COORDINATED SCIENCE LABORATORY

ENGINEERING AT ILLINOIS

UIUC Lablet Report

Bill Sanders

David Nicol

Sayan Mitra

Associate Professor

Electrical and Computer Engineering

and **Information Trust Institute**

ITI.ILLINOIS.EDU

INFORMATIONTRUST INSTITUTE

UIUC Projects

- Hypothesis Testing Framework for Network Security
- Anonymous Messaging
- Data Driven Model-Based Decision Making
- Static-Dynamic Analysis of Security Metrics for Cyber-Physical Systems
- Data Driven Security Models and Analysis
- Science of Human Circumvention of Security

adding…

- A Monitoring, Fusion and Response Framework to Provide Cyber Resiliency

Fundamental Research (by Project)

Hypothesis Testing Framework for Network Security

- Develop effective simulation+emulation methodologies and tools
  - Improved temporal synchronization for higher fidelity
  - DSSNet being open sourced
- Continue development of technology to verify network flow congestion (ConVenus), addressing timing uncertainty
- New project on synthesizing network repair
  - "Wreckless" detects and repairs SDN update in violation of global policy
- New project on transparent optimization
  - Optimize SDN performance while preserving security policies

Publication highlights

Hypothesis Testing Framework for Network Security (continued)

- Jiaqi Yan, Xin Liu and Dong Jin, "Simulation of a Software-Defined Network as One Big Switch", *2017 ACM SIGSIM Conference on Principles of Advanced Discrete Simulation (PADS 2017)*, Singapore, May 24-26, 2017.

- Brighten Godfrey has developed a new tutorial on Network Verification, presented this at the 2nd Hebrew University Networking Summer in Jerusalem in June 2017 also will be presented at the IEEE/ACM International Conference on Software Engineering (ASE) in October 2017.

Fundamental Research (by Project)

Anonymous Messaging

Established fundamental limits to spreading and hiding of messages with and without time-stamp meta-data

Anonymous messaging is a peer-to-peer computation

- Began study of application to bitcoin networking stack (a P2P application)
- Focusing on systematic exploration of loopholes in network protocols (diffusion)
  - Eavesdropper adversary studies time-stamps
  - Spy adversary involves collusion
- Prove that Bitcoin's diffusion offer poor anonymity properties on networks with a regular-tree topology. We validate this claim in simulation on a 2015 snapshot of the real Bitcoin P2P network topology.

Publication highlight

Anonymous Messaging (continued)

- G. Fanti, S. Venkatakrishnan and P. Viswanath, “Dandelion: Redesigning BitCoin Networking for Anonymity”, ACM Sigmetrics 2017, Urbana, IL, June 5-9, 2017.
- Press on this work:

https://btcmanager.com/news/finance/researchers-at-university-of-illinois-present-privacy-focused-cryptocurrency/

https://www.cyberscoop.com/researchers-redesign-bitcoin-anonymity-u-s-law-enforcement-hires-specialists/

Fundamental Research (by Project)

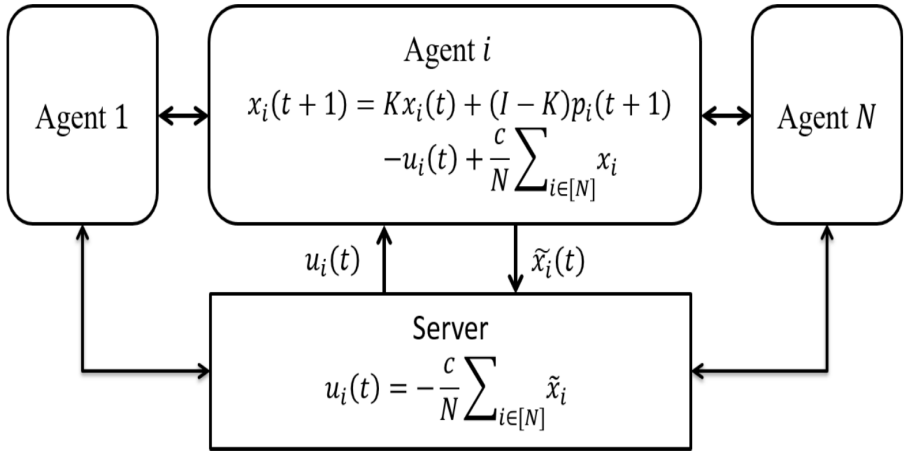
Data Driven Model-Based Decision Making

- Optimize techniques for collecting data used to parameterize probabilistic models
  - Find optimal strategies constrained by budget for given set of model input parameters
  - Parameters needed
    - Data Sources
    - Model input parameters
    - Mean and variance of each input parameter in each data source
    - Cost per sample for each data source
    - Budget
  - Provided as Extension to PRISM
- Developed additional PRISM extension for sensitivity analysis of model's parameters

Fundamental Research (by Project)

Static-Dynamic Analysis of Security Metrics for CPS

- Explore fundamental trade-offs between security and performance / usability
  - Performance of a distributed control system (e.g. crowd-sourced congestion detection) and the privacy of the individual participating
  - Accuracy of a security monitor and the data-footprint of the monitor
- Formalized problem selecting measures of performance and cost
  - Differential privacy of distributed control and optimization
  - Bit rate for monitoring



- Developed the first set of characterizations of the trade-offs
  - Stable systems performance cost of privacy grows as $O(T^3/N\varepsilon^2)$, where T is the time horizon and ε is the privacy parameter.
  - For unstable systems, the cost grows exponentially with time.
- Developed sound and complete algorithm for synthesizing controllers and inductive proofs of those controllers

Publication highlights

Static-Dynamic Analysis of Security Metrics for Cyber-Physical Systems

- Joao Jansch Porto and Geir E. Dullerud, “Decentralized Control with Moving-Horizon Linear Switched Systems: Synthesis and Testbed Implementation”, *American Control Conference 2017*, Seattle, WA, May 24-26, 2017.

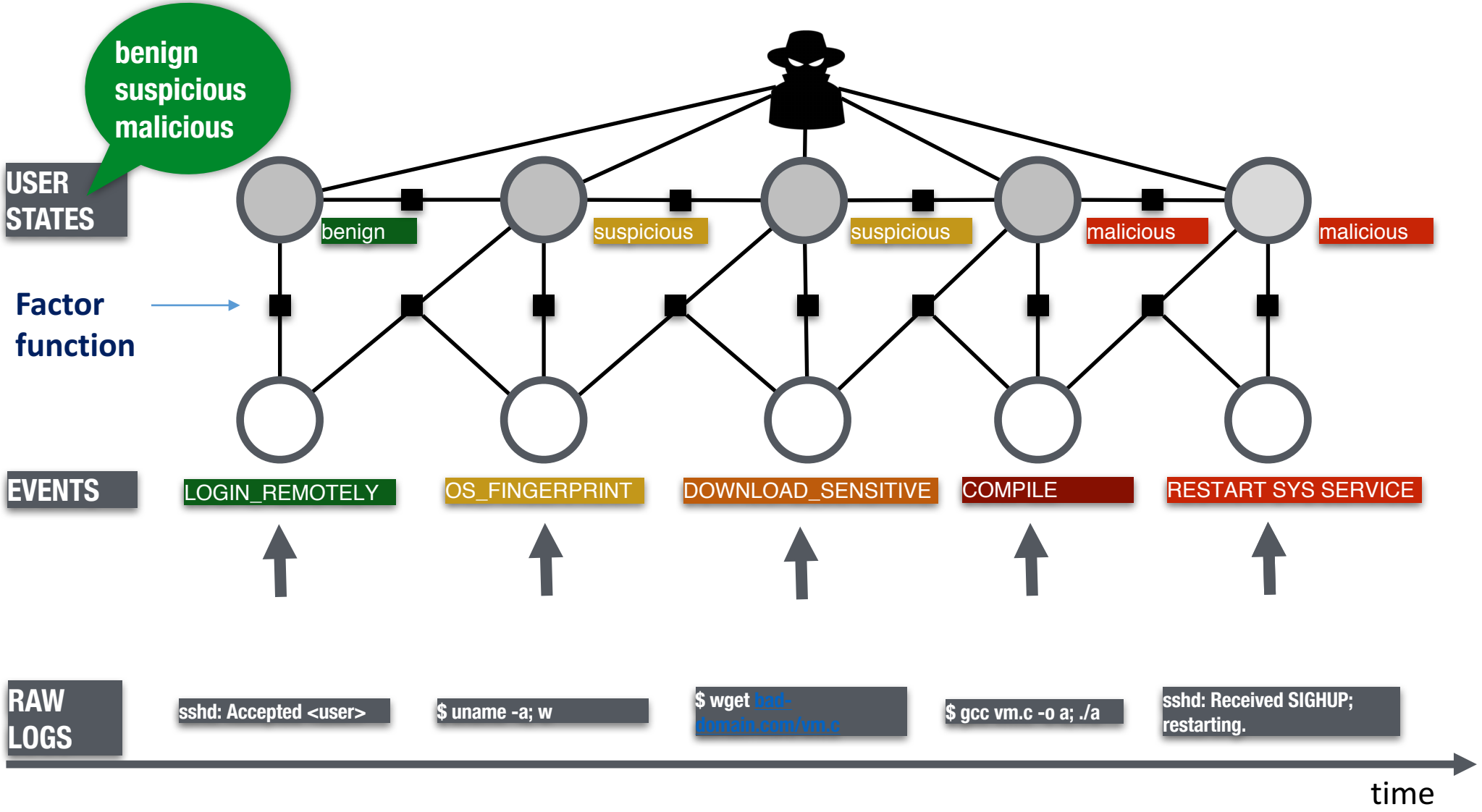
- Hussein Sibaie and Sayan Mitra, “Optimal data rates for estimation and model detection of switched dynamical systems”, *20th ACM International Conference on Hybrid Systems: Computation and Control in conjunction with CPS Week 2017*, Pittsburgh, PA, April 18-21, 2017. **Nominated for Best Student Paper award and invited for special journal issue.**

Fundamental Research (by Project)

Data Driven Security Models and Analysis

- Develop data-driven methodology for security monitoring, with the goal of recognizing, mitigating, and containing attacks
- Use production scale data on security incidents in real-world systems (e.g., NCSA) to drive the research
- Uses Factor Graphs to represent real-world security incidents and develop sound methods for preemptive detection of attacks, i.e., before exploit
  - Refine factor graph model (basis for AttackTagger, attack detection framework) using data from Blue Waters; Functions created to capture new relationships
  - Install AttackTagger in live network traffic of NCSA's logs with attack stage tags
  - Develop techniques for automated learning of factor functions from past data

AttackTagger: Preemptive Detection of Attacks Using Probabilistic Graphical Models



Publications

Data Driven Security Models and Analysis

- Phuong Cao presented poster at HotSoS 2017 on “Learning Factor Graphs for Preempting Multi-Stage Attacks in Cloud Infrastructure”

- P. Cao, E. C. Badger, Z. T. Kalbarczyk, R. K. Iyer, “A Framework for Generation, Replay, and Analysis of Real-World Attack Variants,” in Symposium and Bootcamp on the Science of Security (HotSoS), Carnegie Mellon University, April 19 to 21, 2016.

Fundamental Research (by Project)

Science of Human Circumvention of Security

- Identifying and cataloging types and causes of human circumvention of security measures
- Fieldwork in real-world enterprises leading to categorizing types and causes of human circumvention
  - Help desk logs, records of computer changes, user behavior in situ
- Mechanical Turk based approach for measuring security associated with password composition policy
- Questionnaires for security professionals and general users designed to better understand human perception of security and behaviors, leading to better models

Fundamental Research (by Project)

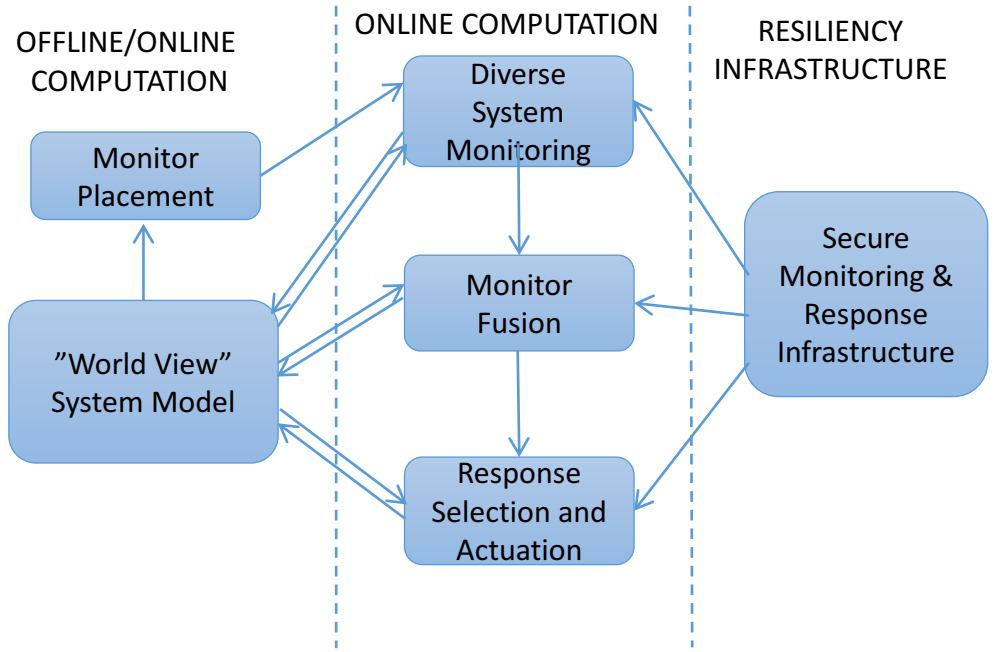
Science of Human Circumvention of Security

- Ross Koppel, Jim Blythe, Vijay Kothari, and Sean Smith, "Password Logbooks and What Their Amazon Reviews Reveal About Their Users' Motivations, Beliefs, and Behaviors", *2nd European Workshop on Usable Security (EuroUSEC 2017)*, Paris, France, April 29, 2017.

- Haibing Zheng, Dengfeng Li, Xia Zeng, Beihai Liang, Wujie Zheng, Yuetang Deng, Wing Lam, Wei Yang, and Tao Xie, "Automated Test Input Generation for Android: Towards Getting There in an Industrial Case", *39th International Conference on Software Engineering (ICSE 2017)*, *Software Engineering in Practice (SEIP),* Buenos Aires, Argentina, May 20-28, 2017.

Fundamental Research (by Project)

A Monitoring, Fusion and Response Framework to Provide Cyber Resiliency



- Provide a method for configuring monitors in a running production system.
- Expand our anomaly detection methods and monitor deployment methods. Specifically, expand our unsupervised learning to more types of data sources.
- Develop one or more multiple response selection algorithms for different attack scenarios using a game theoretic approach.
- Develop a case study that illustrate the use in a realistic application.

Publication highlights

A Monitoring, Fusion and Response Framework to Provide Cyber Resiliency

- B. E. Ujcich, A. Miller, A. Bates, and W. H. Sanders, "Towards an Accountable Software-Defined Networking Architecture." 3rd IEEE Conference on Network Softwarization (NetSoft 2017), Bologna, Italy, July 3-7, 2017, to appear.
- C. Cheh, B. Chen, W. G. Temple, and W. H. Sanders, “Data-Driven Model-Based Detection of Malicious Insiders via Physical Access Logs”, *14th International Conference on Quantitative Evaluation of Systems (QEST 2017),* Berlin, Germany, September 5-7, 2017, to appear.
- Atul Bohara, Mohammad A. Noureddine, Ahmed Fawaz, and William H. Sanders, “An Unsupervised Multi-Detector Approach for Identifying Malicious Lateral Movement”, *36th IEEE International Symposium on Reliable Distributed Systems (SRDS 2017)*, Hong Kong, September 26-29, 2017, to appear.

Other

- 89 Papers published

Education/Outreach

- 2 SoS Series speakers: Peter Popov, City, University of London and Paulo Esteves-Verissimo, University of Luxembourg
- Giulia Fanti and Pramod Viswanath gave a tutorial, “Information Limits on Finding and Hiding Message Sources on Networks: Social Media and Cryptocurrencies” at the IEEE International Symposium on Information Theory (ISIT) in Aachen, Germany June 25, 2017.
- Brighten Godfrey has developed a new tutorial on Network Verification, presented this at the 2nd Hebrew University Networking Summer in Jerusalem in June 2017 also will be presented at the IEEE/ACM ASE in October 2017.
- SoS summer internship program June 5-July 29, concluding with a poster session.