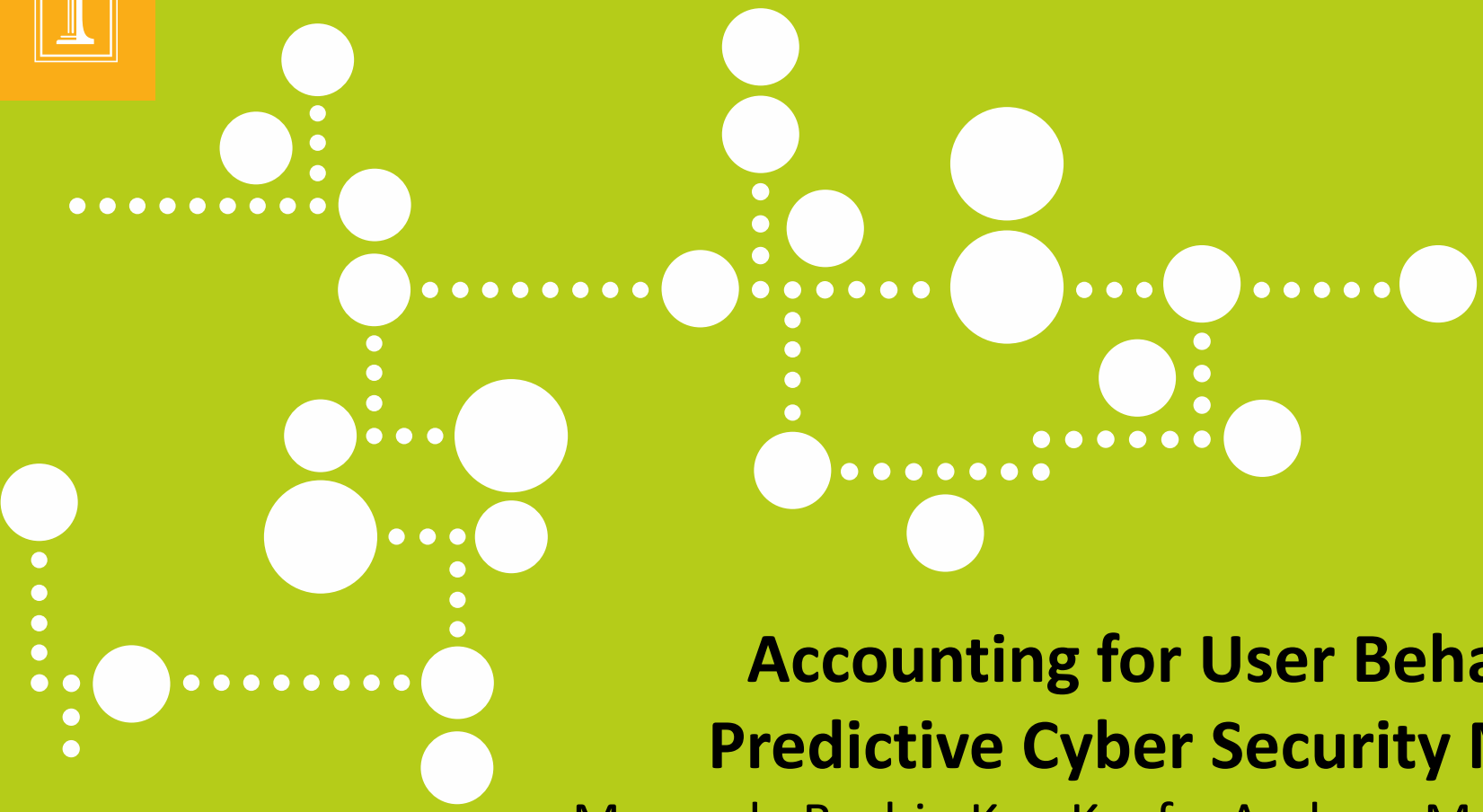




# Accounting for User Behavior in Predictive Cyber Security Models

Masooda Bashir, Ken Keefe, Andrew Marturano, Mohammad Noureddine, **Bill Sanders**

# The Problem: Humans Make Mistakes

- Humans are involved in most security incidents
- Public utility compromised, 2014
  - Hackers took advantage of a weak password security system at a public utility in the US
- Cook County highway department shutdown, 2013
  - A County employee allowed a virus infection by surfing the web, or using a flash drive from home
- US Electric utility virus infection, 2012
  - A third party technician used a USB drive that was infected with a virus

Repository of Industrial Security Incidents (http://www.risidata.com/)

# Motivation: Usable Security

- Attempt to design systems that are usable by non-expert users
- Create designs conforming to the concept of *"psychological acceptability"*
  - security software must not make it harder for users to perform their daily tasks
- Designers use knowledge based on empirical studies to understand how users think and use their designs
- But this approach alone cannot *predict* how effective a particular approach will be

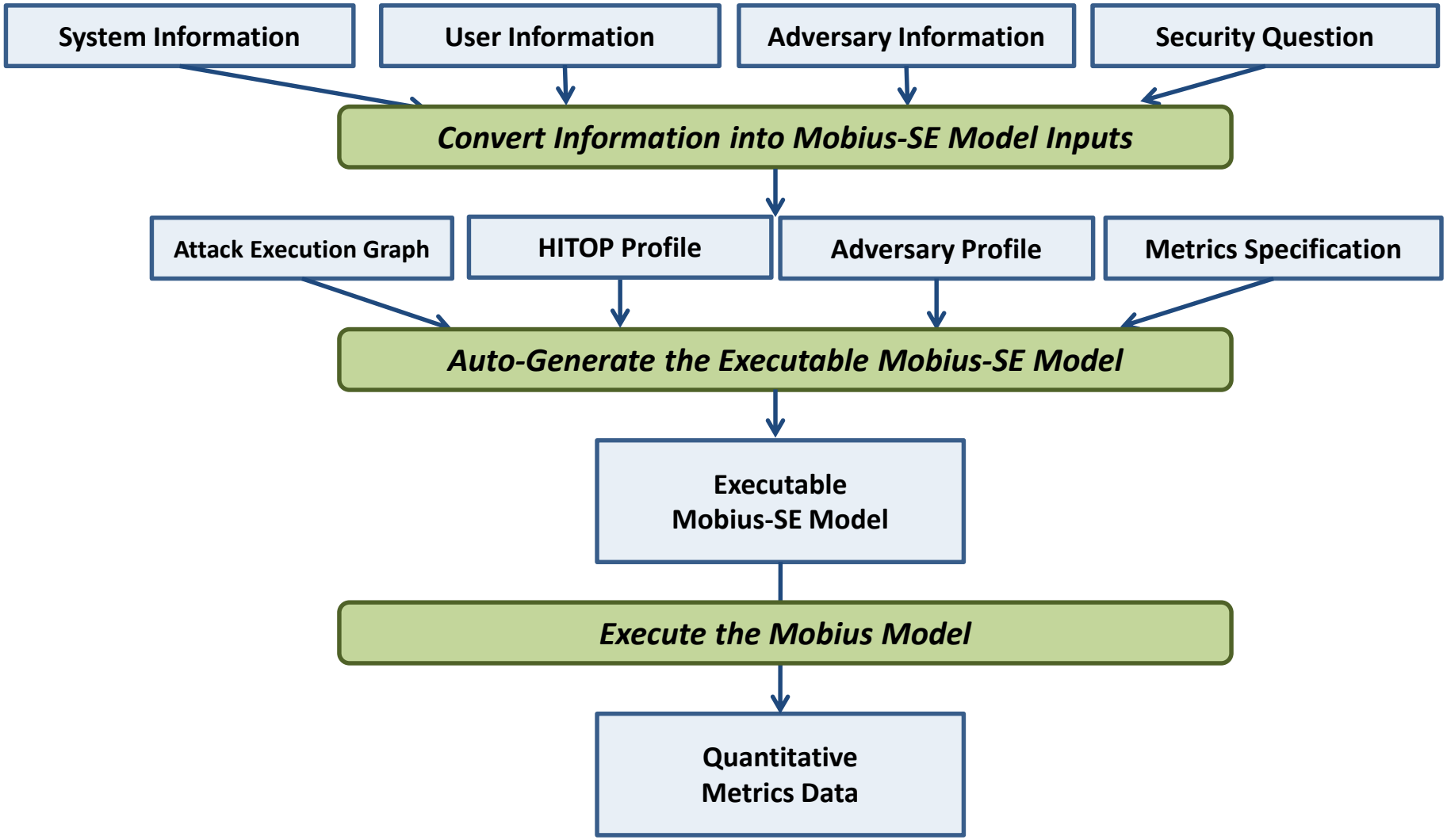
# Quantitative Metrics

- System security is not absolute
  - No real system is perfectly secure
  - Some systems are more secure than others
  - Some policies provide more security
- System metrics often neglect human aspects
  - Does making the password policy more complex make the system more secure?
  - How frequently should we ask users to change their passwords?
  - Should we adopt a sanctions and rewards policy?

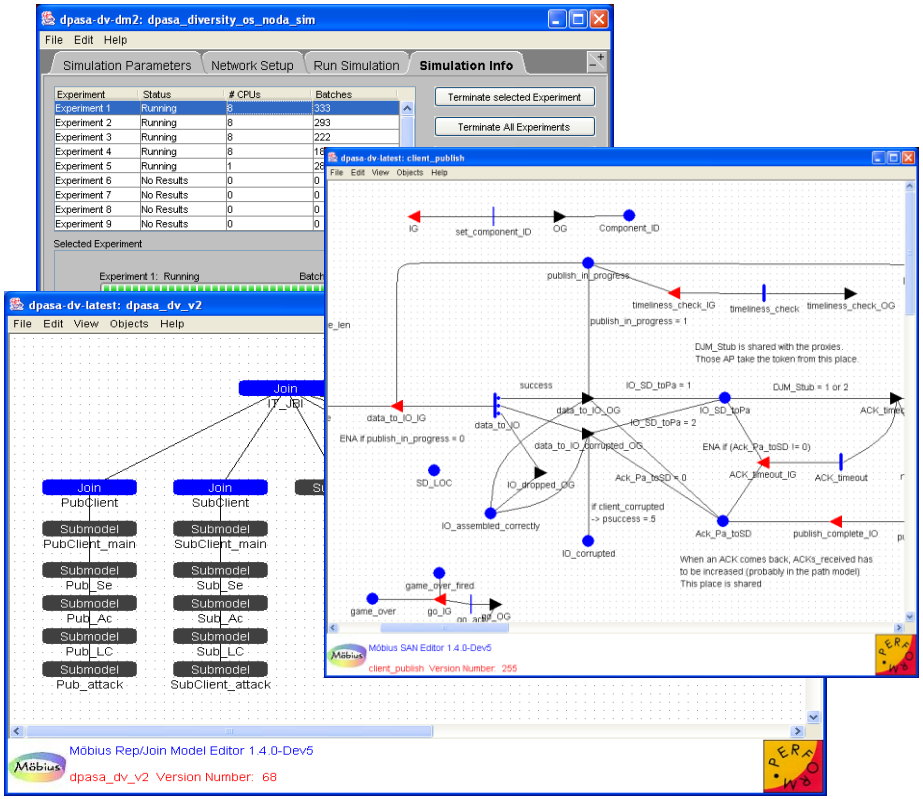
# Mobius-SE Security Evaluation Approach

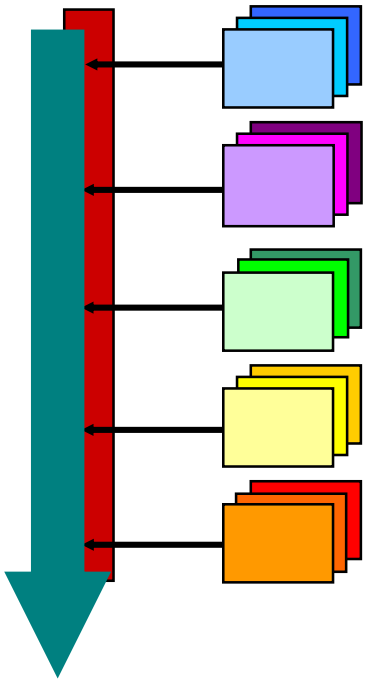
- Adversary-driven analysis
  - Considers characteristics and capabilities of adversaries
- Account for user behavior
  - Account for user behavior and its impact on system cyber security
- State-based analysis
  - Considers multi-step attacks
- Quantitative metrics
  - Enables trade-off comparisons among alternatives
- Mission-relevant metrics
  - Measures the aspects of security important to owners/operators of the system

# Overall Goal: Mobius-SE Quantitative Security Evaluation Tool



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



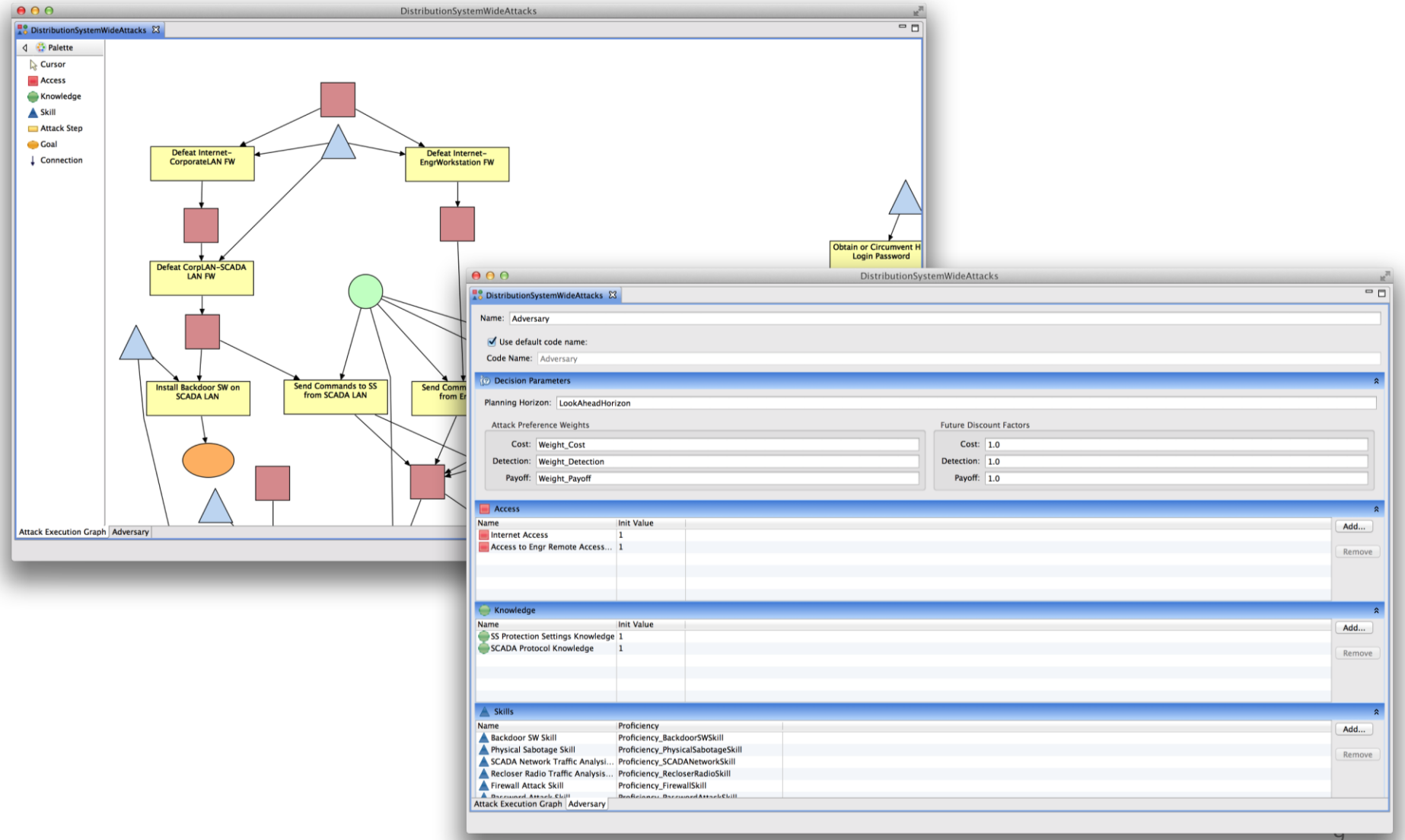
Framework Component

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

## Use:

- Academic 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

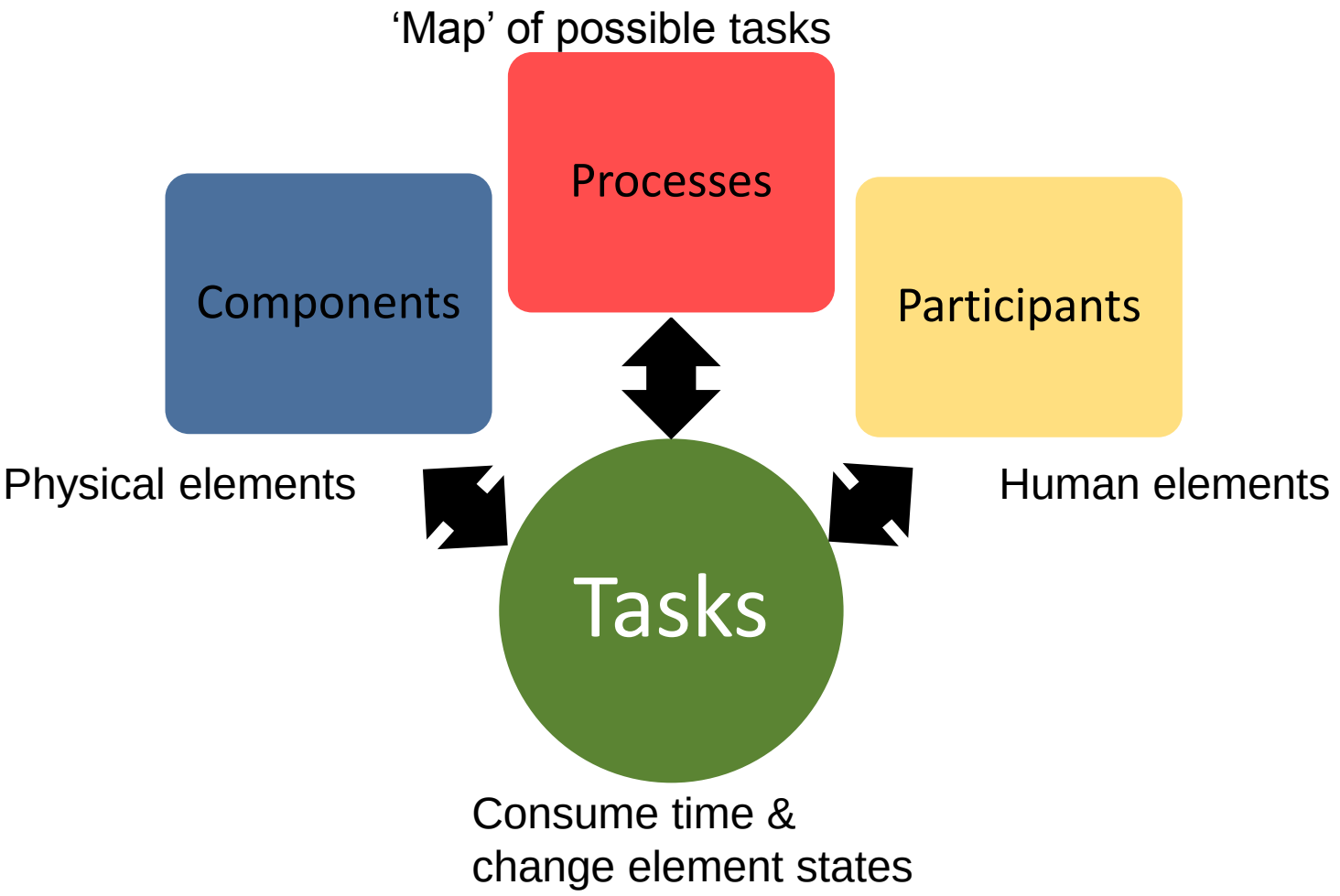
# Adversary Modeling in Mobius-SE



# NSA SoS Project Objective: Account for User Behavior in Quantitative Security Models

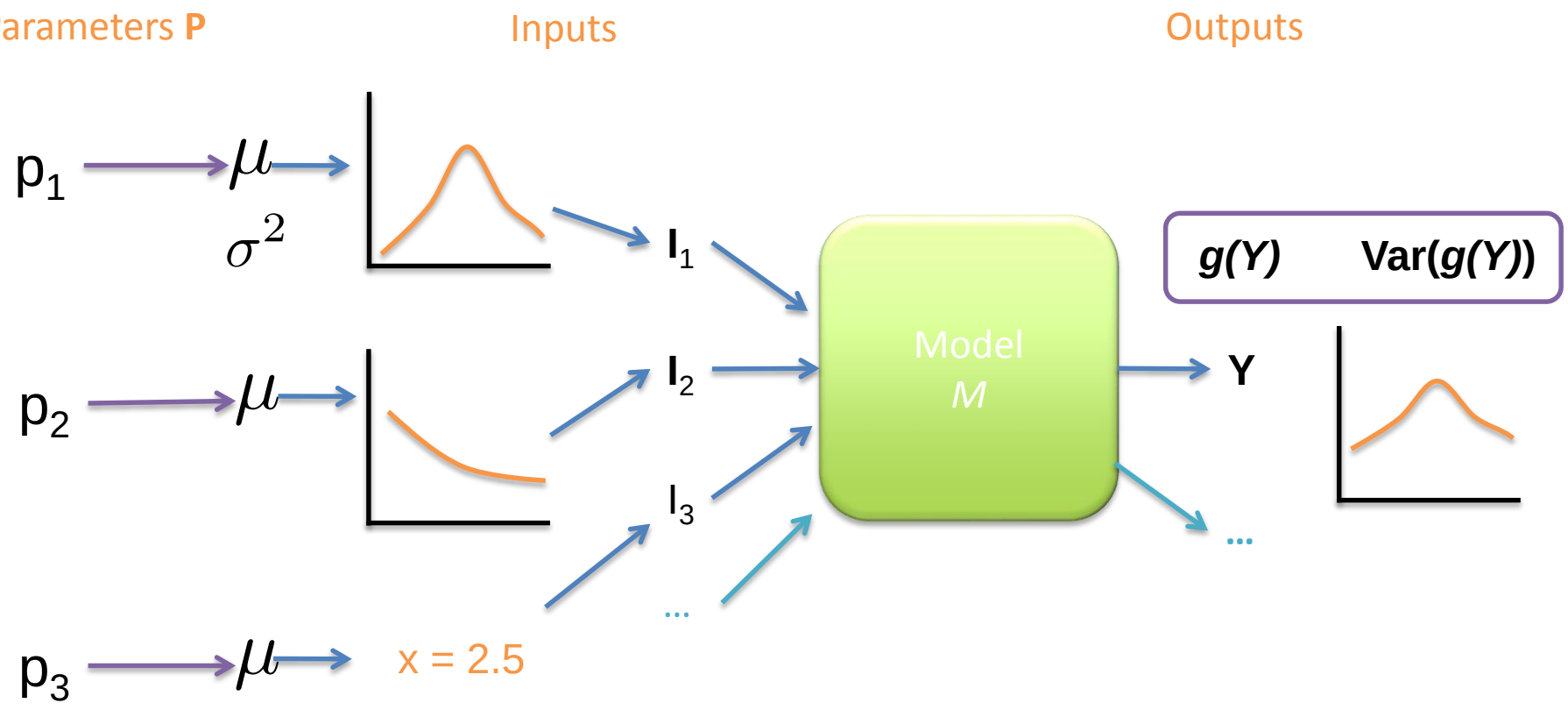
- Year 1
  - Complete HITOP implementation – Complete
  - Design data collection algorithm for model parameters – Complete
- Year 2
  - Develop prototype data collection tool – In Progress
  - Execute case study to test approach – In Progress
  - Refine both implementations base on case study results – Upcoming
- Year 3
  - Build a stable tool for distribution – Upcoming
  - Develop two additional case studies – Upcoming
  - Further refine tools from feedback from case studies and third party users – Upcoming

# HITOP Modeling Formalism




a process is a structured flow of tasks performed by one or more participants using one or more components.

# Statistically-Driven Data Collection Algorithm (HotSoS '15)



# Remainder of This Talk

- Reviews theories that explain the behavior of human users in the cyber world
- Presents a sample case study that illustrates the impact of human decisions on system security
- Suggests directions for future work

# Theories of Human Behavior

- Psychologists, social scientists, as well as computer science researchers have attempted to explain the behavior of users in the cyber world
- They present several theories that provide guidelines to understand and improve the behavior of users
- *Normative theories*: how things should be, ideal behavior
  - Easier to quantify
- *Descriptive theories*: how things are, describe actual behavior
  - Harder to quantify

# Rational Choice Theory

- Ideally, humans should make decisions by balancing costs and benefits of each of the possible actions [Bulgurcu, 2010]
- Bounded rationality
  - Collect bounded information about the possible actions and choose the one that gives the best cost/benefit ratio
- It is frequently used in economics to predict market information
- Highlights factors affecting human decisions in cyber space such as
  - Workload
  - Experience
  - Training [Kreamer, 2007]
- *But it is also criticized by psychologists and social scientists claiming humans are not rational in their decisions* [Schneier, 2008]

# General Deterrence Theory

- Focuses on disincentives or sanctions against "bad" security behavior and decision making [D'Arcy, 2009]
- Originally popular in the Cold War
  - Have enough nuclear power to *deter* a more powerful opponent from attacking you (before the attack happens)
- For security policies
  - Impose enough sanctions on the employees of a company to prevent them from neglecting security policies
- It can be useful in the context of firms, but what about clients or home users?

# Other Theories

- Theory of Planned Behavior [Ifinedo, 2012]
  - Highlights personal as well as social factors that affect human users in the cyber world
  - What is the user's perception of security? How do the beliefs of other people affect individual users' views?
- Social Learning Theory [Theoharidou, 2005]
  - Describes the effect peers and superiors have on the individual decisions of employees and general users
- Neutralization Theory [Siponen, 2010]
  - Users rationalize non-compliant behavior to avoid guilt
  - Example: "my bank should handle all my data and money very carefully so I do not have to worry about it"

# Challenges

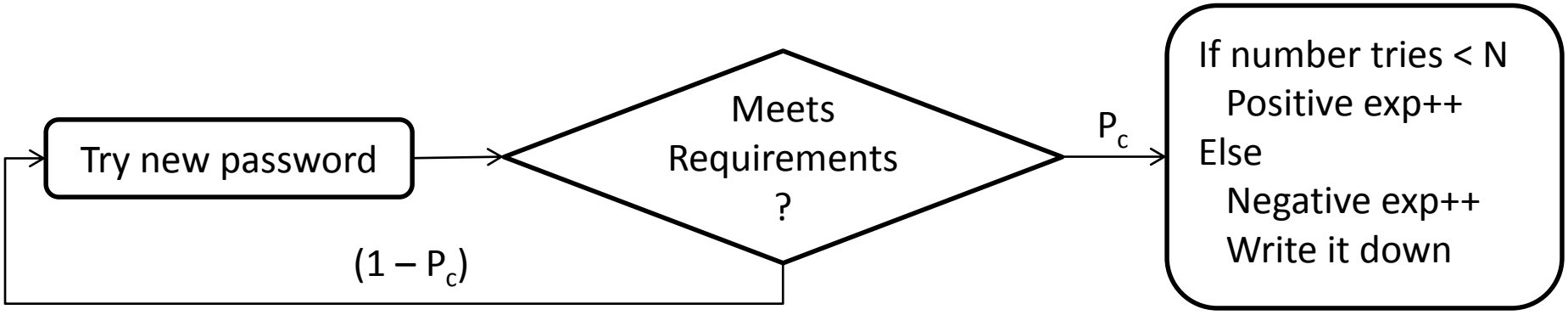
- Turning human behavior models into executable mathematical models that can be used for analysis
  - Descriptive theories are closer to reality but are harder to quantify
  - Normative theories are easier to quantify but they can be different than the real world behavior
- Our initial case study illustrates the use of bounded rationality and deterrence theory in the context of cyber-security

# Motivating Case Study

- Model the password dynamics in a typical firm
- The firm's managers define the complexity of the password policy
- They make recommendations about the frequency of password reset requests
- The firm performs regular audits every two weeks and sanctions violating employees
- We study the correlation between the security policy and the system's security, taking into consideration the behavior of the employees

# Password Change Process

- $P_c$: probability the tried password meets requirements
- The employee tries to compose new passwords
  - If she creates a successful password in less than N tries, she considers it to be a positive experience
  - If she fails to create it, she considers the password to be too complex and writes it down on a sticky note next to the computer



# Attacker model

- We assume attackers are attempting to steal data from the firm
- The attackers are both insiders and outsiders
  - Outsiders attempt brute force attacks to gain access to employee accounts
  - Insiders seek written down passwords to gain unauthorized access
- The probability of a successful brute force attack depends on the complexity of the password policy
  - We assume it is 0.10 lower than $P_c$
- The probability of a successful insider attack depends on whether employees have written down their passwords
  - We assume is it 0.7 if employee have written it down, 0.05 otherwise

# Security Utility

- We use utility functions to study the impact of the security policy on the security of the system

$$\text{Security utility} = \frac{\text{Successful attacks}}{\text{Total attacks}}$$

- We vary the password complexity ($P_c$) and the password write threshold (N)

# Employee Utility

- The employee utility illustrates the relative "happiness" of the employee given the firm's security and sanctions policy
- It incorporates sanctions, positive and negative experiences and their cognitive load
  - Our future work also focuses on availability and productivity as part of the employee's utility

$$\text{Employee utility} = \alpha \times \frac{\text{positive exp}}{\text{total exp}} - \beta \times \text{sanctions} + \gamma \times \text{rewards} - \epsilon \times \text{cognitive load}$$

- α and $\gamma$ are positively scaling parameters
- β and **ε** is a negatively scaling parameters

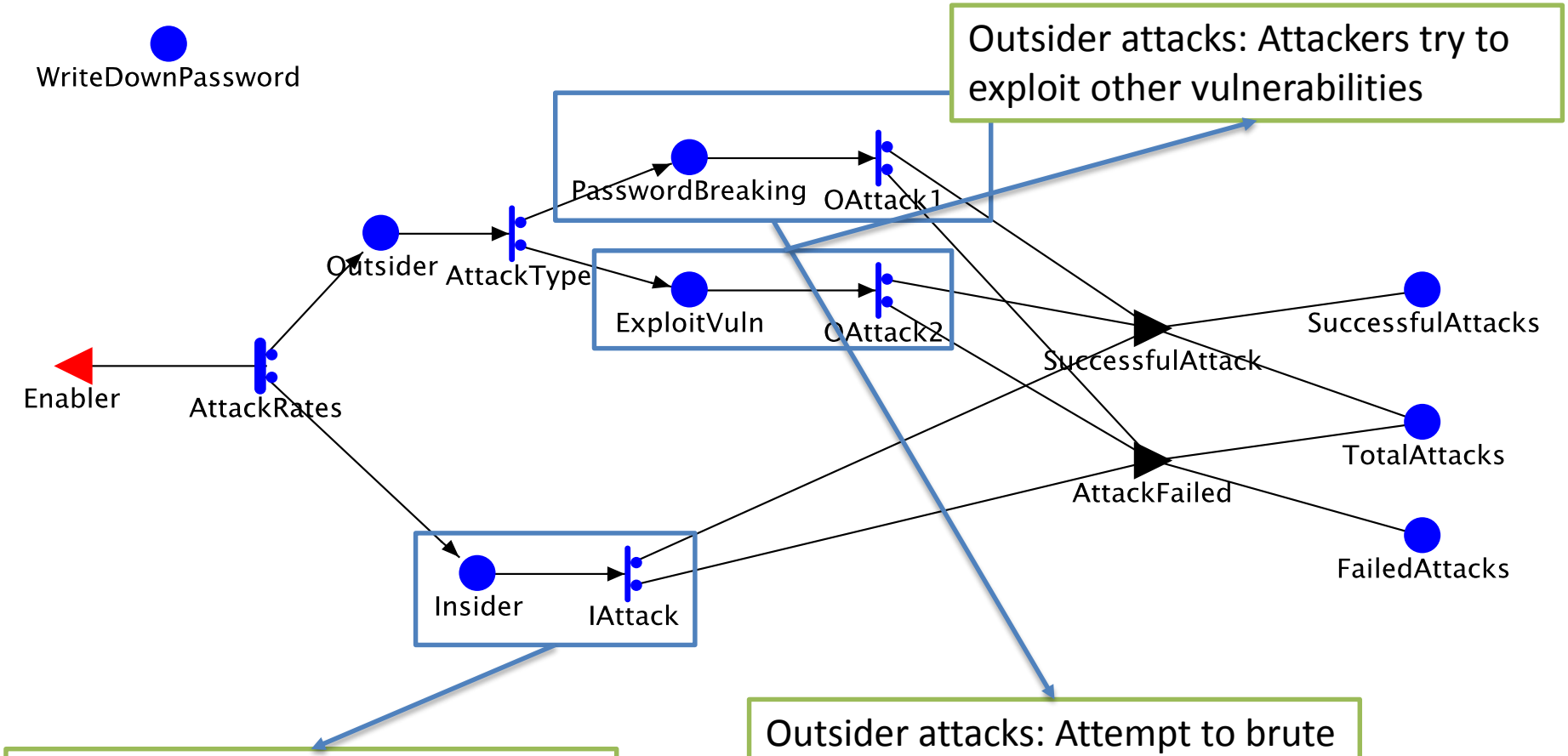
# Utilities

- Utility functions are an application of the bounded rationality theory
  - We used $\alpha = 0.1$, $\beta = 0.3$, $\gamma = 0.2$, $\boldsymbol{\varepsilon} = 0.1$
- Setting $\beta = 0.3$ will assign more weight on the sanctions
  - This is in accordance with the general deterrence theory

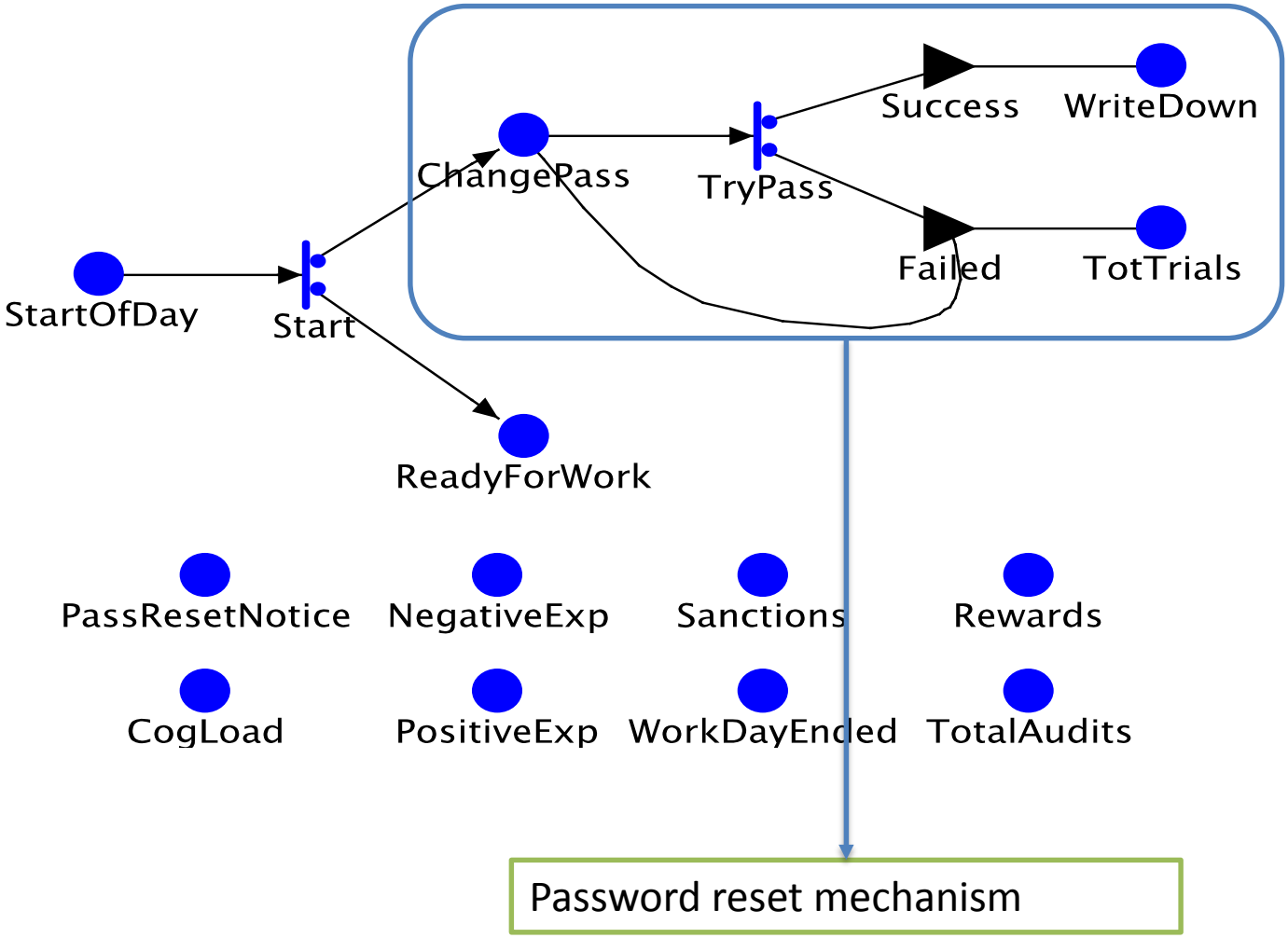
# Implementation and Simulation

- We modeled the attacker, the employee and the password reset mechanism using Stochastic Activity Networks (SAN)
- We ran our simulation for a period of 6 simulation months
- We gathered results for the security utility for various password complexities and password write-down thresholds

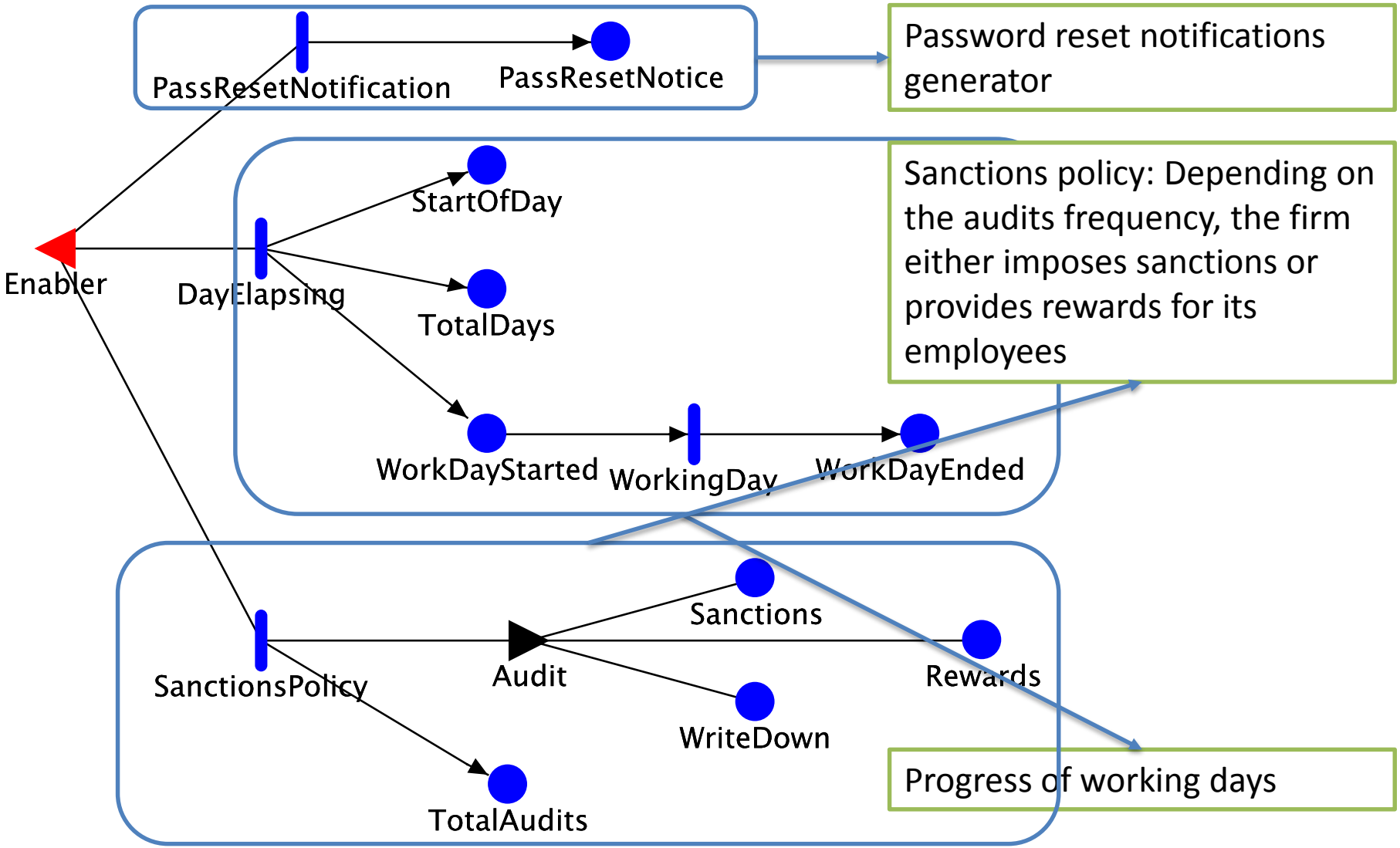
# SAN Models: Attackers



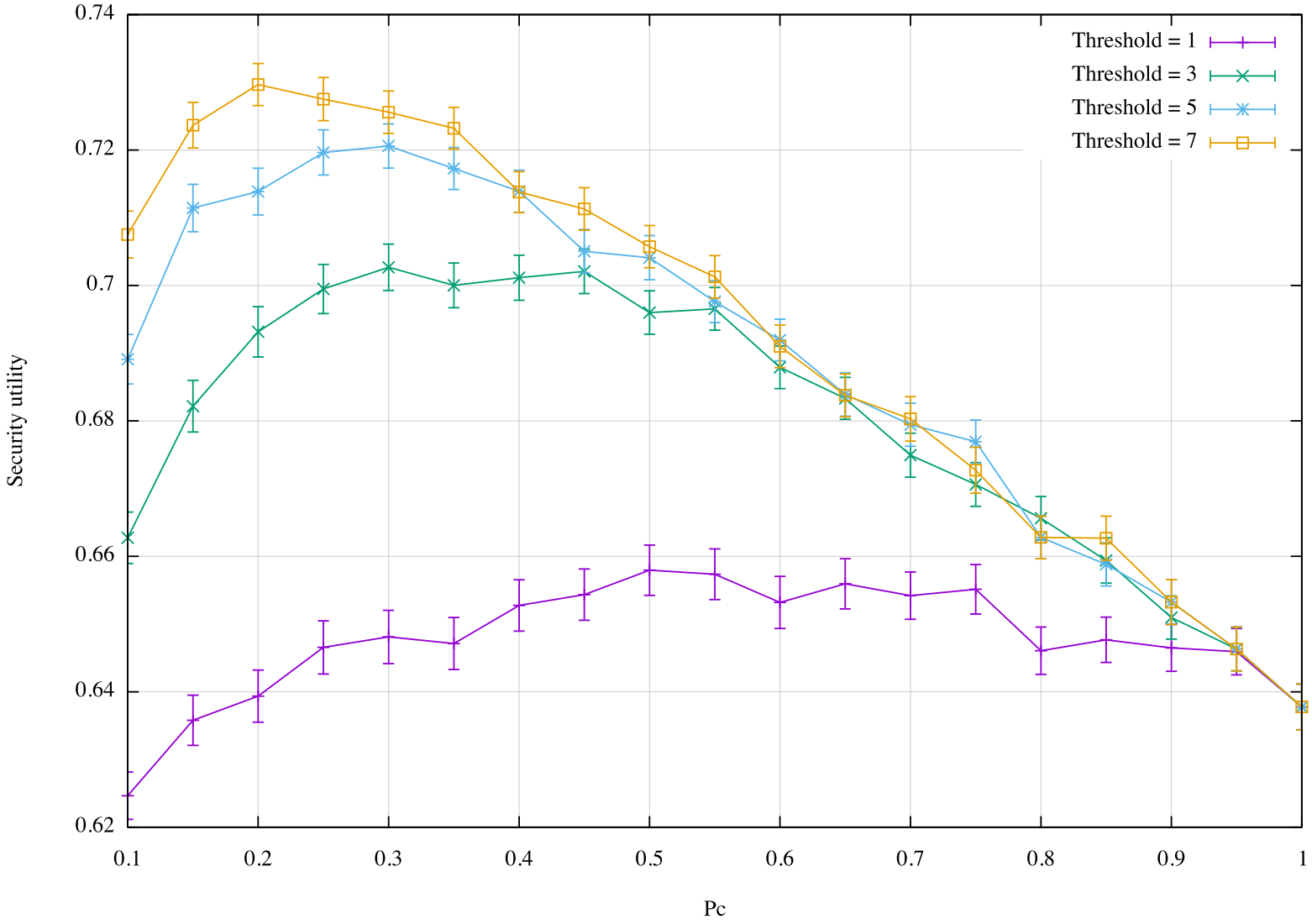
# SAN Model: Employee



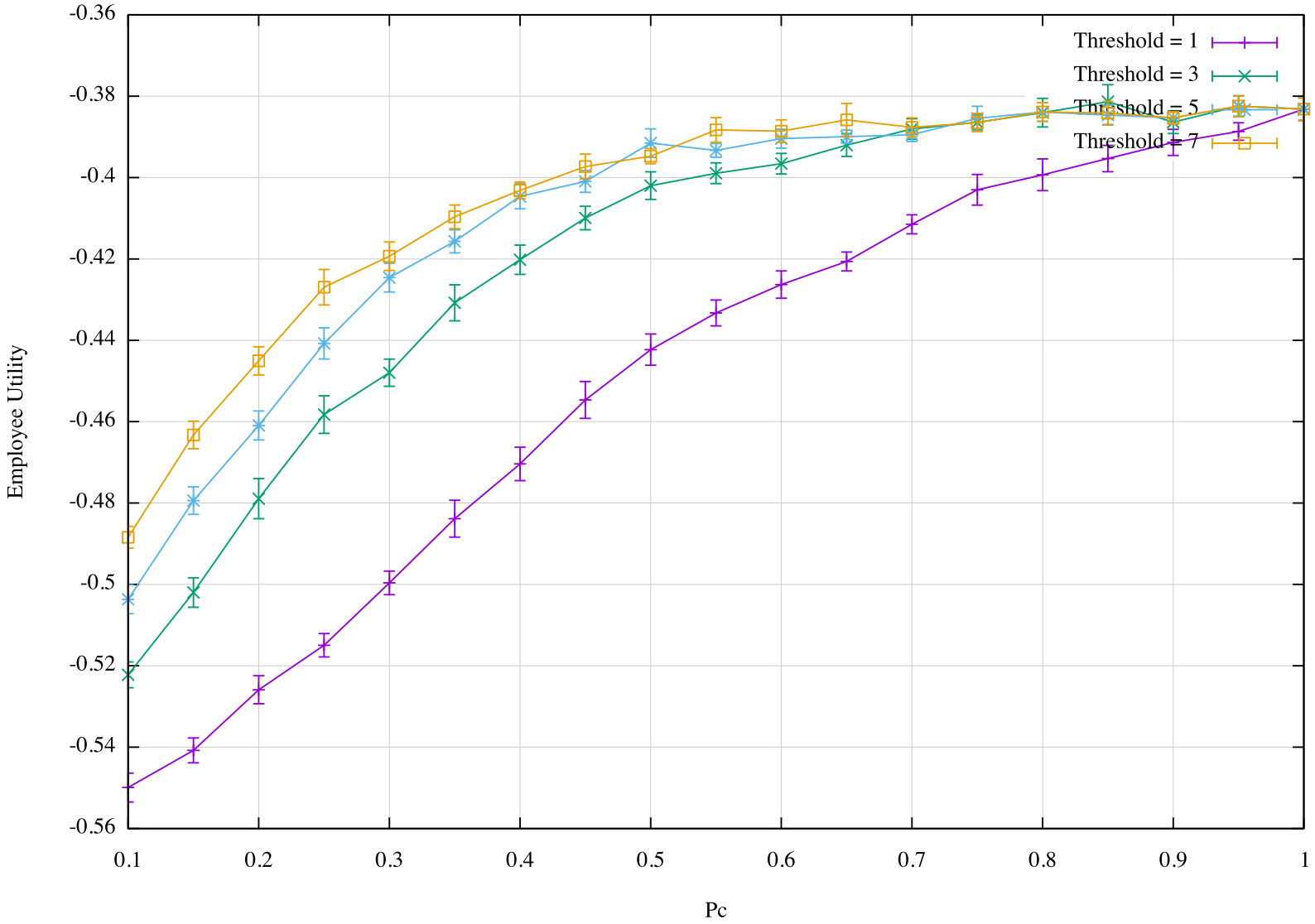
# SAN Model: Security Policy



# Preliminary Results: Security utility



# Preliminary Results: Employee Utility



# Discussion

- Our results conform with general deterrence theory
  - Imposing frequent sanctions on the employees makes them try harder to comply with security policy, shown by the highest utility with a threshold of 7
- Having a very complex security utility is not always the best choice, as employees writing their passwords down can outweigh the apparent benefits of complex passwords
- We are working on an extension that includes other factors and choice
  - Phishing emails, malware

# Challenges

- Designing accurate utility functions for both the employees and the system
  - That's what the presented theories are there for
- Characterizing the model
  - How to determine input probabilities and distributions
- Validation
  - The results give us important insights into the relationships between the different components of the system
  - Varying policy requirements can help judge which systems can be more secure

# Conclusion and Future Directions

- It is important to include human behavior in our modeling of systems for security assessment
- Empirical studies suggest several theories to explain human behavior and decision making in cyber security
- We provided evidence on the importance of modeling human behavior for giving insights into security analysis and assessment

# Selected References


- Bulgurcu, B., et al. (2010). "Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness." MIS Quarterly **34**(3): 523-548
- D'Arcy, J., et al. (2009). "User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach." Information Systems Research **20**(1): 79-98.
- Ifinedo, P. (2012). "Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory." Computers & Security **31**(1): 83-95.
- Siponen, M. and A. Vance (2010). "Neutralization: new insights into the problem of employee information systems security policy violations." MIS Quarterly **34**(3): 487.
- Theoharidou, M., et al. (2005). "The insider threat to information systems and the effectiveness of ISO17799." Computers & Security **24**(6): 472-484.
- Sara Kraemer, Pascale Carayon (2007). “Human errors and violations in computer and information security: The viewpoint of network administrators and security specialists”. Applied Ergonomics **38**(2):143-154.
- Bruce Schneier (2008), “The Psychology of Security”. Progress in Cryptology (AFRICARCRYPT) **5023**: 50-79.