

COORDINATED SCIENCE LABORATORY

ENGINEERING AT ILLINOIS

Science of Security for Systems  
The UIUC SoS Labet

David M Nicol

ITI. ILLINOIS.EDU

INFORMATION TRUST INSTITUTE



### Overview

Research

- Five research projects
  - Spans hard problems space, but with concentration on metrics, scalability, and resiliency
  - 7 universities other than UIUC (Rice, IIT, Berkeley, Dartmouth, USC, UPenn, Newcastle)
  - Over 25% of total budget supports these

Project	Scalability	Policy	Metrics	Resiliency	Humans
Metrics for CPS	✓		✓	✓	
Data Driven Security Models	✓		✓	✓	
Network Hypothesis Testing	✓	✓	✓	✓	
Human Circumvention					✓
Model-based Decisions	✓		✓		✓

3





## Overview

Outreach

- Speaker series
  - SoS speakers coming to Illinois, UIUC SoS speakers going out
- Technical workshops
  - In association with other technical workshops (e.g. Allerton)
  - Planning for Dagstuhl
  - Two Summer School offerings

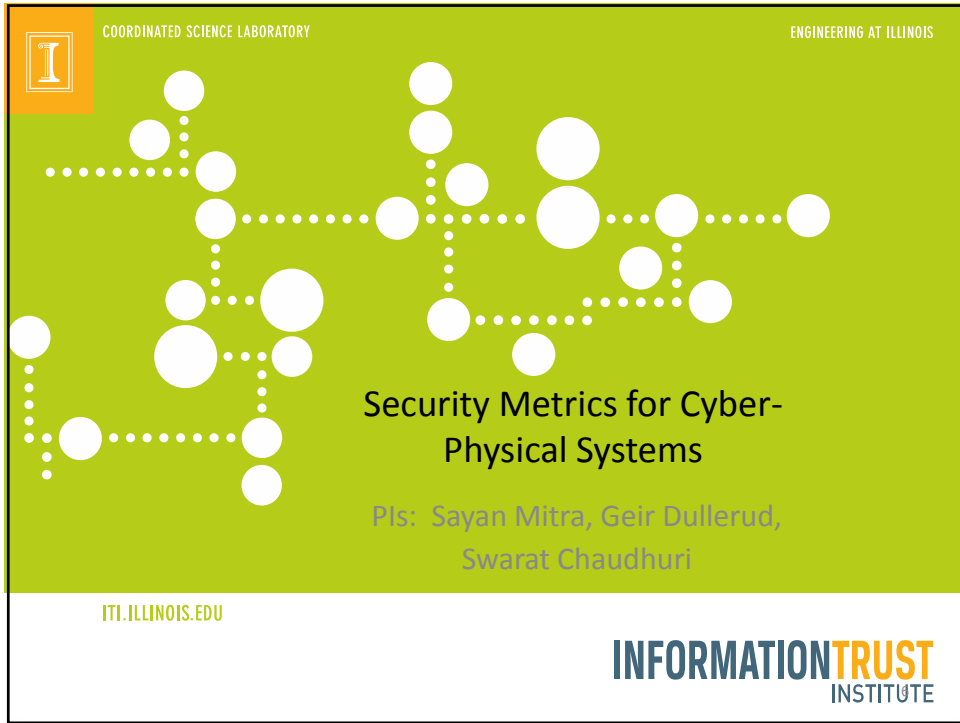
4



## Overview

- Summer internships
  - Competitive program, up to 6 students @ summer
  - Students write proposals, top picks brought to UIUC where they work on these under UIUC faculty mentors
  - Posters at SoS technical workshop
- Education
  - Incorporate SoS modules into existing security courses
  - Develop graduate course in SoS
  - Apply to UIUC for support to develop MOOC on SoS

5



COORDINATED SCIENCE LABORATORY

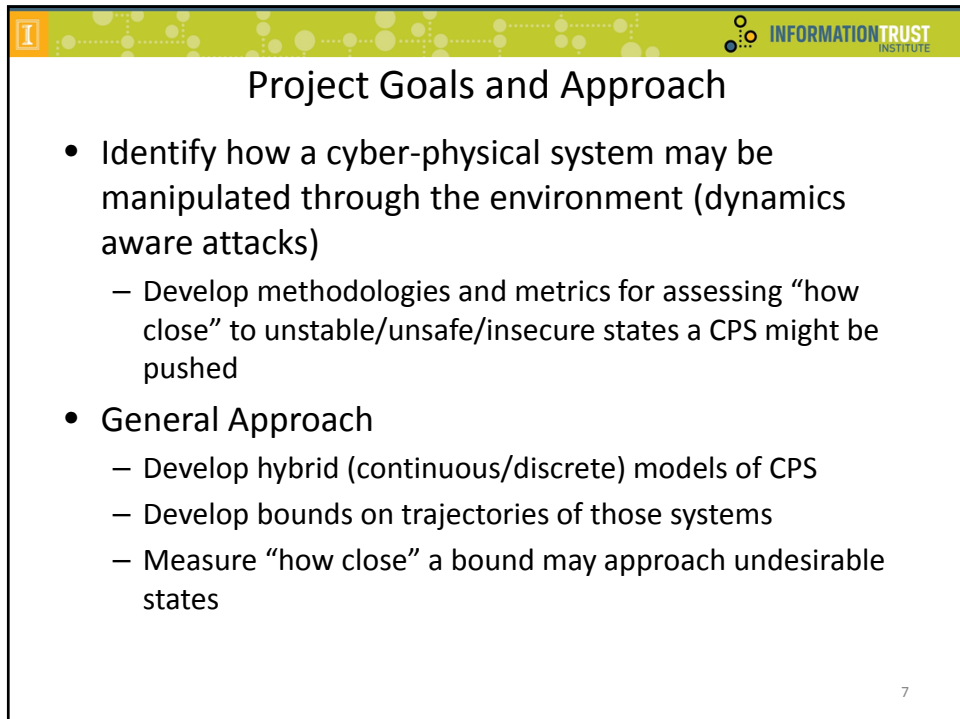
ENGINEERING AT ILLINOIS

ITI. ILLINOIS.EDU

**INFORMATION TRUST INSTITUTE**

# Security Metrics for Cyber-Physical Systems



PIs: Sayan Mitra, Geir Dullerud, Swarat Chaudhuri



## Project Goals and Approach

- Identify how a cyber-physical system may be manipulated through the environment (dynamics aware attacks)
  - Develop methodologies and metrics for assessing “how close” to unstable/unsafe/insecure states a CPS might be pushed
- General Approach
  - Develop hybrid (continuous/discrete) models of CPS
  - Develop bounds on trajectories of those systems
  - Measure “how close” a bound may approach undesirable states

7






## Specific Technical Goals

Project aims to develop



- Security metrics ( $\epsilon$ -stability, availability)
- Adversary classes that capture different attacks on CPS
- Annotations and algorithms that bound state trajectory
- Evaluation in context of CPS benchmark examples

8

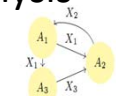
## Builds on previous project

- Two problems addressed in the past year:
  - (a) Define different threat classes for CPS & analysis of CPS under these classes of attacks
  - (b) Study the cost of privacy in distributed control
- More details in the following two slides:
- Highlights:
  - **Proofs from Simulations and Modular Annotations**, presented by Zhenqi Huang at the *17th International Conference on Hybrid Systems*: **nominated for best student paper award**.
  - **Invariant Verification of Nonlinear Hybrid Automata Networks of Cardiac Cells**, Z. Huang, C. Fan, A. Mereacre, S. Mitra, and M. Kwiatkowska. To appear in *Computer Aided Verification (CAV)*, LNCS, 2014.
  - **Control of Linear Switched Systems with Receding Horizon Modal Information**, R. Essick, J.-W. Lee, and G.E. Dullerud. To appear in *IEEE Transactions on Automatic Control*, 2014.
- Training and HR development
  - Zhenqi Huang completed MS thesis in Summer 2013 and is continuing PhD; made several conference presentations
  - Yu Wang finishing MS thesis this summer (2014); will continue to PhD.

## Problem (a): CPS adversaries and their analysis

- For analyzing a CPS model under attack we need to be able to compute or approximate the behavior of the system under attack
- Our work has focused develops and implements algorithms for these approximations



Interacting network of dynamical systems


**Proofs from Simulations and Modular Annotation** (HSCC 2014), gives algorithm for compositionally analyzing dynamical system models using numerical simulations. It is sound (always gives right answer) and relatively complete (i.e., terminates whenever system satisfies property robustly).

**Switched Systems with Receding Horizon Modal Information** (IEEE TAC 2014), provides exact and automatic analysis and synthesis algorithms for worst-case evaluation of adversary ability to degrade and interrupt metric-based system performance. Adversary can switch or manipulate CPS system parameters and structure; can also inject stochastic and non-stochastic disturbances. Next steps: more detailed statistical adversary models; game-oriented analysis of CPS switching.

**Invariant Verification of Nonlinear Hybrid Automata Networks of Cardiac Cells** (CAV 2014), extends HSCC to handle **deterministic hybrid models** and shows that it is effective for a very challenging benchmark (a network of cardiac cells stimulated by a pacemaker)


**Verification of Nonlinear Hybrid Systems with Simulation Traces and Compositional Reasoning.** (Zhenqi Huang's MS thesis) develops algorithms for reasoning about *nondeterministic hybrid* models--which are essential for capturing large classes of adversaries

**Proving Abstractions of Dynamical Systems through Numerical Simulations** (HOTSOS 2014) shows that the HSCC ideas can be used to compute the distance between *an ideal system and the same system under attack*



COORDINATED SCIENCE LABORATORY

ENGINEERING AT ILLINOIS




## Data-Driven Security Models and Analysis

PIs: Ravi Iyer, Zbigniew Kalbarczyk  
Robin Sommer

ITI.ILLINOIS.EDU

Ravishankar K. Iyer



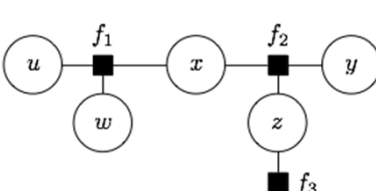
I
INFORMATION TRUST INSTITUTE

## Goal and Challenges

- **Goals**
  - Represent security incidents using factor graphs
  - Create scientifically sound methods for preemptive detection of attacks, i.e., before the system misuse
- **Challenges**
  - Operate on a partial knowledge on the attack
  - Semantics of event logs difficult to correlate with attacker's actions
    - examining an event in isolation may not be sufficient
  - Attackers may enter the target system using stolen credentials

12

## An Overview of Factor Graphs



A variable node represents a random variable.

A factor node is a function that links random variables and define their relationships. E.g.,  $f_2(x,y,z)$

A factor graph of five variables ( $x,y,z,w,u$ ) and three factor functions ( $f_1,f_2,f_3$ )

$$P(X) = \frac{1}{Z} \prod_{v \in V} f(v)$$

$X$  Random variables

$Z$  Normalization factor

$V$  Cliques (group of variables)

**A factor graph is an undirected, bipartite graph representing functional relations between random variables**

- Factor graph is an effective representation of complex dependencies between random variables, including both causal and non-causal dependencies
- The joint probability distribution of random variables can be factorized into factor functions
  - Factorization simplifies calculation (such as inferring value of hidden variables) on factor graph

## Application of Factor Graphs to Attack Detection

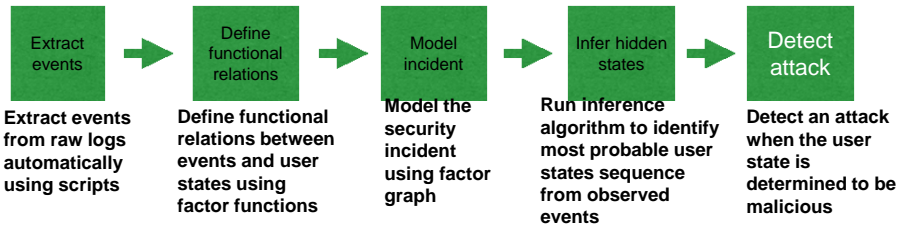
### Input

- Set of observable events  $X$ ,  
(generated by system monitoring tools, e.g., IDS alerts, netflows, syslogs)
- User profile  $u$  (e.g., places user usually logs from, applications user usually runs)
- Set of possible system/user states  $Y = \{\text{benign, suspicious, malicious}\}$

### Output

**Given an event sequence  $E$  infer security state  $S$  of the target system/user**

Use factor graphs to represent functional relation between the **observed evidence** (the event sequence) and the **hidden system/user states** to determine the most probable sequence state transitions



## Factor Graph Representation of an Example Incident at NCSA

Raw log (syslog, IDS alerts, netflows)	Event	User State
sshd: Accepted <user> from <remote-host> (a user logs into a computing node using ssh)	login remotely ( $e^0$ )	$s^0$
HTTP GET vm.c (server6.bad-domain.com) (a source file (vm.c) downloaded from a server)	download sensitive ( $e^1$ )	$s^1$
sshd: Received SIGHUP; restarting (the Secure Shell server (SSHD) restarted)	restart system service ( $e^2$ )	$s^2$

Post-incident analysis of attacker actions:

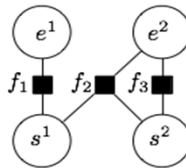
- compromise a user account and log in from a remote location,
- download, compile, and execute a privilege escalation exploit (CVE-2008-0600)
- inject credential collecting code (to harvest user credentials) into the node's SSHd server,
- restart the SSHd server

A *Factor Graph* representation of the incident

#### Variable nodes

(defined based on the data from security/system logs)

- $e^1$ : download sensitive
- $e^2$ : restart system service
- $s^1$ : user state when observing  $e^1$
- $s^2$ : user state when observing  $e^2$



#### Factor functions/nodes

(defined based on the data from security/system, knowledge of the system, security experts opinion)

$$f_1 = \begin{cases} 1 & \text{if } e^1 = \text{download sensitive} \\ & \& s^1 = \text{suspicious} \\ 0 & \text{otherwise} \end{cases}$$

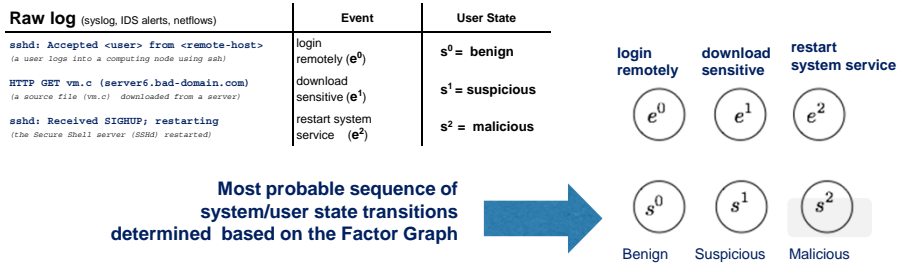
$$f_2 = \begin{cases} 1 & \text{if } e^2 = \text{restart service} \\ & \& s^1 = \text{suspicious} \\ & \& s^2 = \text{malicious} \\ 0 & \text{otherwise} \end{cases}$$

*The factor function  $f_2$  can improve detection accuracy by incorporating prior information*



$$f_3 = \begin{cases} 1 & \text{if } e^2 = \text{restart sys service} \\ & \& s^2 = \text{benign} \\ 0 & \text{otherwise} \end{cases}$$

**Note:** Unlike Bayesian Networks which require pairwise conditional dependency, factor graphs can combine a group of two or more variables and has lower computational complexity, e.g., function  $f_2$ )

## Output of Factor Graph Based Analysis for the Example Incident at NCSA



- **Benefits of the proposed approach**
  - **Early detection and prevention of attacks**
    - when a user is suspicious, additional monitors can be enabled for monitoring
  - **Timely identification of users' security state in a large enterprise network**
    - based on output user state sequence, a security analyst can identify most suspicious users and progress of potential attacks without having to examine a large amount of raw logs

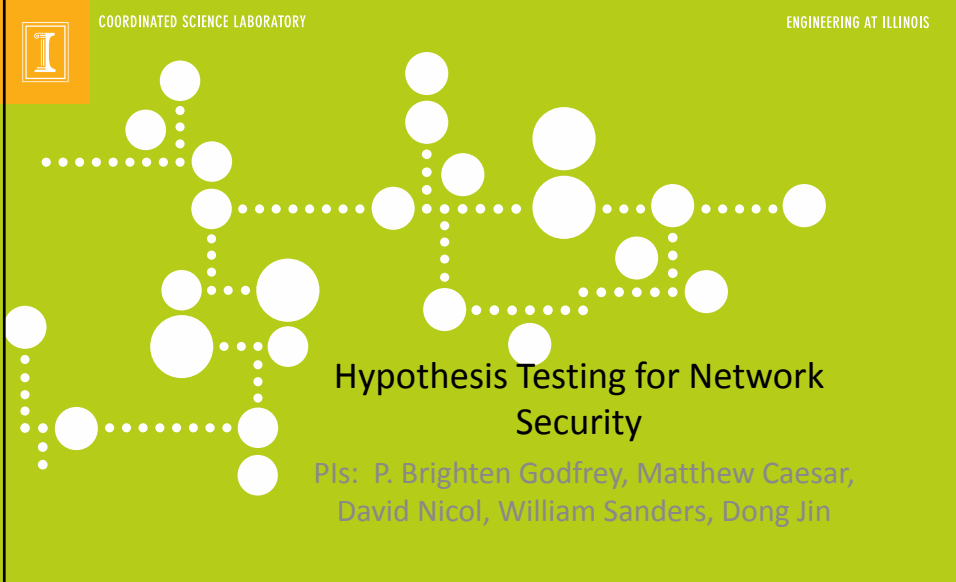



### Impact on Science of Security

- A new trend of thinking: building a common sensing infrastructure for reliability and security monitoring
- A new type of intrusion detection system that detects attacks from initial stage, using only partially observed traces.
- A theoretical foundation of orthogonal monitoring framework, where monitoring data from all layers of a system can be combined to make more accurate attack detections.

17





COORDINATED SCIENCE LABORATORY


ENGINEERING AT ILLINOIS

Hypothesis Testing for Network Security

PIs: P. Brighten Godfrey, Matthew Caesar, David Nicol, William Sanders, Dong Jin

ITI.ILLINOIS.EDU

INFORMATION TRUST INSTITUTE





INFORMATION TRUST INSTITUTE

## Project Goals

- Increasingly complex, large scale nature of networks makes it difficult to understand network's behavior
- Even very simple behaviors (e.g., packet reachability) are difficult for operators to test
  - Synthesizing simple behaviors into high-level qualitative understanding has been beyond reach
- Our work: **Network Hypothesis Testing Methodology**
  - Analysis methodology needed to support **scientific reasoning about the security of networks**
  - Focus on information and data flow security
  - Adds to both theoretical underpinnings and practical realization of Science of Security



19

## Project Goals

- Example: App-oriented access control policies in enterprise or mission-oriented network. Network designer needs to test various hypotheses:
  - All network paths traverse a firewall
  - Drone Operator will with 99% confidence be assured at least 50% of bandwidth for connection with drone
  - Fewer than 5% of stepping stone attacks that use no more than 3 compromised hosts could allow for data leakage from database DB
- Key challenges:
  - Scalability: large amounts of fast-changing network data
  - Modeling: policies' cross-layer interactions, possible subversion

20


## Project Approach

- Our approach: Network Hypothesis Testing
  - General formal model representing diversity of multi-layer network behavior and testing formal hypothesis against that model, resulting in quantitative metrics
  - Leverages results from two of our SoS tablets
    - “Towards a Science of Securing Network Forwarding” [Godfrey, Caesar] developed real-time Data Plane Verification, found real-world vulnerabilities
    - “Quantitative Assessment of Access Control in Complex Distributed Systems” [Nicol, Sanders] developed mathematical techniques to assess completeness of firewall protection
- Key tasks:
  1. Develop metrics for expressing quantitative hypotheses on network behavior
  2. Develop techniques to compose and evaluate metrics across system components
  3. Enhance core evaluation methodologies to scale to large and complex systems
  4. Formulate a hypothesis language and automatically design experiments to test hypotheses within the language

21

COORDINATED SCIENCE LABORATORY

ENGINEERING AT ILLINOIS

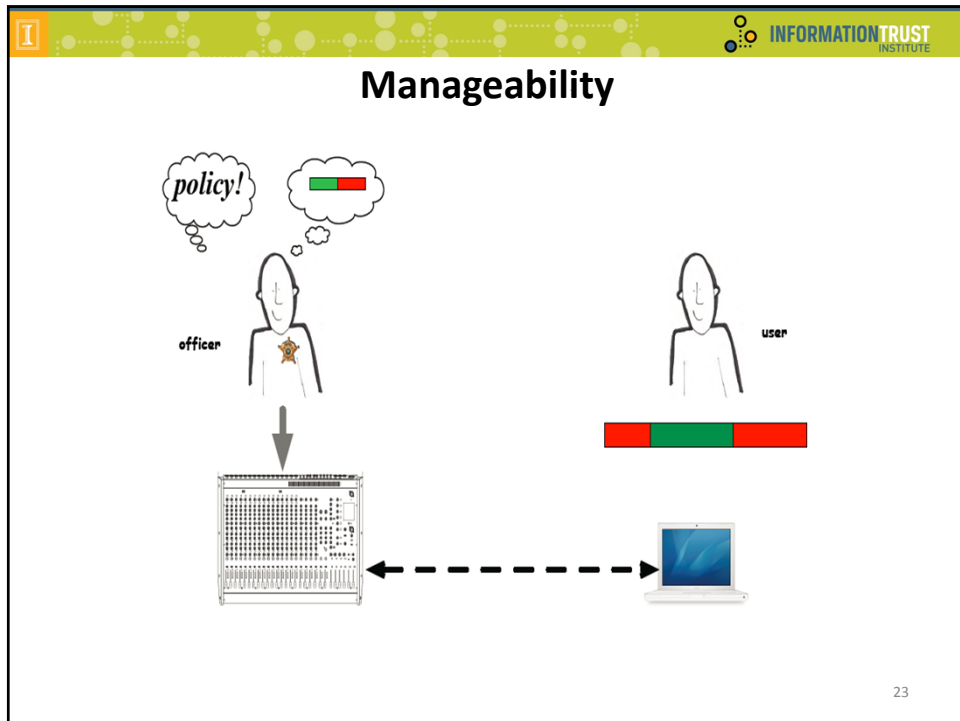


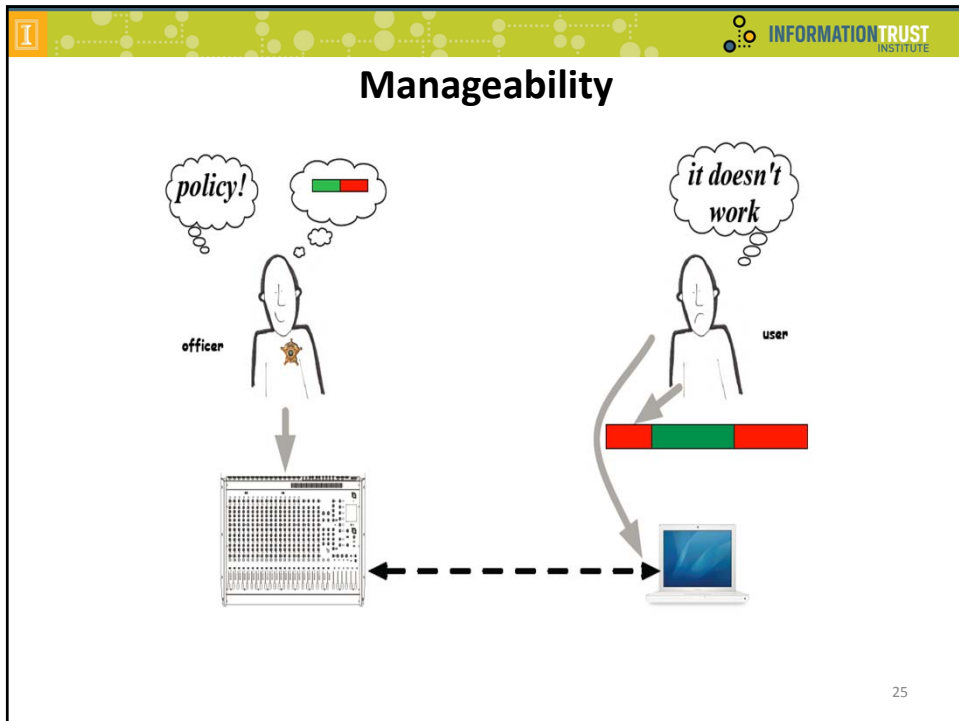
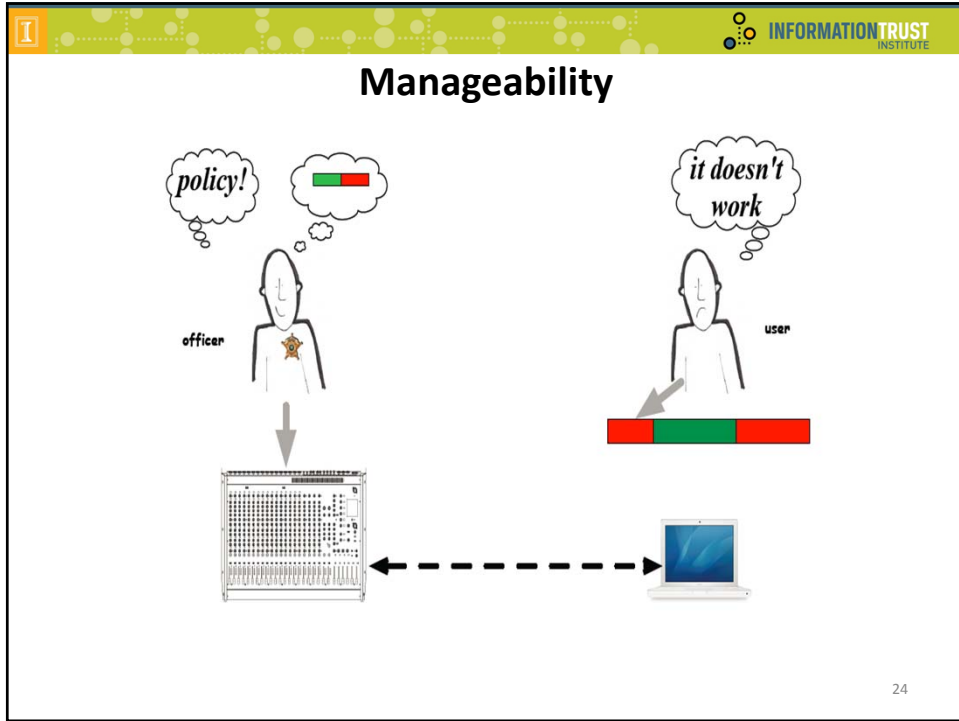
# Science of Human Circumvention of Security

PIs: Tao Xie, Jim Blythe, Ross Koppel, Sean Smith

ITI.ILLINOIS.EDU

**INFORMATIONTRUST**  
INSTITUTE





**Manageability**



The diagram shows an officer on the left with a thought bubble saying "policy!" and a small progress bar. An arrow points from the officer to a server rack. On the right, a user has a thought bubble saying "it doesn't work" and is looking at a laptop. A curved arrow points from the user to the laptop, and a dashed arrow points from the laptop back to the server rack.

26

**White Hats**

People just trying to do their work  
Workarounds – especially to cyber access  
**Good intent: unintended outcomes**  
Usually unfortunate rules: with lousy  
outcomes: lost productivity, frustration;  
more circumvention? **Security engineering  
doesn't work if we base it on the fantasy  
that all good users fully comply!**

The slide features a white hat on the left and a red and white striped barrier on the right. The text below discusses the concept of "White Hats" and the challenges of security engineering based on the fantasy of full user compliance.



## Science of Human Circumvention of Security


To better understand and *to model* computer access workarounds—their:

- Reasons, norms, and justifications
- Tasks, urgency, and environments
- Role in others rule-following behaviors
- Methods of discovery
- Sensible (responsible & used) controls

via

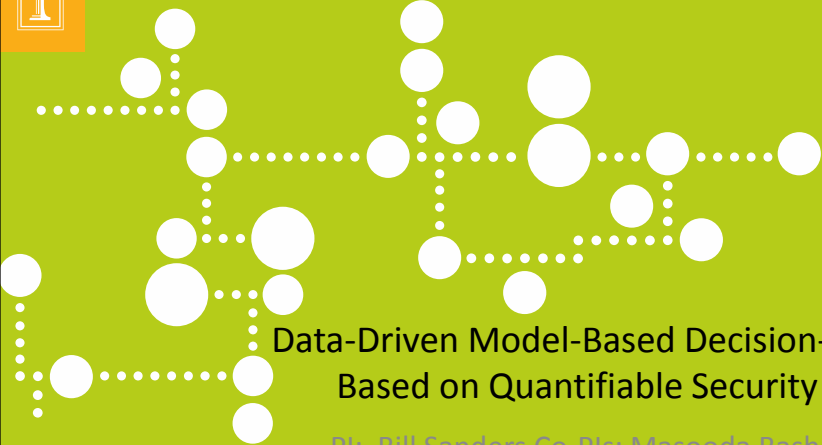
- Fieldwork
- Modeling individuals and systems
- Validation
- Application to hard problems in the real world

28



COORDINATED SCIENCE LABORATORY


ENGINEERING AT ILLINOIS





### Data-Driven Model-Based Decision-Making Based on Quantifiable Security Metrics

PI: Bill Sanders Co-PIs: Masooda Bashir, David Nicol, and Aad Van Moorsel

ITI.ILLINOIS.EDU





## Project Goals

**Hypothesis:** Quantitative security models, augmented by collected data, can be used to make credible business decisions about the use of particular security technologies to protect an organization's infrastructure.

**Goals:**

- Develop quantitative, scientifically grounded, decision-making tools to guide information security investments in private or public organizations, combining human and technological concerns
- Demonstrate their use in two or more real-life case studies
- Validate the usefulness of the developed tools through analysis of the results of the completed case studies



30

## Research Strands

- Stochastic modeling of human-behavioral aspects that influence the use of security policies in a private or public sector organization (led by Illinois)
- Development of a data collection strategy that is optimal with respect to a combination of factors, including sensitivity of the model to the data, statistical accuracy of the model inputs/outputs, and the cost of collecting the data (led by Newcastle Univ.)
- Validation of our project hypothesis, through a series of case studies (together)

31



## Project Timeline

**Year 1:**

- A complete implementation of HITOP in Mobius. This work was started as part of a project in the original UIUC lablet, and a substantial portion of the development has been completed. The completed work from that project will be the starting point for this project, enabling us to focus on the construction of the quantitative models themselves, their integration with security data collection strategies.
- Design of a generalized implementable data collection optimization algorithm which makes use of statistical techniques to quantify the amount of data that needs to be collected, and the sensitivity of each data value on the with respect to the security measures of interest.

**Year 2:**

- A prototype software tool development to assist data collection strategy formulation.
- Initial case study to test efficacy of approach. (3) Refined modeling formalisms and data collection algorithms, based on results of initial case study

**Year 3:**

- Distributable tool for use by others.
- Two or more case studies on cyber chosen infrastructure or critical infrastructure systems to validate our hypothesis.
- Tool refinements based on use by us and others

32