University of Central Florida

IDC 6601

Behavioral Aspects to Cybersecurity

"Modeling Threats"

Bruce D. Caulkins, Ph.D.
Institute for Simulation and Training
University of Central Florida

A Good Quote, revisited again…

“If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle.”

— Sun Tzu, *The Art of War*

A Good Quote, revisited again…

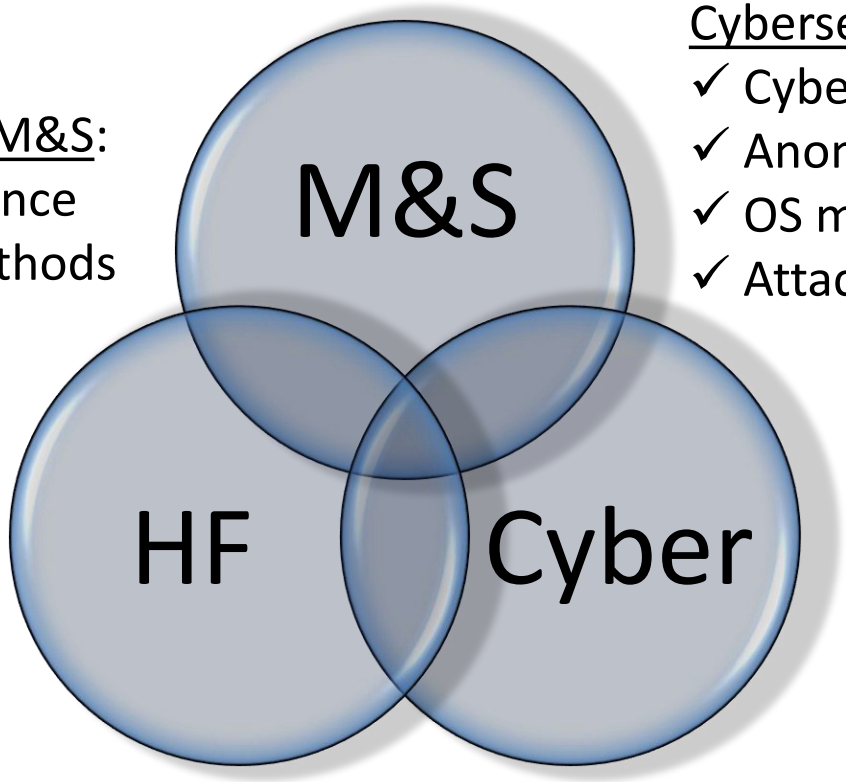
"If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle."

— Sun Tzu, *The Art of War*

…and we need to know ourselves and our enemy to create models…

M&S of Behavioral Cybersecurity

Behavioral Aspects of M&S:
- ✓ Training & performance
- ✓ Interdisciplinary methods for problem solving
- ✓ Cognitive modeling
- ✓ HSI



Cybersecurity for M&S:
- ✓ Cyber ranges
- ✓ Anomaly detection
- ✓ OS modeling
- ✓ Attack vector simulation

Behavioral Aspects of Cybersecurity:
- ✓ Insider threat detection
- ✓ Cyber workforce development
- ✓ Attack prediction
- ✓ Hacker motivations

Cyber Actors

White Hat Hackers

Black Hat Hackers

Gray Hat Hackers

Suicide Hackers

Script Kiddies

So how do these actors conduct their work?

Common Hacking Methodologies

Planting Backdoors

Covering Tracks

Escalation of Privilege

System Hacking

Enumeration — *gathers more info like usernames*

Scanning — *more active like ping*

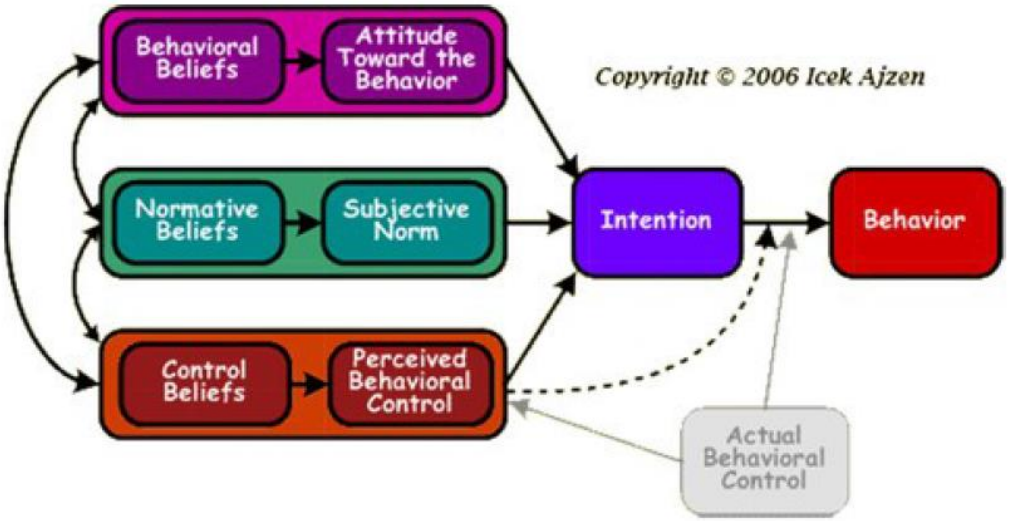
Footprinting — *passive query like whois*

So, how do we model threats in general and what are the questions to ask?

We can model insider threats… both intentional and unintentional varieties…

THEORIES OF BEHAVIORAL CHANGE

- **Theory of planned behavior (Ajzen, 1988)**
  - Behaviors depend on:
    i. Attitudes toward behavior
    ii. Perceived social norms
    iii. Perceived behavioral control



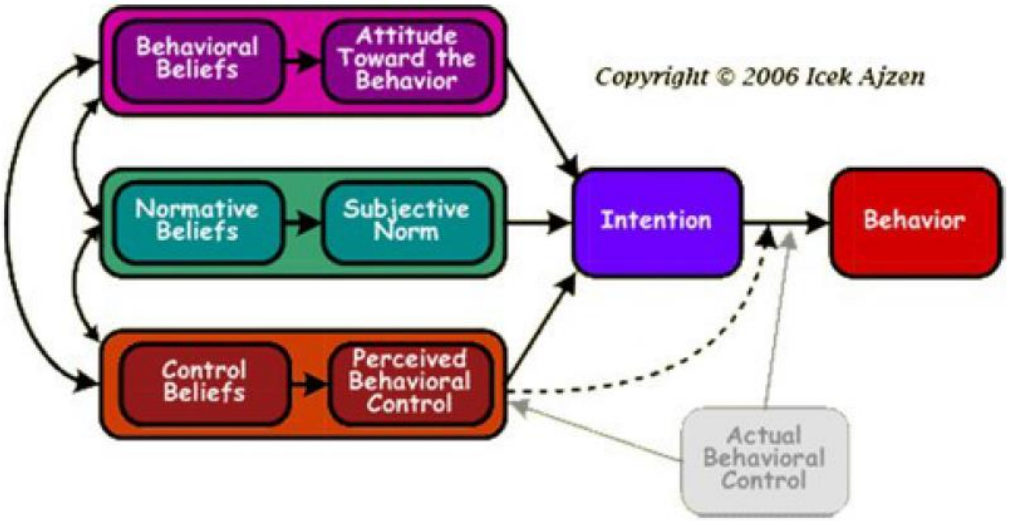
Source: Ajzen, I. (2006). *Theory of Planned Behavior Diagram.* Retrieved from http://people.umass.edu/aizen/tpb.diag.html.

We can model insider threats… both intentional and unintentional varieties…

THEORIES OF BEHAVIORAL CHANGE

- **Theory of planned behavior (Ajzen, 1988)**
  - Behaviors depend on:
    i. Attitudes toward behavior
    ii. Perceived social norms
    iii. Perceived behavioral control

But how do we go about modeling outsider threats?

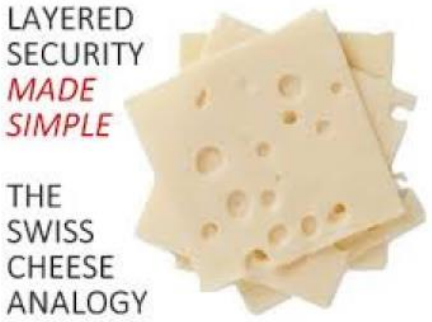


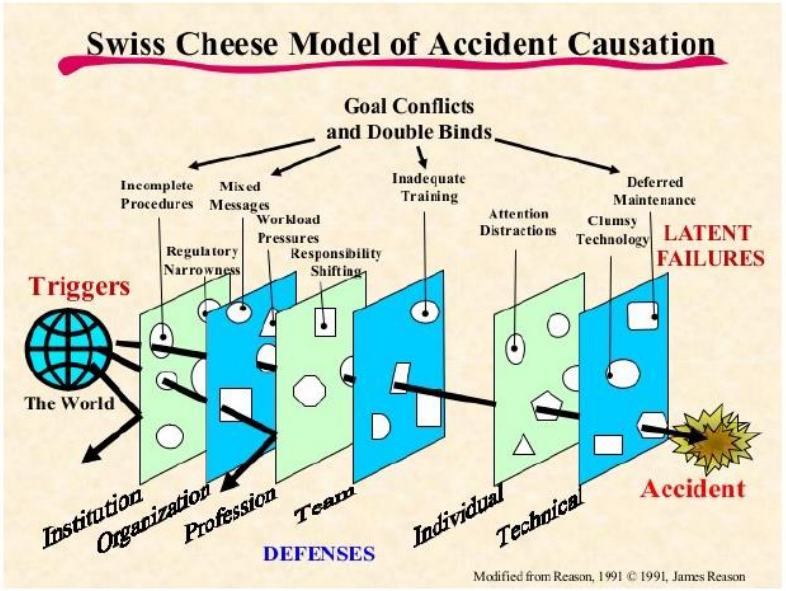
Source: Ajzen, I. (2006). *Theory of Planned Behavior Diagram.* Retrieved from http://people.umass.edu/aizen/tpb.diag.html.

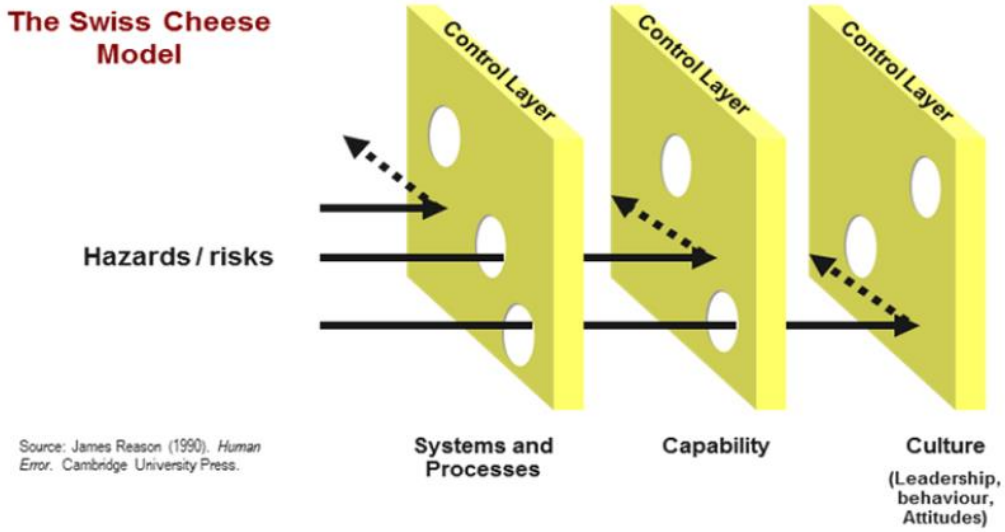
Defense in Depth … what the cyber threat works against

HUMAN FACTORS & CYBERSECURITY

- Reason's (1990) Swiss Cheese model







Modeling Cyber Threats

Questions to ask:

- What type(s) of targets (banking, HR, website, etc) do we want to model?
- How can that target get attacked? How do we model those ways?
- What type(s) (insider, outsider, natural, etc) of threats do we want to model?
- What type(s) of attacks (DDoS, phishing, etc) do we want to model?
- What type of tool to use (agent-based, DES, continuous) for modeling?

Modeling Cyber Threats

Questions to ask:

- What type(s) of targets (banking, HR, website, etc) do we want to model?

For now, let's use a non-cyber example (Nuclear Power plant)

- How can that target get attacked? How do we model those ways?

Attack trees can help!

What are Attack Trees?

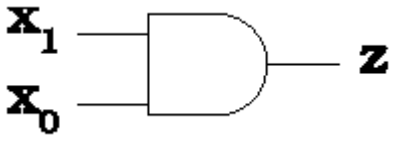
- Formal method to graphically represent the security of systems
- Let’s you look closer at system’s vulnerabilities
- Can be applied to cyber and non-cyber systems
- Can use AND/OR gates
- Can use weights too

https://www.schneier.com/academic/archives/1999/12/attack_trees.html

Digital Logic: AND and OR Truth Tables

AND:

$x_1 * x_0 = z$

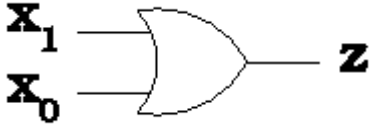


So, both inputs must be true ("1") for output to be true

x_1	x_0	Z
0	0	0
0	1	0
1	0	0
1	1	1

OR:

$x_1 + x_0 = z$

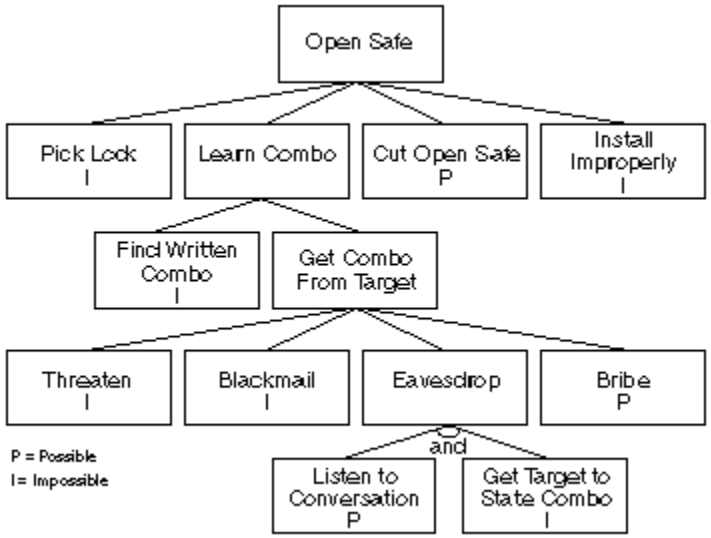


So, if either input or both inputs are true ("1"), output is true

x_1	x_0	z
0	0	0
0	1	1
1	0	1
1	1	1

Attack Trees

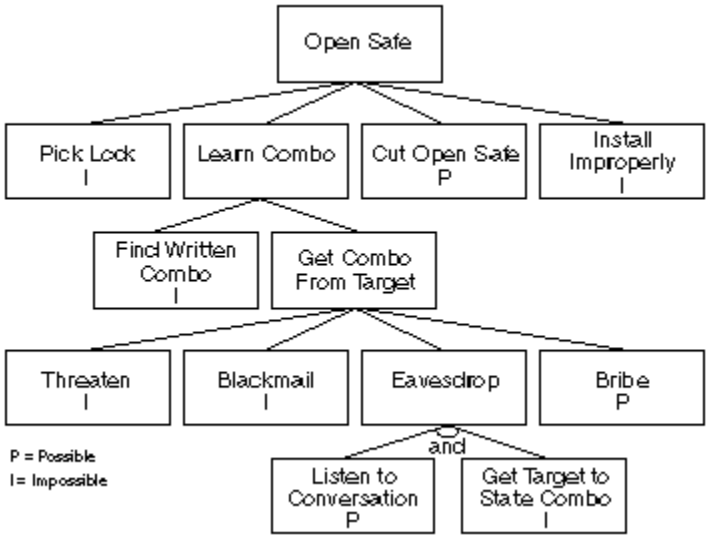
- Formal method to graphically represent the security of systems
- Lets you look closer at system's vulnerabilities
- Can be applied to cyber and non-cyber systems
- Can use AND/OR gates
- Can use weights too

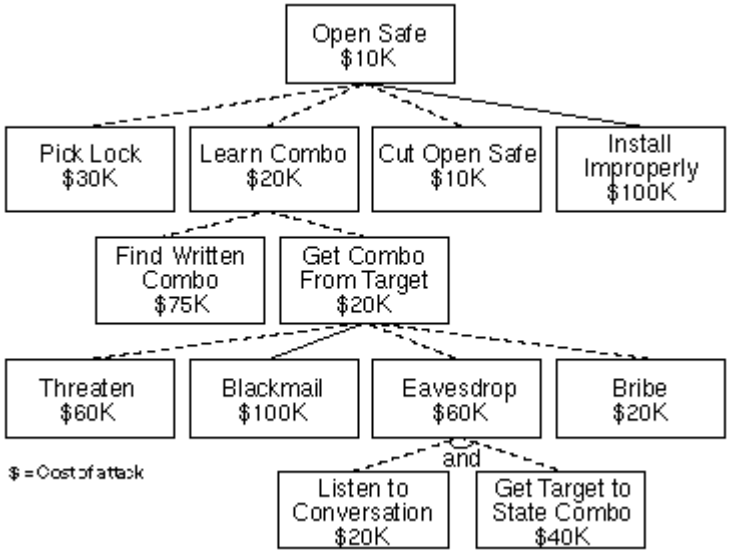


https://www.schneier.com/academic/archives/1999/12/attack_trees.html

Attack Trees

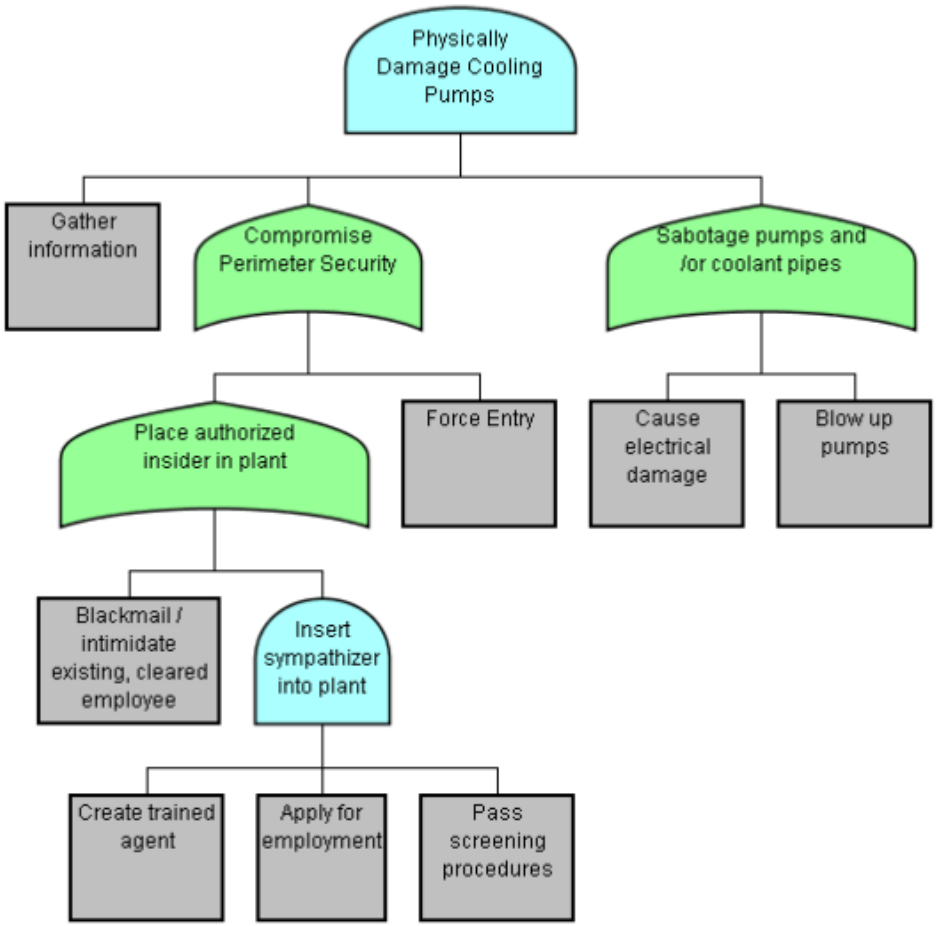
- Formal method to graphically represent the security of systems
- Let's you look closer at system's vulnerabilities
- Can be applied to cyber and non-cyber systems
- Can use AND/OR gates
- Can use weights too





https://www.schneier.com/academic/archives/1999/12/attack_trees.html

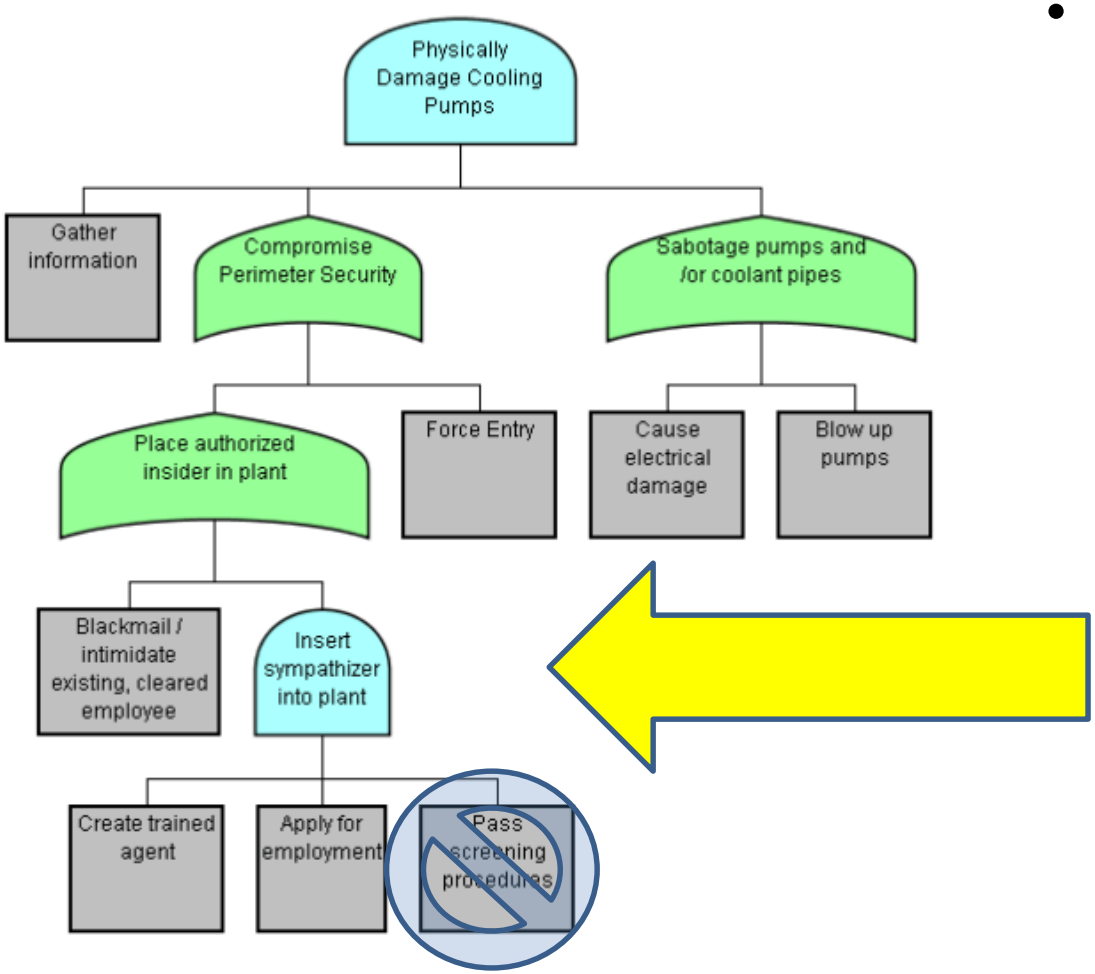
Attack Tree Example (non-cyber)



- Read from bottom up to top/root
- Root node usually shown at top → goal
- Green/Blue nodes below root represent sub-goals
- Blue nodes = AND
- Green nodes = OR

Source: https://www.amenaza.com/AT-whatAre.php

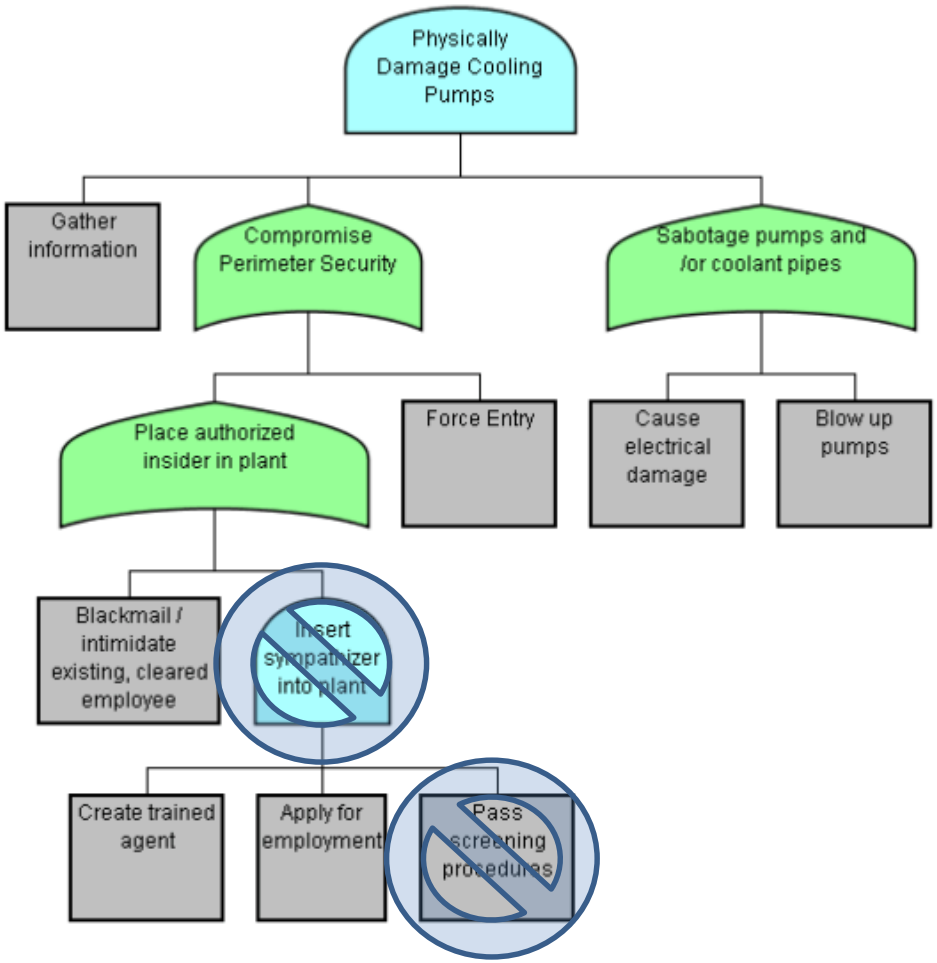
Attack Tree Example (non-cyber)



- For "Insert sympathizer into plant," what happens if last leaf node is denied?

Source: https://www.amenaza.com/AT-whatAre.php

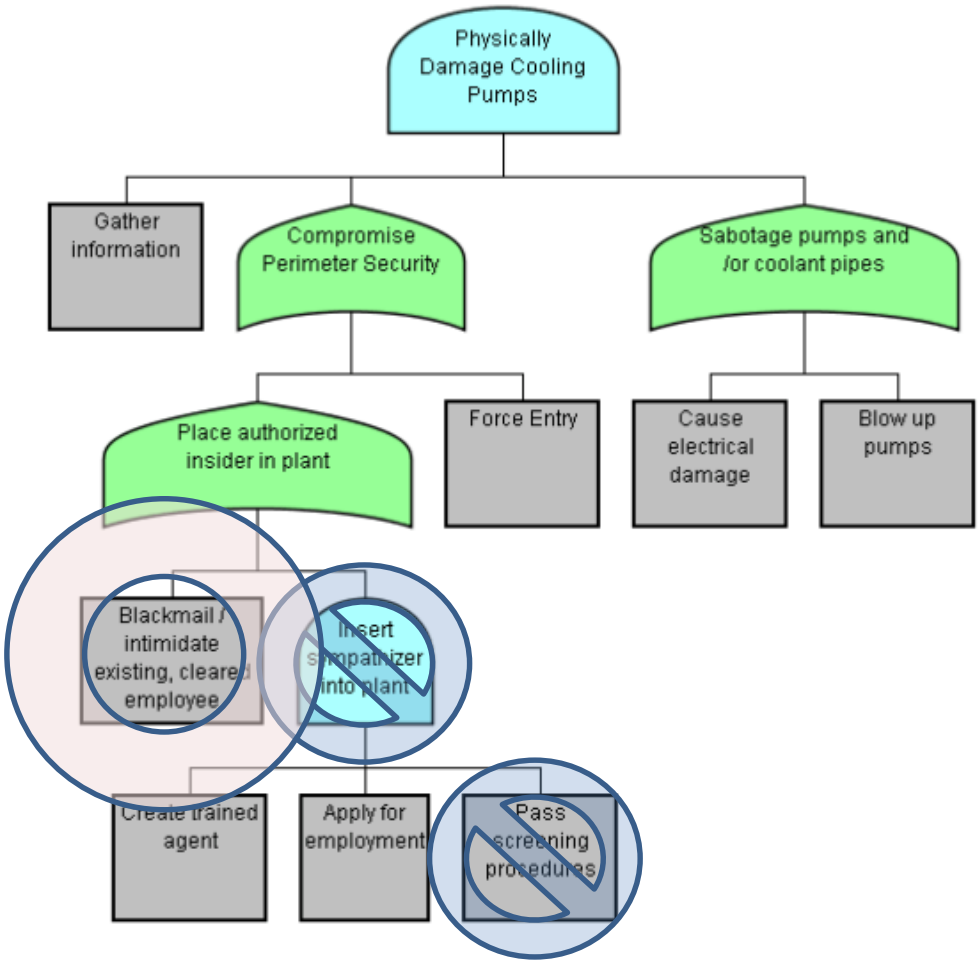
Attack Tree Example (non-cyber)



- For "Insert sympathizer into plant," what happens if last leaf node is denied?
- ANSWER: the sub-goal is denied as well

Source: https://www.amenaza.com/AT-whatAre.php

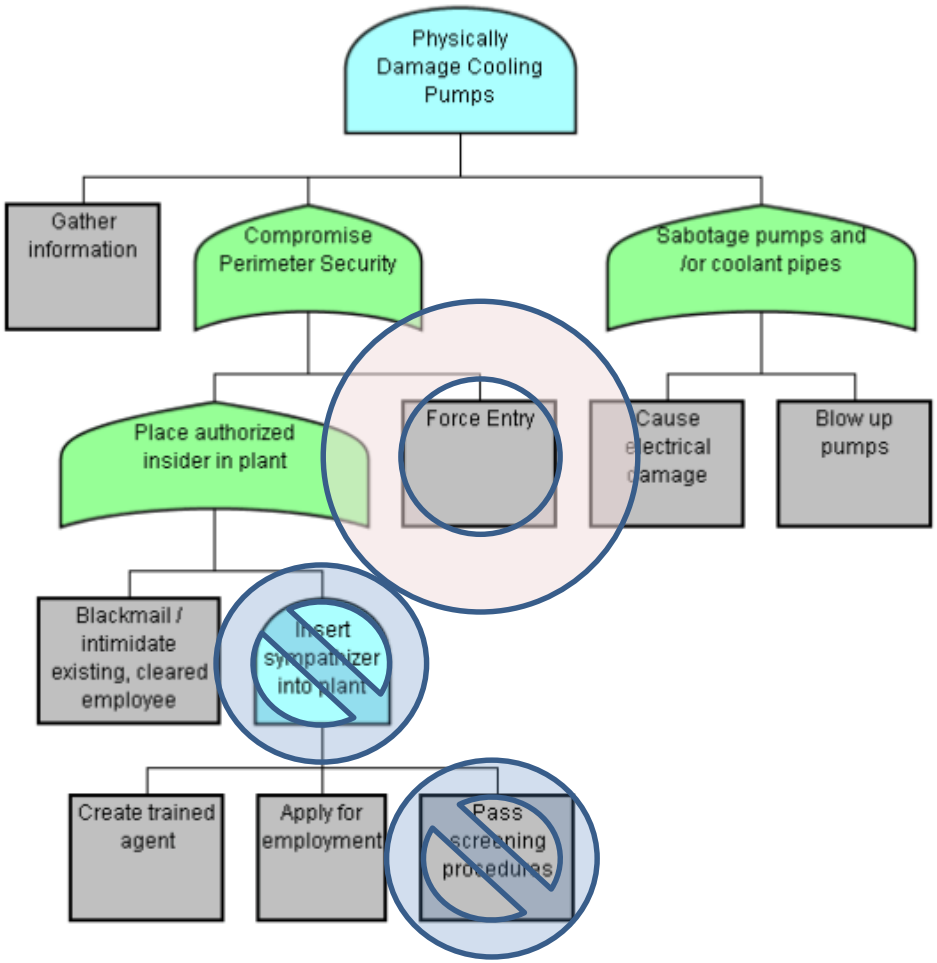
Attack Tree Example (non-cyber)



- For "Insert sympathizer into plant," what happens if last leaf node is denied?
- ANSWER: the sub-goal is denied as well
- Now, "blackmail" is the only apparent option for the attacker here

Source: https://www.amenaza.com/AT-whatAre.php

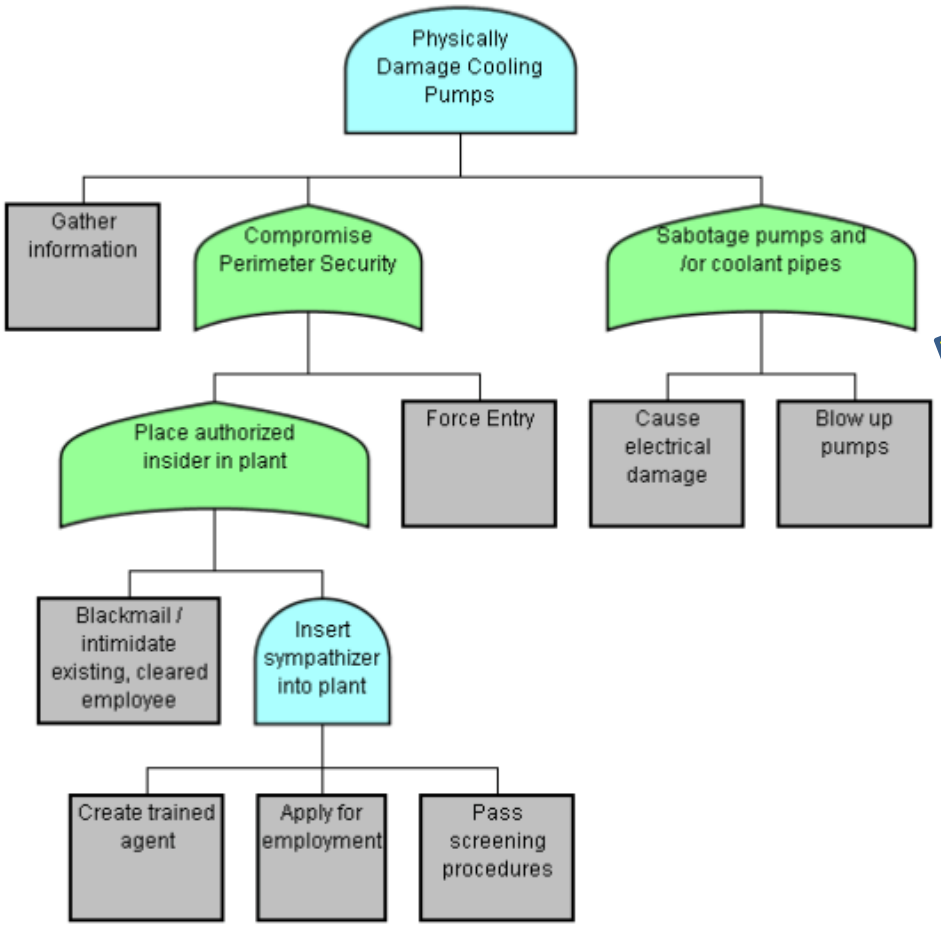
Attack Tree Example (non-cyber)



- For "Insert sympathizer into plant," what happens if last leaf node is denied?
- ANSWER: the sub-goal is denied as well
- Now, "blackmail" is the only apparent option for the attacker here
- OR, "forced entry"

Source: https://www.amenaza.com/AT-whatAre.php

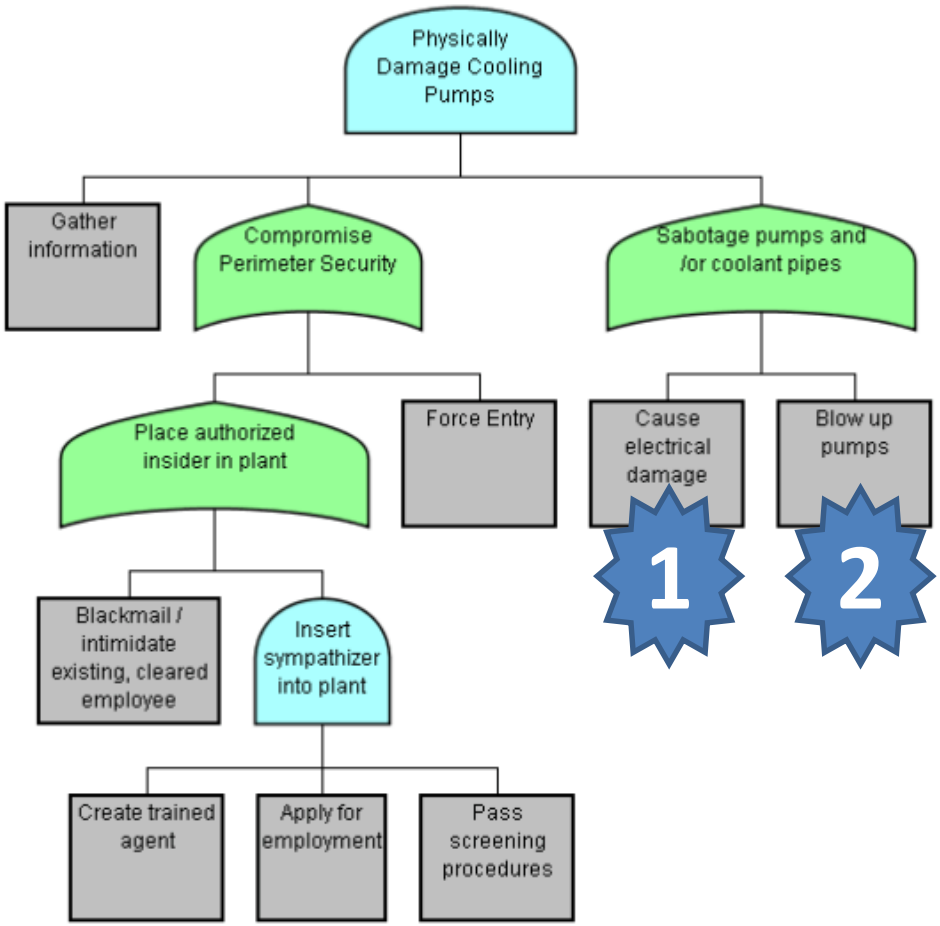
Attack Tree Example (non-cyber)



- At "Sabotage pumps and/or coolant pipes," you can obtain this sub-goal in 1 of 2 ways…

Source: https://www.amenaza.com/AT-whatAre.php

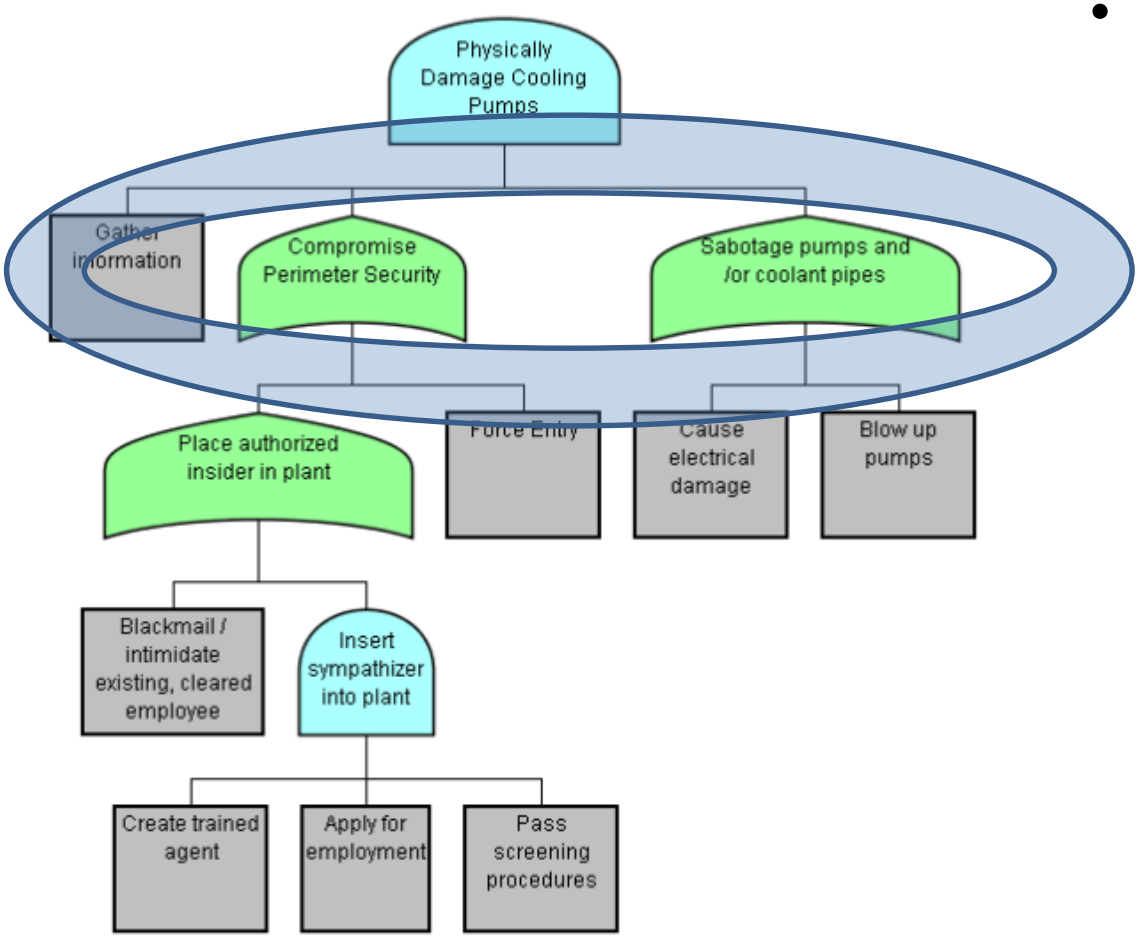
Attack Tree Example (non-cyber)



- At "Sabotage pumps and/or coolant pipes," you can obtain this sub-goal in 1 of 2 ways…

Source: https://www.amenaza.com/AT-whatAre.php

Attack Tree Example (non-cyber)



- At the top two rows, you must obtain "yes" at all three nodes below root to achieve overall goal

Source: https://www.amenaza.com/AT-whatAre.php

Modeling Cyber Threats

Questions to ask:

- What type(s) of targets (banking, HR, website, etc) do we want to model?
- How can that target get attacked? How do we model those ways?
- What type(s) (insider, outsider, natural, etc) of threats do we want to model?
- What type(s) of attacks (DDoS, phishing, etc) do we want to model?
- What type of tool to use (agent-based, DES, continuous) for modeling?

Modeling Cyber Threats

Questions to ask:

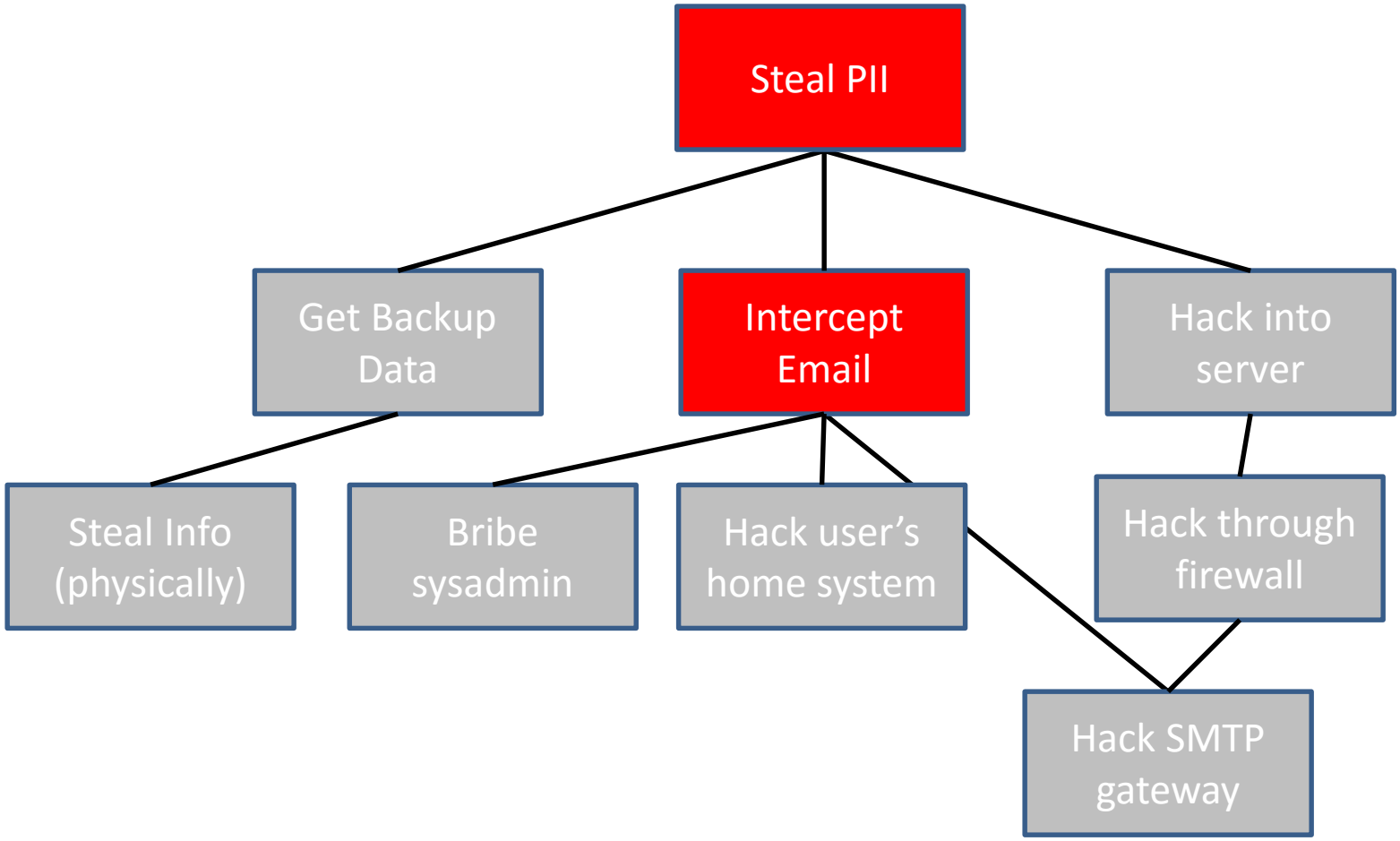
- What type(s) (insider, outsider, natural, etc) of threats do we want to model?

Outside in this case

- What type(s) of attacks (DDoS, phishing, etc) do we want to model?

Let's look at Stealing Personally Identifiable Information (PII)

“Steal PII” attack tree example (all red nodes are OR nodes)



https://www.openlearning.com/u/deveshmitra/blog

Modeling Cyber Threats

Questions to ask:

- What type(s) of targets (banking, HR, website, etc) do we want to model?
- How can that target get attacked? How do we model those ways?
- What type(s) (insider, outsider, natural, etc) of threats do we want to model?
- What type(s) of attacks (DDoS, phishing, etc) do we want to model?
- What type of tool to use (agent-based, DES, continuous) for modeling?

Modeling Cyber Threats

Questions to ask:

- What type of tool to use (agent-based, DES, continuous) for modeling?

Let's look at Discrete Event Simulation (DES)

One Perspective

"Using Discrete Event Simulation to Model Attacker Interactions with Cyber and Physical Security Systems"

Perkins, C., & Muller, G. (2015). Using discrete event simulation to model attacker interactions with cyber and physical security systems. *Procedia Computer Science*, *61*, 221-226.

Premise

In this paper, the authors describe a discrete event simulation model that uses data about integrated physical and cyber security systems, attacker's responses and behavioral characteristics to identify key safeguards that will mitigate the extent of the attacker's success in penetrating a system

Perkins, C., & Muller, G. (2015). Using discrete event simulation to model attacker interactions with cyber and physical security systems. Procedia Computer Science, 61, 221-226.

Background

- Physical security analysts have been performing vulnerability assessments (VAs) for years
- Cybersecurity VAs are still in their very early stages
- Both are not integrated well together yet
- But, due to their integration with each other in Cyber-Physical Systems (CPSs), VAs will need to be better integrated in the near future
- Modeling CPSs allow deeper understanding of the systems and their possible vulnerabilities and threat vectors

Perkins, C., & Muller, G. (2015). Using discrete event simulation to model attacker interactions with cyber and physical security systems. Procedia Computer Science, 61, 221-226.

Premise – CPS Representation in DES

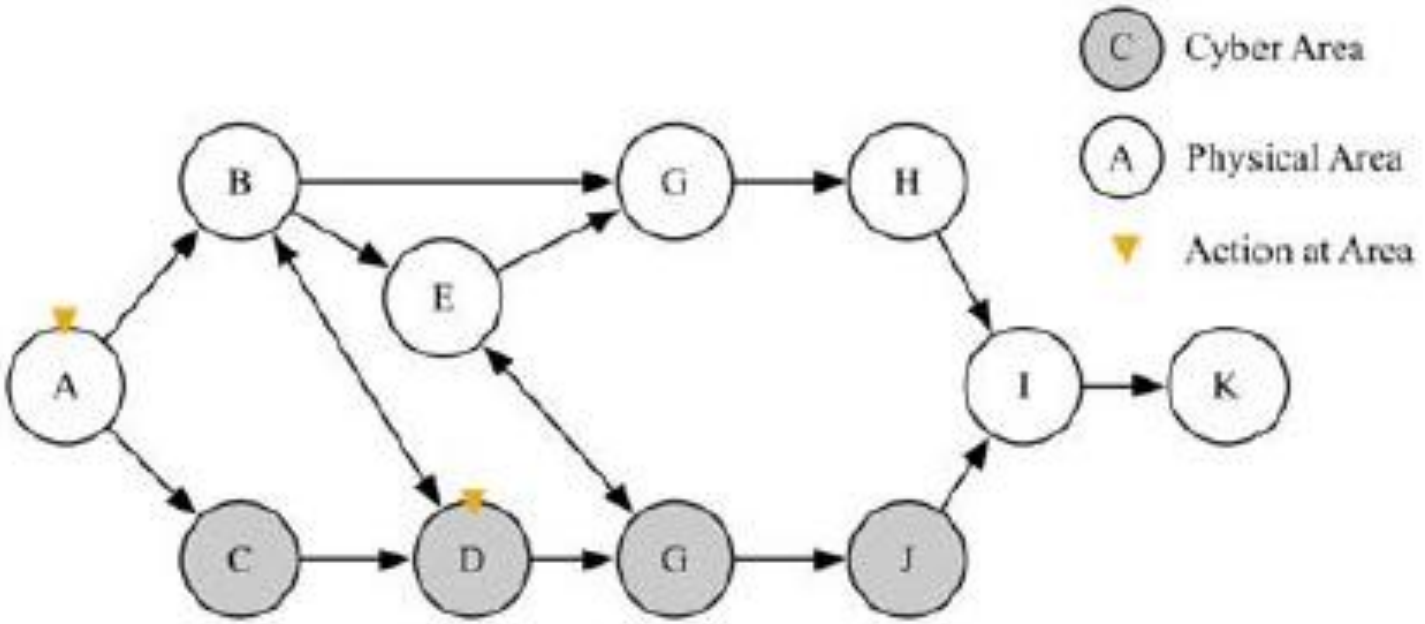


Figure 1. Graph representation of integrated cyber-physical system.

Perkins, C., & Muller, G. (2015). Using discrete event simulation to model attacker interactions with cyber and physical security systems. Procedia Computer Science, 61, 221-226.

Premise – CPS Representation in DES

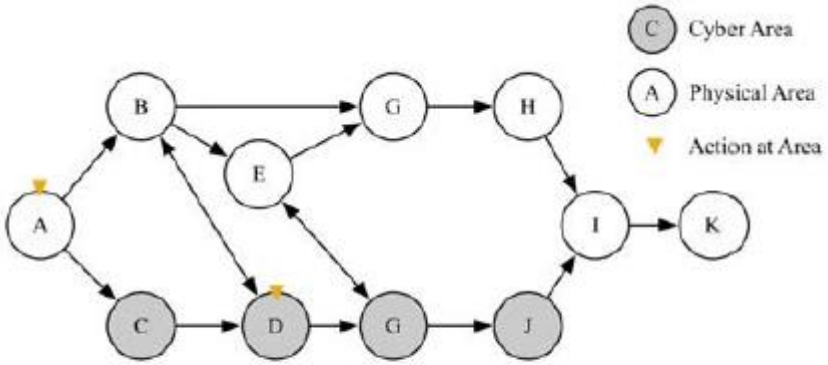


Figure 1. Graph representation of integrated cyber-physical system.

- Cyber-Physical System (CPS) represented as graph

Perkins, C., & Muller, G. (2015). Using discrete event simulation to model attacker interactions with cyber and physical security systems. Procedia Computer Science, 61, 221-226.

Premise – CPS Representation in DES

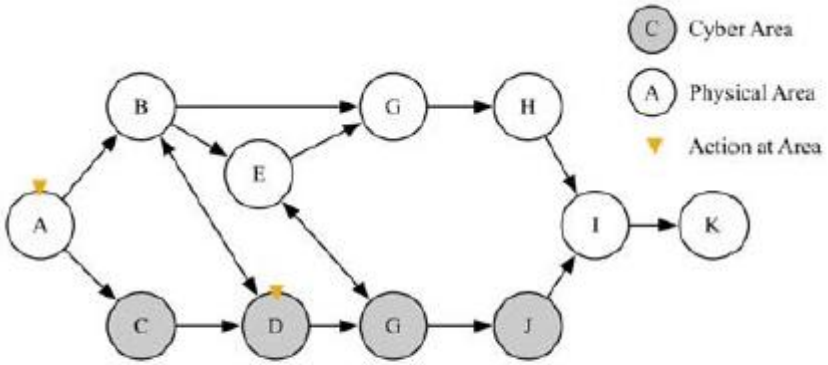


Figure 1. Graph representation of integrated cyber-physical system.

- Cyber-Physical System (CPS) represented as graph
- Shows integration of physical area (white nodes) and cyber area (gray nodes)
- Arcs on **physical side** represent avenues of access – doors, hallways, etc

Perkins, C., & Muller, G. (2015). Using discrete event simulation to model attacker interactions with cyber and physical security systems. Procedia Computer Science, 61, 221-226.

Premise – CPS Representation in DES

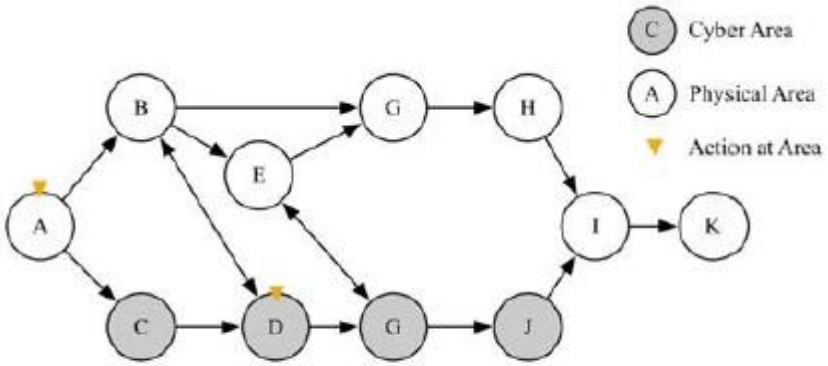


Figure 1. Graph representation of integrated cyber-physical system.

- Cyber-Physical System (CPS) represented as graph
- Shows integration of physical area (white nodes) and cyber area (gray nodes)
- Arcs on **cyber side** represent network domains or zone connections

Perkins, C., & Muller, G. (2015). Using discrete event simulation to model attacker interactions with cyber and physical security systems. Procedia Computer Science, 61, 221-226.

Premise – CPS Representation in DES

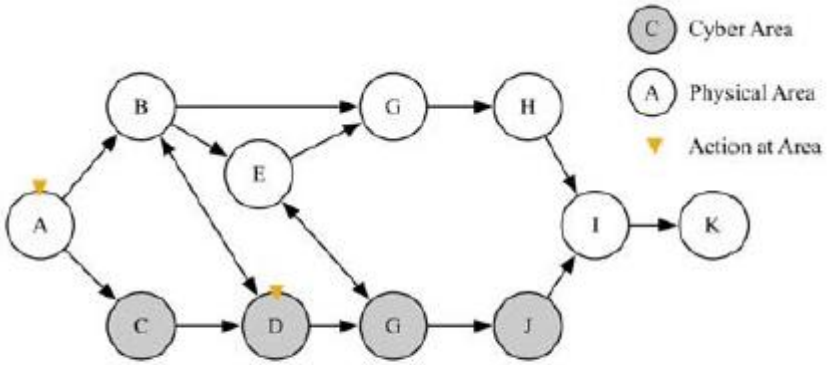


Figure 1. Graph representation of integrated cyber-physical system.

- Cyber-Physical System (CPS) represented as graph
- Shows integration of physical area (white nodes) and cyber area (gray nodes)
- Arcs **between the two sides** represent workstations or other access points

Perkins, C., & Muller, G. (2015). Using discrete event simulation to model attacker interactions with cyber and physical security systems. Procedia Computer Science, 61, 221-226.

Premise – Simulation-Generated Pathway

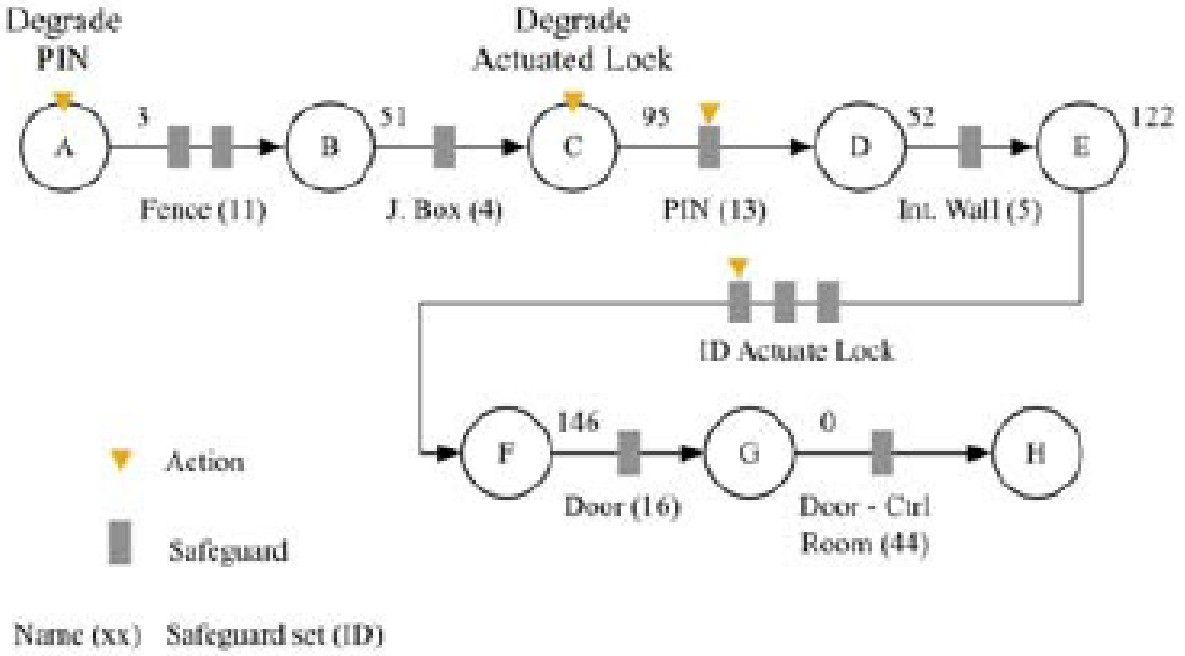


Figure 2. A pathway generated by the simulation. These pathways result from the integrated cyber-physical system, which allow effects to propagate.

Perkins, C., & Muller, G. (2015). Using discrete event simulation to model attacker interactions with cyber and physical security systems. Procedia Computer Science, 61, 221-226.

Premise – Simulation-Generated Pathway

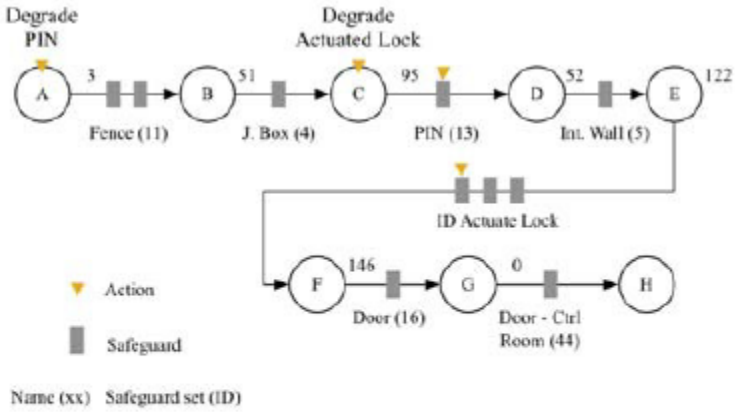


Figure 2. A pathway generated by the simulation. These pathways result from the integrated cyber-physical system, which allow effects to propagate.

- "Actions" are denoted by triangles

Perkins, C., & Muller, G. (2015). Using discrete event simulation to model attacker interactions with cyber and physical security systems. Procedia Computer Science, 61, 221-226.

Premise – Simulation-Generated Pathway

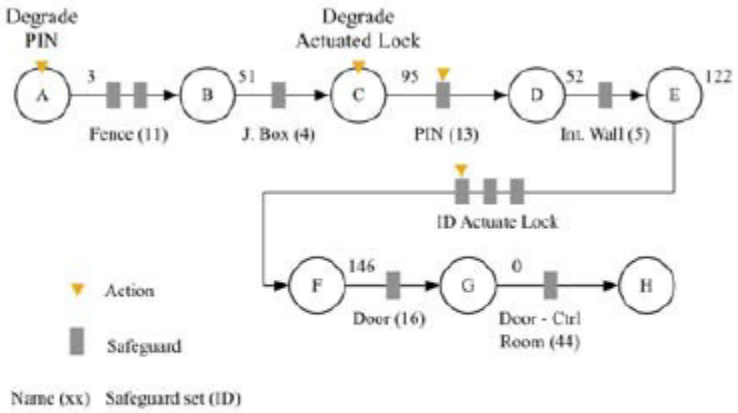


Figure 2. A pathway generated by the simulation. These pathways result from the integrated cyber-physical system, which allow effects to propagate.

- "Actions" are denoted by triangles
- "Safeguards" are denoted by vertical blocks

Perkins, C., & Muller, G. (2015). Using discrete event simulation to model attacker interactions with cyber and physical security systems. Procedia Computer Science, 61, 221-226.

Premise – Simulation-Generated Pathway

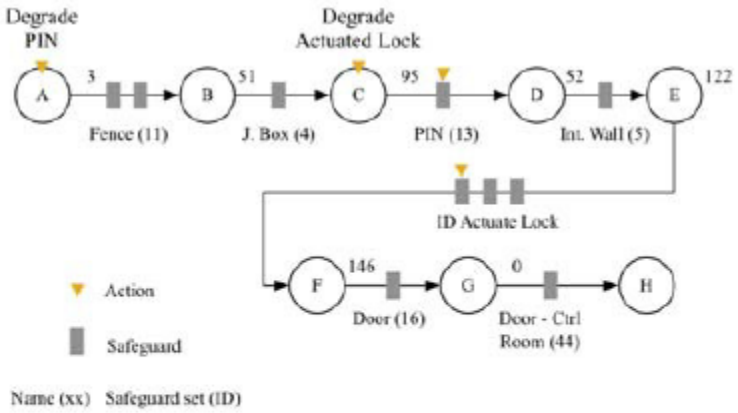


Figure 2. A pathway generated by the simulation. These pathways result from the integrated cyber-physical system, which allow effects to propagate.

- "Actions" are denoted by triangles
- "Safeguards" are denoted by vertical blocks
- Entities include attacker and response types

Perkins, C., & Muller, G. (2015). Using discrete event simulation to model attacker interactions with cyber and physical security systems. Procedia Computer Science, 61, 221-226.

Premise – Simulation Event Graph

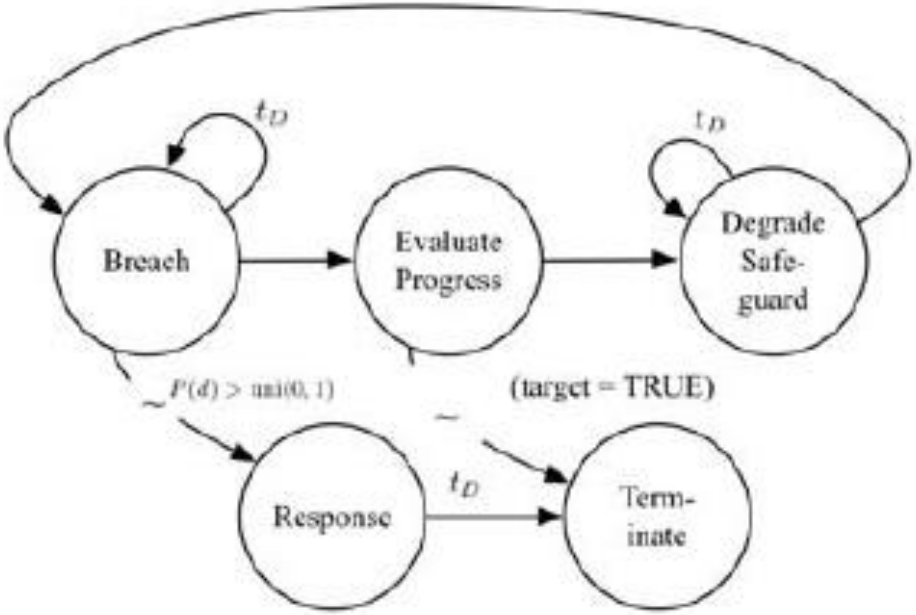


Figure 3. The event graph of the discrete event simulation includes time delays and detection likelihoods for both cyber and physical security measures.

Perkins, C., & Muller, G. (2015). Using discrete event simulation to model attacker interactions with cyber and physical security systems. Procedia Computer Science, 61, 221-226.

Premise – Simulation Event Graph

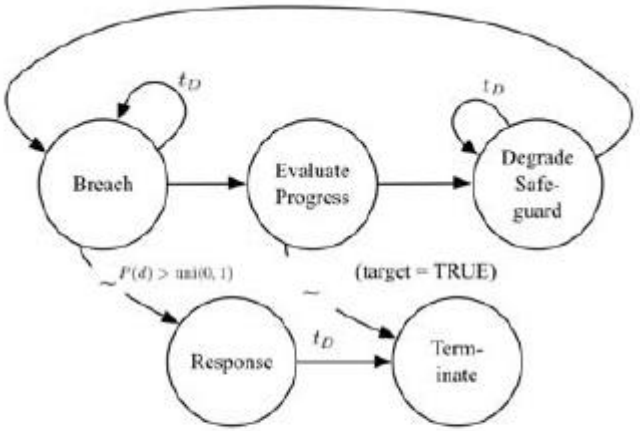


Figure 3. The event graph of the discrete event simulation includes time delays and detection likelihoods for both cyber and physical security measures.

- Time delays
- Safeguards
- Responses
- etc

Perkins, C., & Muller, G. (2015). Using discrete event simulation to model attacker interactions with cyber and physical security systems. Procedia Computer Science, 61, 221-226.

Future Directions?

- More work needs to be done with respect to DES-based simulations
- Research ongoing at IST for attacker/responder cognitive models
- While continuous models are not appropriate for this mission, agent-based models need to be explored along with more in-depth look at DES simulations

University of Central Florida

IDC 6601

Behavioral Aspects to Cybersecurity

"Modeling Threats"

Bruce D. Caulkins, Ph.D.
Institute for Simulation and Training
University of Central Florida