Making Sound Cyber Security Decisions Through a Quantitative Metrics Approach

April 25, 2011

Bill Sanders

Joint work with Elizabeth LeMay, Ken Keefe,
and Carol Muehrcke

University of Illinois at Urbana-Champaign

1st International Workshop on Resilience Assessment of Critical Infrastructures

Coordinated Science Laboratory

Disciplinary Excellence with Interdisciplinary Breadth

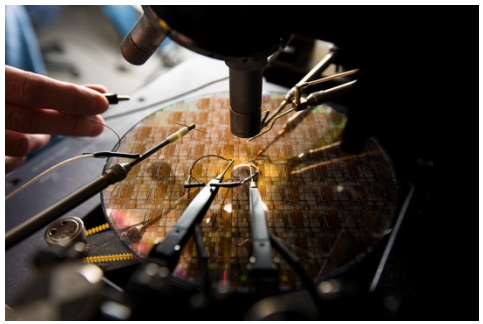
•Excellence in:

- Computing and Networks
- Circuits, Electronics & Surface Science
- Communications & Signal Processing
- Decision & Control

•Interdisciplinary Initiatives:

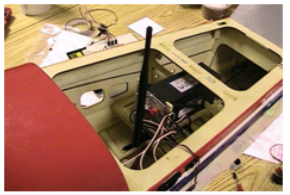
- Management & Control of Complex Systems
- Parallel Computing
- Multi-modal, Multimedia Imaging & Visualization
- Sustainable Energy Systems

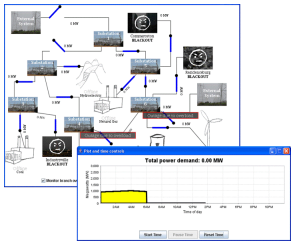
- Recent Funded Research:
  - Advanced Digital Sciences Center (ADSC) in Singapore, NVIDIA CUDA Center for Excellence, Neuroengineering IGERT Center, Illinois Center for Wireless Systems, Ethics Center
- Almost 60 years as a premier national research facility
- 550 Researchers: 110 professors, 330 graduate students, 60 undergraduate students, & 50 professionals
- Over $300M in active research projects as of Jan. 2011

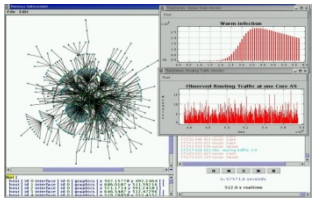


Information Trust Institute

- Providing World-Wide Excellence in Information Trust and Security
  - Critical Applications, Infrastructures & Homeland Defense
  - Multimedia and Distributed Systems
  - Embedded & Enterprise Computing
- Multi-disciplinary excellence from 102 researchers across 28 academic departments, 11 colleges, and 10 institutes/labs
- Major Specialized Research Centers Within ITI:
  - Trustworthy Cyber Infrastructure for the Power GRID (TCIPG)
  - Boeing Trusted Software Center
  - Center for Assured Critical Application & Infrastructure Security
  - SHARPS Health Care IT Security Center
  - Formal Methods and Security Center (NSA-funded)
  - Smart Grid Validation Center (pending with State of Illinois)







Anti-Tamper | Authentication | Autonomous vehicle collision avoidance | Botnets | Counter-Terrorism | Cyber infrastructure security | Data mining for security | Embedded systems | Fault Tolerance | Formal methods for security | Information Assurance (IA) | SCADA security | Simulation and modeling for trust | Smart Grid security | Social trust | System Resiliency & Reliability | Traffic analysis | Wireless network security

The Problem

- Systems operate in adversarial environments
  - Adversaries seek to degrade system operation by affecting the confidentiality, integrity, and/or availability of the system information and services
  - "Secure" systems must be able to meet their operational objectives despite attack attempts by adversaries
- System security is not absolute
  - No real system is perfectly secure
  - Some systems are more secure than others
  - *But how much more secure are they*?

Quantifying Security

- At design time
  - System architects make trade-off decisions to best meet all design criteria
  - Other design criteria can be quantified: performance, reliability, operating and maintenance costs, etc.
  - *How can we quantify the security of different system designs*?
- During system operation and maintenance
  - Modifying the system architecture can improve or worsen system security
  - *How can we compare the security of different possible system configurations?*

Model-based system-level security evaluation

ITI

Contrasting Approaches

Typical Situation Today:

- Process:
  - Rely on a trusted analyst (wizard?) that examines situation, and gives advice based on experience, or
  - Form decision in a collective manner based on informal discussions among stakeholder experts
- *Limitations:*
  - *No* way to audit decision process
  - *No* quantifiable ranking of alternative options

Goal For Tomorrow:

- Usable tool set that enables diverse stakeholders to express
  - Multi-faceted aspects of model
  - Multiple objectives
- Way for diverse stake holders to express concerns and objectives in common terminology
- Quantifiable ranking of alternate security policies and architectures
- Auditable decision process

Everyone says it is important, few approaches exist …

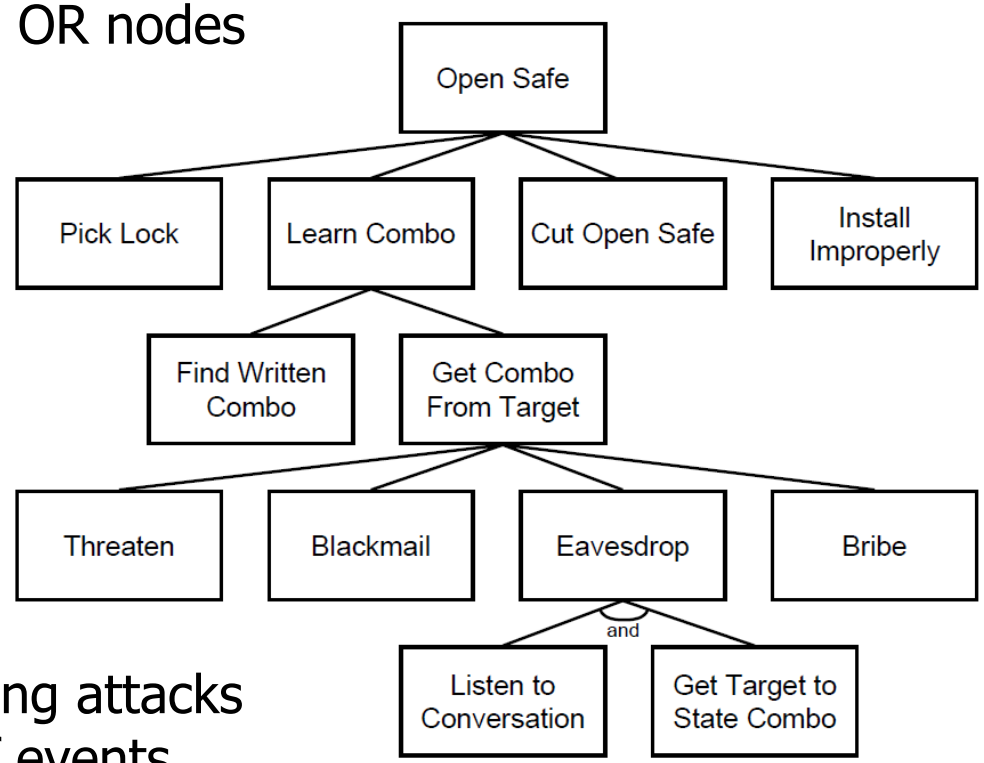
- Security metrics were an important problem in the 2005 INFOSEC Research Council Hard Problems List
- New security metrics that are linked to the business were ranked first among six key security imperatives developed by over twenty Fortune 500 firms
- New regulatory requirements of Sarbanes-Oxley and the Basel II Accord have created more urgency for metrics that integrate security risk with overall business risk
- Almost every critical infrastructure roadmap lists security metrics as a critical challenge
- The list goes on …

Related Work

- System Model-based security analysis
  - Attack Trees
  - Attack Graphs and Privilege Graphs
- Adversary-based security analysis
  - MORDA and MIRROR
  - NRAT

Attack Trees

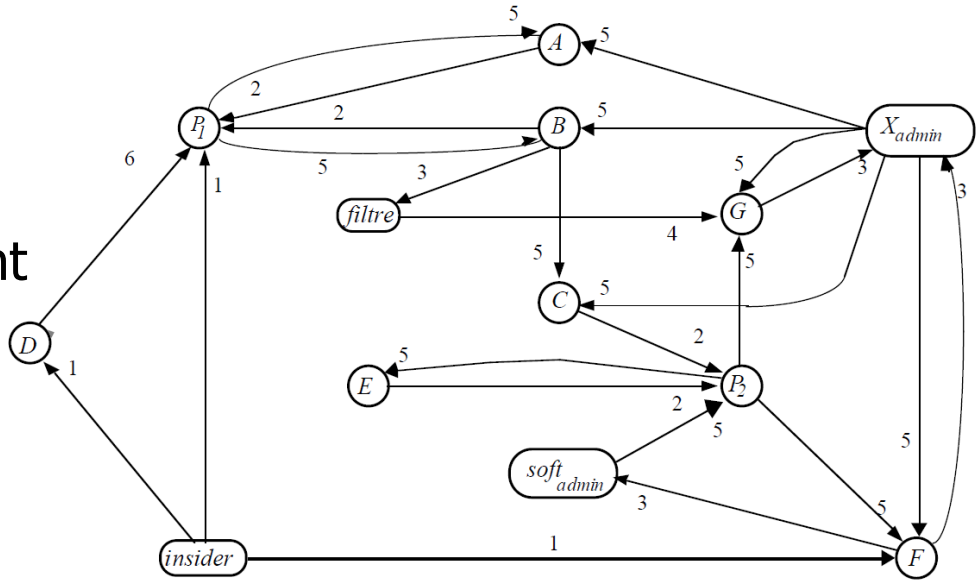
- Attack trees describe how sets of events can constitute a security compromise
  - Events are represented as leaf nodes and are joined together with AND and OR nodes
  - A security compromise is represented as the root node
- Contribution
  - Useful for thinking about multiple ways an attacker can reach an attack goal
- Limitation
  - Do not contain a notion of time, which prohibits expressing attacks as time-ordered sequences of events



From:
B. Schneier, "Attack trees: Modeling security threats," in Dr. Dobb's Journal: CMP Media, Dec. 1999.

Attack Graphs and Privilege Graphs

- Attack graphs and privilege graphs are both state-based attack analysis methods.
  - The nodes in a privilege graph represent privilege states
  - An attacker starts at one node and works toward an attack goal by transitioning to new privilege states
- Contribution
  - Enable state-based analysis
- Limitation
  - Do not consider the different attack goals and attack preferences of individual adversaries



1) X can guess Y's password; 2) X is in the Y's ".rhost"; 3) Y is a subset of X; 4) X can attack Y via Email; 5) Y uses a program owned by X ; 6) X can modify a "setuid" program owned by Y.

From:

M. Dacier, Y. Deswartes, and M. Kaaniche. Quantitative assessment of operational security models and tools. Technical Report Research Report 96493, LAAS, May 1996.

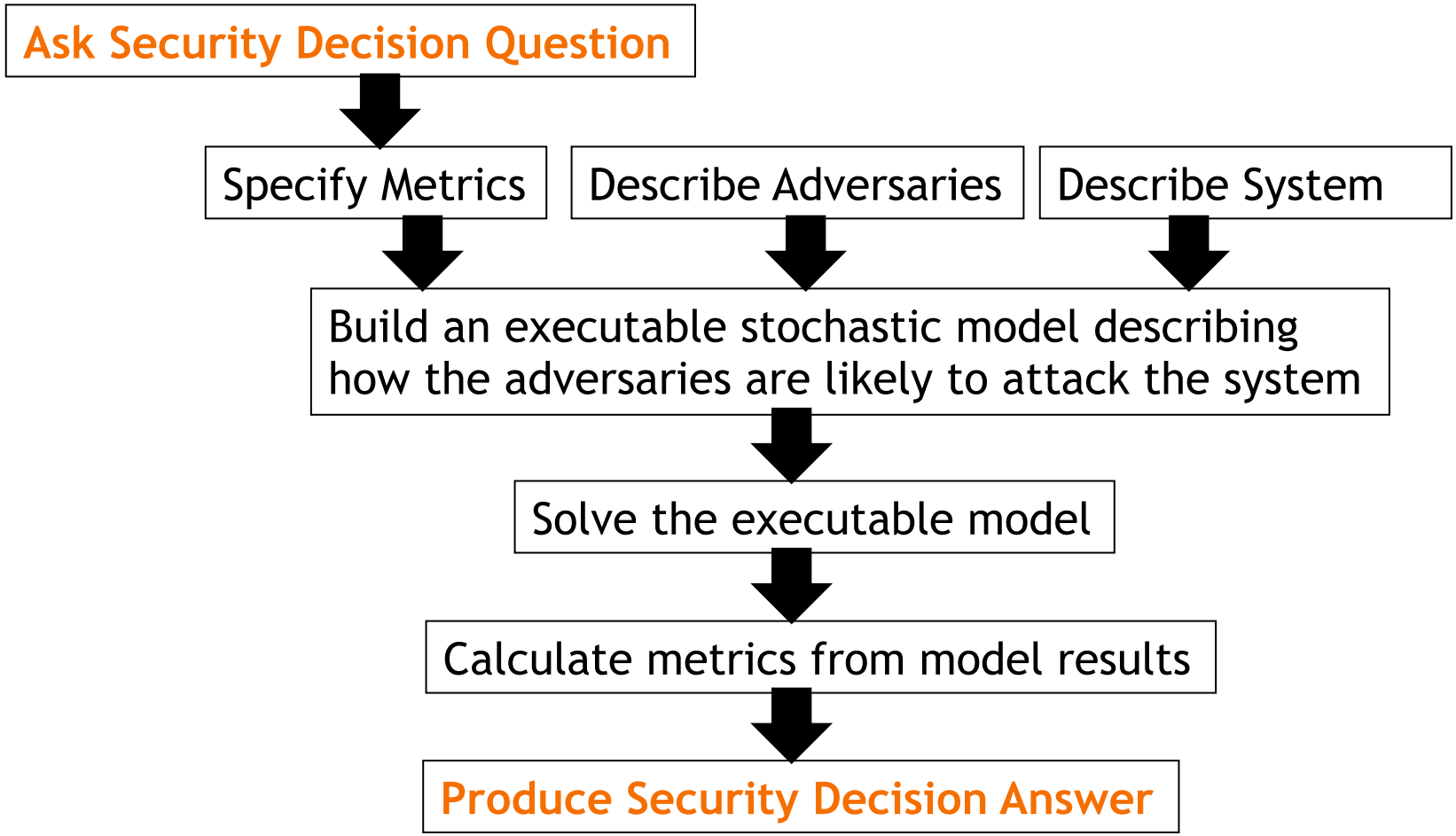
Adversary-based security analysis

- MORDA
  - MORDA assesses system risk by calculating attack scores for a set of system attacks. The scores are based on adversary attack preferences and the impact of the attack on the system mission.
  - A version of MORDA is commercially available as MIRROR
- NRAT
  - NRAT assesses mission risk by computing the attack competency of potential attackers and the system vulnerability.
  - These computations are performed by examining attributes of the threat actors (adversaries), the attacks, and the information system protection (defense).
- Contribution
  - Provide a security analysis informed by adversaries' attributes
- Limitation
  - Not designed for state-based analysis. The adversarial decision is represented as a one-time selection of a full attack vector.

ADversary VIew Security Evaluation (ADVISE) approach

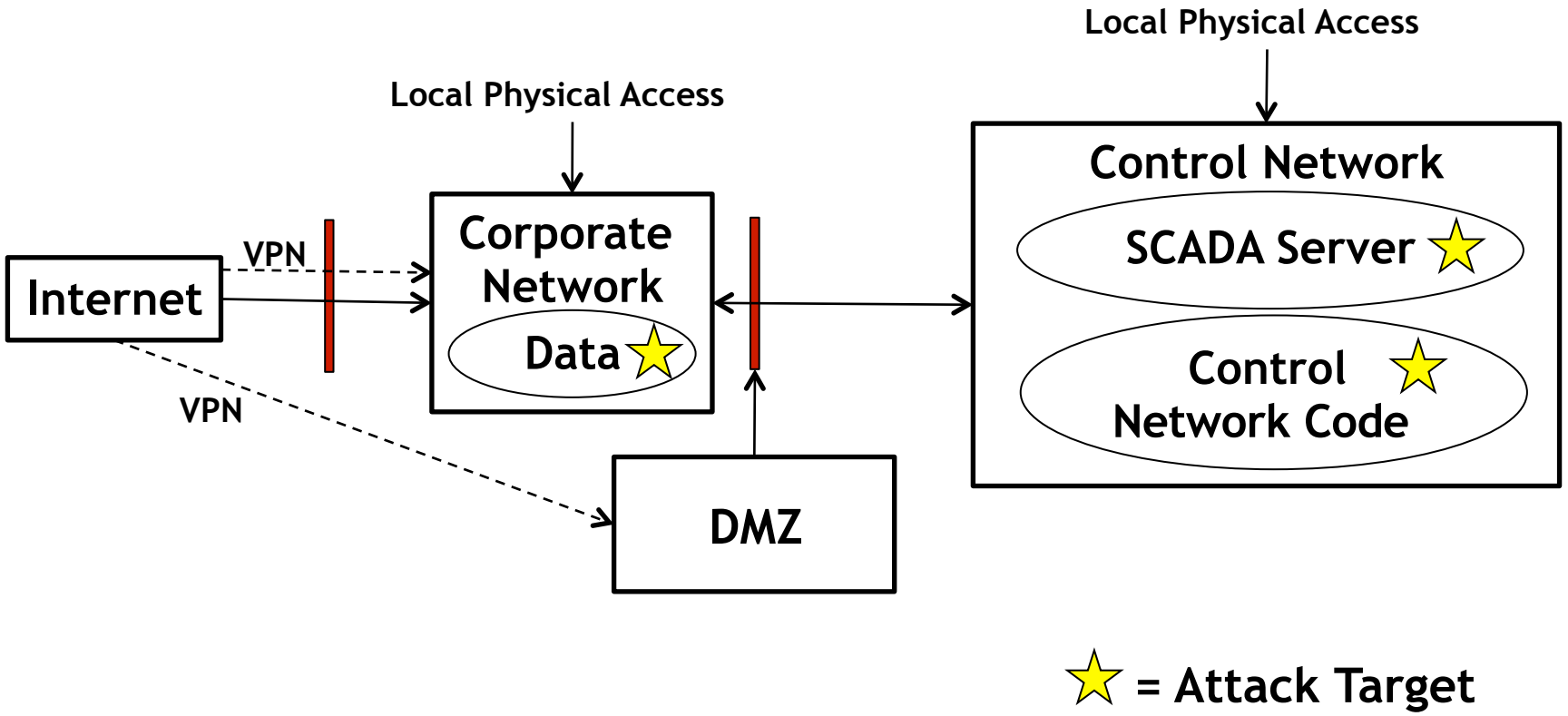
- Adversary-driven analysis
  - Considers characteristics and capabilities of adversaries
- State-based analysis
  - Considers multi-step attacks
- Quantitative metrics
  - Enables trade-off comparisons among alternatives
- Mission-relevant metrics
  - Measures the aspects of security important to owners/operators of the system
- Auditable and repeatable analysis method

ADVISE Model-Based Metrics Vision

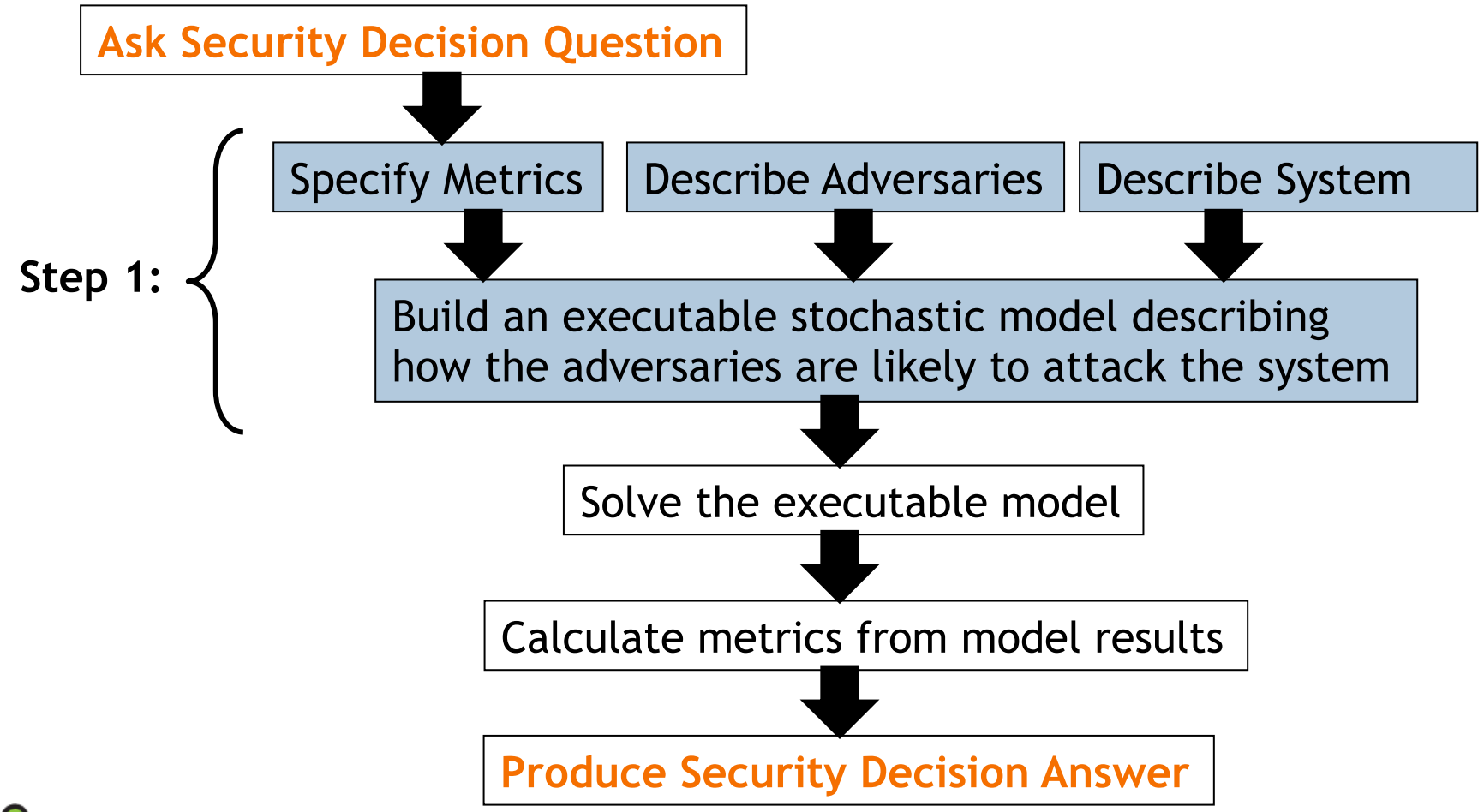


ITI

Example: SCADA System

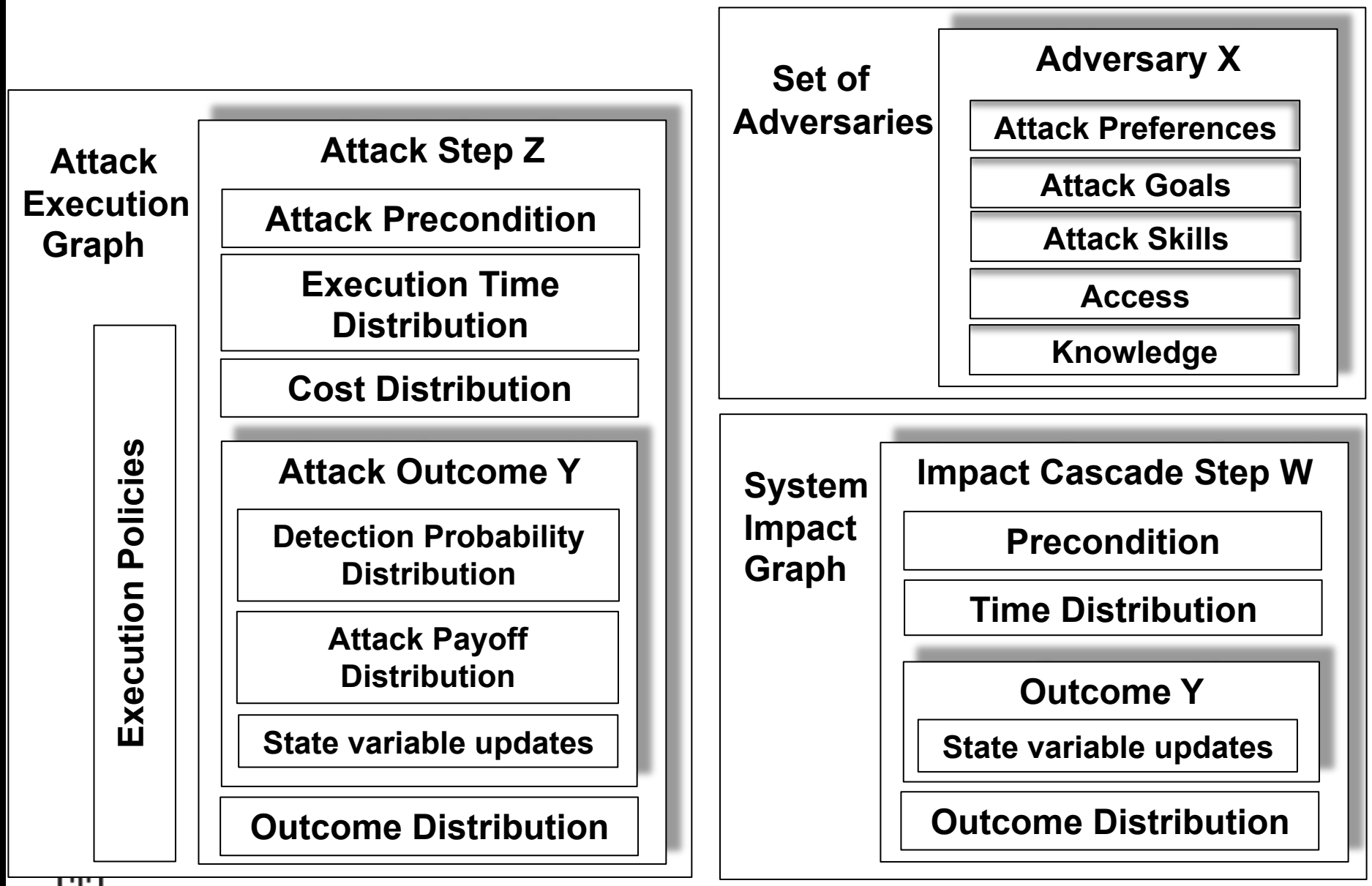


Process for Producing Metrics



ITI

ADversary VIew Security Evaluation (ADVISE)

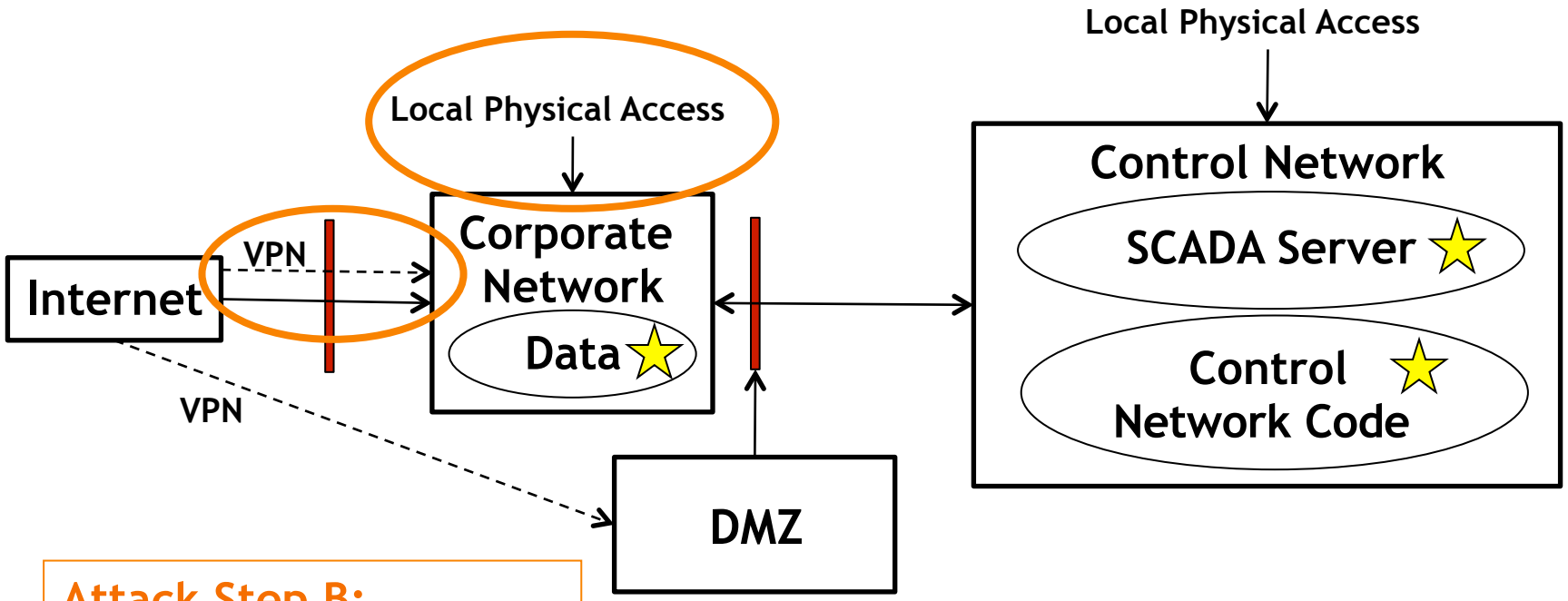


Example: Security Decision

- Question
  - Is the corporate network security budget better spent on upgrading the local physical security or the remote access network security?
- Adversary
  - Economic competitor who wants confidential corporate data
- Metric
  - Probability of confidential corporate data compromise in one year
- System configurations to compare
  - Baseline: current system configuration
  - Physical security upgrade
  - Network security upgrade

Example: SCADA System Attack

Attack Step A:
Gain Corporate Network Access Through Local Physical Access



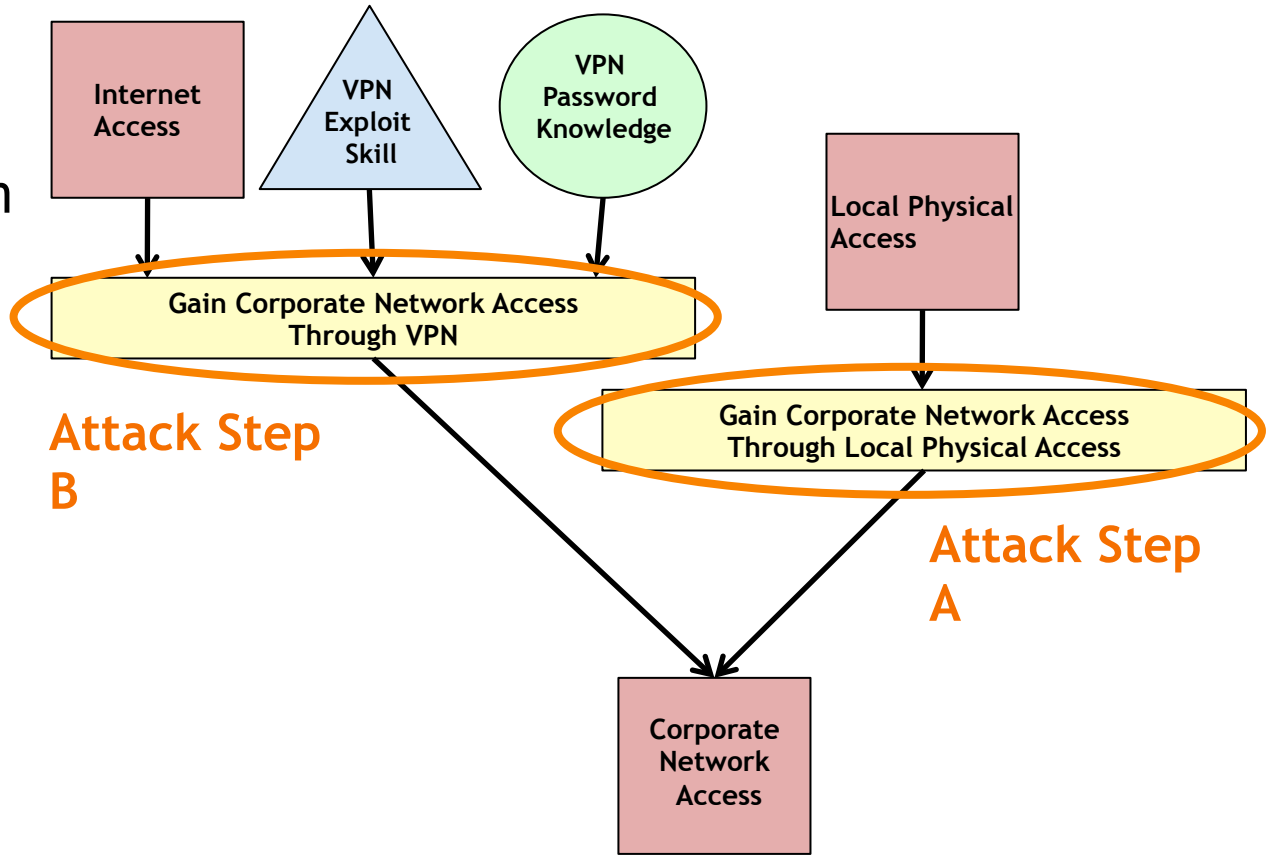
Attack Step B:
Gain Corporate Network Access Through VPN

★ = Attack Target

ITI

Representing Attacks Against the System

An "attack execution graph" describes potential attack vectors against the system from an attacker point of view. Attempting an attack step requires certain skills, access, and knowledge about the system. The outcome of an attack can affect the adversary's access and knowledge about the system.



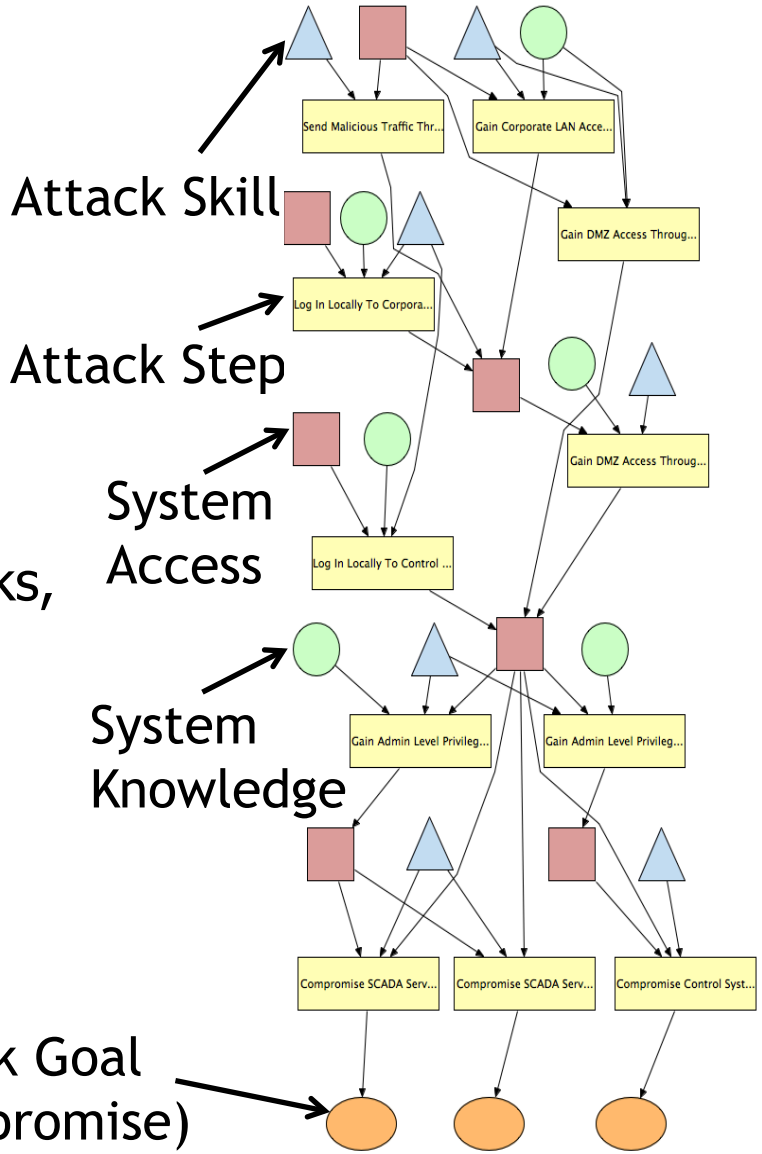
ITI

Attack Execution Graph

Formally, an attack execution graph is defined by the tuple

$$<G, S, A, K, Q>$$

where
G is the set of attack goals,
S is the set of attack skills,
A is the set of system access domains,
K is the set of system knowledge chunks,
and *Q* is the set of attack steps.



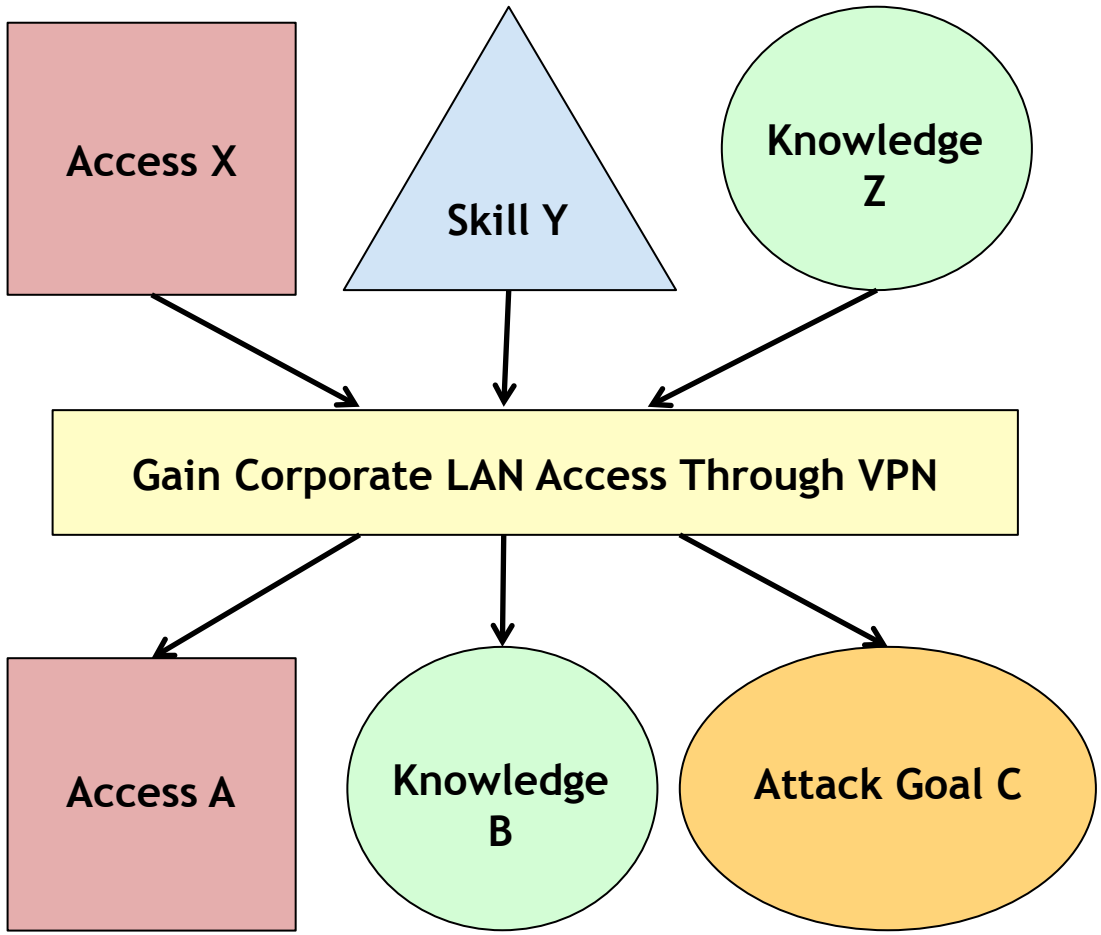
ITI

Describing an Attack Step

Inputs to Attack Precondition

Attack Step

Affected by Attack Outcomes



ITI

Specifying an Attack Step

Category	Definition	Examples
Attack Precondition	Skills, knowledge, and access the adversary must have to attempt this attack step	(firewall traffic exploit skill > 0.6) && (Internet access)
Execution Time Distribution	Time required for the adversary to attempt this attack step	Normal with mean 300 minutes and variance 50 minutes
Cost Distribution	Resource cost to the adversary to attempt this attack step	Deterministic $6000
Outcome Distribution	If the attack step is attempted, the likelihood of each outcome	P[success] = 0.4 P[partial failure] = 0.2 P[complete failure] = 0.4
Set of Outcomes	The set of all possible outcomes if the attack step is attempted	Success, partial failure, complete failure

ITI

Specifying an Attack Step Outcome

Category	Definition	Examples
Detection Probability Distribution	Likelihood of the attack step attempt being detected by the system defense	For success outcome, P[detection] = 0.1 For failure outcome, P[detection] = 0.4
Attack Payoff Distribution	Value to adversary of achieving this attack step outcome	For success outcome, payoff = $1000 For failure outcome, payoff = -$600
State Variable Updates	How the state of the model changes due to this attack set outcome	For success outcome, Corporate_LAN_Access = true

Representing an Adversary

- The security-relevant resources of adversaries are described by the sets of attack skills, system access, and system knowledge that they possess
  - ***Attack skills*** are exploit skills such as using attack tools, writing malware, finding vulnerabilities, etc.
  - ***System access*** domains describe the system as a set of domains where getting from one access domain to another requires an attack step, such as logging in to a file system
  - ***System knowledge*** is the key security information about a system such as user account names and passwords, configuration settings, etc.
- ***Attack preferences*** describe how heavily adversaries factor risk (detection probability and success probability), payoff, and cost into their attack decisions
- ***Attack goals*** describe what system compromise(s) the adversaries desire

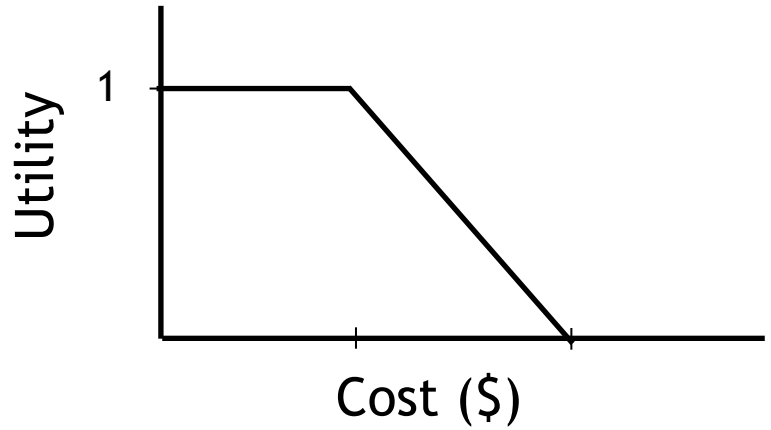
ITI

Adversary Parameter Values

Category	Definition	Examples	Value Ranges
Attack Preferences	The relative importance of each decision criterion when evaluating the options for the next attack step	preference weights for … low cost, low probability of detection, high probability of success, high payoff	Between 1 (important) and 0 (not)
Attack Goals	System-specific definitions of system security compromise	compromise control system database integrity, compromise server availability	1 (a goal) or 0 (not a goal)
Attack Skills	General skills or abilities that increase the adversary's probability of success when attempting some attack step	firewall traffic exploit skill, local network log-in exploit skill	Between 1 (proficient) and 0 (not)
Access (dynamic)	Access to network domains within a system; physical access to system components	Internet access, Corporate Network access, Control System Network access	1 (access) or 0 (no access)
Knowledge (dynamic)	Possession of information useful for attacks: user account and passwords, system architecture details	Corporate Firewall VPN user account and password, Control System architecture	1 (known) or 0 (not)

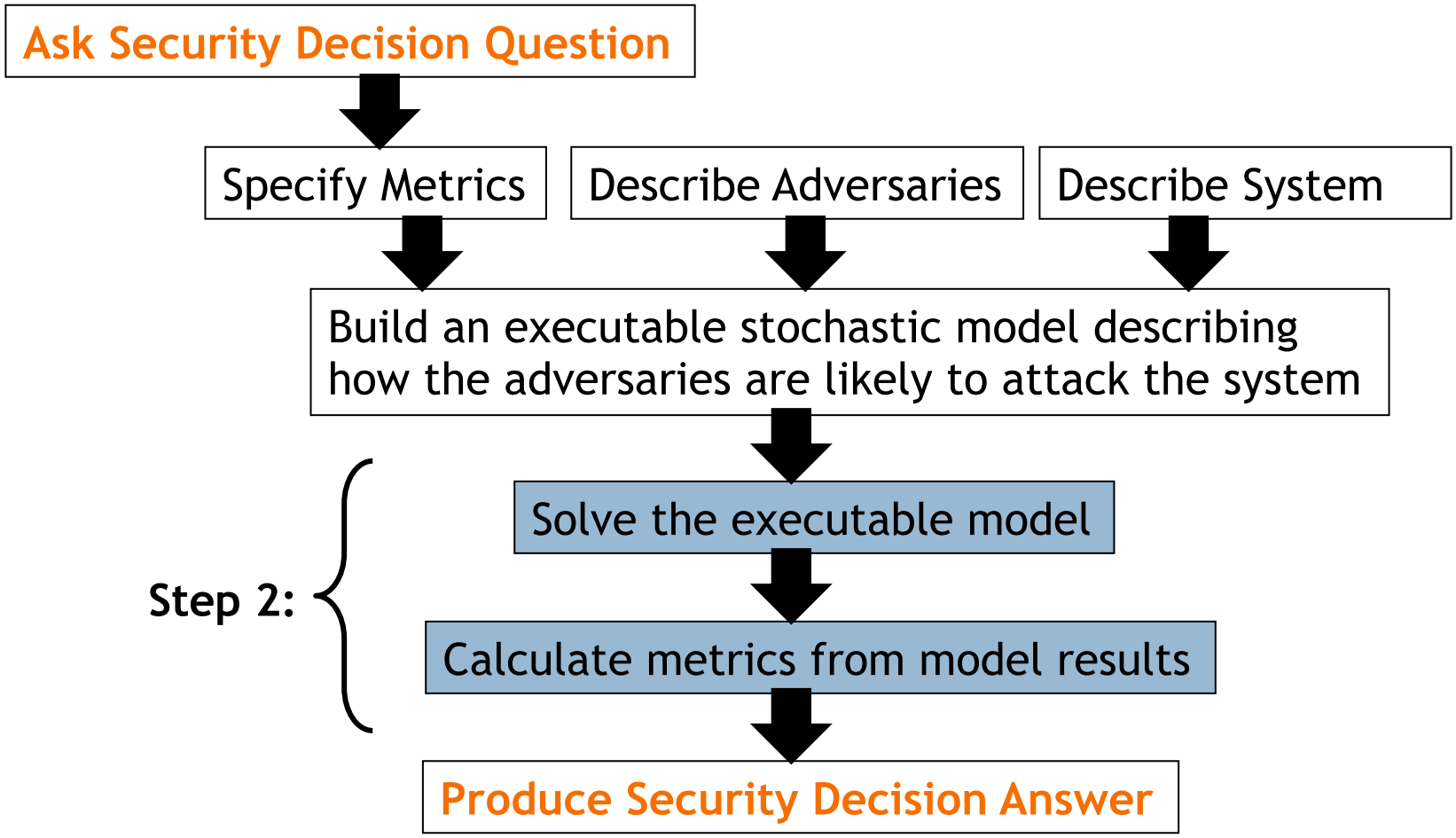
Utility Functions

- Uc_X, Up_X, Ud_X, and Us_X are the utility functions for cost, payoff, detection probability, and success probability, respectively
- Utility functions convert from conventional units to the value to an adversary on a [0,1] scale
- For example,



ITI

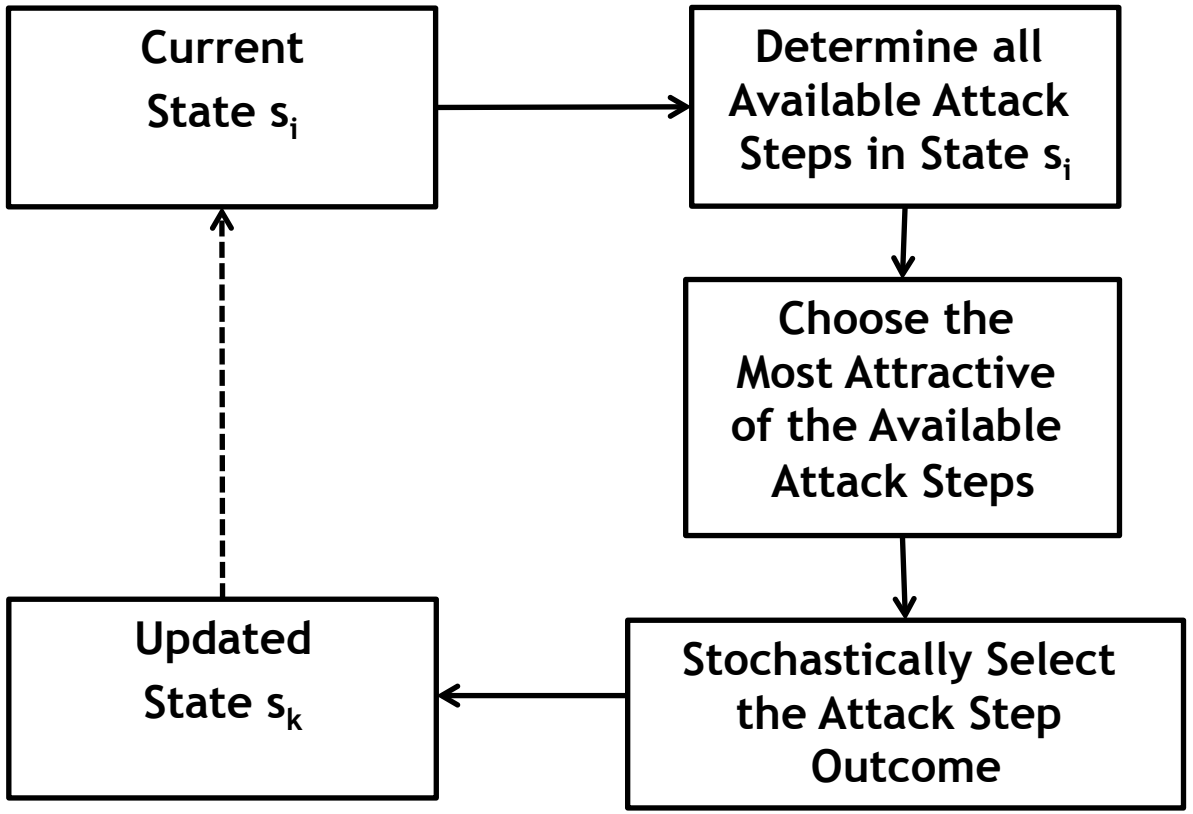
Process for Producing Metrics



ITI

Model Execution: the Attack Decision Cycle

- The adversary selects the most attractive available attack step based on his attack preferences.
- State transitions are determined by the outcome of the attack step chosen by the adversary.



Attack Step Attractiveness Calculation

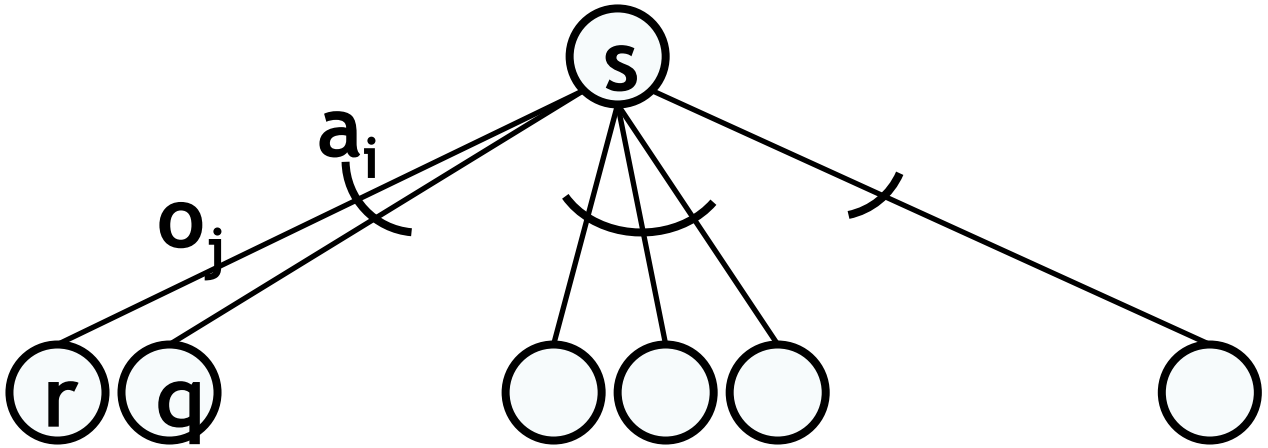
The adversary evaluates the attractiveness of all available attack steps and selects one to attempt next.

- Consider the following properties of the attack step
  - Cost
  - Expected probability of detection
  - Expected payoff
- Consider the attack preference weights of this adversary (W_{cost}, W_{payoff}, *and* $W_{detection}$)

Attractiveness of an attack step to the adversary =
Cost * W_{cost} + *E[Payoff]* * W_{payoff} + *E[Detection]* * $W_{detection}$

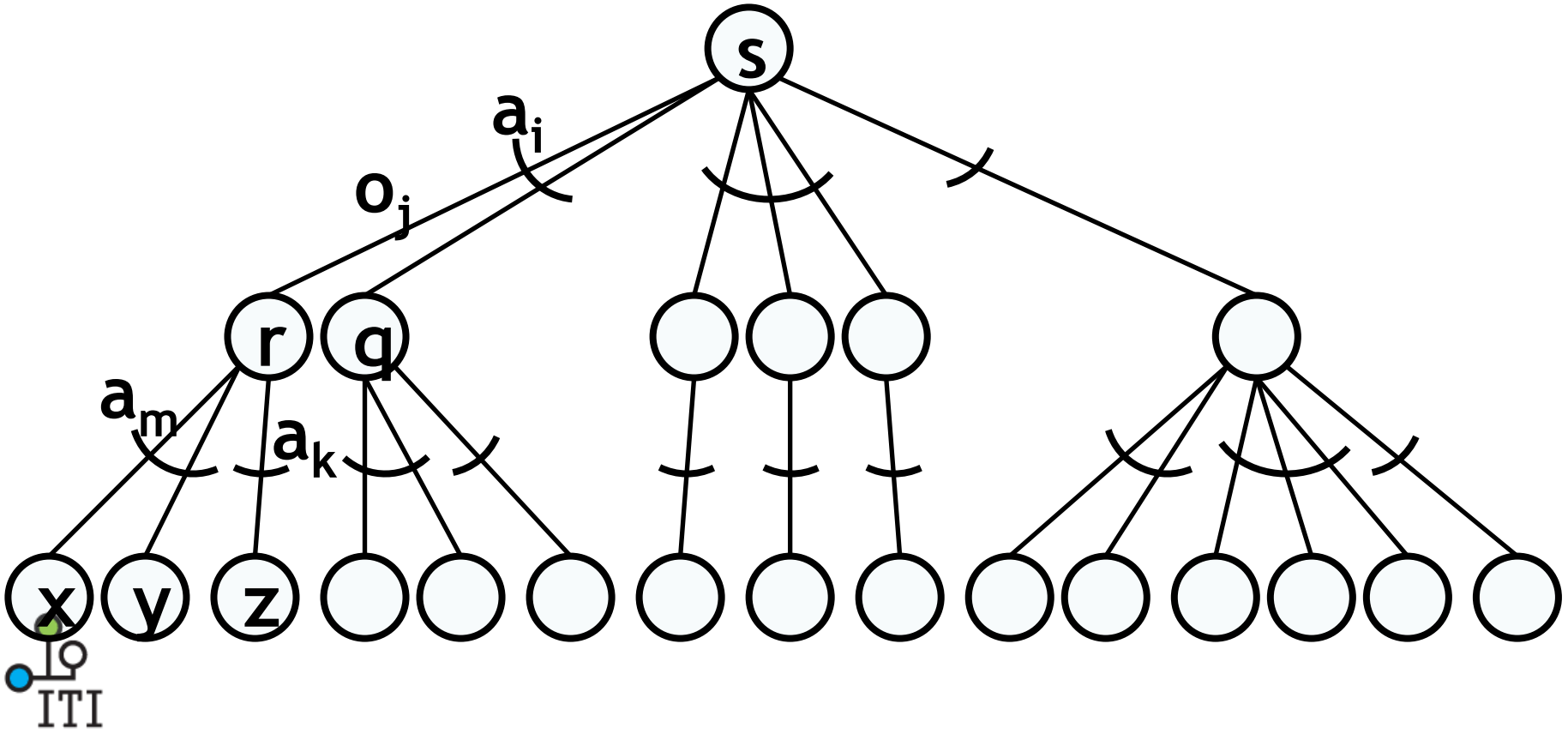
But this attractiveness calculation only considers the immediate next attack step and the immediate next states. An adversary with a planning horizon can consider future attack steps and future next states.

Selecting the Most Attractive Attack Step using a State Look-Ahead Tree (SLAT) (Planning horizon = 1)

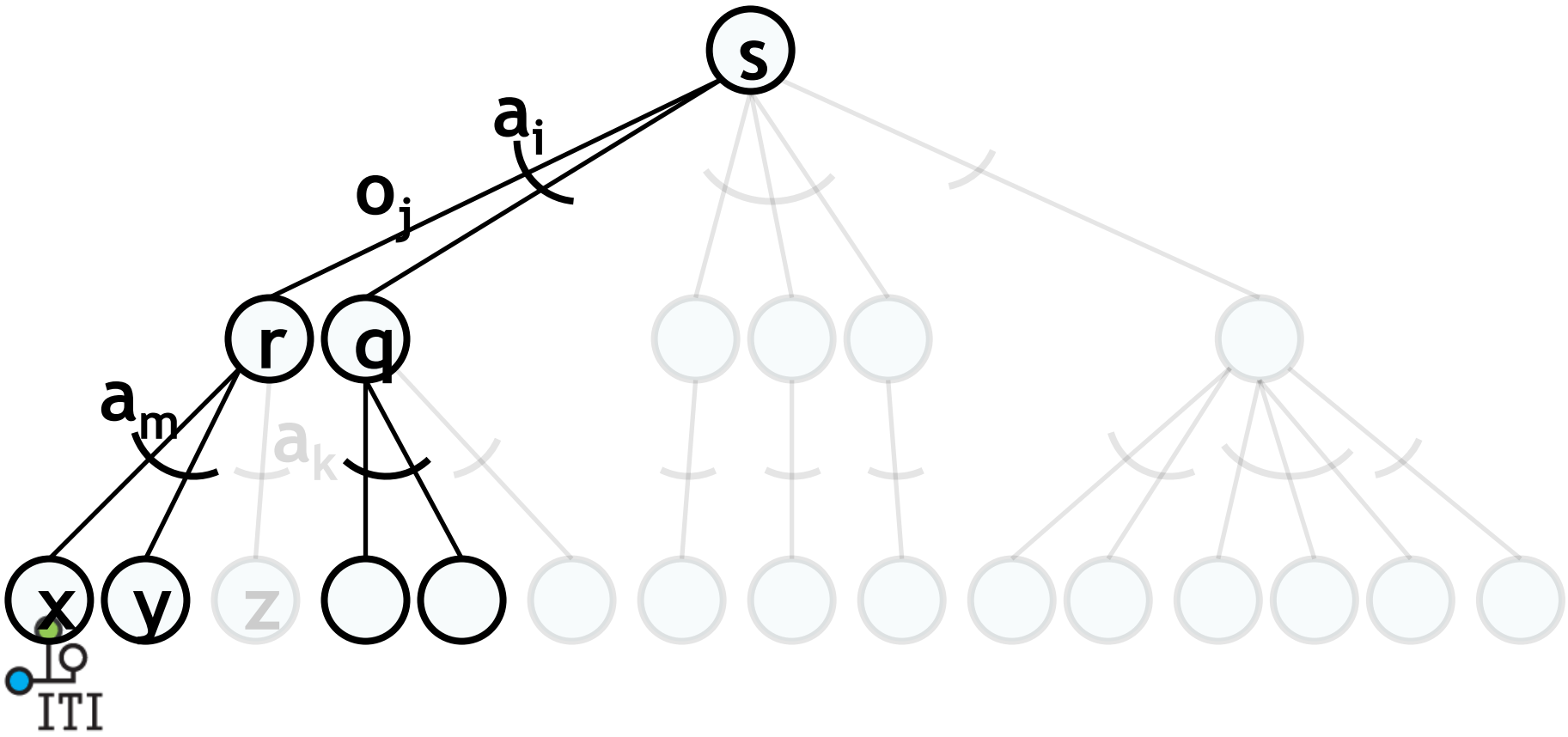


ITI

SLAT with planning horizon = 2



Pruning the SLAT (working from the bottom to the top, leaving only the most attractive attack step in each state in the SLAT)



Recursive Attractiveness Calculation Algorithm

$$\beta^N(s) \in \{a^* \in A_s | attr^N(a^*, s) = \max_{a_i \in A_s} attr^N(a_i, s)\}.$$

$$attr^N(a_i, s) = w_C \cdot C_i^N(s) + w_P \cdot P_i^N(s) + w_D \cdot D_i^N(s)$$

$$C_i^N(s) = \begin{cases} C_i(s), & \text{when } N = 1 \\ C_i(s) + \sum_{o \in O_i} (C_*^{N-1}(r) \cdot Pr_i(s,o)), & \text{when } N > 1, \end{cases}$$

$$P_i^N(s) = \begin{cases} \sum_{o \in O_i} (P(E_i(s,o)) \cdot Pr_i(s,o)), & \text{when } N = 1 \\ \sum_{o \in O_i} (P_*^{N-1}(r) \cdot Pr_i(s,o)), & \text{when } N > 1. \end{cases}$$

$$D_i^N(s) = \begin{cases} \sum_{o \in O_i} (D_i(s,o) \cdot Pr_i(s,o)), & \text{when } N = 1 \\ \sum_{o \in O_i} ((1 - (1 - D_i(s,o)) \cdot (1 - D_*^{N-1}(r))) \cdot Pr_i(s,o)), & \text{when } N > 1. \end{cases}$$

ITI

ADVISE Simulation Algorithm

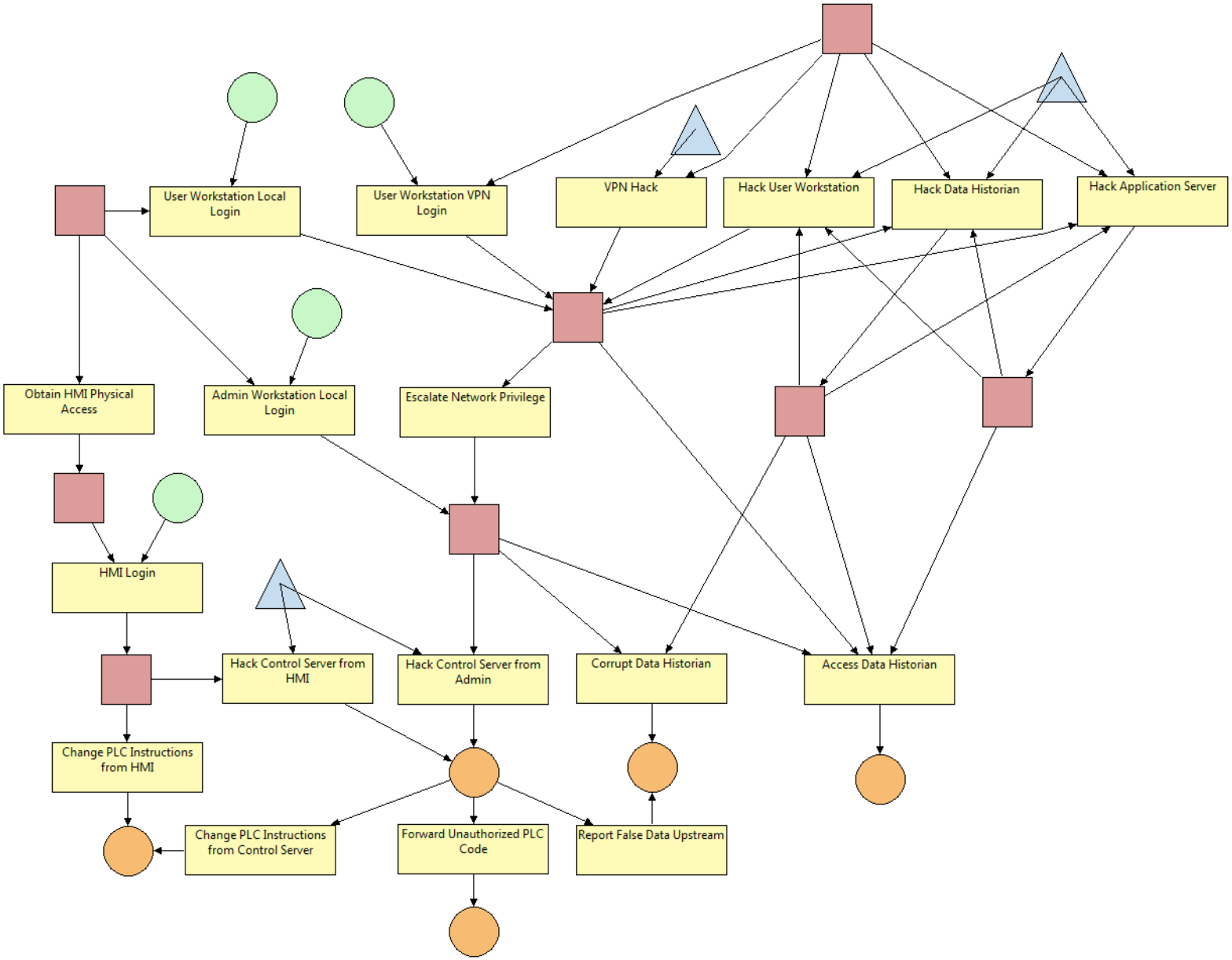
Algorithm 1 ADVISE Model Simulation

1: Time $\Leftarrow 0$
2: State $\Leftarrow s_0$
3: **while** Time $< \tau$ **do**
4: Attack$_i \leftarrow \beta^N$(State)
5: Outcome $\leftarrow o$, where $o \sim Prob_i$(State)
6: Time $\leftarrow$ Time + t, where $t \sim T_i$(State)
7: State $\leftarrow E_i$(State,Outcome)
8: **end while**

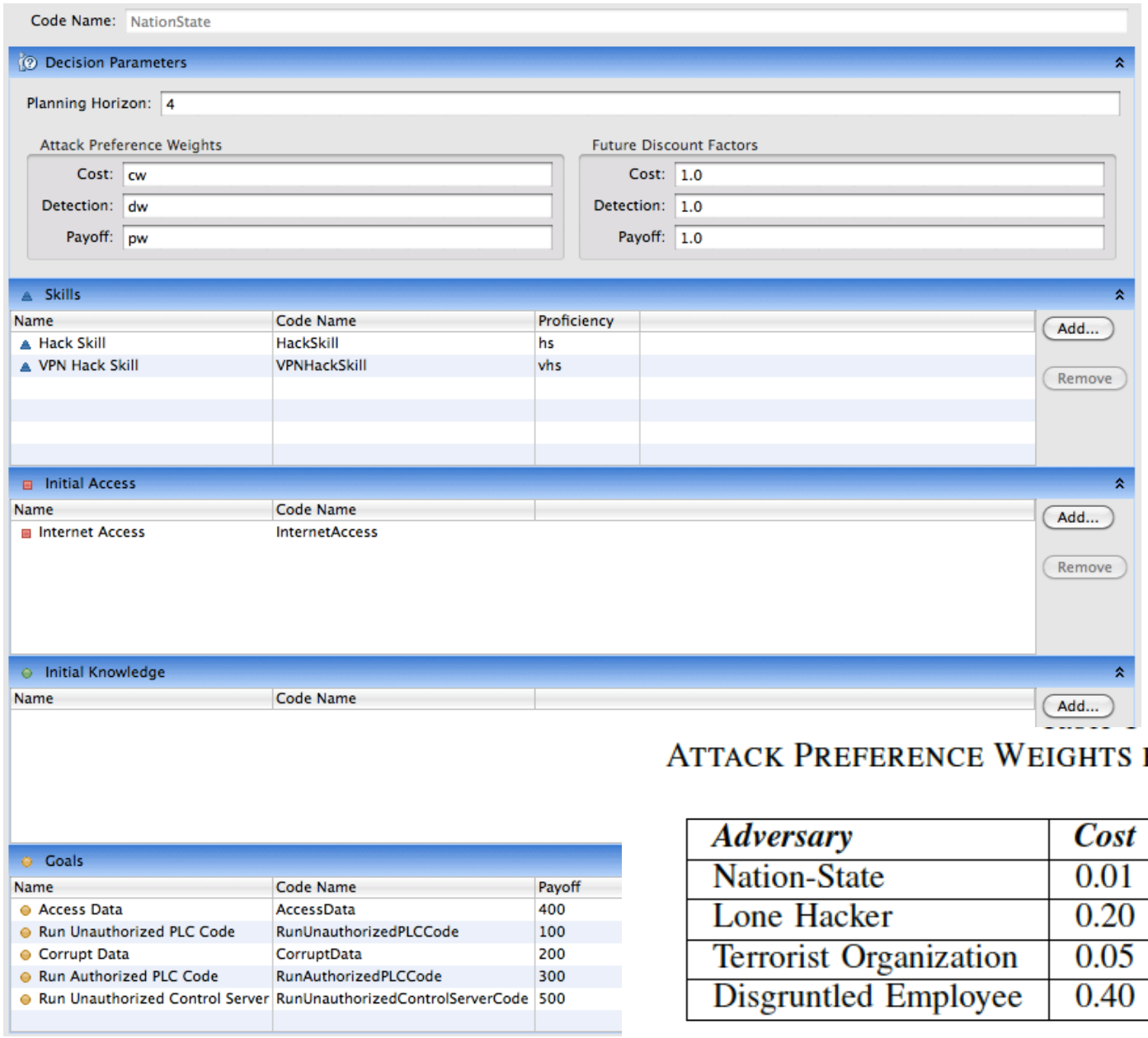
Calculating Metrics from Model Results

- Question
  - Is the corporate network security budget better spent on upgrading the local physical security or the remote access network security?
- Metric
  - Probability of confidential corporate data compromise in one year
- System configurations to compare
  - Baseline: current system configuration
  - Physical security upgrade
  - Network security upgrade
- Simulation solution: the model simulation is executed many times (10,000+), and the average metric value is calculated for each system configuration

Example SCADA System



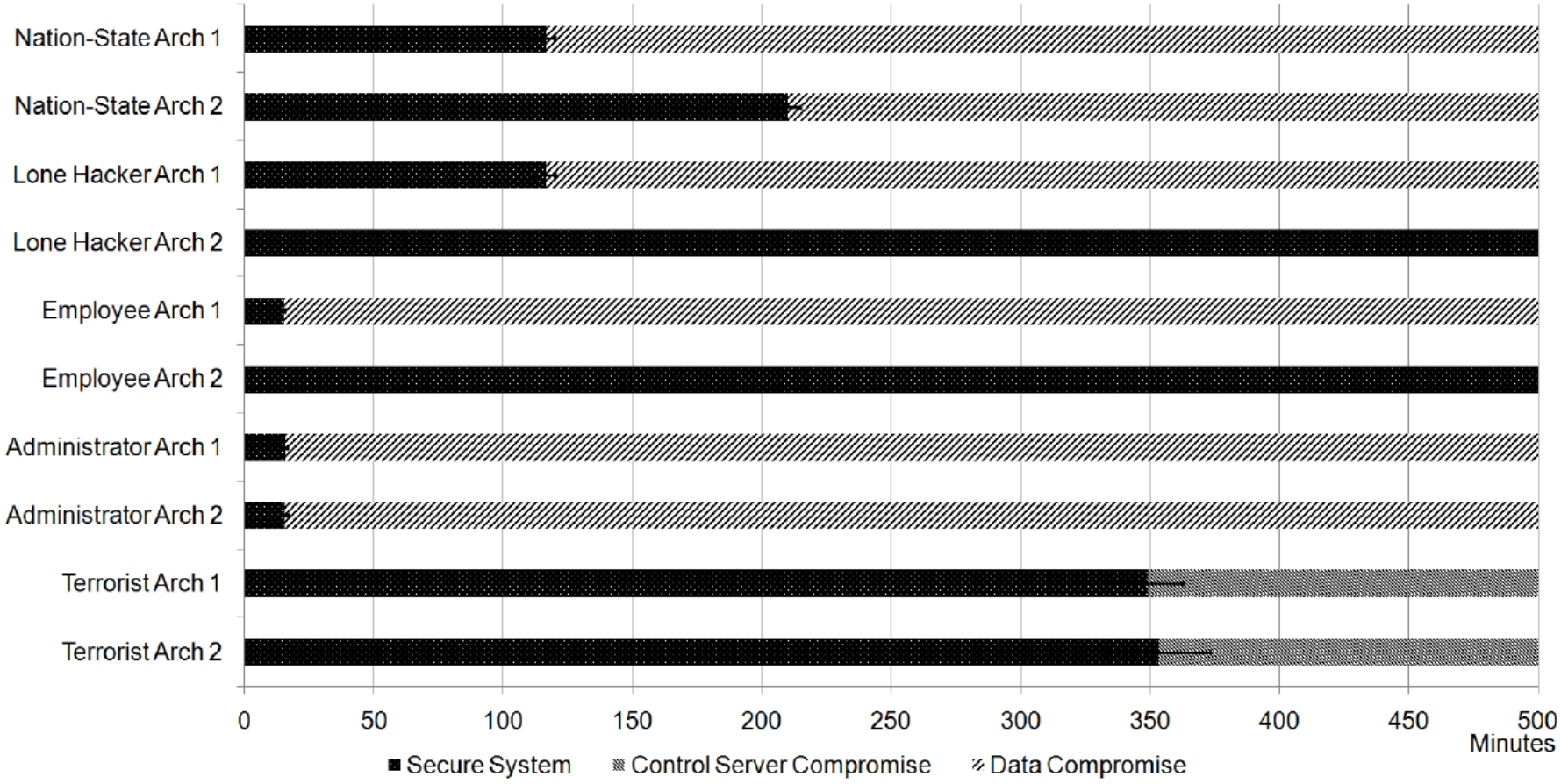
Adversary Models



ATTACK PREFERENCE WEIGHTS FOR FOUR ADVERSARIES

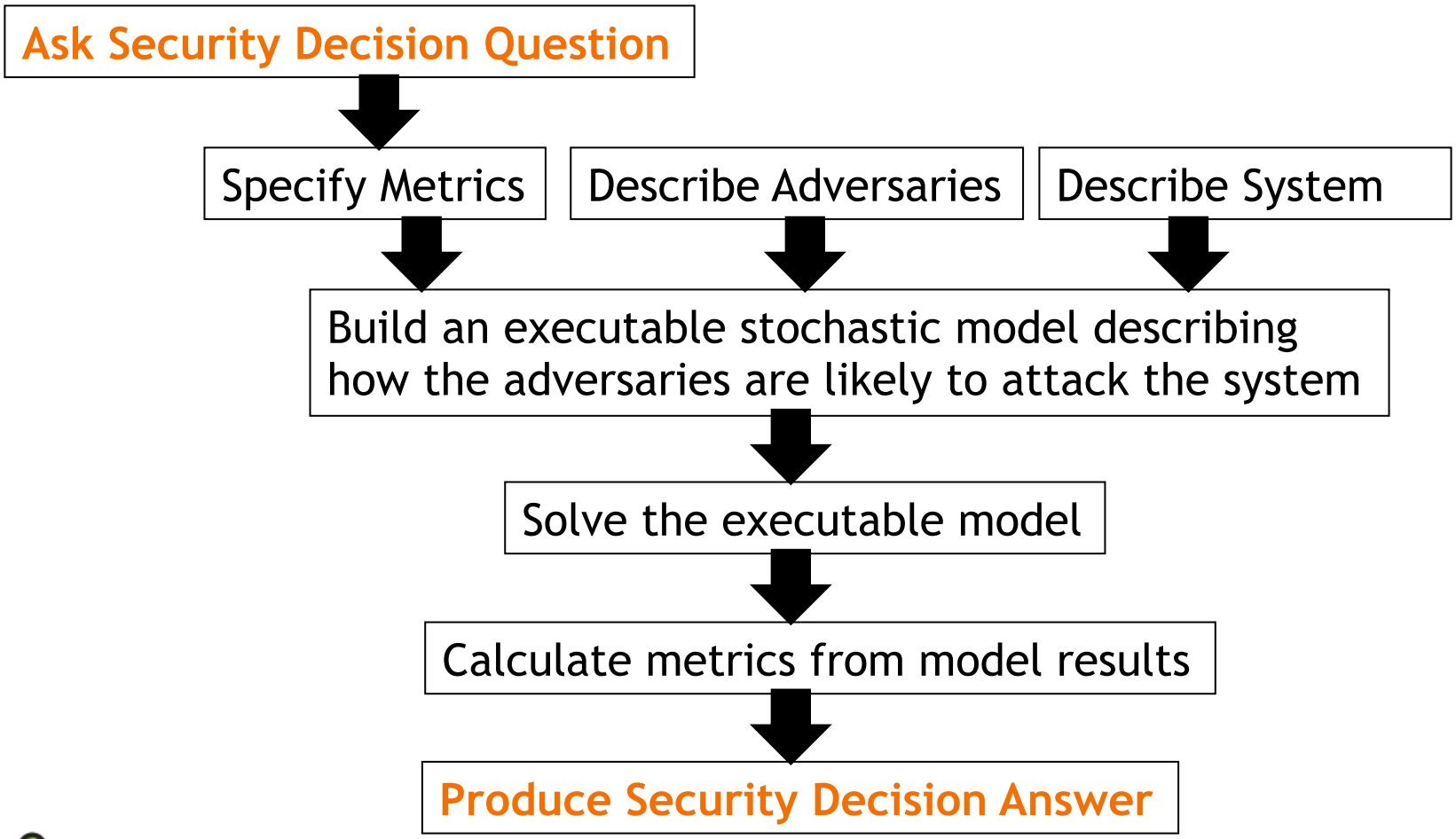
Adversary	*Cost*	*Payoff*	*Detection*
Nation-State	0.01	0.40	0.59
Lone Hacker	0.20	0.40	0.40
Terrorist Organization	0.05	0.80	0.15
Disgruntled Employee	0.40	0.50	0.10

Model Results



ITI

Summary of Metrics Process



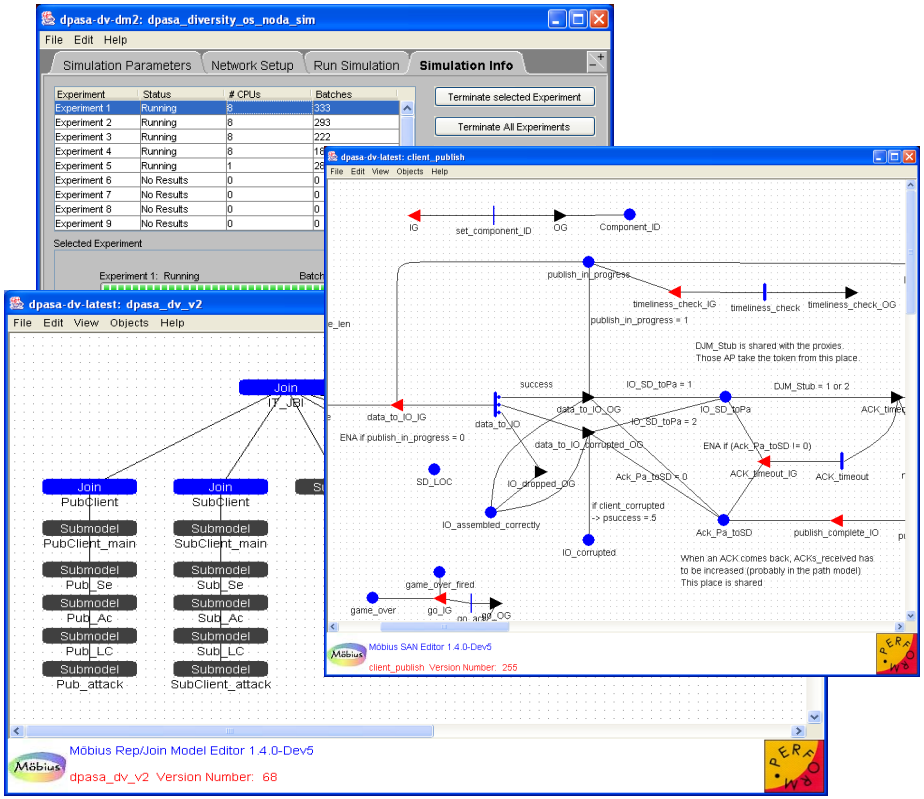
ITI

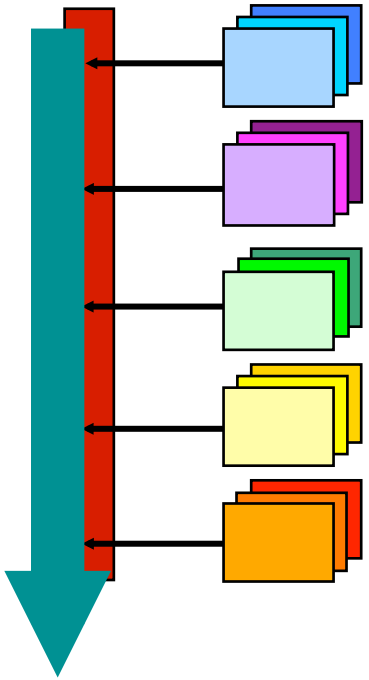
Tool Development

- Build on existing Mobius modeling toolset:
  - Enhance Mobius modeling tool to support Adversary and Attach Execution Graph Models as Atomic Models
  - Metrics results generated by discrete event simulator and analytic solvers in Mobius
  - Link to Mobius analytic solvers to provide proofs of certain (non-stochastic) properties

ITI

Möbius: Model-Based Evaluation of System Dependability, Security, and Performance





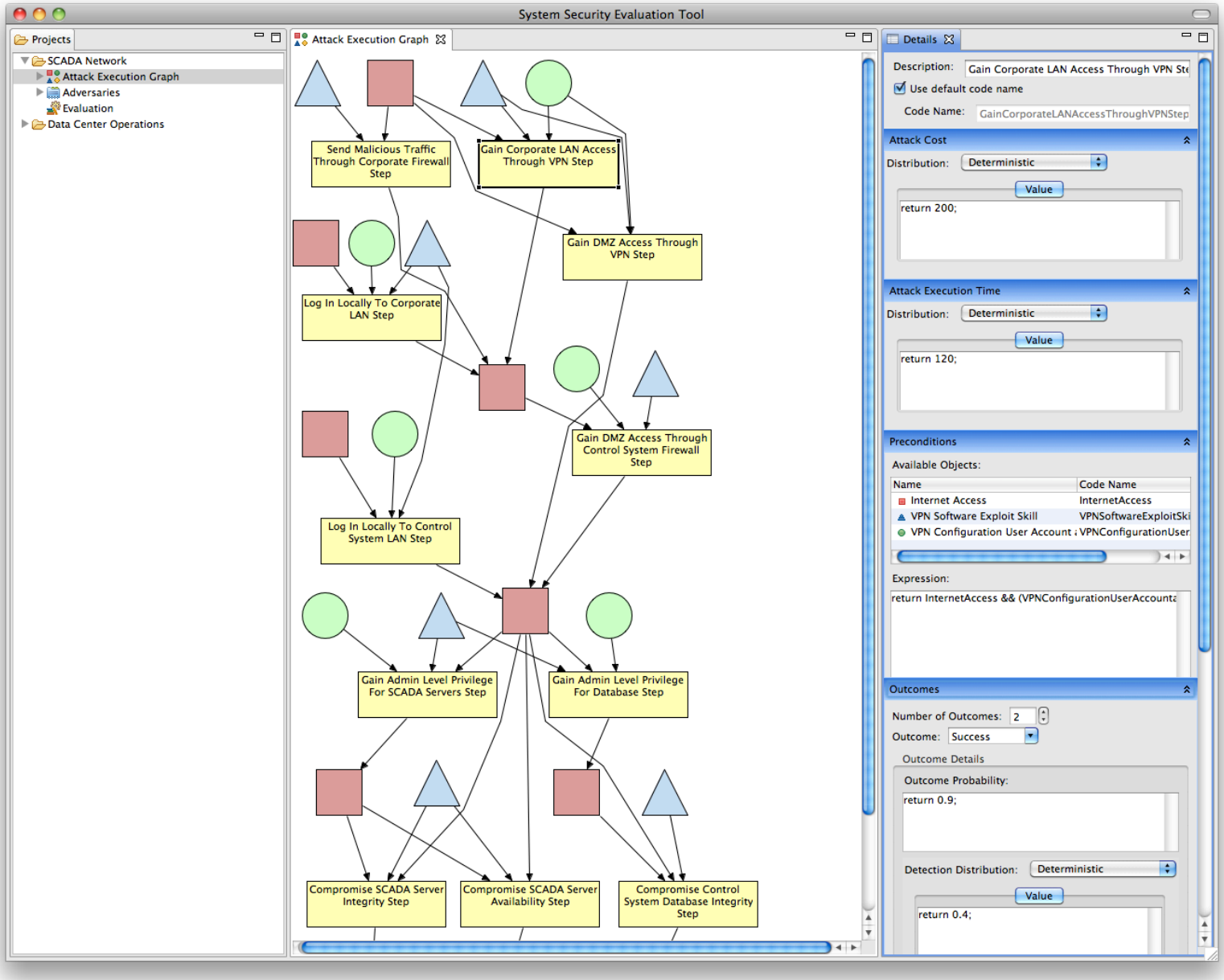
Framework Component

- Atomic Model
- Composed Model
- Solvable Model
- Connected Model
- Study Specifier (generates multiple models)

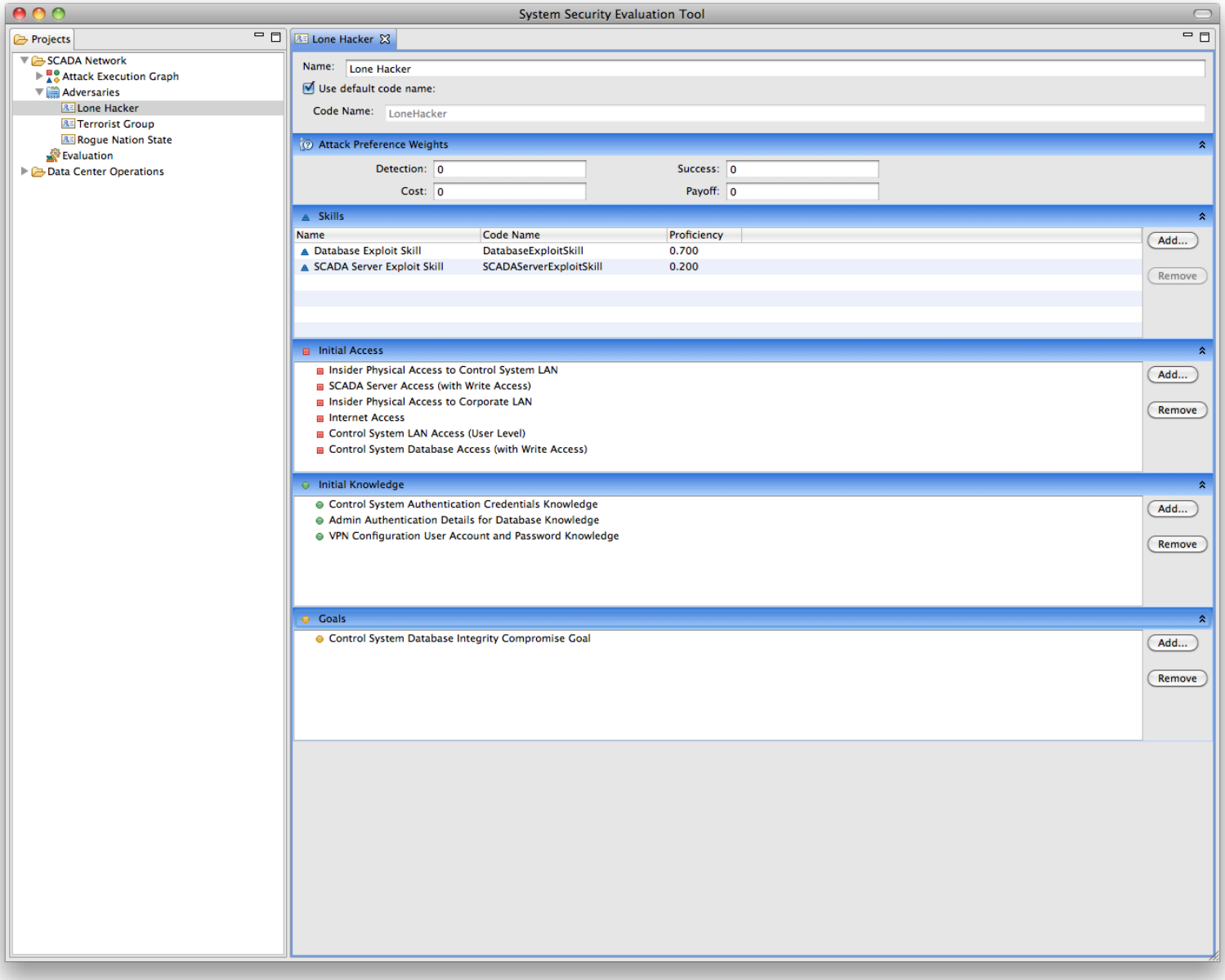
Use:

- Site licenses at hundreds of academic sites for teaching and research.
- Corporate licenses to a range of industries: Defense/Military, satellites, telecommunications, biology/genetics
- Development of new plugins for Möbius: Univ. of Dortmund, Univ. of Edinburgh, Univ. of Twente, Carleton University, and many others

Attack Execution Graph Atomic Model Editor



Adversary Atomic Model Editor

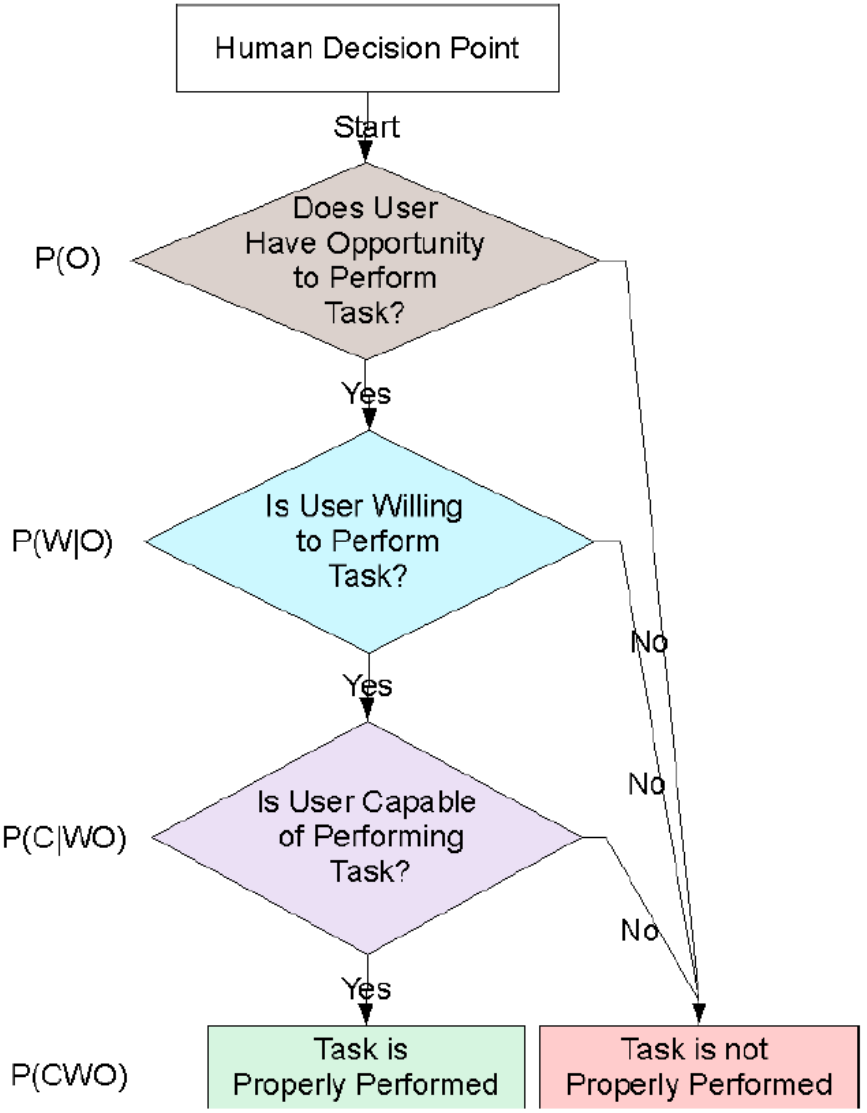


ITI

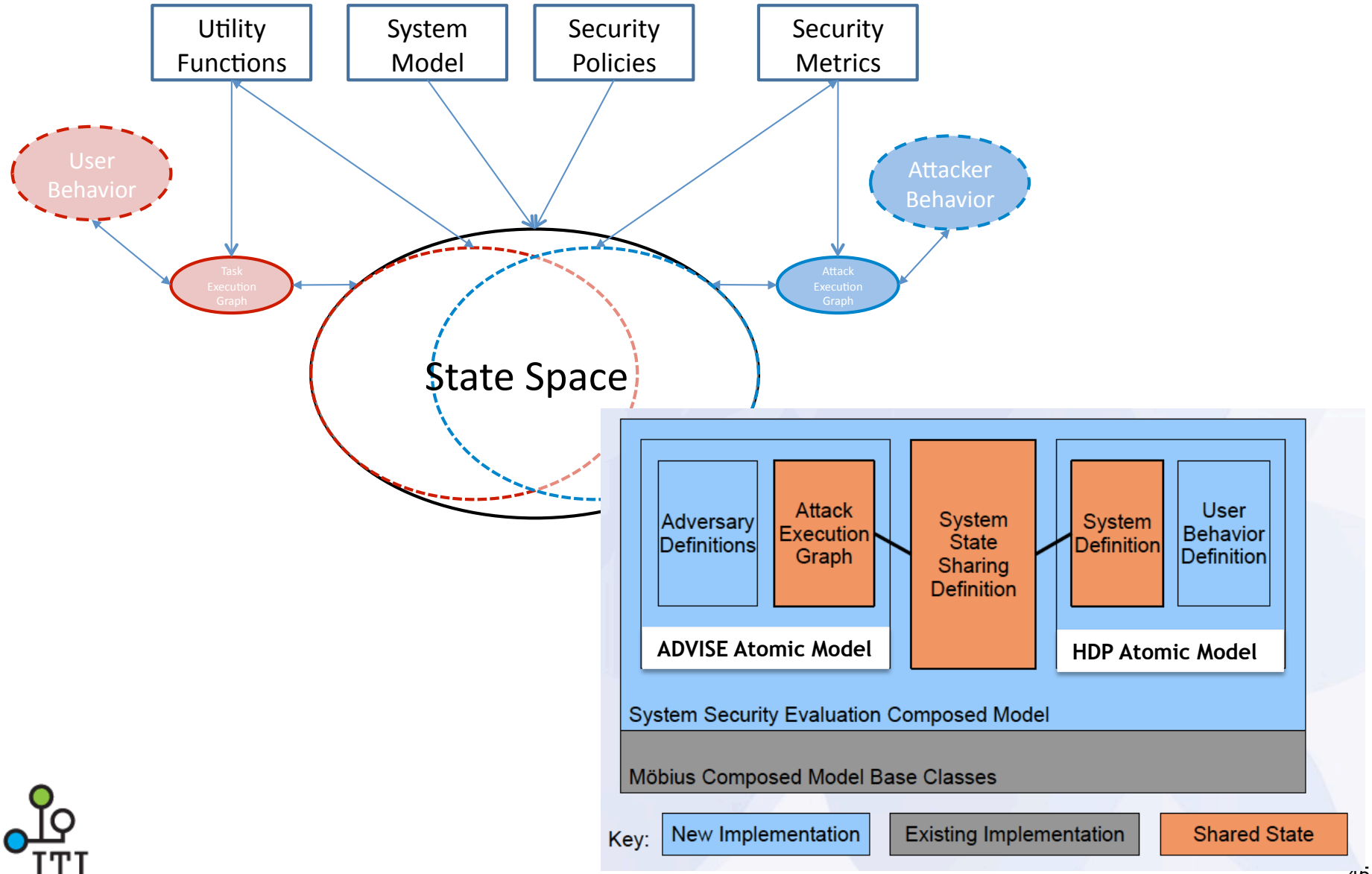
New Work: Model Impact of HDPs on System Security

Model "Good" humans, as well as attackers in the system

- *Users can significantly effect system security*
- *Example: More stringent security measures can lead to behaviors that compromise security*
- *Solution: Model user behavior using Human Decision Points*
- Human Decision Point (HDP) – Task in which Human decision is "deemed" significant
- Understand: Opportunity, Willingness, and Capability



Putting it all together: Understanding User-Attacker Behavior Tradeoffs



Conclusions

- Since system security cannot be absolute, quantifiable security metrics are needed
- Metrics are useful event if not perfect; e.g., relative metrics can aid in critical design decisions
- New formalisms/modeling approaches are needed that
  - Are rich enough to adversary, user, and system behavior
  - Natural for security analysts
  - Semantically precise
- Work in these directions is ongoing (e.g. see other work in RACI and MetriSEC workshops) but must more needs to be done