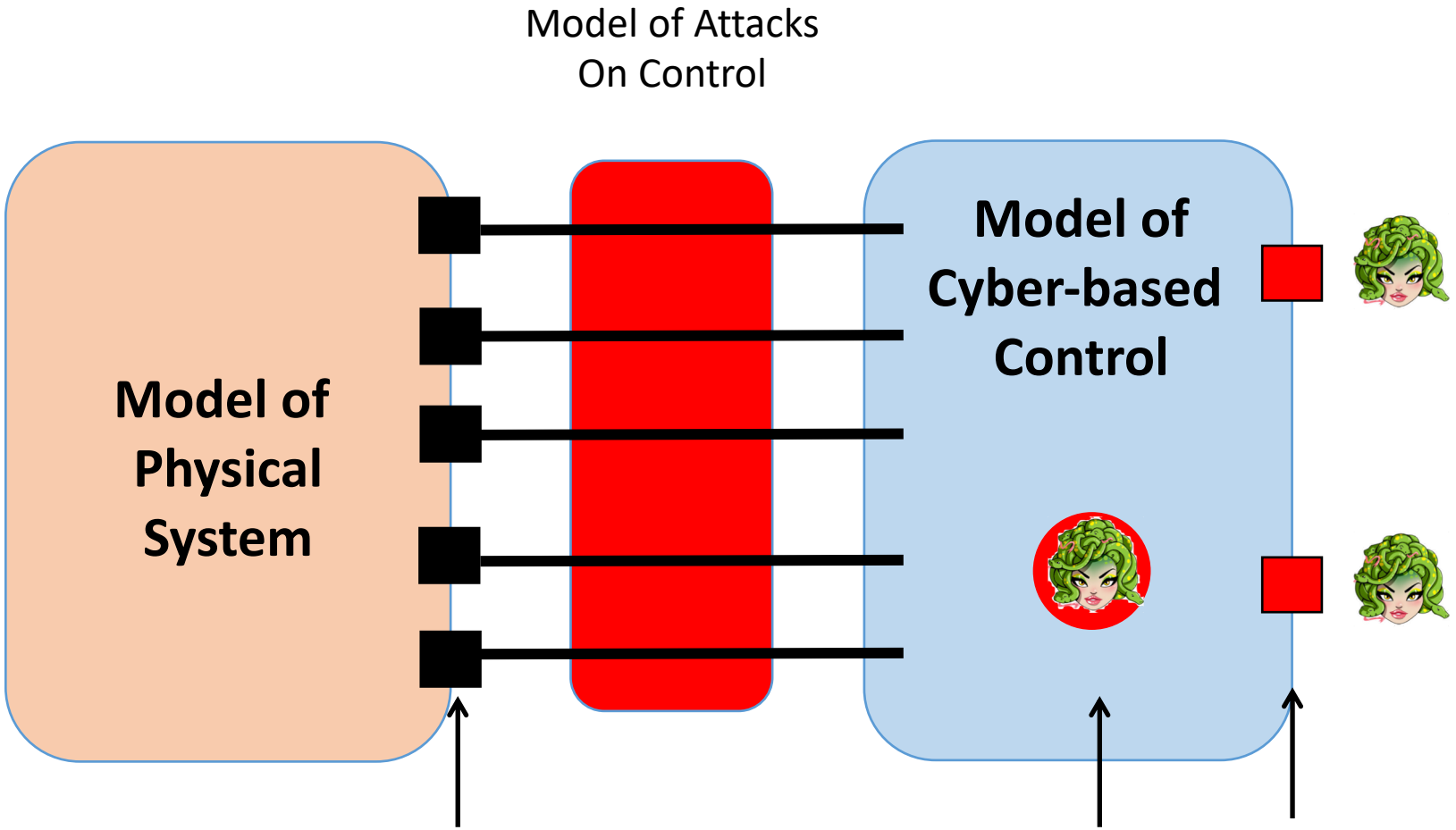
ILLINOIS
Information Trust Institute

David M Nicol
Franklin W. Woeltge Professor of ECE
Director, Information Trust Institute
University of Illinois at Urbana-Champaign

Challenges in Quantifying An Adversary's Cyber Access to Critical Infrastructures

Risk Assessment of Network Insecurity

Big Picture



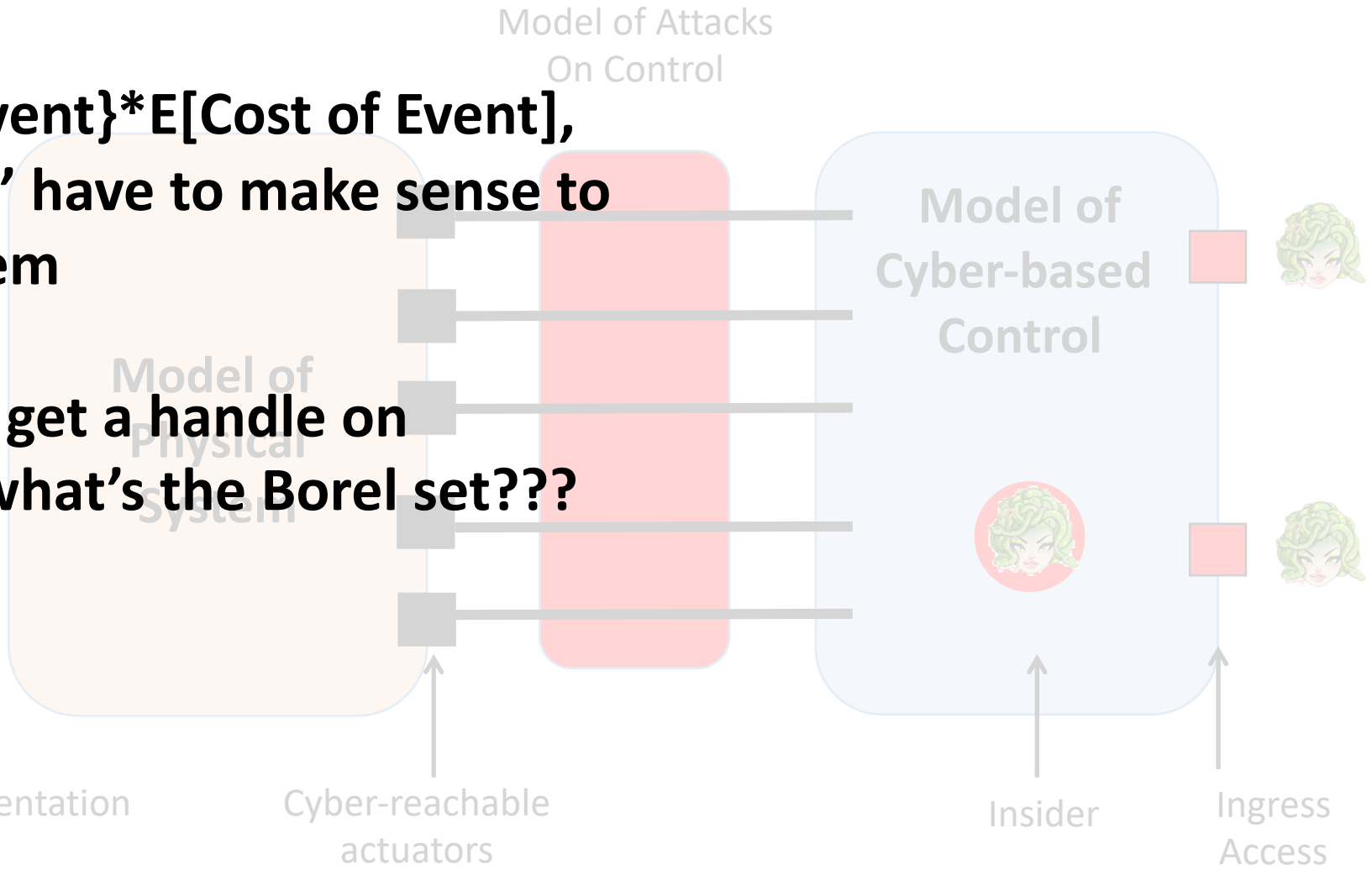
"model" means representation
In a computer

Risk Assessment of Network Insecurity

Big Picture

If Risk = Pr{Event}*E[Cost of Event], units of "cost' have to make sense to physical system

Aside: I can't get a handle on Pr{Event} … what's the Borel set???



Risk Assessment of Network Insecurity

Power Generation

Model of Attacks On Control

Model of Cyber-based Control

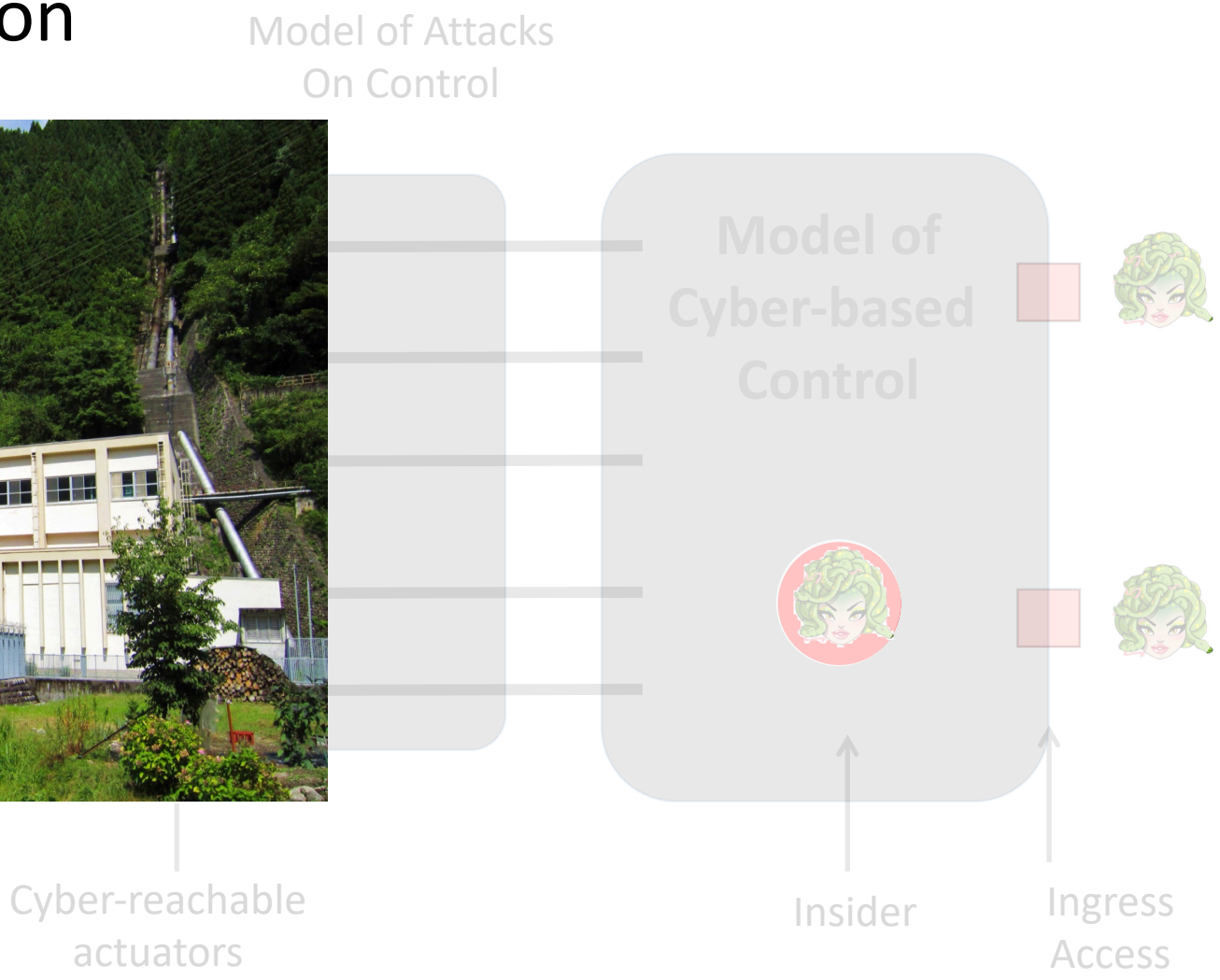
Cyber-reachable actuators

Insider

Ingress Access

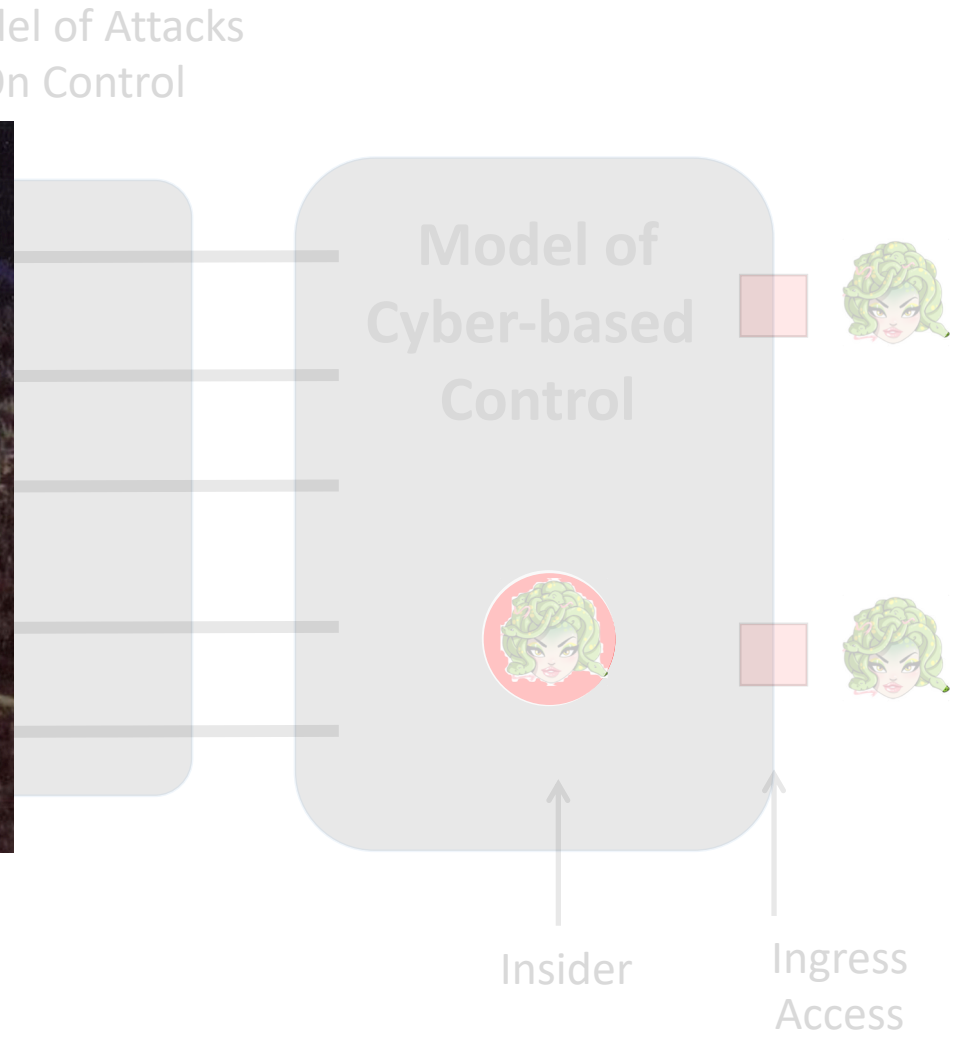
Risk Assessment of Network Insecurity

Power Transmission



Risk Assessment of Network Insecurity

Dams



Risk Assessment of Network Insecurity

Manufacturing

Model of Attacks On Control

Model of Cyber-based Control

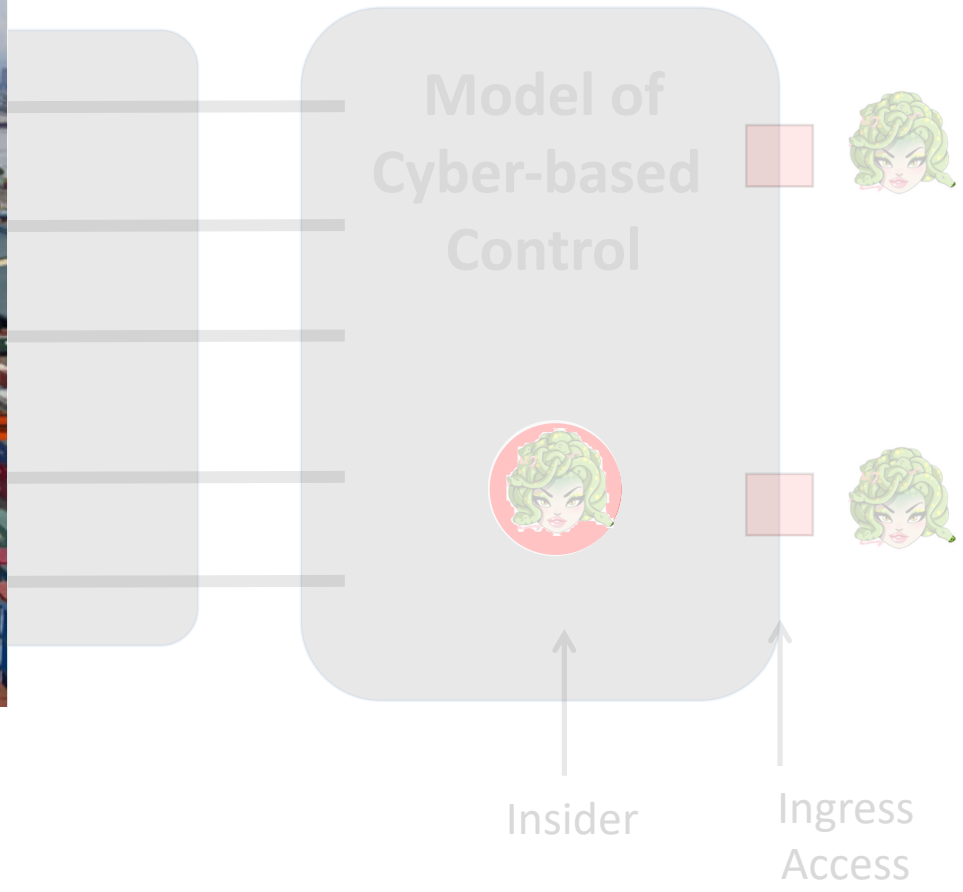
Cyber-reachable actuators

Insider

Ingress Access

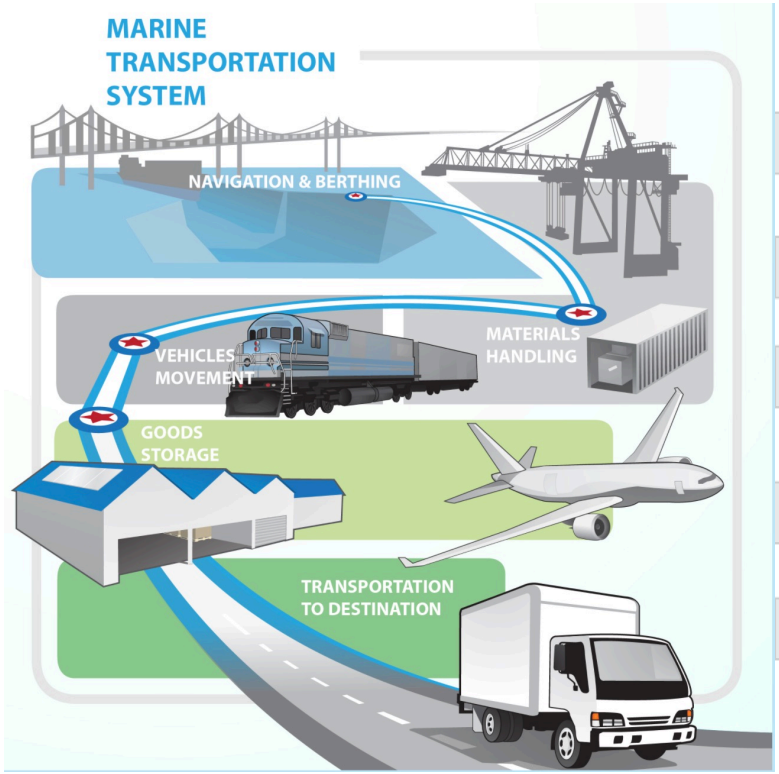
Risk Assessment of Network Insecurity

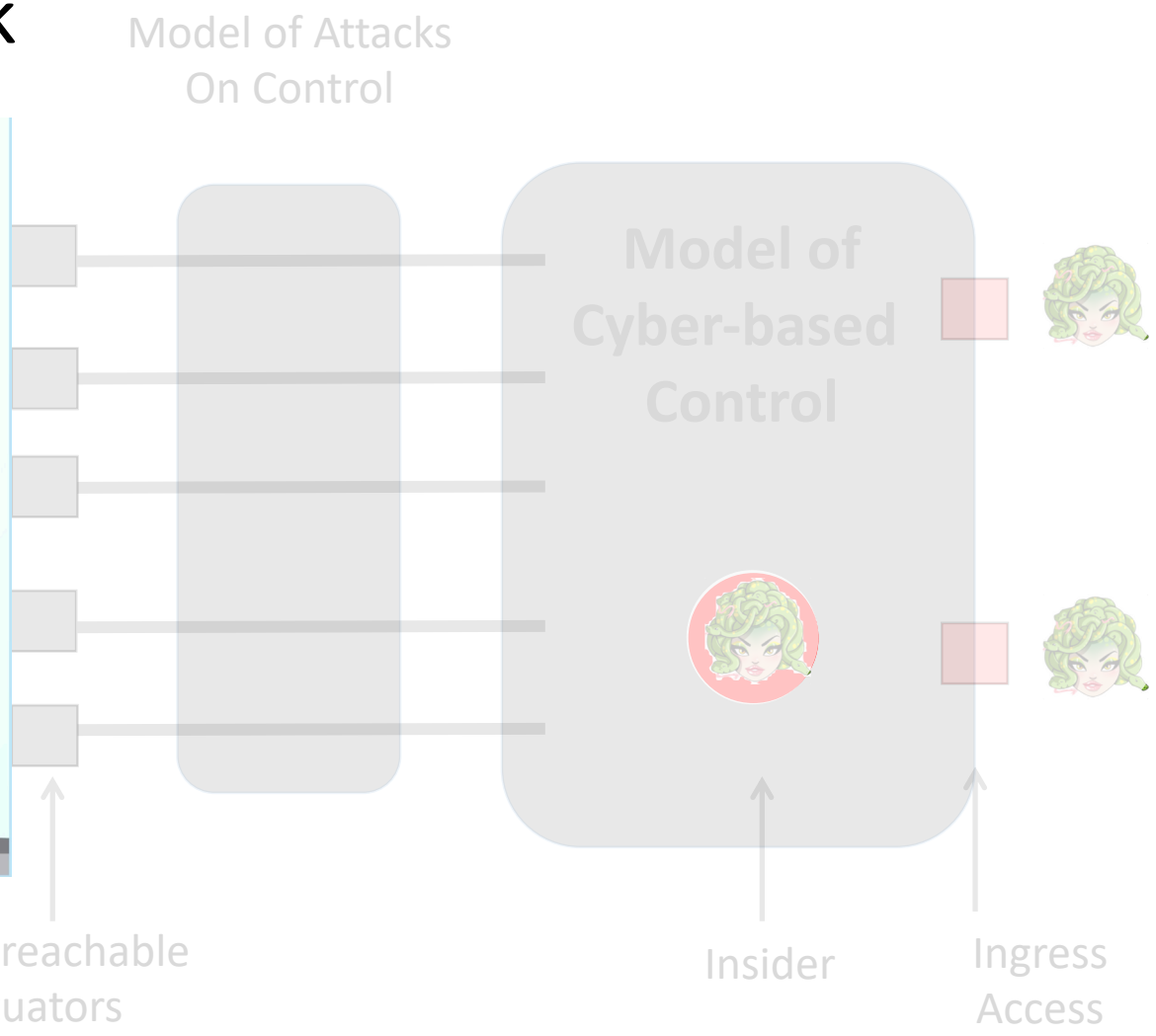
Container Management



Risk Assessment of Network Insecurity

Transportation Network

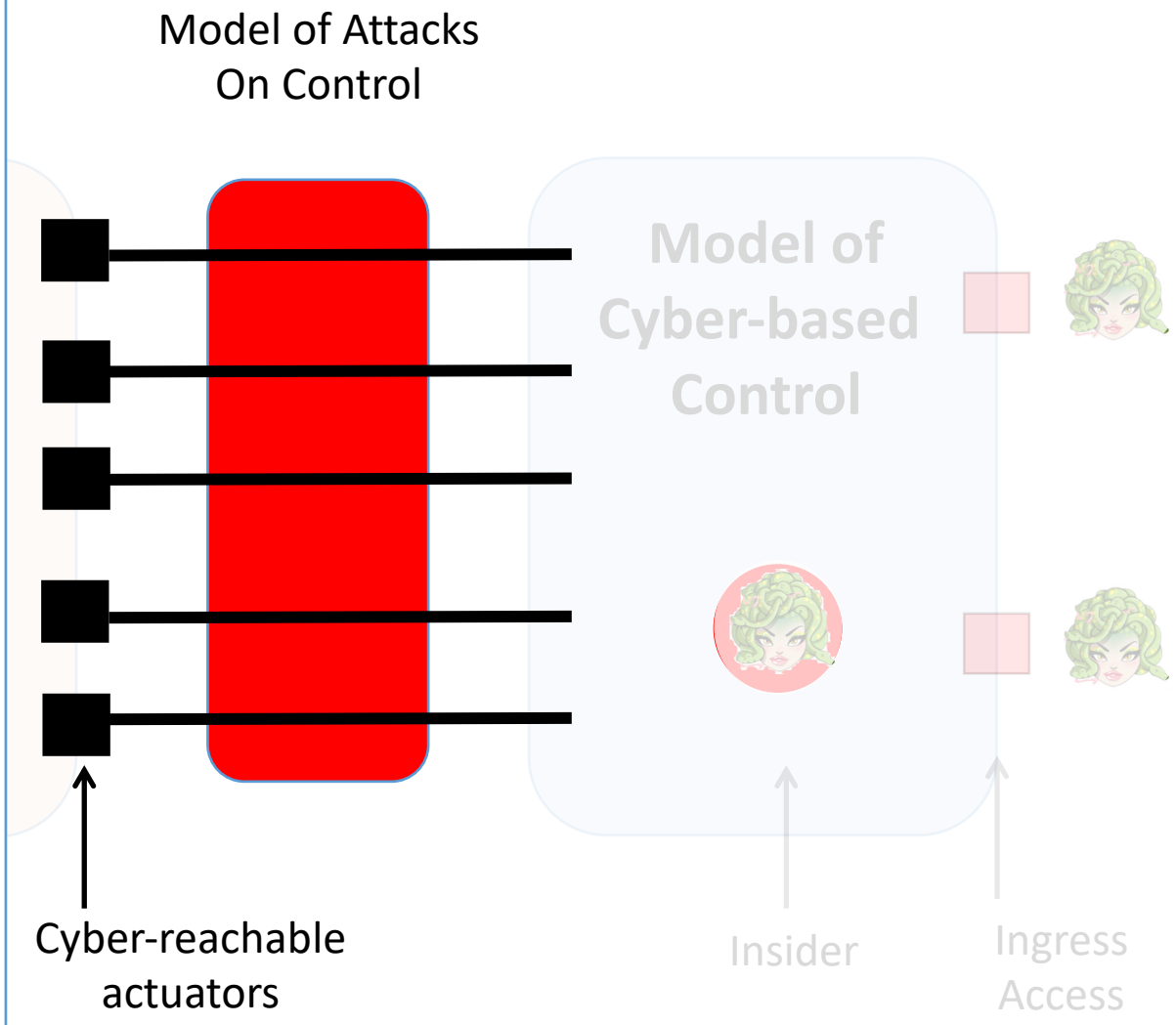




Models of cyber-attack impact on actuators

Classes of attacks include

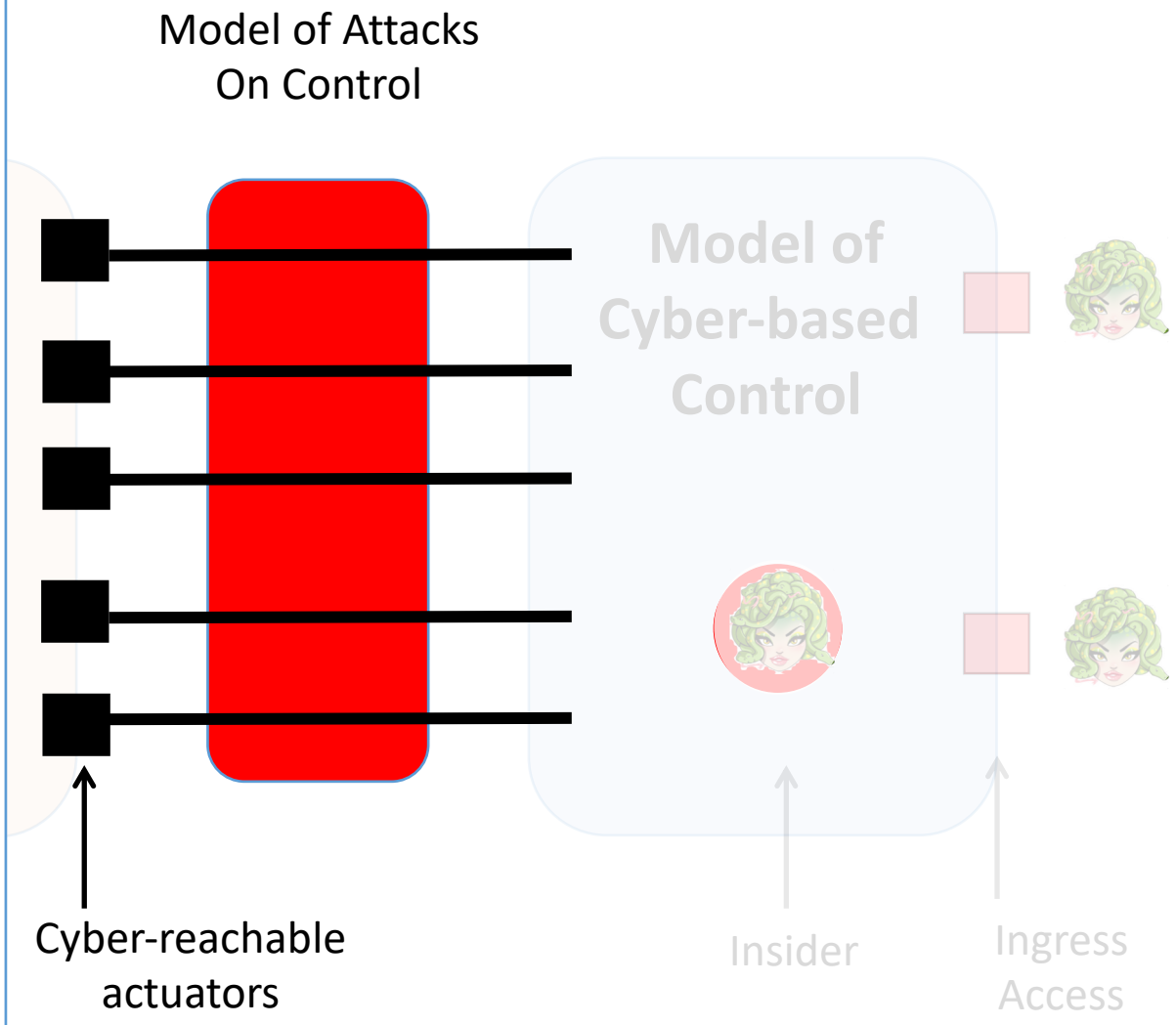
- Denial of access
  - DOS on network
  - Input causing failure
- Malicious commands
- Corrupted firmware
- Cycling of commands
- Replay of commands
- Corrupted data
- **Coordinated attacks on multiple actuators**



Models of cyber-attack impact on actuators

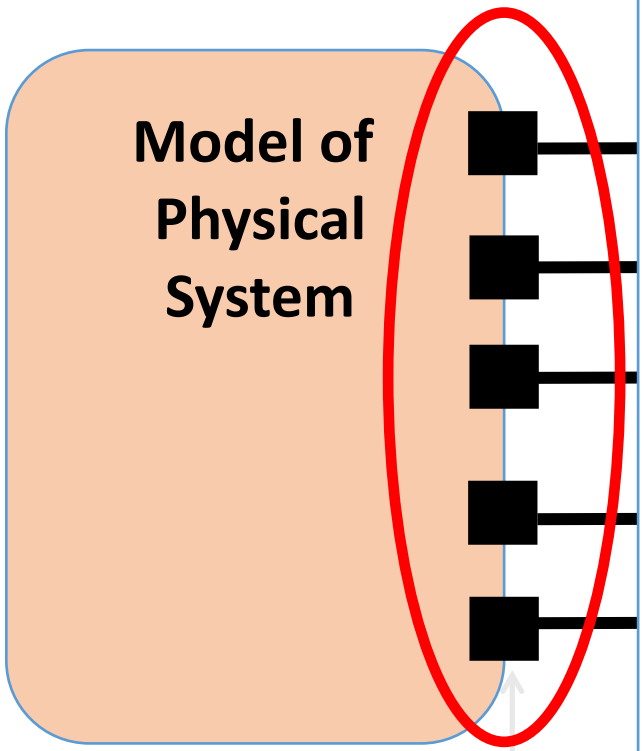
Each actuator in one of four states (from CVSS vulnerability report)

- Uncompromised
- Compromised with no execution privileges
- Compromised with low execution privileges
- Compromised with high execution privileges



Risk Assessment of Network Insecurity

Characterize intersection of cyber and physical components



What actions can actuators implement?

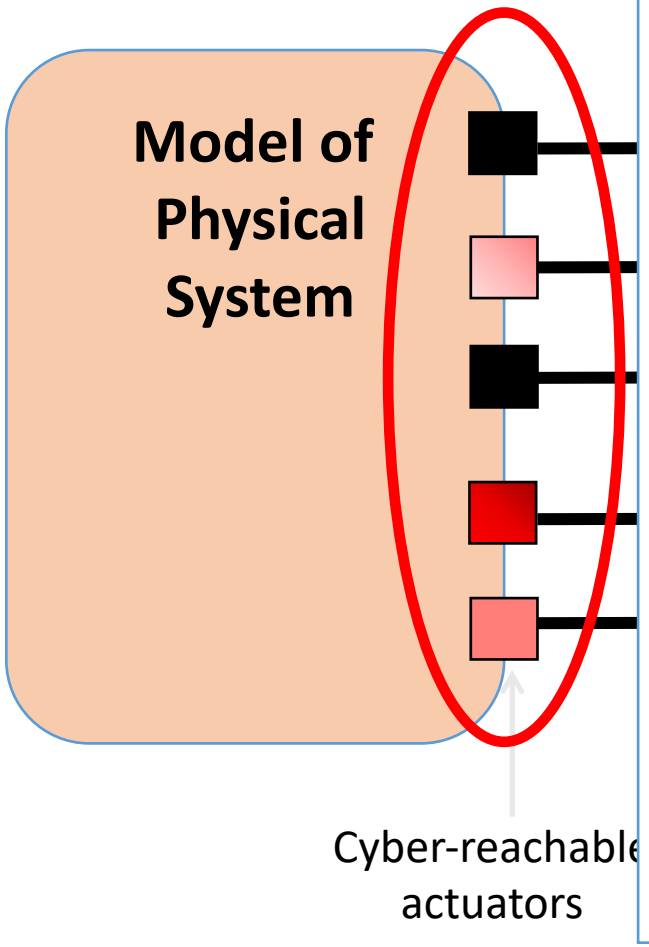
e.g.

- Breakers in power system affect flow topology
- LNG pump moves liquid or not
- Ship throttle affects engines
- Robot control moves arm, opens/closes grabber

Cyber-reachable actuators

Risk Assessment of Network Insecurity

Characterize intersection of cyber and physical components



For a given **Compromise Vector** (subset of actuators at a given selection of compromise states)

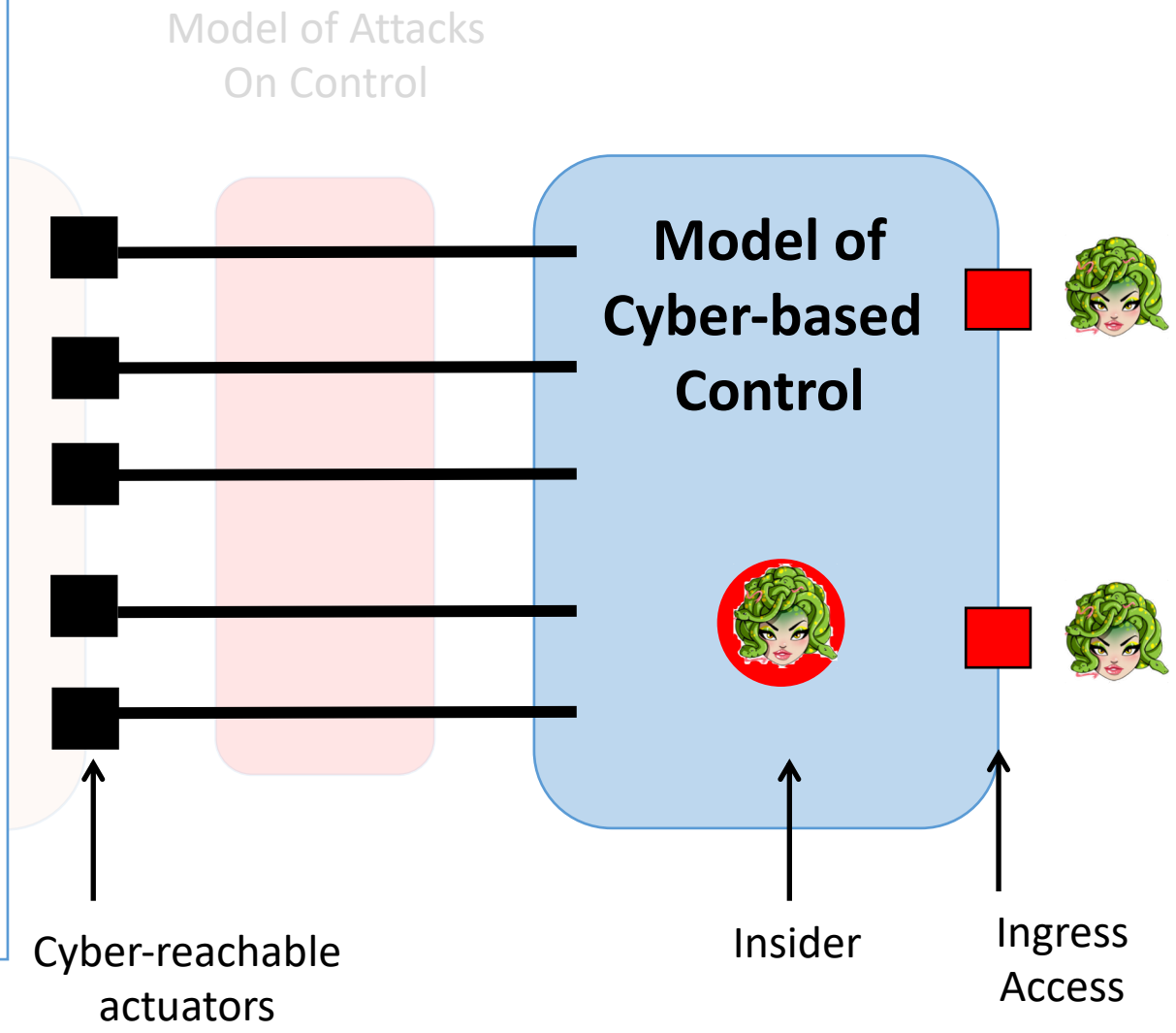
- What attacks are possible on physical system
  - For each attack, what is the cost (in units meaningful to the physical system) of a successful attack?
- Note added realism but added complexity of multiple actuators, each with multiple possible states

Risk Assessment of Network Insecurity

Determine cyber access to actuators

Include what you can, e.g.

- Connectivity information w.r.t. access control
- Knowledge of software running on network devices
- Vulnerability information about known services



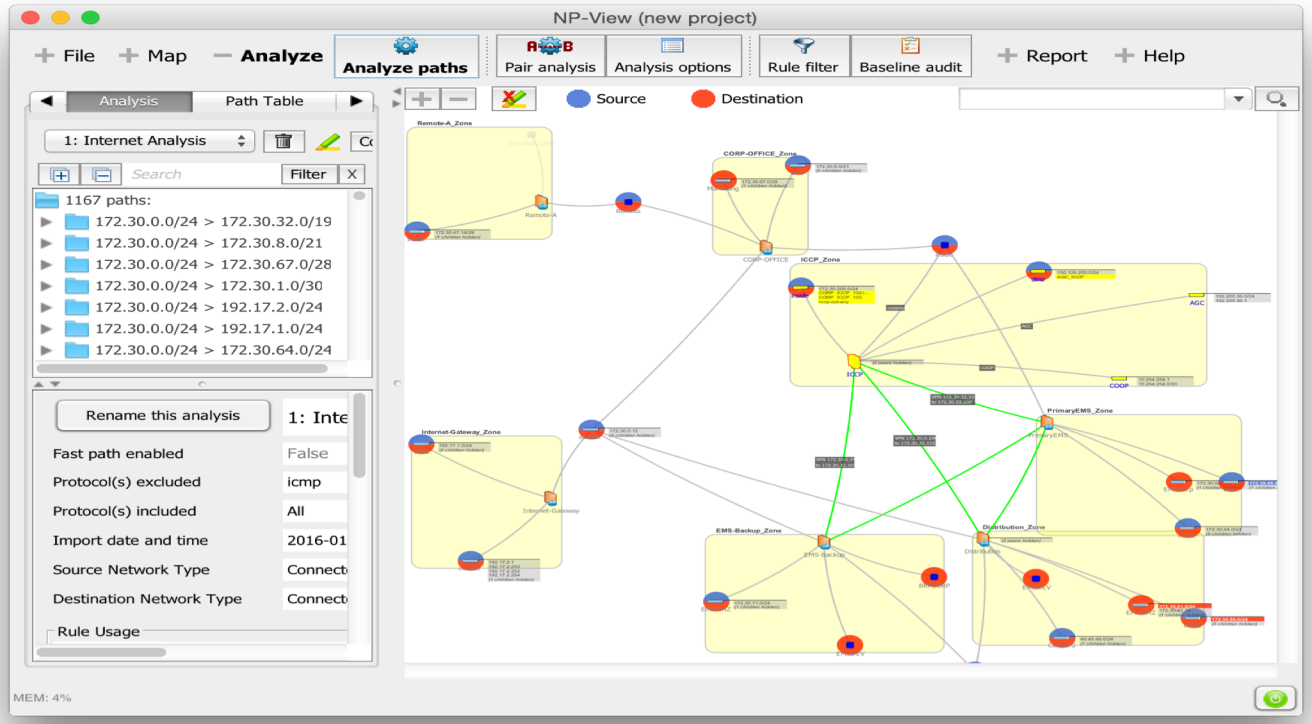
Access Through Network

Computer network may have multiple zones, access control

- For external access to actuators we need to consider lateral movement

All of the individual steps permitted by the access control rules:

- (srcIP,srcPort,protocol) -> (dstIP,dstPort,protocol)



Access Through Network

Models of vulnerability (per service) at hosts

Common Vulnerability Scoring System (CVSS)

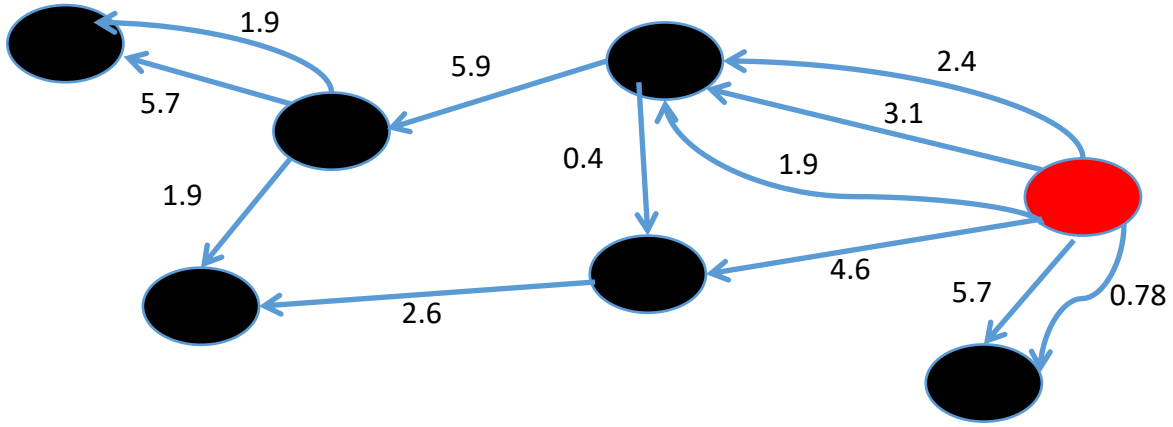
- Industry standard for scoring
- NIST assessment in National Vulnerability Database (NVD)
- Different metric groups, e.g.

AccessVector (A_v)	local access required	0.395
	accessible from adjacent network	0.64
	accessible from remote network	1.0
AccessComplexity (A_c)	high	0.35
	medium	0.61
	low	0.71
Authentication (A_a)	requires multiple authentications	0.45
	requires single authentication	0.56
	no authentication required	0.704

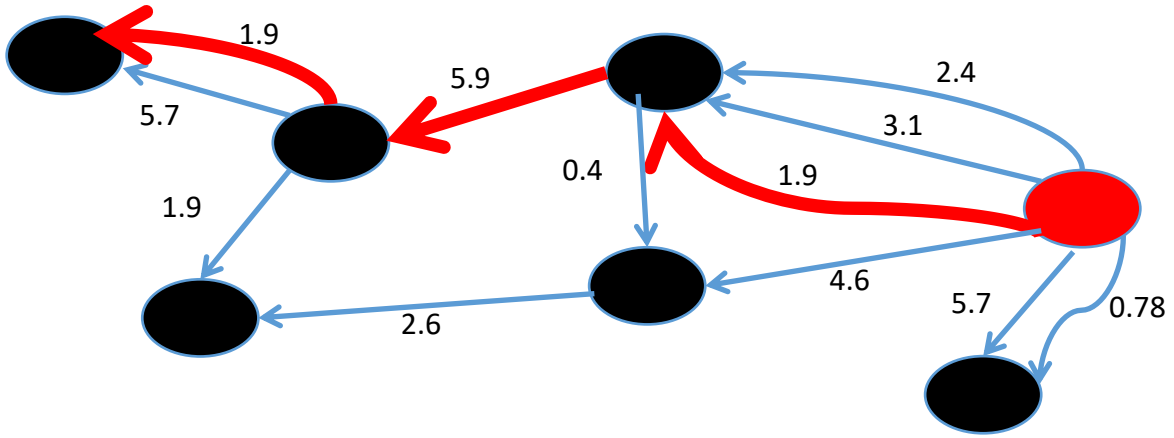
Access Through Network

In principle one can *sometimes*

- Scan the network for applications and vulnerabilities
- Score each in terms of access required and access complexity
- Leads to a graph
- Nodes are hosts, edges correspond to permitted connections and a vulnerability
  - An attacking host may have multiple points of entry to a victim
  - Weights designed to say something about difficulty of exploiting
  - From CVSS ascribe compromise state as result of exercising vulnerability
    - Compromise state depends on vulnerability exercised



Access Through Network



Attacker uses “stepping stone” attack (lateral movement) to get through access control points

One is naturally led to think about paths and path costs, but there be dragons

- Is “shortest path” a good metric?
- Is “all paths” a good metric?
- Exploit difficulty may be state dependent

Exploit Difficulty may be State Dependent

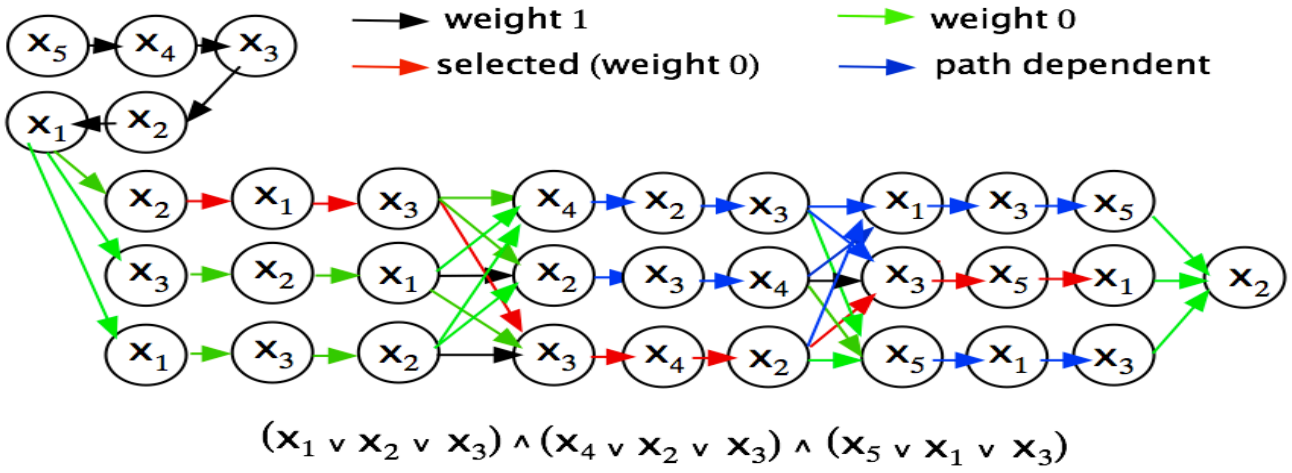
- An attacker learns how to exploit a given vulnerability, the “next” ones are easier
- An attacker may be detected by one exploit, triggering defender actions that make other exploits harder
- Graph edge weights may change as a function of history (i.e., existing stepping stone path)

Theory Stuff

Theorem 1 Let (G, E) be a directed multi-graph, with every edge $e \in E$ labeled with non-negative weight $w(e)$. Suppose $E_1, E_2, \ldots, E_{k-1}$ is a non-cyclic stepping stone path and consider a host h_k not yet visited but is accessible from the last host h_{k-1} in the path. For every v in $chan_{k-1,k}$ suppose that if v appears in any prior step, then the cost of exploiting v is no larger than its edge weight in (G, E), and may be smaller, as a function of $E_1, E_2, \ldots, E_{k-1}$. Then the problem of finding a min-cost stepping stone path between any two hosts is NP-hard.

Theorem 2 Let (G, E) be a directed multi-graph, with every edge $e \in E$ labeled with non-negative weight $w(e)$. Suppose $E_1, E_2, \ldots, E_{k-1}$ is a non-cyclic stepping stone path and consider a host h_k not yet visited but is accessible from the last host h_{k-1} in the path. For every v in $chan_{k-1,k}$ suppose that the cost of exploiting v is at least as large as its edge weight in (G, E), as a function of $E_1, E_2, \ldots, E_{k-1}$. Then the problem of finding a min-cost stepping stone path between any two hosts is NP-hard.

Reduction of Monotone XSAT



At an actuator

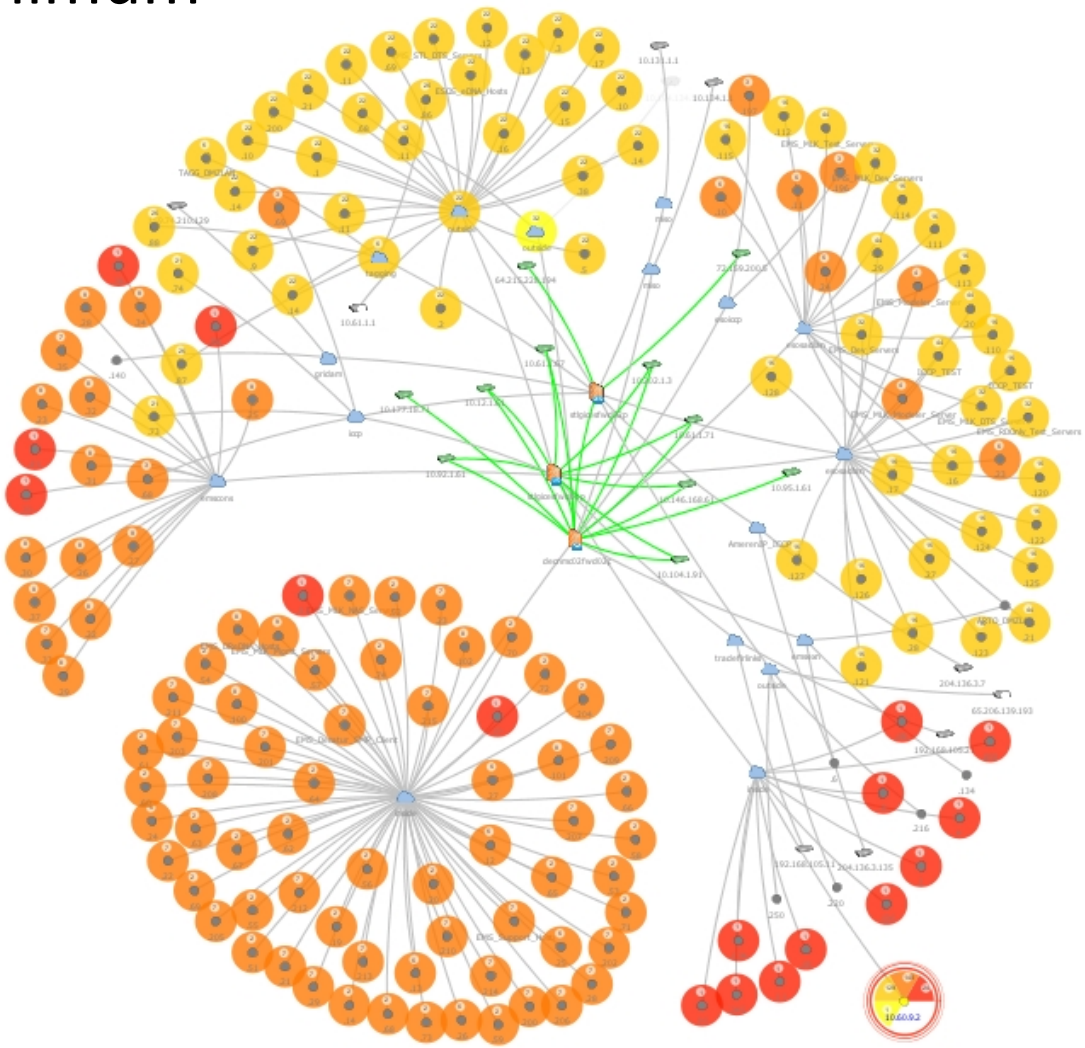
Actual example: color coding describes minimum #exploits needed to touch actuator

Files selected

File	Device	Size
decnmc02fwd02p	cisco	1560 lines
stlgicesfwd01p	cisco	1667 lines
stlgicesfwd02p	cisco	722 lines

Topology summary

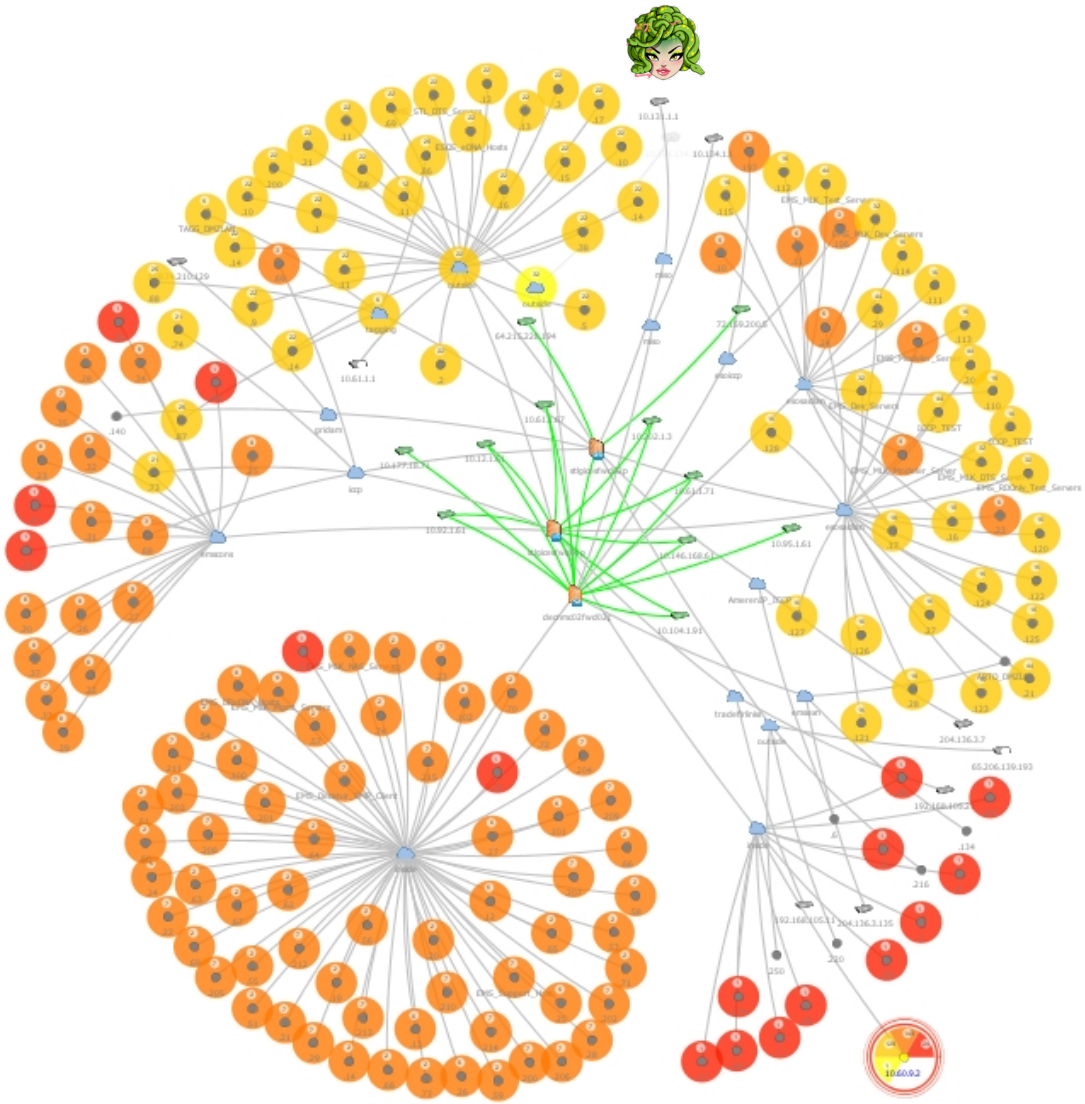
3 Devices
21 Gateways
84 Networks
479 Hosts
42 unmapped IP addresses
3 Border Gateway



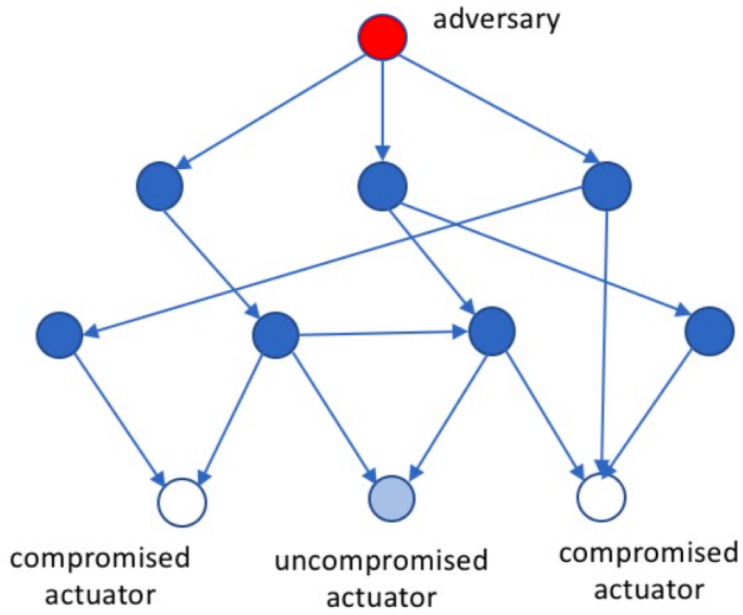
At an actuator

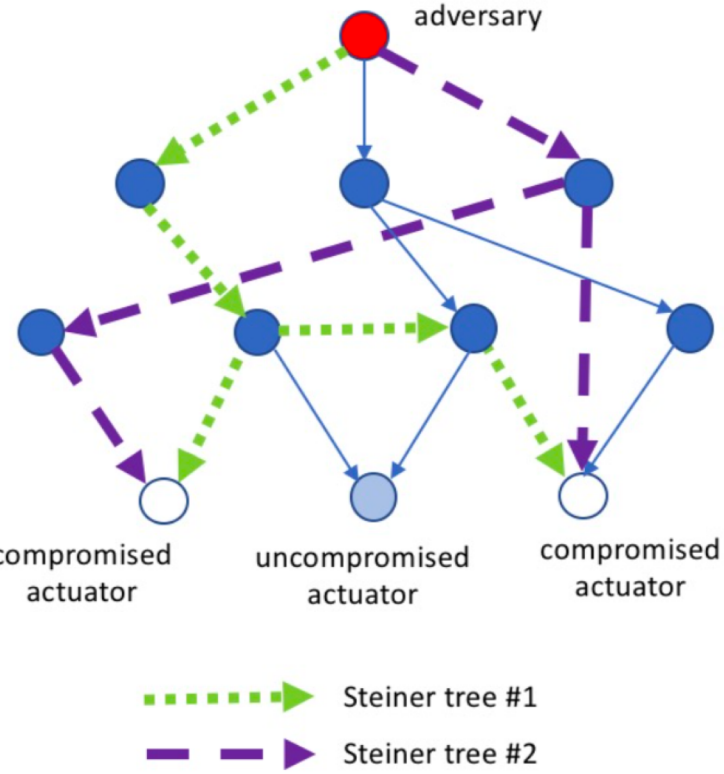
What makes sense to “score” this access?

- Shortest path?
  - Insensitive to breadth
  - Limited to one actuator
  - Computationally tractable only if edge weights are insensitive to exploit history
  - Realistic model of attacker behavior? No….
- What is the analog for correlated attacks?
  - least effort discovery of exploits leading to a ***set*** of actuators
  - Enter Steiner Trees

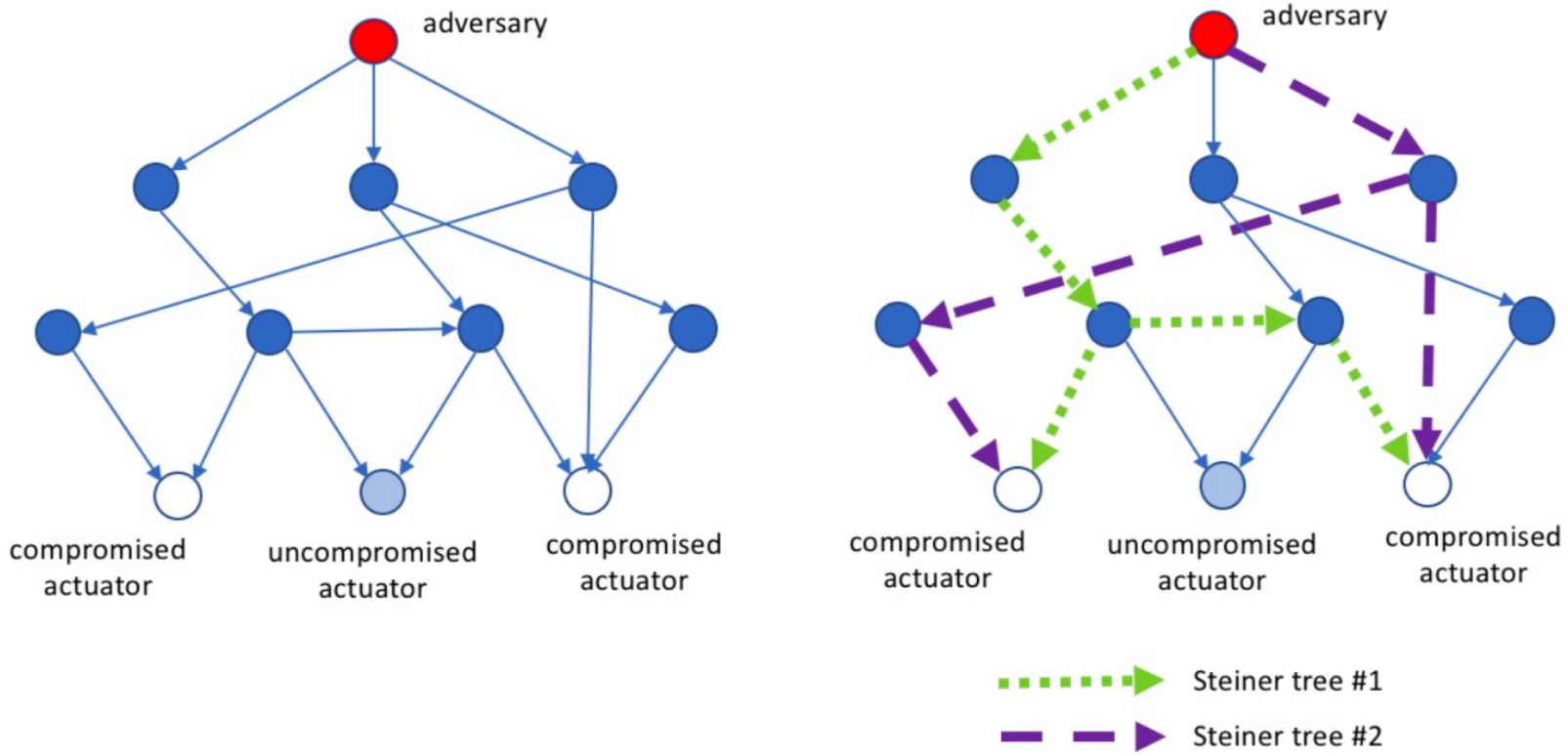


Steiner Tree





Steiner Tree



BUT computation of minimum cost Steiner tree is intractable

- All the disadvantages of minimum cost path amplified

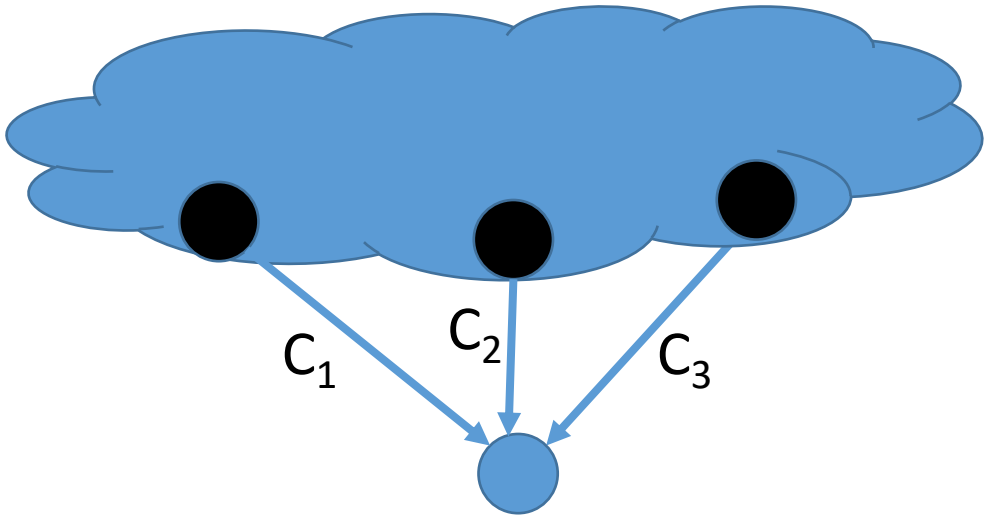
Furthermore, "units" of cost differ from units of impact on physical system

- How do we combine cyber-access to costs to physical system???

Number of paths?

One can compute the total number of unique paths between entry point and actuator

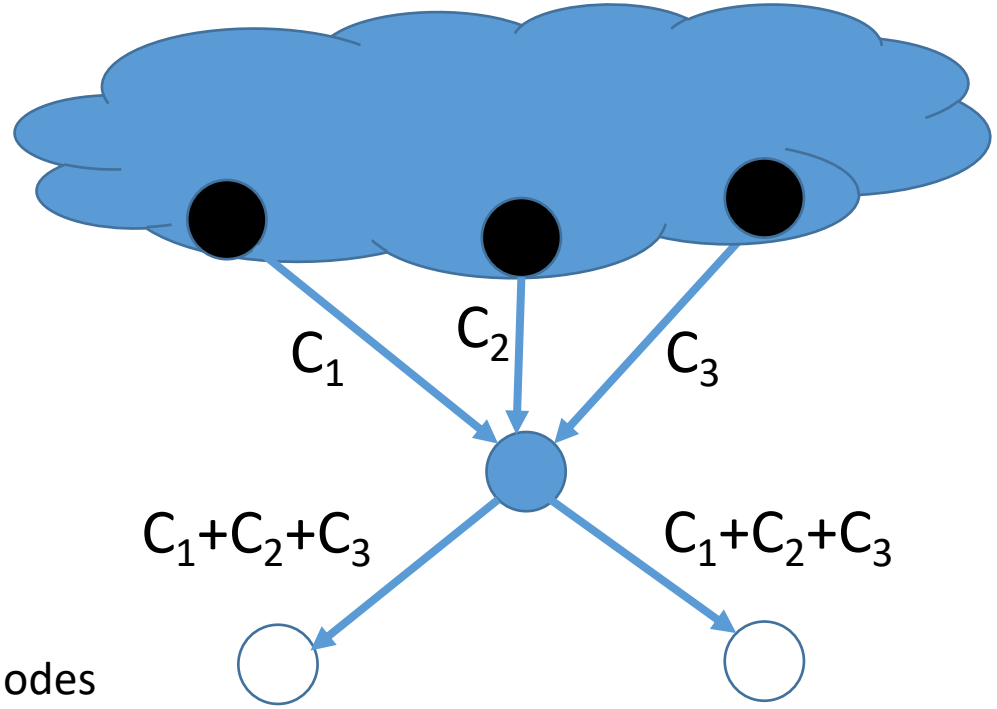
- Breadth-first-search expansion to avoid loops
  - Accumulate counts from nodes in wave-front



Number of paths?

One can compute the total number of unique paths between entry point and actuator

- Breadth-first-search expansion to avoid loops
  - Accumulate counts from nodes in wave-front



Expand aggregate counts to reachable as-yet unvisited nodes

Number of unique paths tells us….?

Problems

- Different paths may share edges
  - We might compute or estimate the number of edge-disjoint paths, but…

- Suppose we take a system with vulnerabilities that led to 100,000,000 paths, and then patch vulnerabilities or apply controls that reduces the number of paths to 1,000,000 …. Is the system 100x more secure ?

- The question of combining analysis of cyber-access with impact on physical system remains

Access Through Network

One approach is to compute a lower bound on time of access through network by removing decision making from model---every branch taken as “soon as possible”

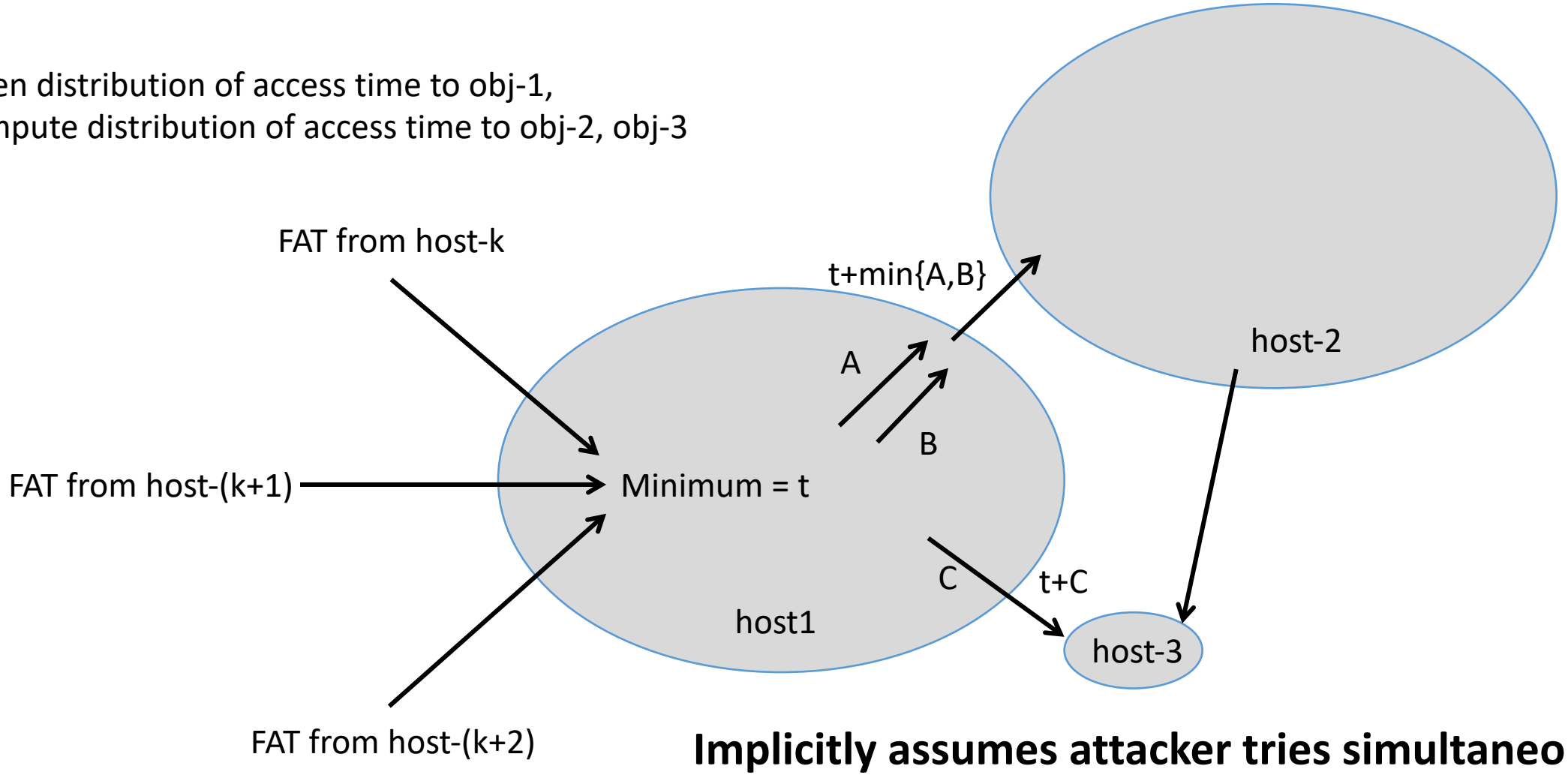
Somehow associate exploit time distributions on vulnerability edges

For each node now consider the ‘First Access Time’ (FAT) distribution from a given attacker ingress point

FAT impacted by both shortest path and number of paths

At a host

Given distribution of access time to obj-1,
Compute distribution of access time to obj-2, obj-3



Implicitly assumes attacker tries simultaneously to exploit all vulnerabilities at wavefront of compromised hosts

Computational challenges

Can formalize using structure of Bayesian networks

- Key idea to use is conditional independence in computation
- Computational complexity depends on structure of network interdependencies
  - Worst case is bad

Practical idea

- Estimate FAT with histogram obtained by Monte Carlo sampling of access time distributions
  - Shortest path defines FAT
  - But need to assume independence of access time distributions among the random variables
    - But coupling is OK, e.g., could give times related to same vulnerability the same time

At an actuator

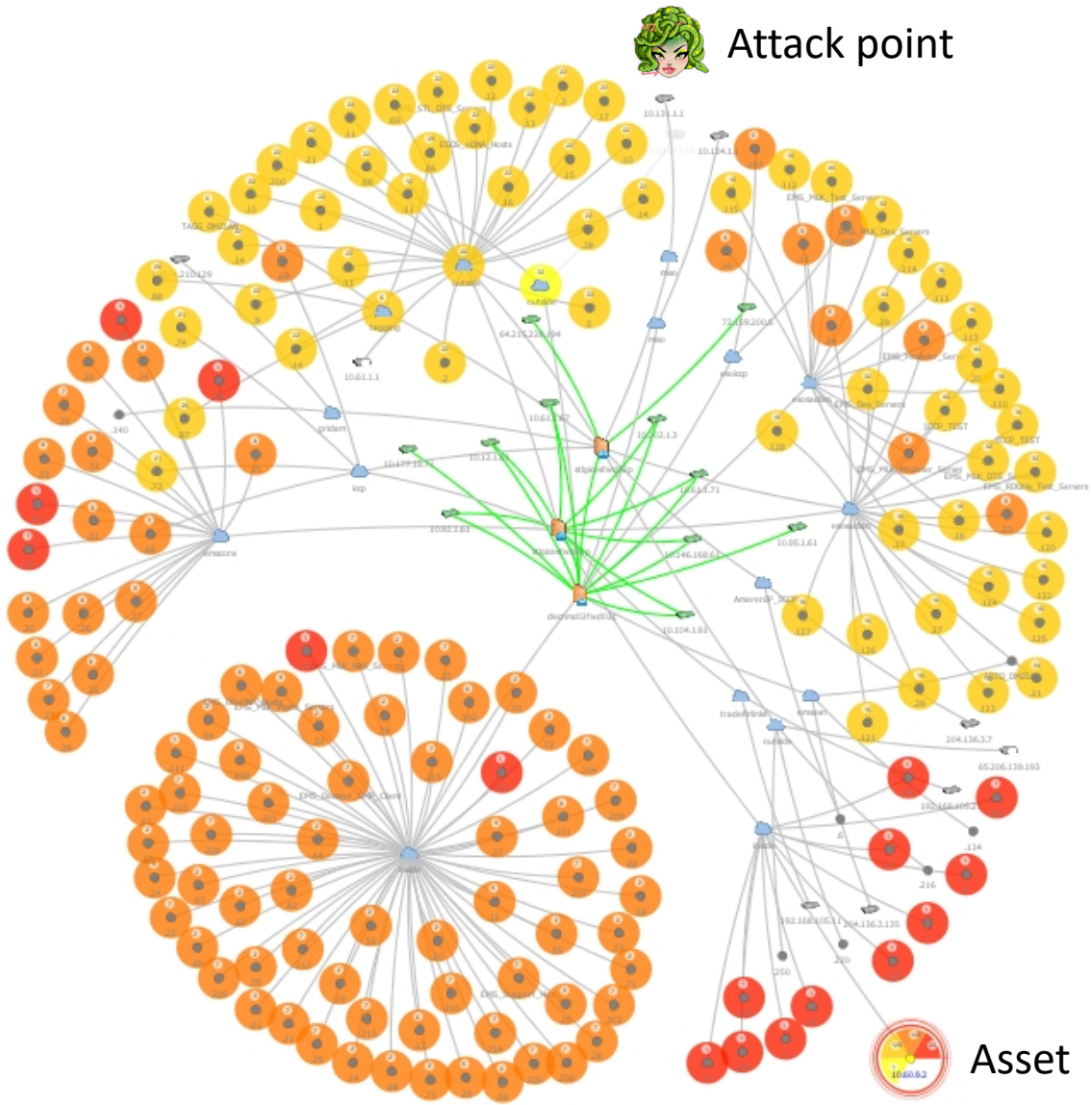
Actual example

Files selected

File	Device	Size
decnmc02fwd02p	cisco	1560 lines
stlgicesfwd01p	cisco	1667 lines
stlgicesfwd02p	cisco	722 lines

Topology summary

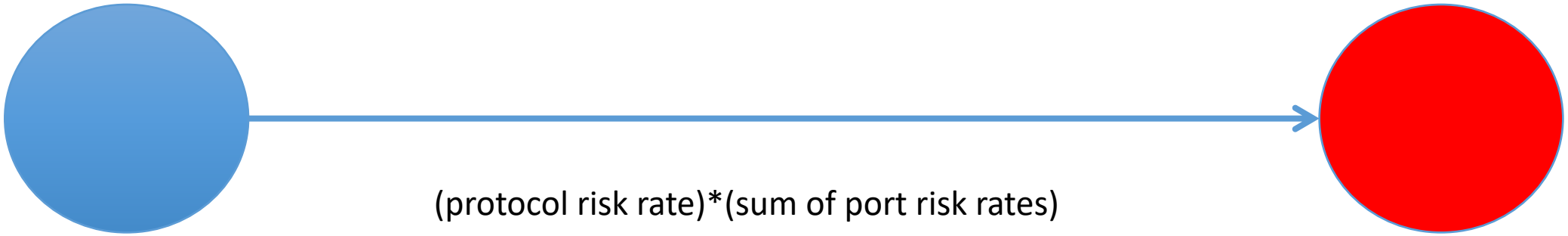
3 Devices
21 Gateways
84 Networks
479 Hosts
42 unmapped IP addresses
3 Border Gat



FAT Estimation

Completely fabricated cost ***rate*** function to graph edges….

- Risk factor assigned to protocols (highest risk to ‘any’, tcp, udp)
- Risk factor assigned to ports
  - High risk : ftp, gopher, login, uucp, telnet, http
  - Use risk : ssh, sftp, https
  - All others, marginal, based on logarithm of range

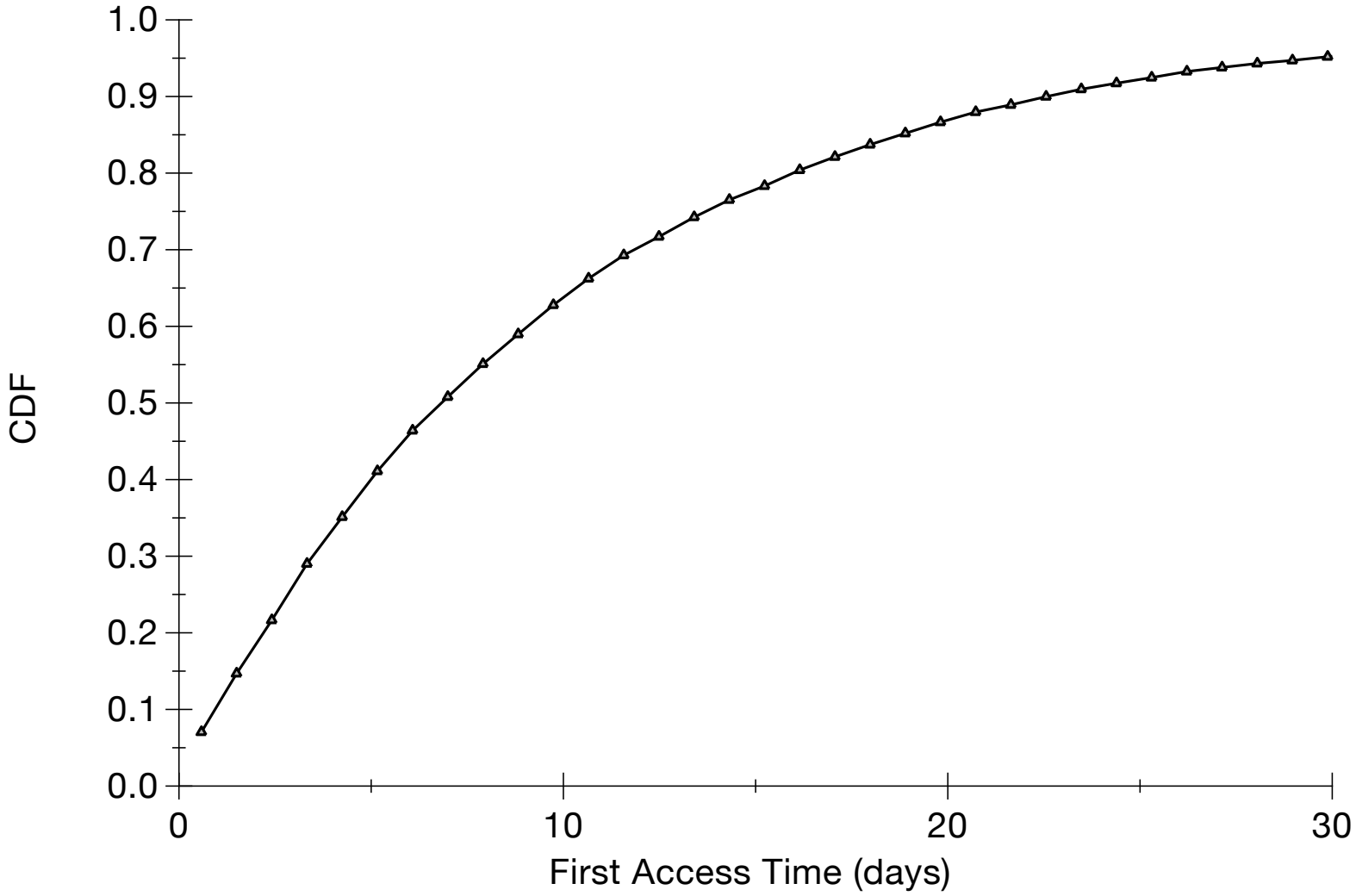


Use Monte Carlo simulation that samples edge costs from exponential, defines FAT as shortest path to asset from any attacker

FAT curve, access from designated ingress point

50% of FAT metric accumulates in just over 1 week

Inspection reveals FAT time is overwhelmingly dominated by time to overcome single connection from ingress point

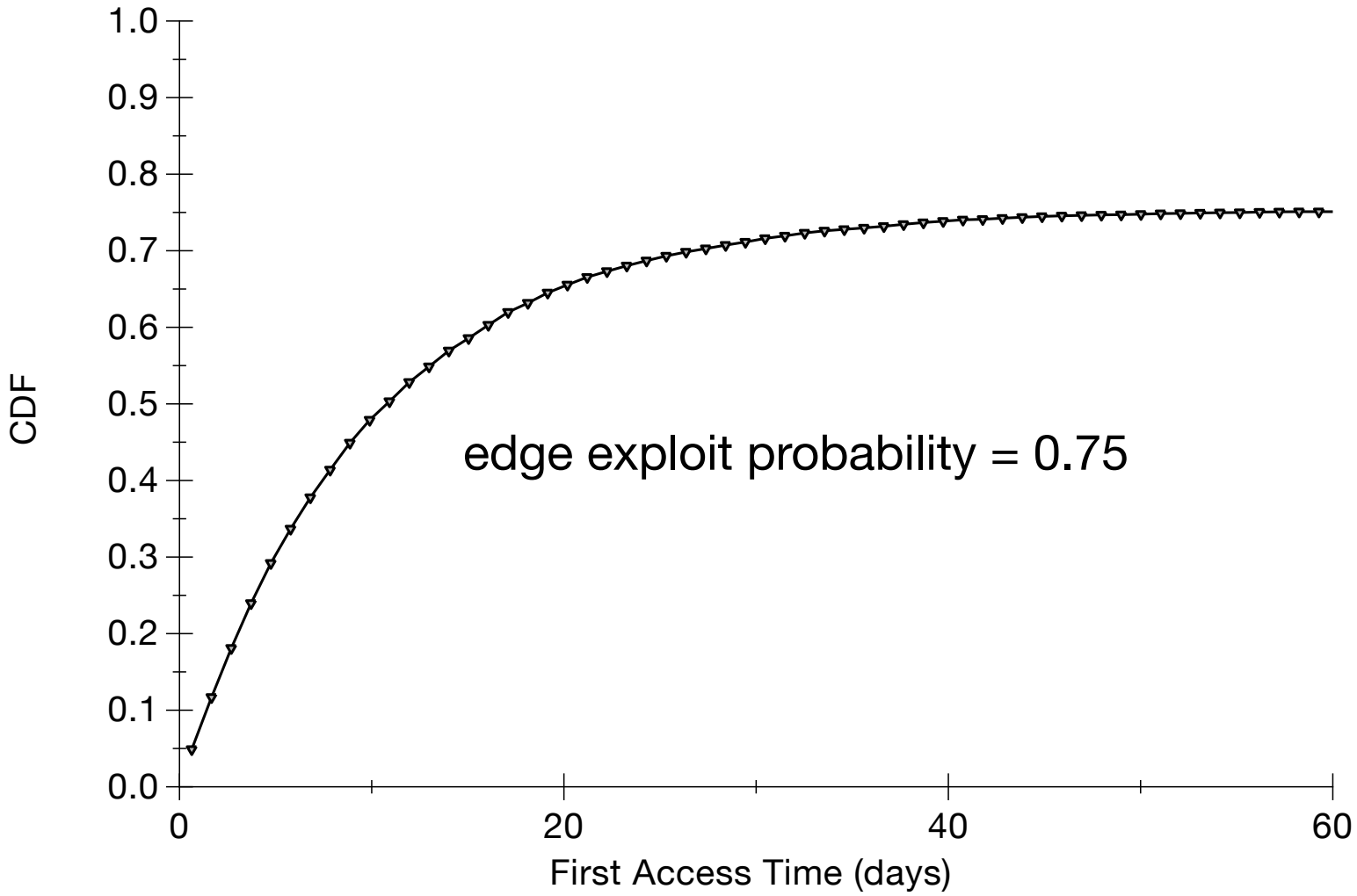


FAT curve, access from designated ingress point

50% of FAT metric accumulates in 2 weeks

Each experiment flip coin on whether an edge can be traversed

We will shortly revisit this issue of uncertainty in edge existence



Network paths analysis made an critical assumption

It assumed you

- Know with certainty when there are connections between hosts
- Know with certainty when a host has an exploitable vulnerability
- Know with certainty the impact on flows of filtering rules (e.g. firewalls, routing)

Network paths analysis made an critical assumption

It assumed you

- Know with certainty when there are connections between hosts
- Know with certainty when a host has an exploitable vulnerability
- Know with certainty the impact on flows of filtering rules (e.g. firewalls, routing)

You don’t

Our approach to uncertainty quantification

Generalize and apply the notion of ‘uncertain graphs’

- A standard UG ascribes an (independent) existence probability to each potential edge
- You can ask questions about the probability of an s-t connection

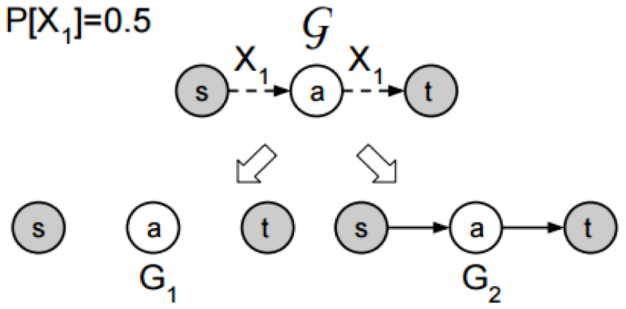
Our extensions

- Use expressions of random (Bernoulli) Booleans to describe edge existence probability
  - Allows for edge existence correlations, e.g., due to common vulnerability
- Extend Bernoulli Booleans to be “Beta Booleans”
  - Use Beta distribution shape to quantify level of knowledge about edge existence probability

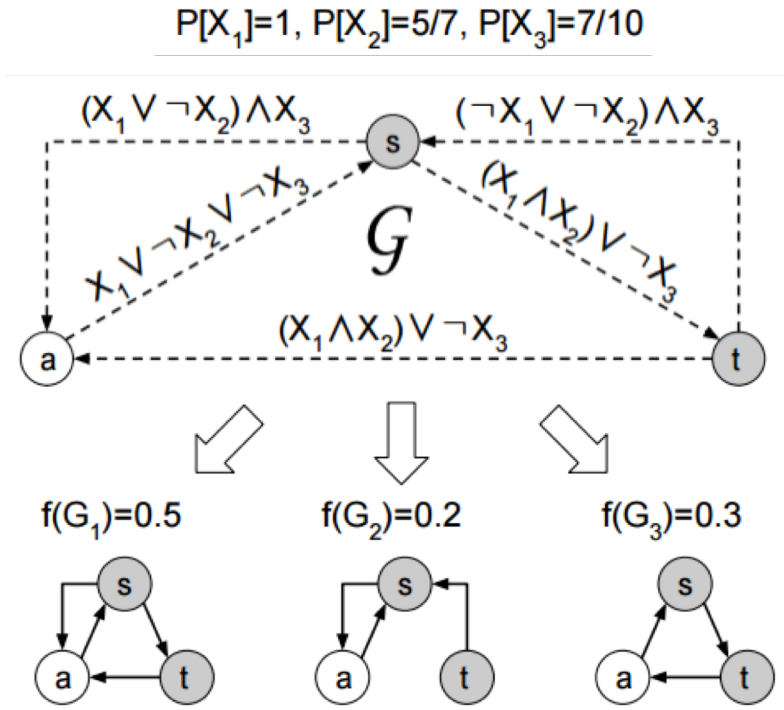
Edge Existence Correlation

- **Question 1:** How to capture correlation among edges in an UG?
  - Associate edges with Boolean function of indicator random variables
  - We call them the **extended** UGs

Example 1:



Example 2:



Beta Binomial Model

Cons:

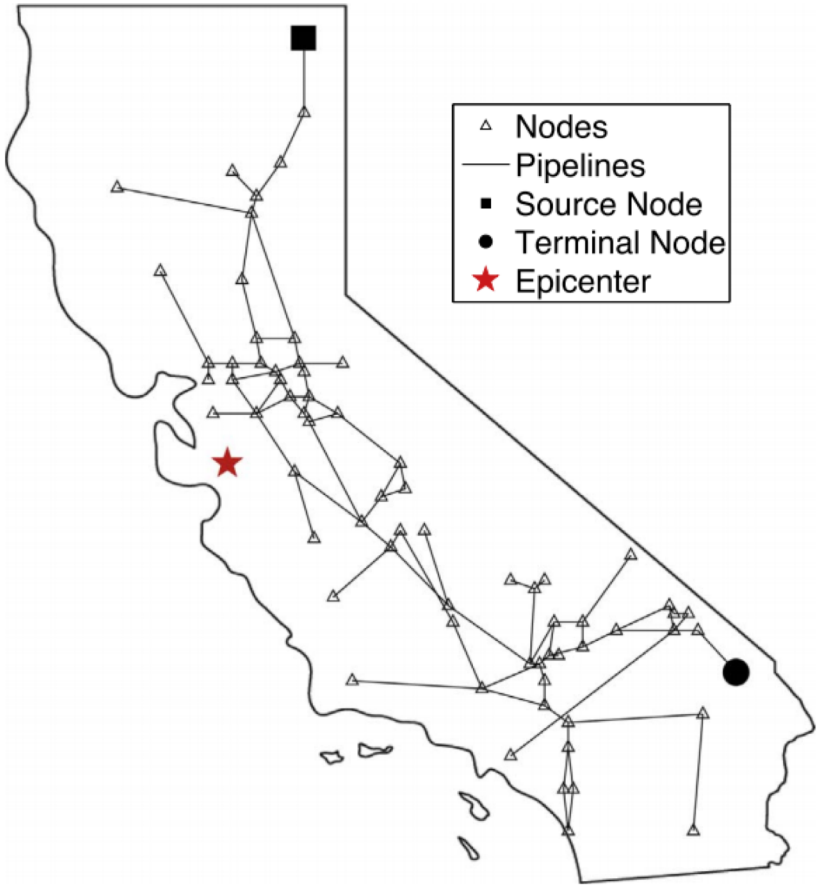
- Beta distribution not closed under operations used to establish path connectivity
  - BUT (!) we developed very good approximation techniques when edge correlation is monotone

Pros:

- Use of MC sampling to estimate *parameters* of distribution yields an order of magnitude improvement in computational effort over naïve MC to get same quality of result

Case Study: Pipeline disruption and earthquake

Example: California gas distribution network

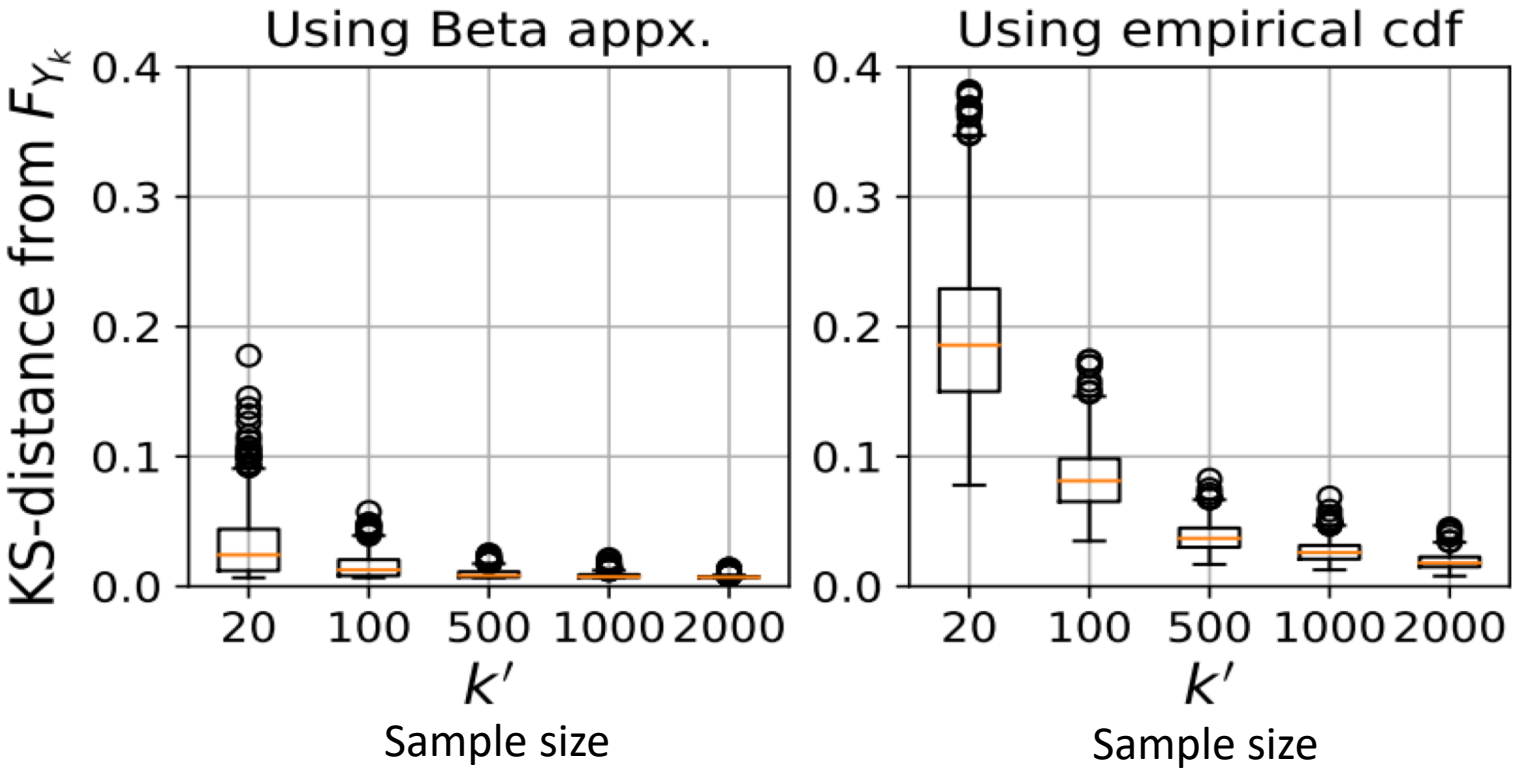


- Adopted from

  Stern, R. **Accelerated Monte Carlo system reliability analysis through machine-learning-based surrogate models of network connectivity**, Reliability Engineering & System Safety (2017).
- Total 87 pipelines
- Various optimizations to construct reliability polynomial
  - For a given set of edge probabilities one can exactly compute the s-t connection probability
  - You get a *distribution* for the s-t probability when the edge probabilities are themselves distributions (to capture uncertainty in the edge probabilities estimation process)
- Data obtained from 6.5 degree earthquake
  - Paper estimates mean Pr., we randomly added variance
- Total 100,000 samples

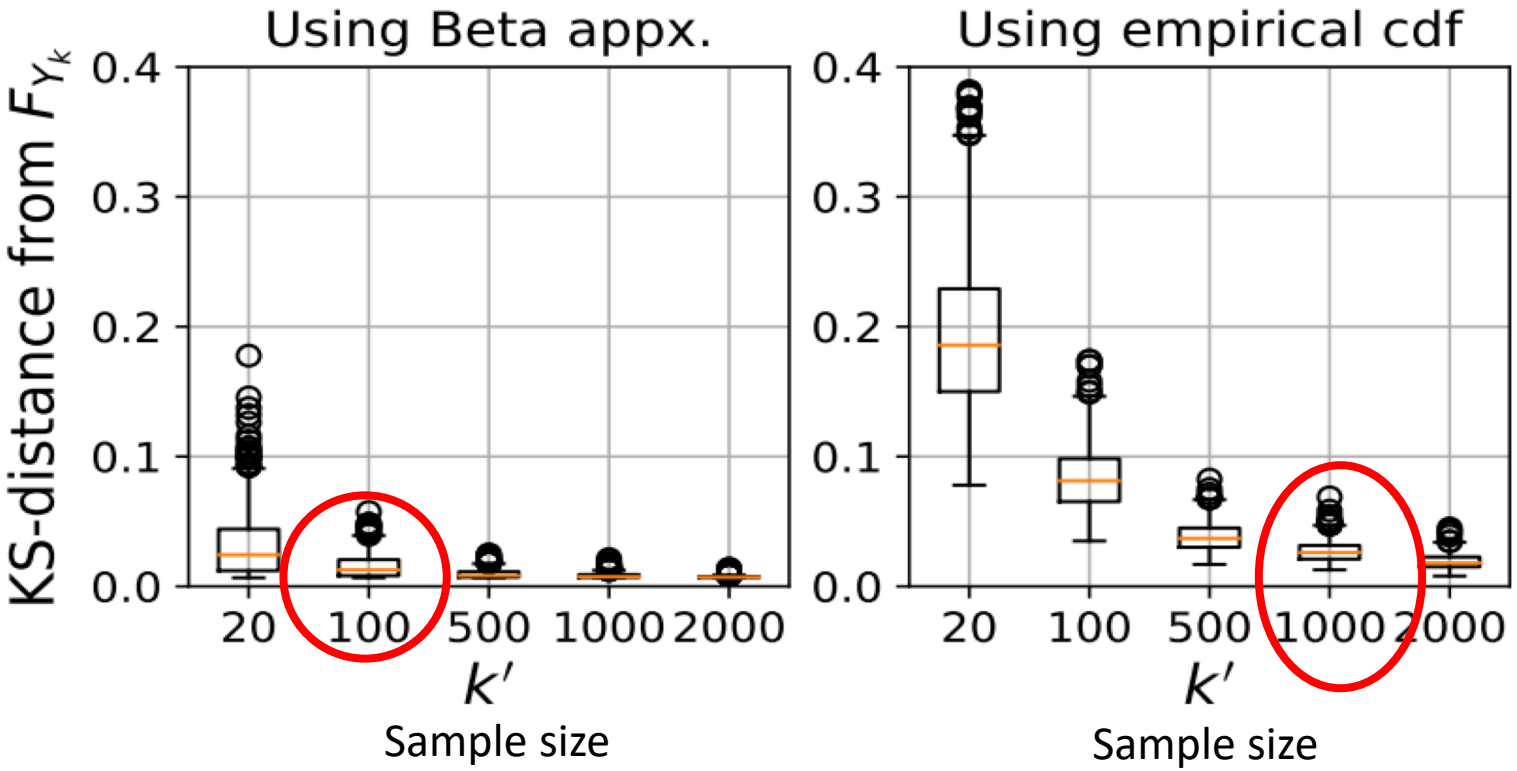
Quality of Model

- Created 100,000 samples of edge probabilities, constructed s-t probability for each
- For varying values of k', randomly choose k' s-t probabilities
- **Method 1:** given samples, construct the **empirical cdf**
- **Method 2:** given samples, estimate parameters of the **approximating Beta**



Quality of Model

- Created 100,000 samples of edge probabilities, constructed s-t probability for each
- For varying values of k', randomly choose k' s-t probabilities
- **Method 1:** given samples, construct the **empirical cdf**
- **Method 2:** given samples, estimate parameters of the **approximating Beta**



Conclusion

To assess cyber-risk to physical system requires integrated models

Combinatorial complexity to rely on purely algorithm approaches to computing reduction in physical risk as function of cyber protection

Monte Carlo sampling provides means of estimating cost curves

- Opportunities for intelligent sampling

Different avenues of investigation

- Minimum cut set analysis to estimate cost of complete protection
- Integration of models of attacker and defender actions (game theory)