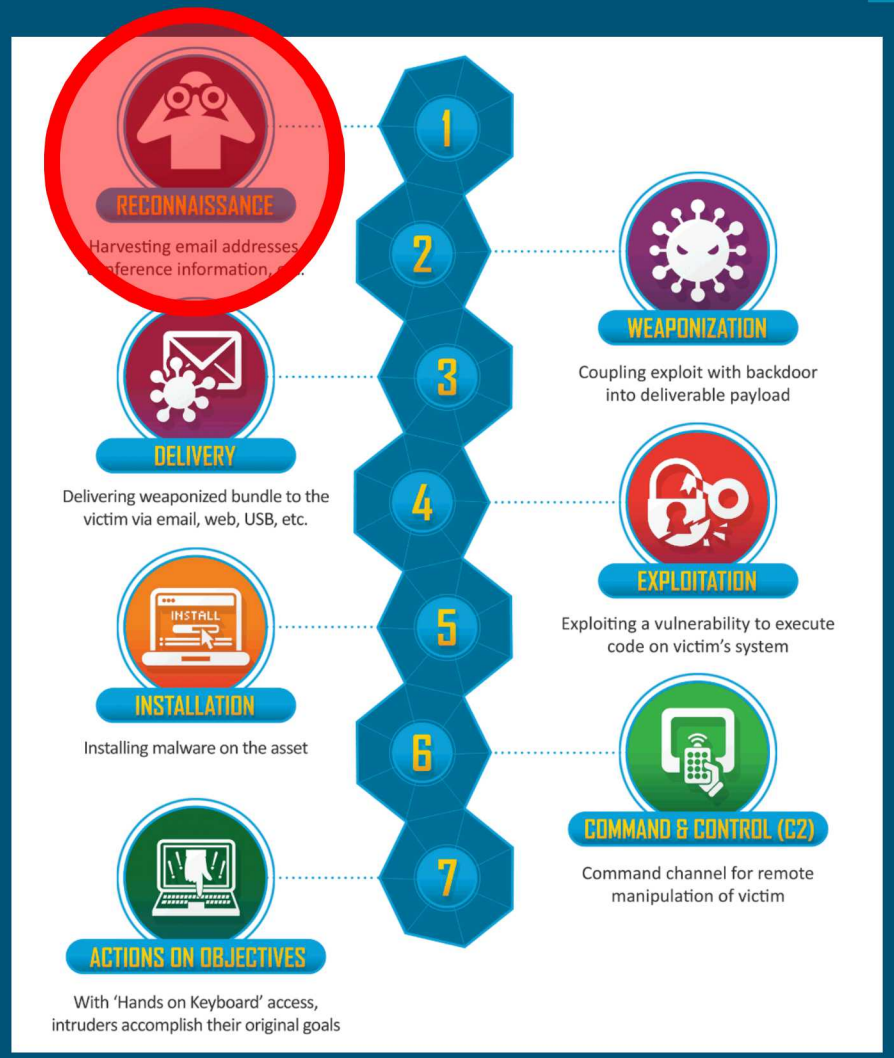
Cyber threats can be complex, multi-step, adaptive

Threat models need to consider

- Attacker and defender goals
- Tools and Capabilities
- Strategies

Objective: develop and validate credible threat models for use in cybersecurity analyses

This talk describes development of a scanning and detection model.



Lockheed Martin Cyber Kill Chain

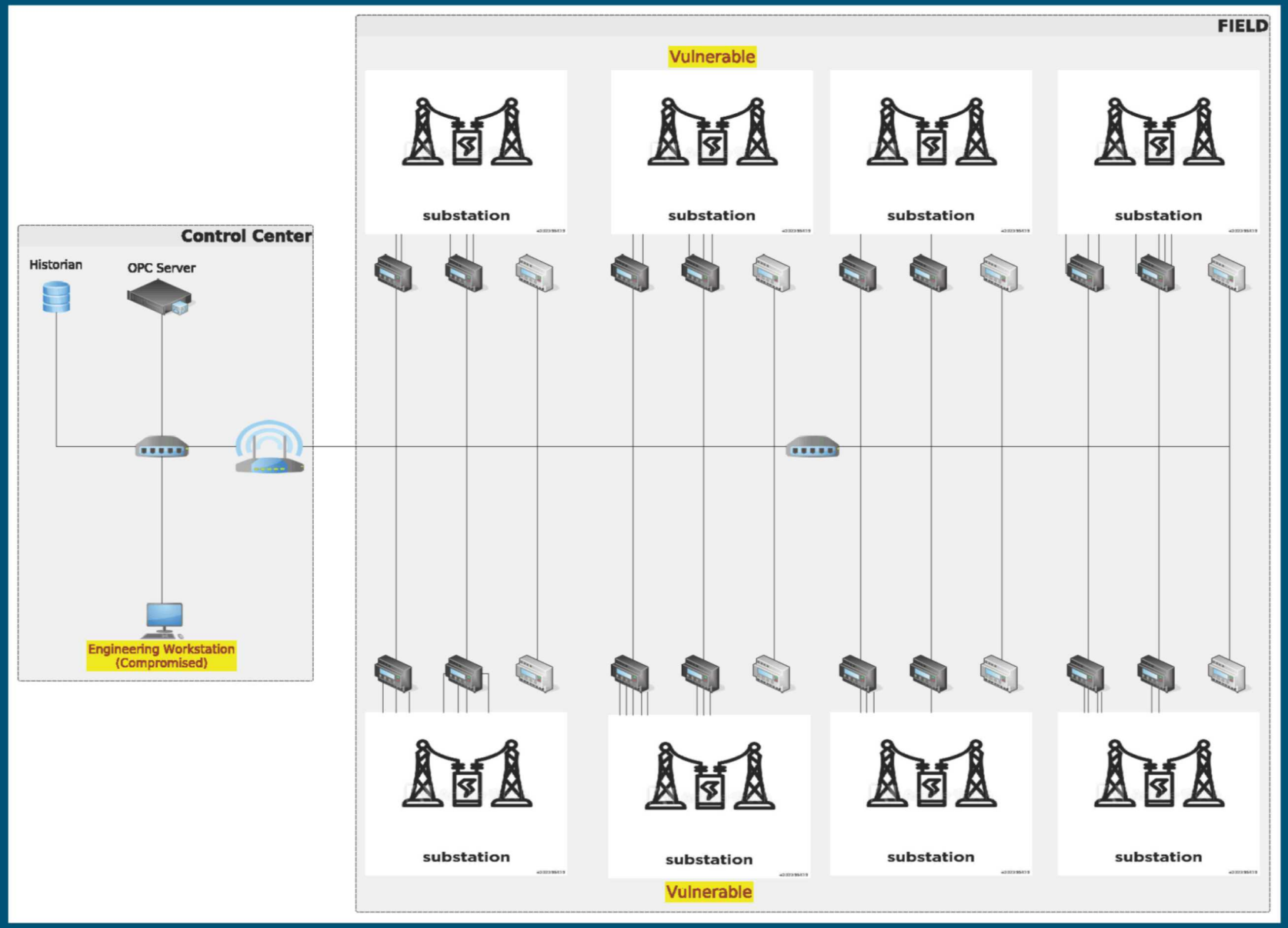
https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

Scenario: Attack on Power Grid

Power grid structure
- 8 substations, 24 remote terminal units (RTU)
- Vulnerable RTUs not behind firewalls (for maintenance)

Attacker
- Compromised engineering work station
- Scanning network to find potential vulnerabilities

Defender
- Monitors network traffic to detect attacks

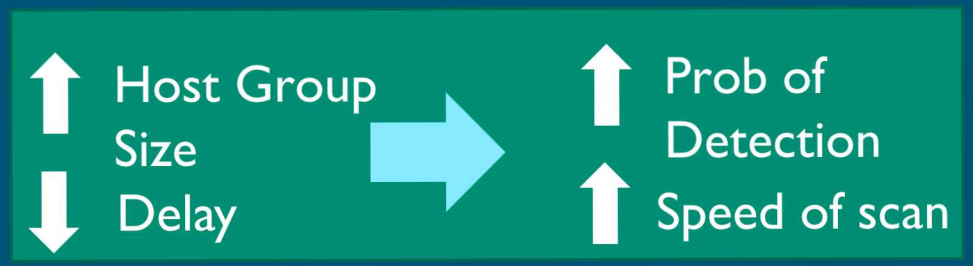


Tools

Attacker

Goal: find vulnerable RTUs quickly without being detected

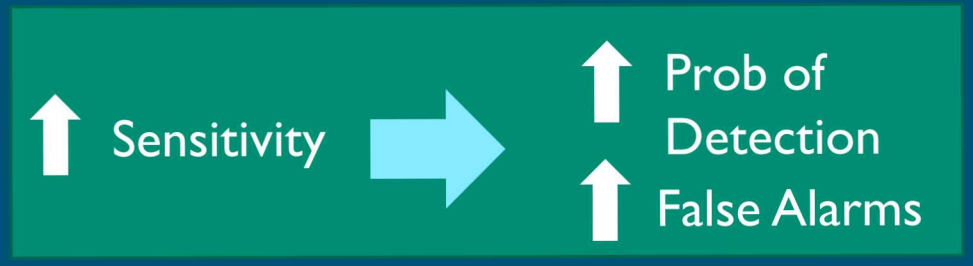
- Tool: Nmap Network Mapper
- Approach: TCP Syn Scan
- Scan port 22
- Key parameter settings: host group size and delay
- Stochastic features: ordering of addresses for scanning and time-outs

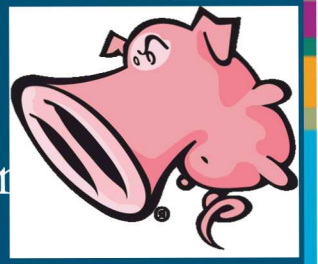


Defender

Goal: detect attack before attacker can exploit vulnerabilities

- Tool: Snort
- Approach: sfportscan
- Event = TCP reset
- Key parameter setting: sensitivity setting, i.e., detection alert occurs when >4 events occur within rolling 60 s window for LOW setting





Research Questions

For specified Nmap and Snort settings,

- Can we estimate the rate at which the attacker gains identifies vulnerabilities?
- What is the probability (over time) that the attacker is detected?
- What are the associated uncertainties?
- Can we validate our estimates?

This effort developed Emulytics and mathematical models to analyze a scanning and detection scenario.

Virtual Testbed Set-up

Virtualization tool: minimega – launches and manages virtual machines

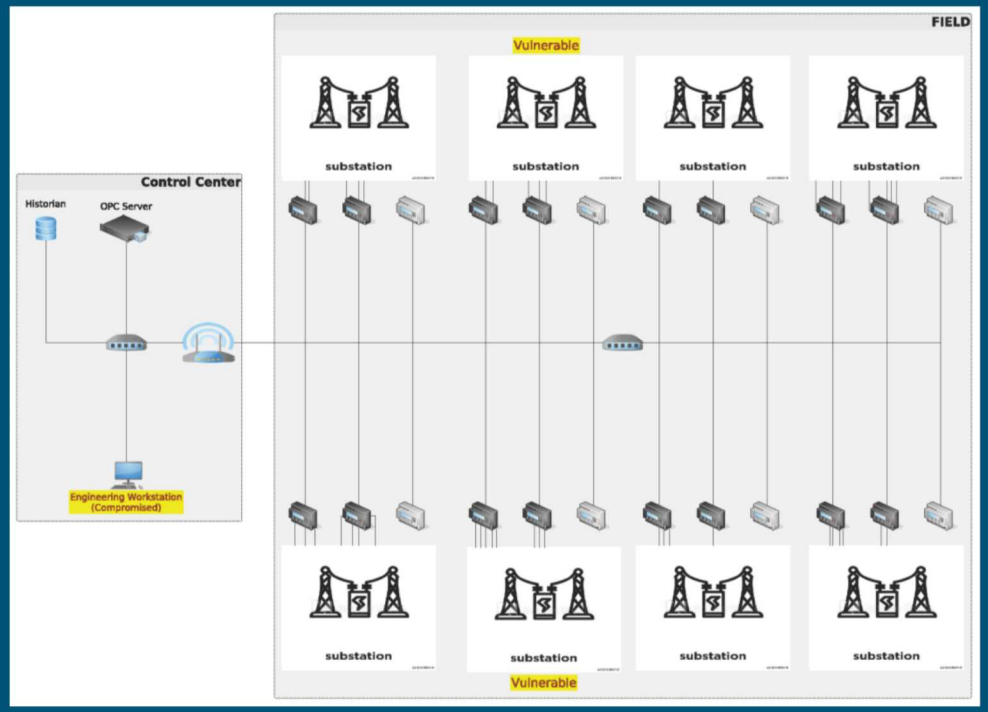
- Can scale to run on massive clusters
- Orchestrates Kernel-based Virtual Machines (KVM) to run unmodified OSes on emulated hardware
- Uses 802.1q VLAN tagging via Open vSwitch to support arbitrary network topologies

(In-experiment) Software

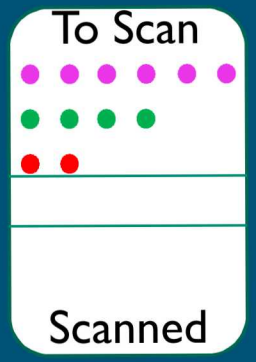
- Node OS: pared down Ubuntu 18.04
- Snort 2.9.13
- Nmap 7.60
- Router OS: VyOS 3.13.11

Host hardware

- Dual Socket Intel E5-2683v4 2.10GHz CPUs (32 total cores)
- 512 GB DDR3 Memory
- 100 GbE experiment network
- 10 GbE boot/storage network

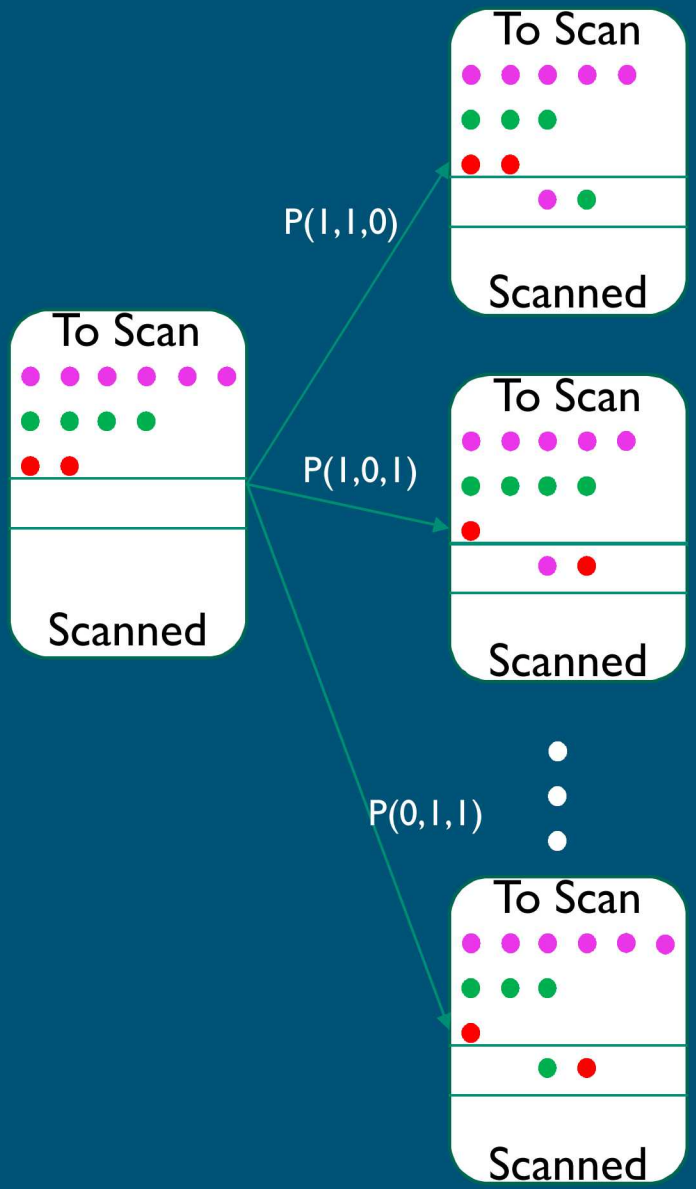


Mathematical Model



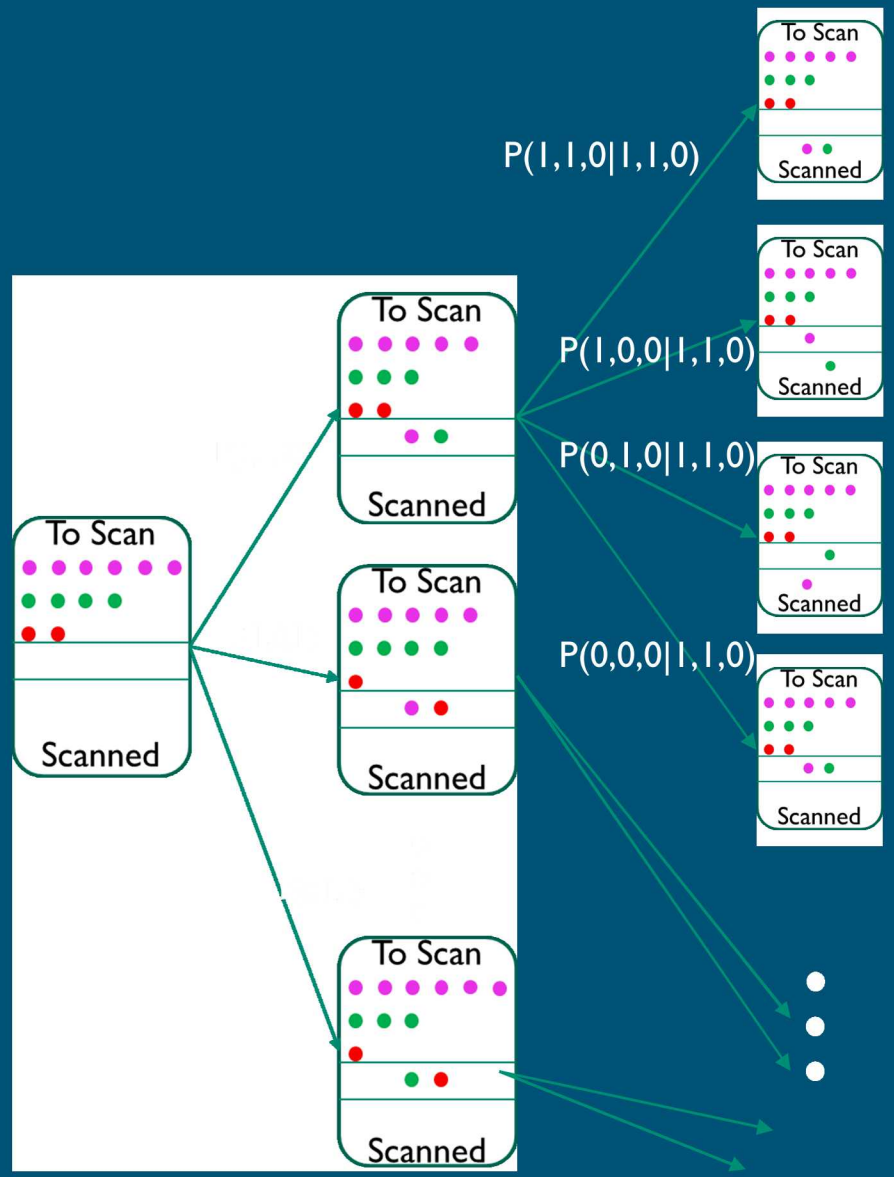
Step 1: initial conditions

Mathematical Model



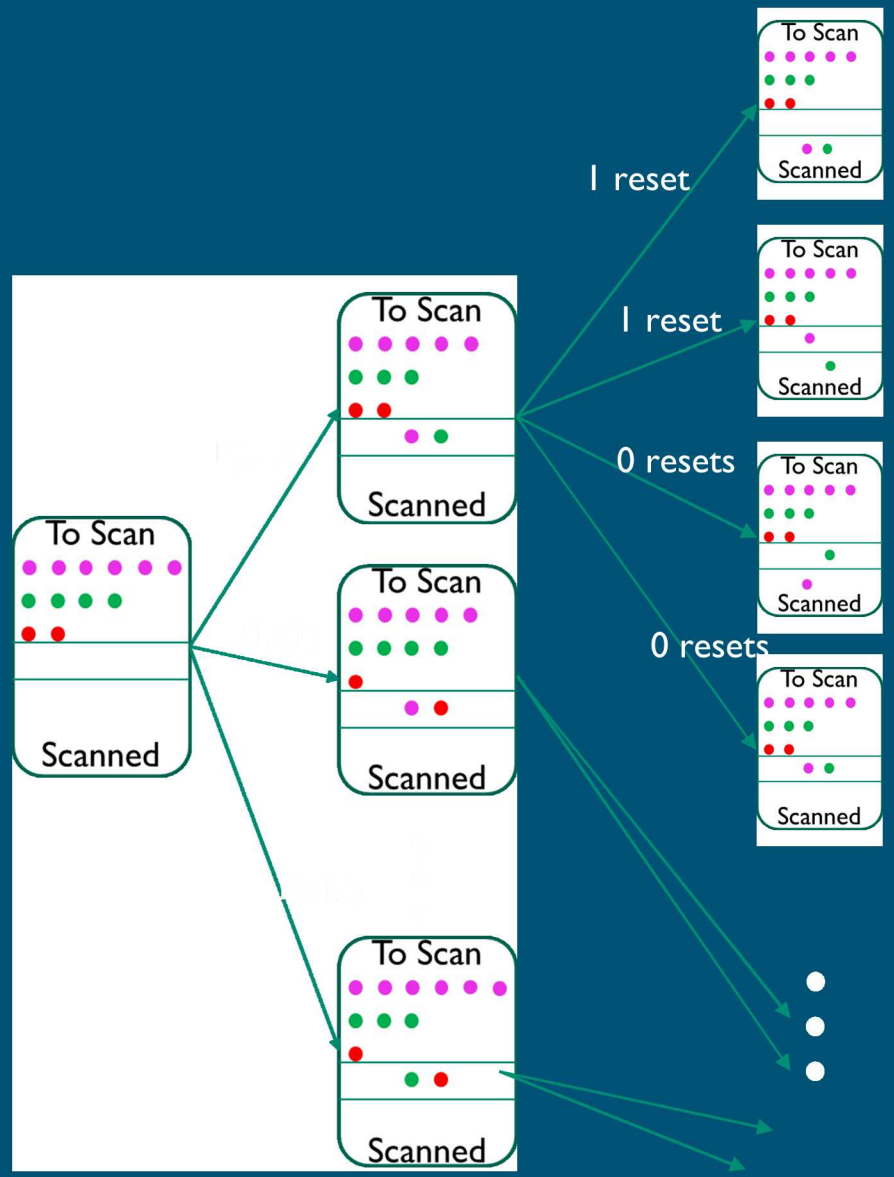
Step 2: select RTUs to scan

Mathematical Model



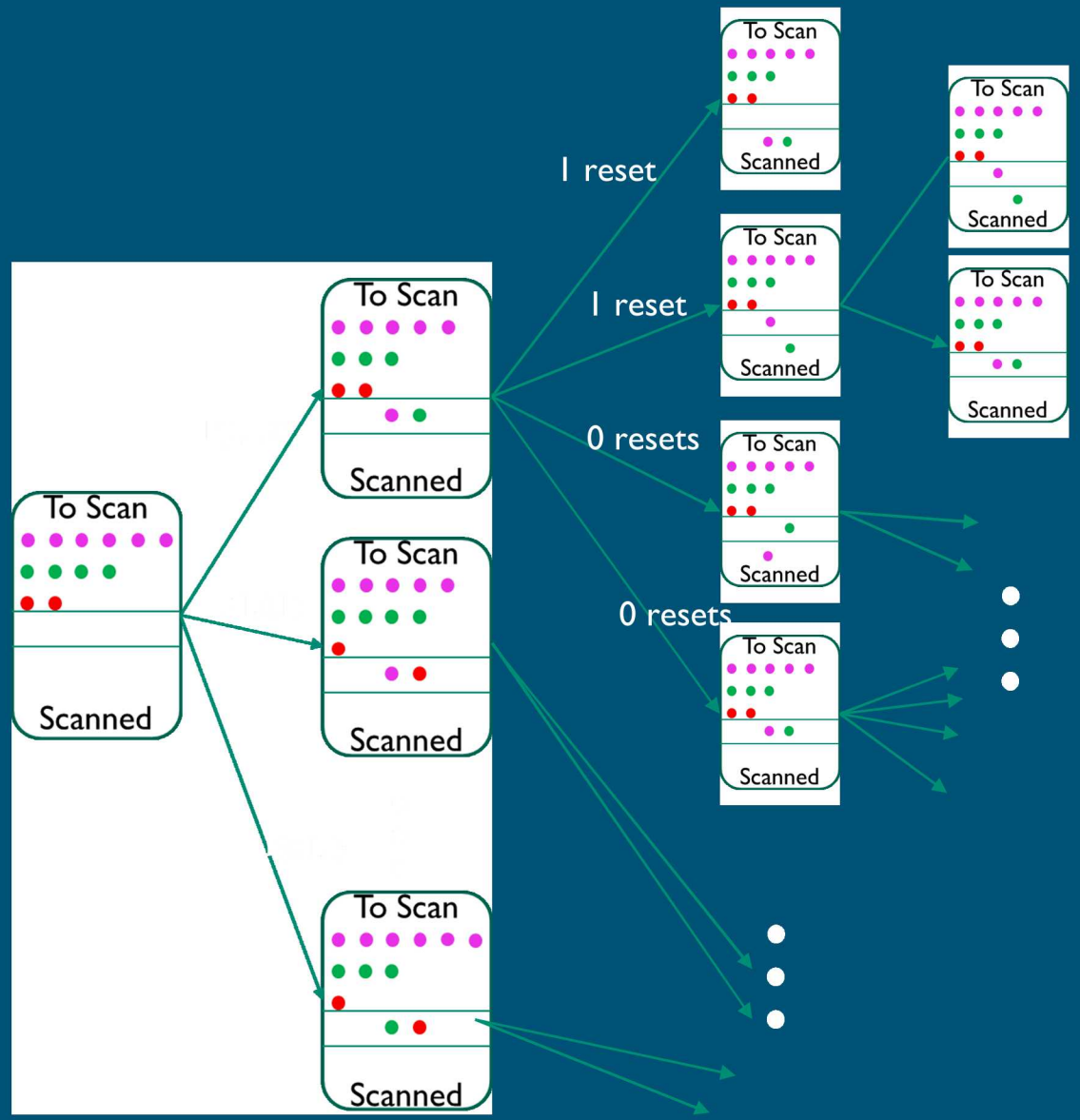
Step 3: determine if scan succeeds or times out

Mathematical Model



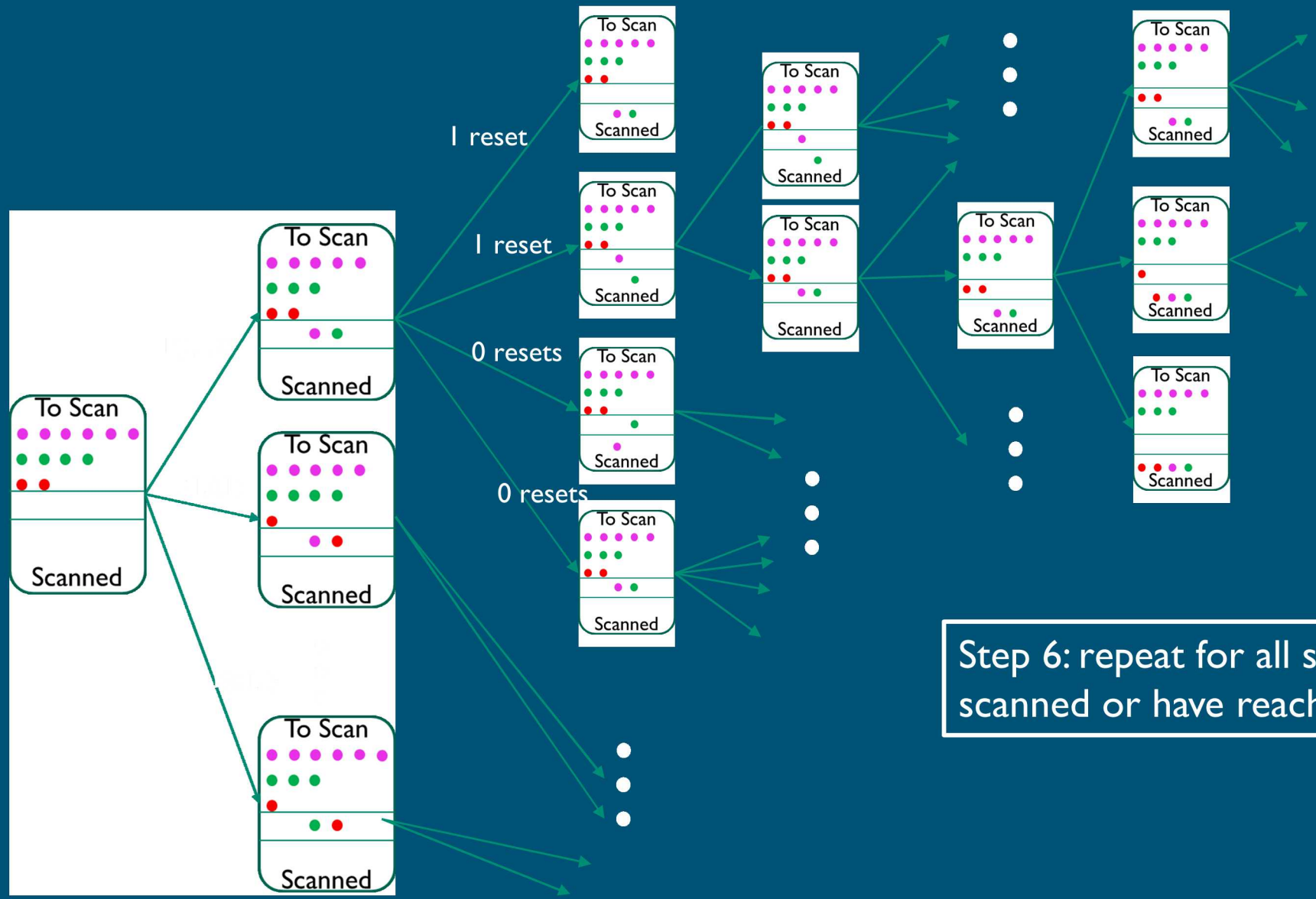
Step 4: determine if TCP resets occurred

Mathematical Model



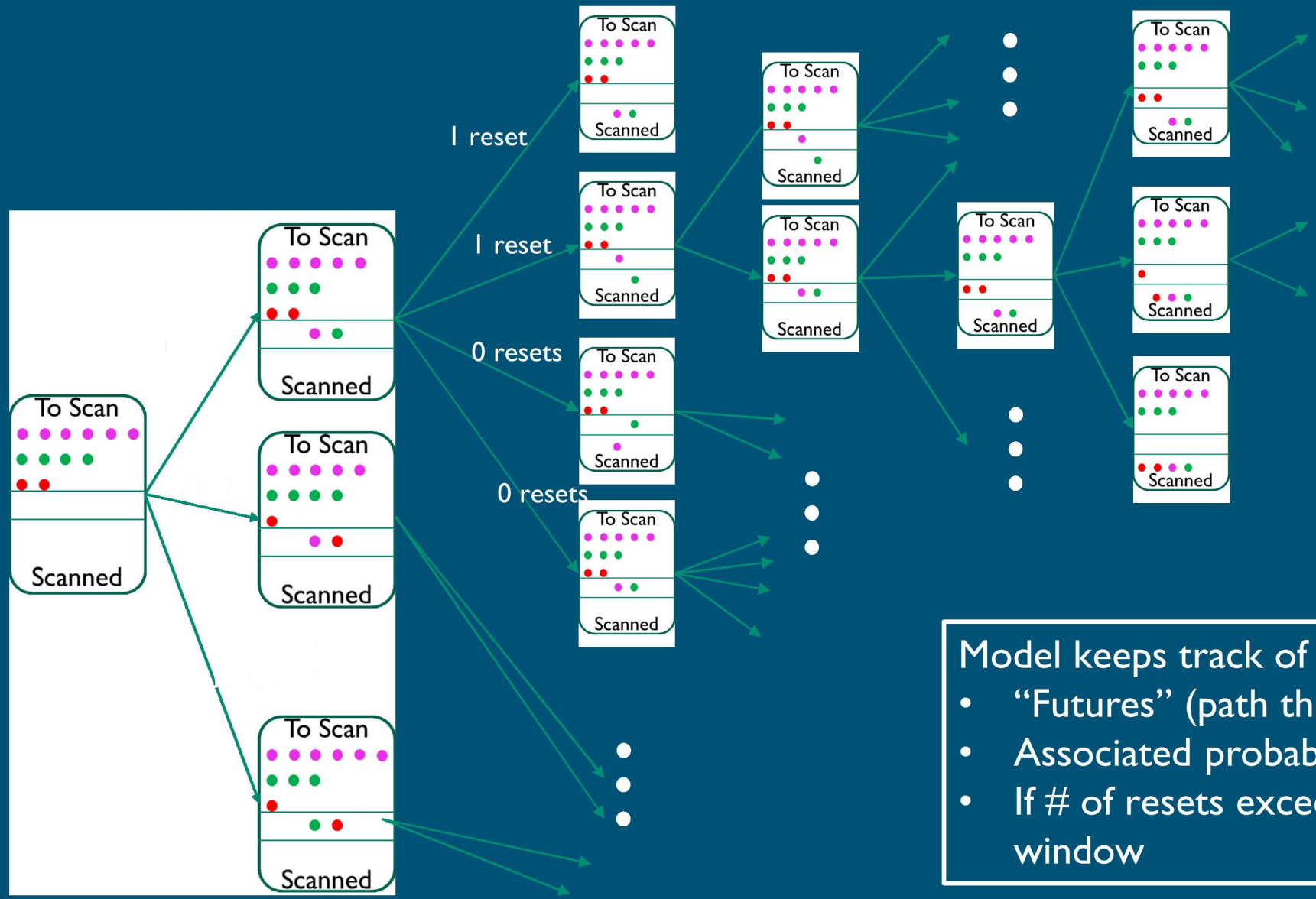
Step 5: if time out occurred, re-send and determine if timed out again; check for TCP resets

Mathematical Model



Step 6: repeat for all states until all RTUs are either scanned or have reached maximum # of time outs

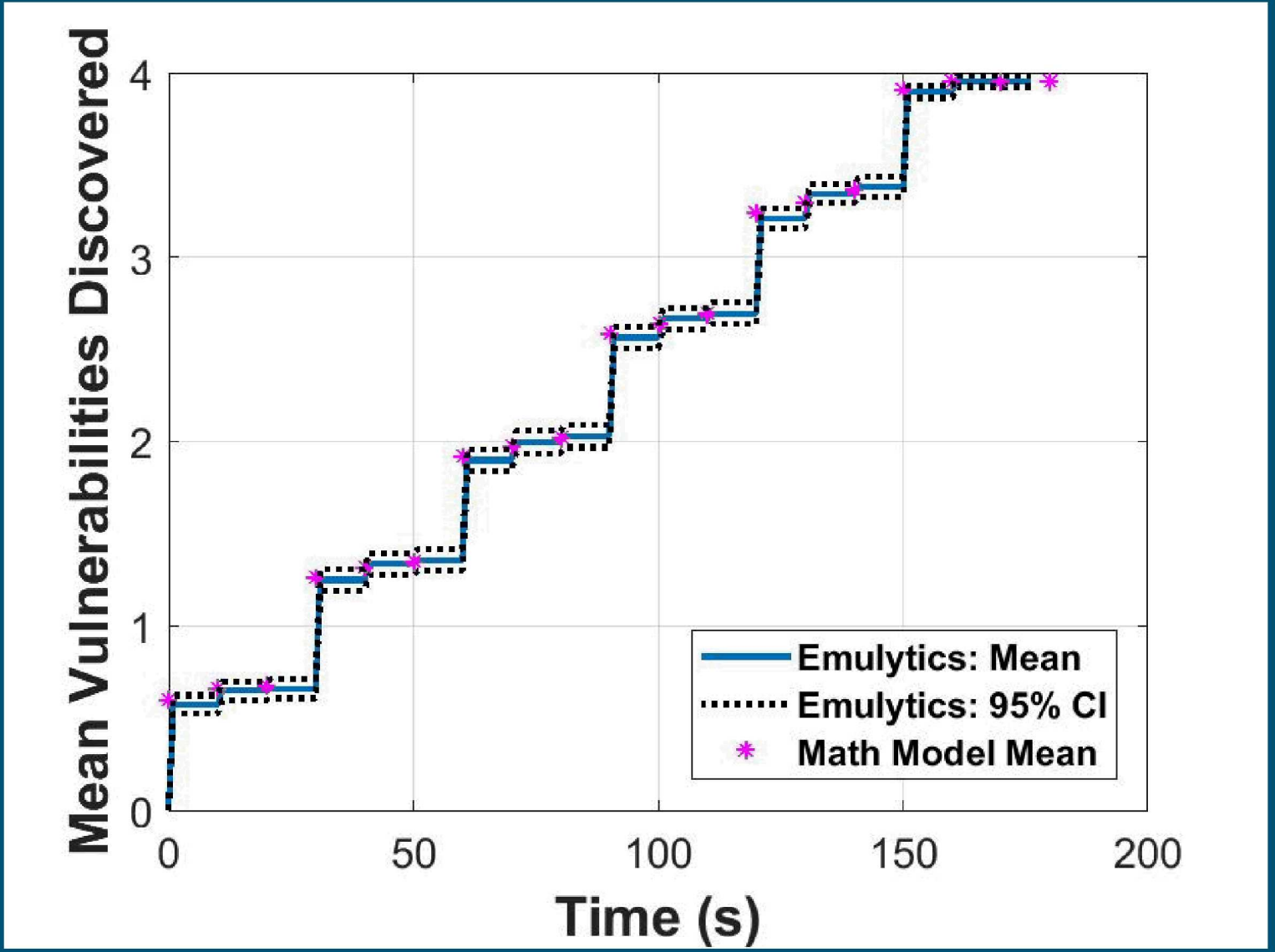
Mathematical Model



Model keeps track of

- "Futures" (path through the tree)
- Associated probabilities
- If # of resets exceeds threshold within time window

Results: Attacker Progress



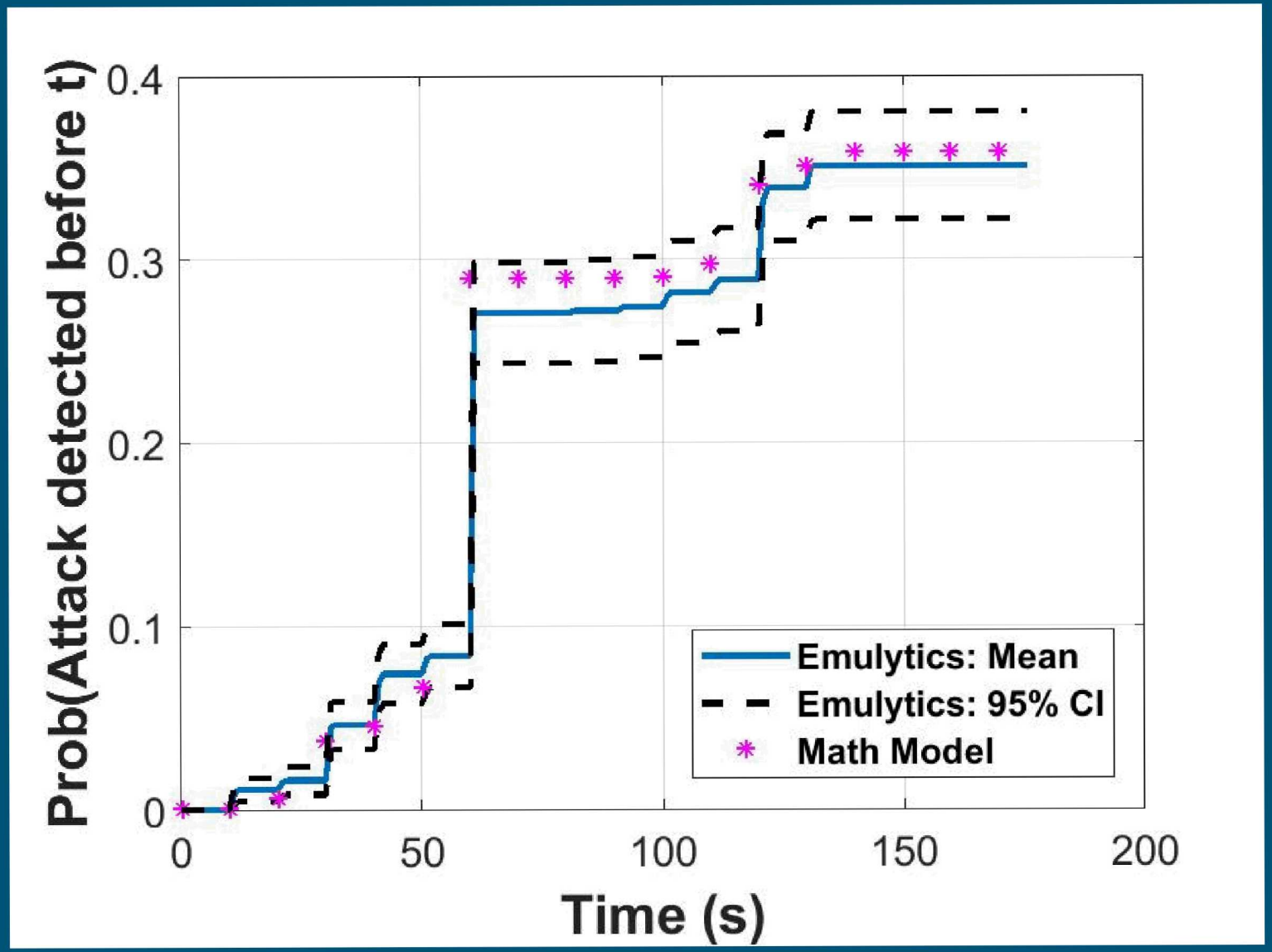
System Parameters
- 24 hosts up
- 4 open (susceptible to CRASH payload)
- 8 closed (inactive RTUs)
- 12 filtered (active but firewalled)
- Timeout prob: 0.1

Nmap setting
- Host group: 4
- Scan delay: 10s
- Max timeouts: 2

Snort sfportscan setting: low

1000 Emulytics Runs

Results: Detection Probabilities



System Parameters
- 24 hosts up
- 4 open (susceptible to CRASH payload)
- 8 closed (inactive RTUs)
- 12 filtered (active but firewalled)
- Timeout prob: 0.1

Nmap setting
- Host group: 4
- Scan delay: 10s
- Max timeouts: 2

Snort sfportscan setting: low

1000 Emulytics Runs

Summary and Insights Gained

Development of credible cyber threat models is one of SECURE's goals

This effort modeled the reconnaissance portion of a hypothetical grid attack

- Used Emulytics and mathematical models to model scanning and detection
- Model co-development benefitted each approach

Challenges:

- Discrete vs. continuous time comparisons
- Scale

"Simple" example exhibited more complexity than was expected.

Backups

Mathematical Model: Step 2, select RTUs to scan