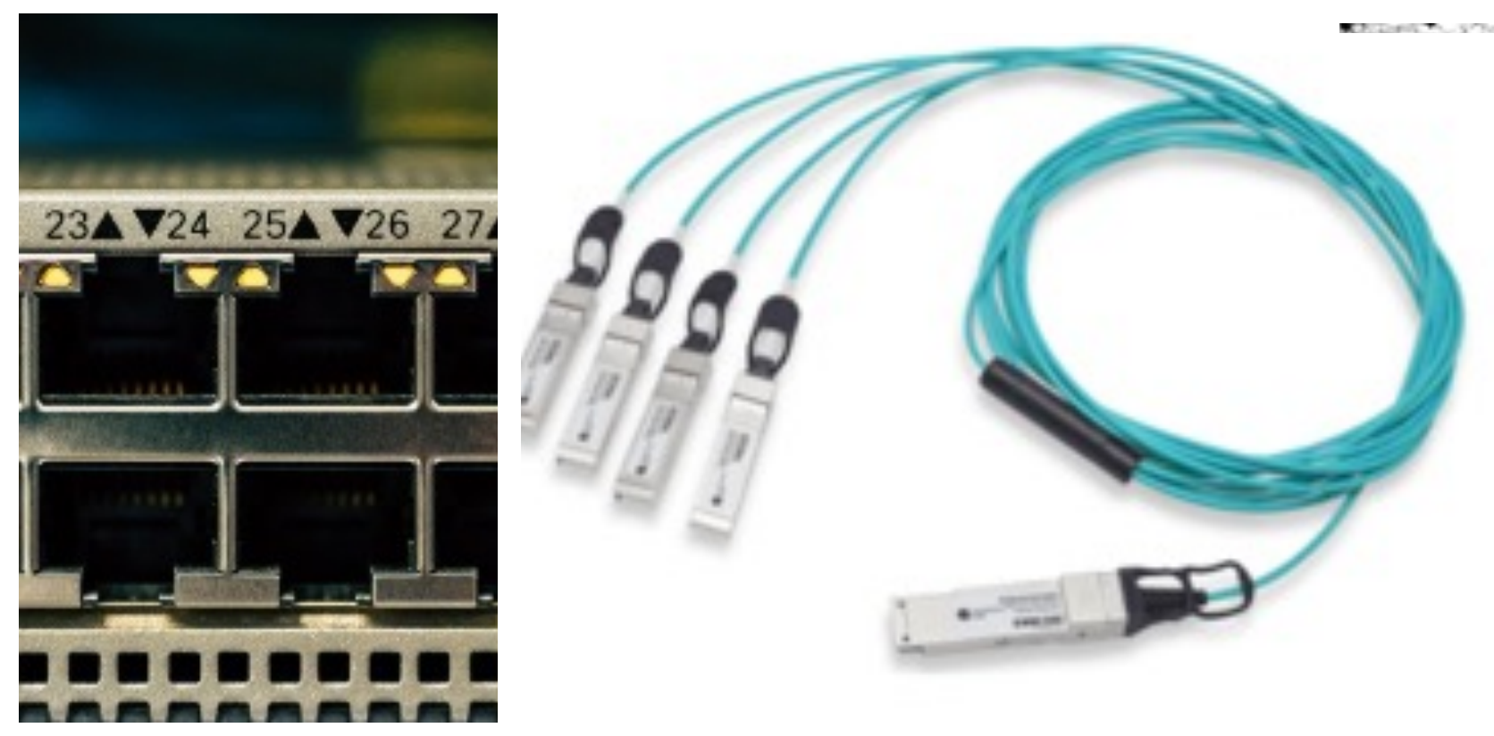
# Preemptive Intrusion Detection: Real-world Measurements, Bayesian-based detection, and AI-driven countermeasures

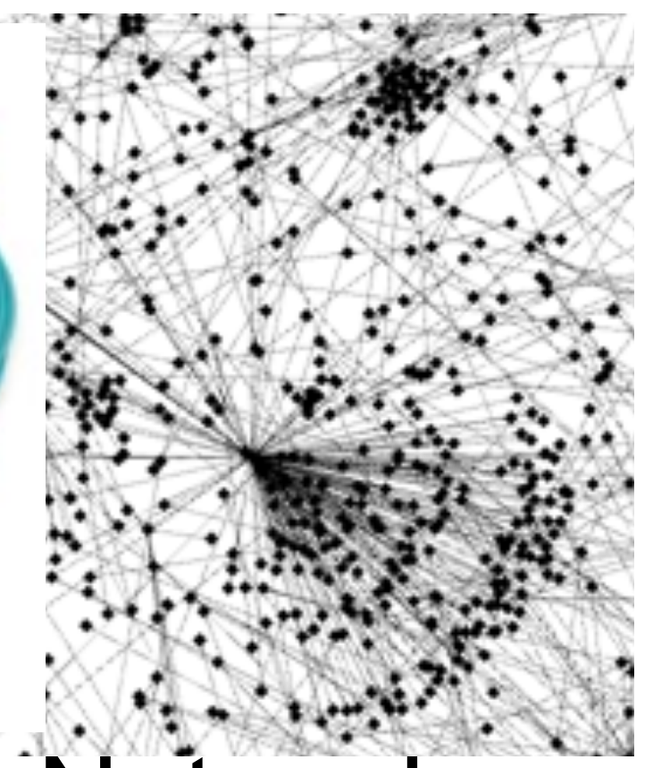
Phuong Cao
National Center for Supercomputing Applications, University of Illinois at Urbana-Champaign

NCSA

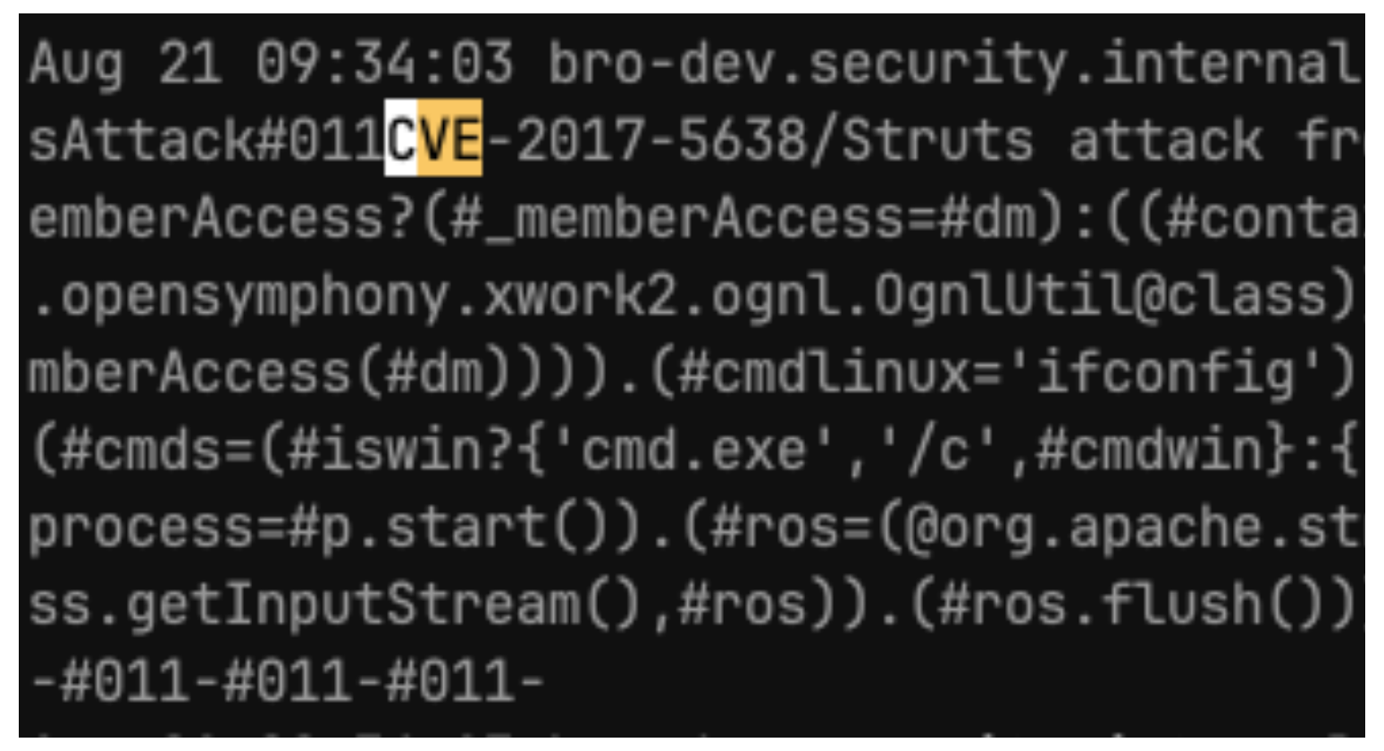
## Sensing & Measurement of Multimodal Data



400Gbps Network Optical tap



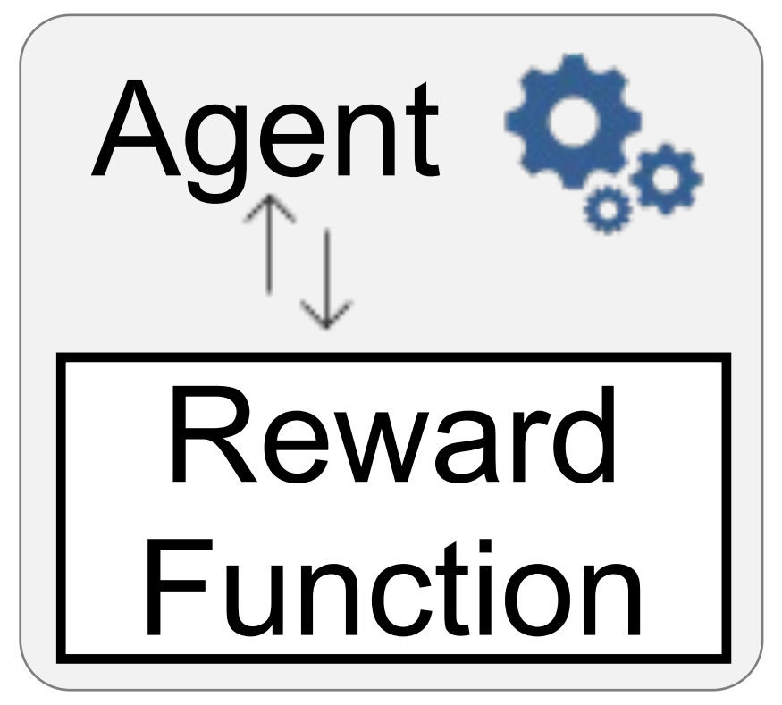
Network connections (1PB/day)



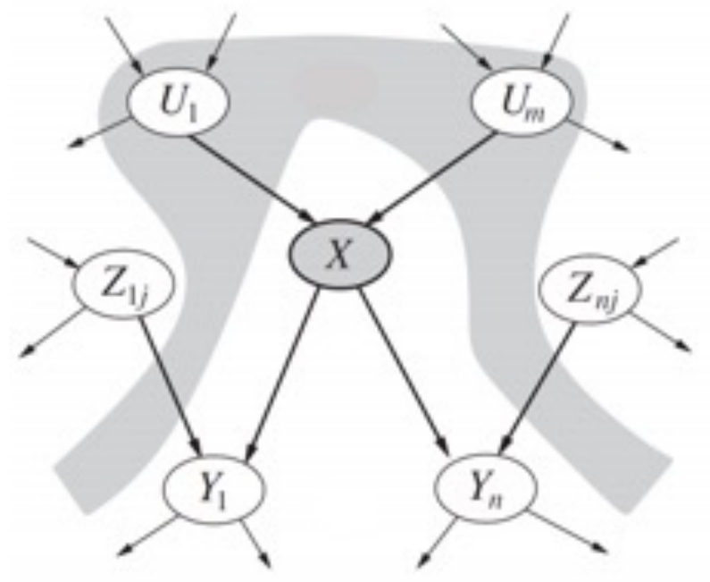
```
Aug 21 09:34:03 bro-dev.security.internal
sAttack#011CVE-2017-5638/Struts attack fr
emberAccess?(#_memberAccess=#dm):((#conta
.opensymphony.xwork2.ognl.OgnlUtil@class)
mberAccess(#dm)))).(#cmdlinux='ifconfig')
(#cmds=(#iswin?{'cmd.exe','/c',#cmdwin}:{
process=#p.start()).(#ros=(@org.apache.st
ss.getInputStream(),#ros)).(#ros.flush())
-#011-#011-#011-
```

Host logs
100,000 notices/day

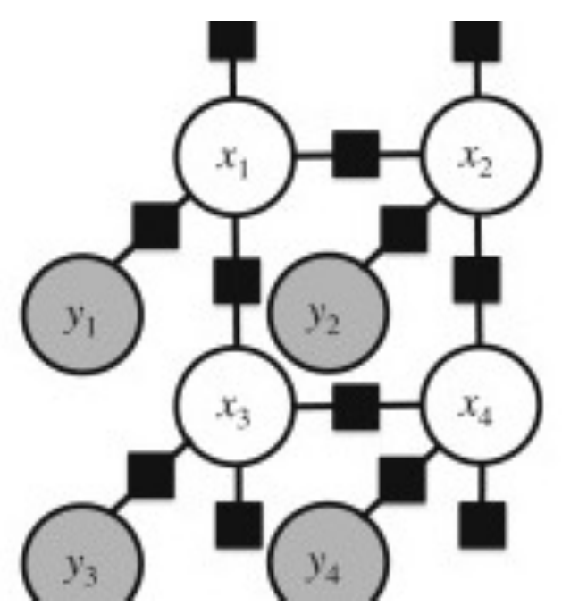
## Bayesian & Markov Learning



Reinforcement Learning + POMDP



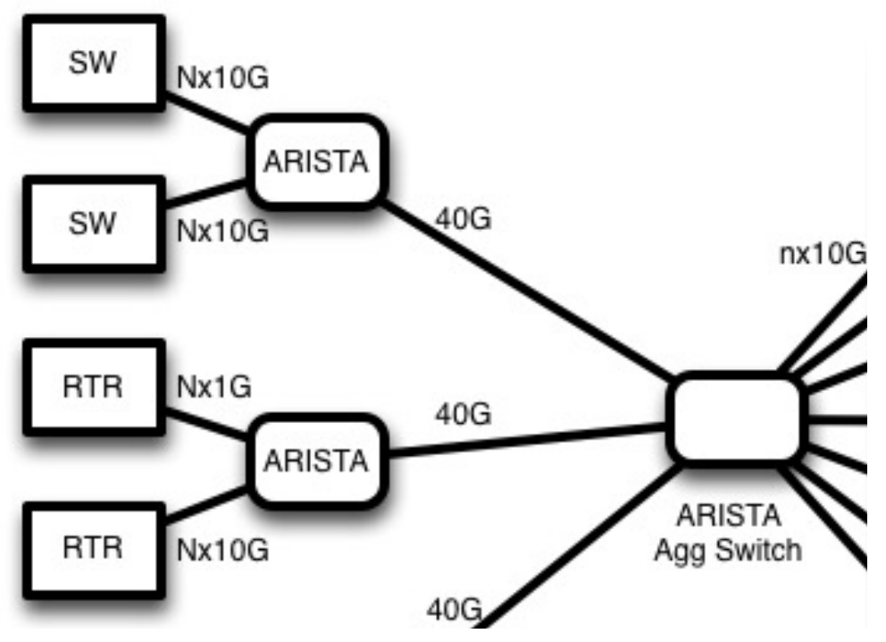
Bayesian Networks



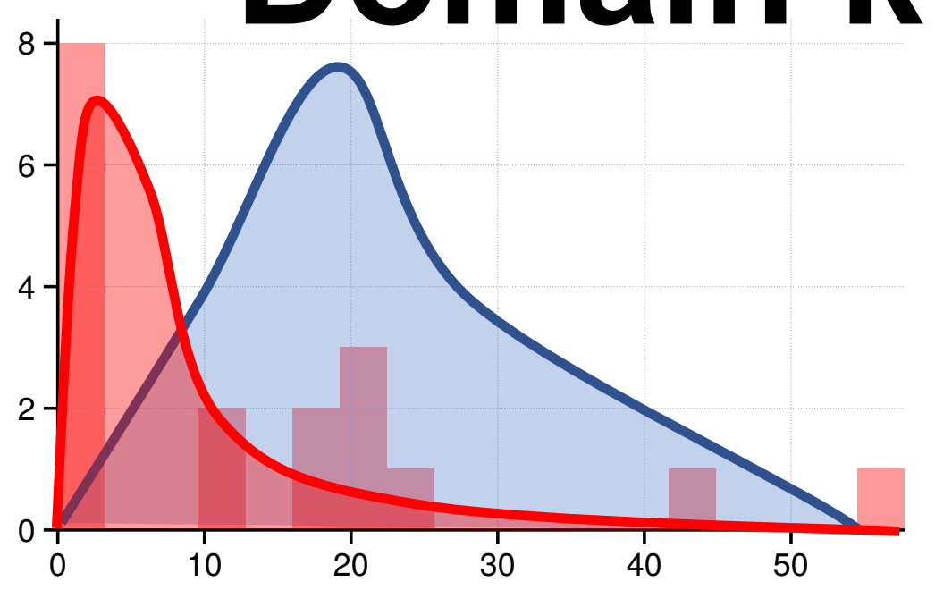
Markov Random Fields

## Probabilistic Graphical Models

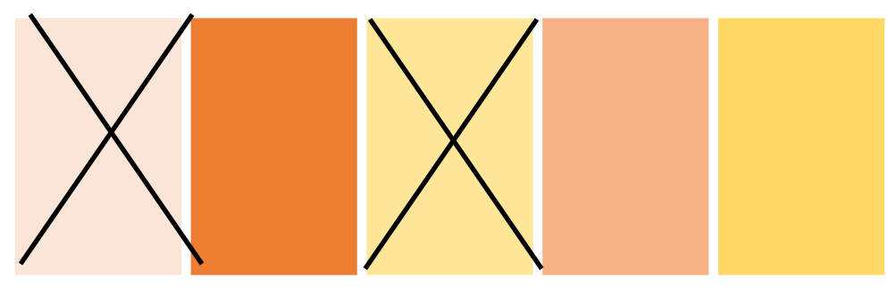
## Domain knowledge



Network Topology



Conditional Probabilities



Alert Patterns

Expert' insights

## Early prediction of attacks

Host eBPF monitoring

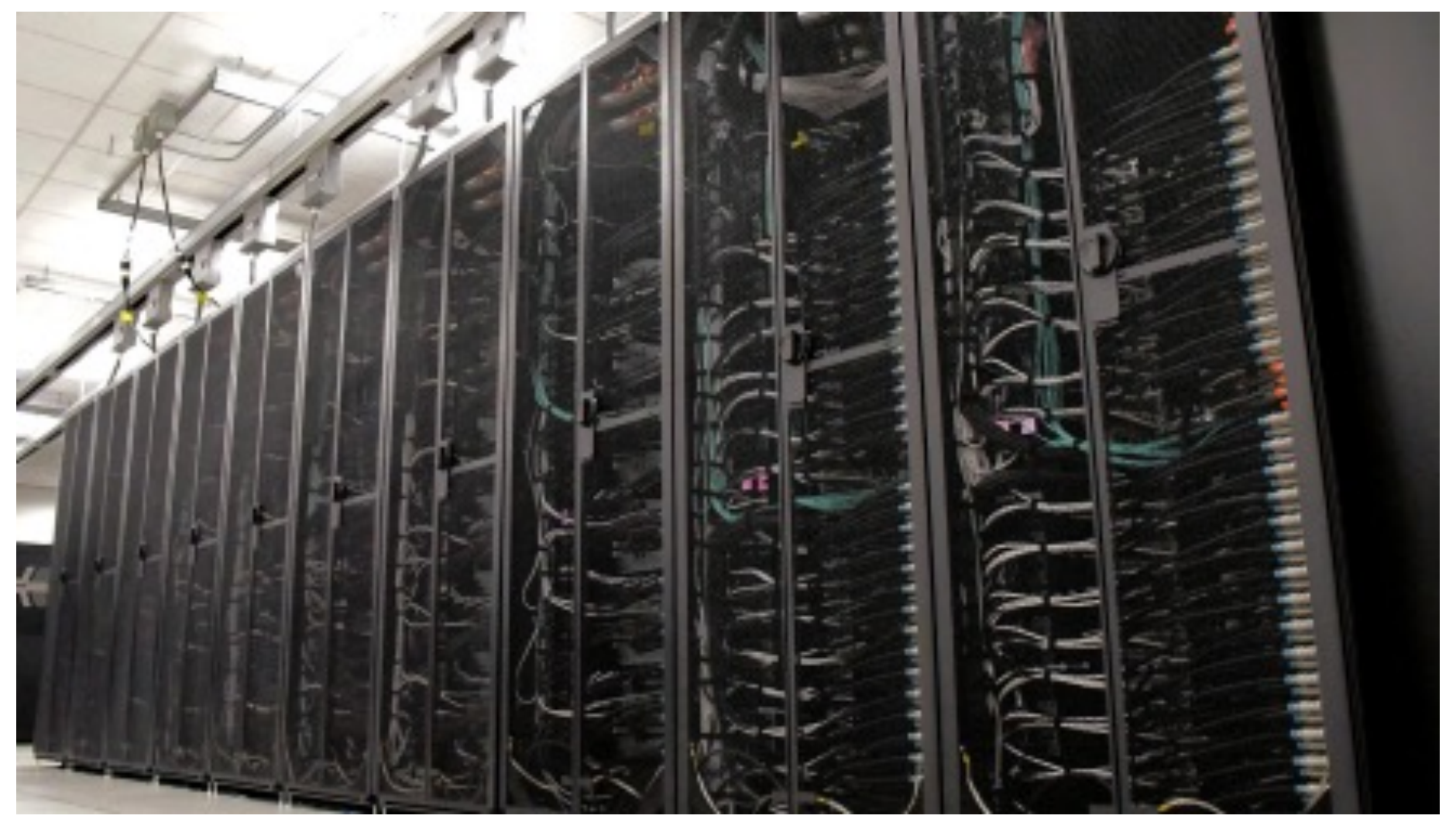
## Automated Reasoning

Machine Assisted Proof For Oauth/SAML

## Automated Response

RLHF
Black Hole Router

## Dependable petascale systems



## Network Cyber range

LLM-boosted adversary

## AI-driven Honeypot

SSH Honeypot

SCADA Simulator

## Futuristic Attacks

*Autonomous Malware*

*Stealthy ransomware*

## REFERENCES:

stealthML: Data-driven Malware for Stealthy Data Exfiltration
Keywhan Chung, Phuong Cao, Zbigniew Kalbarczyk, Ravishankar K Iyer
IEEE International Conference on Cyber Security and Resilience (CSR) 2023

stealthML: Data-driven Malware for Stealthy Data Exfiltration
Keywhan Chung, Phuong Cao, Zbigniew Kalbarczyk, Ravishankar K Iyer
IEEE International Conference on Cyber Security and Resilience (CSR) 2023

Mining Threat Intelligence from Billion-scale SSH Brute-Force Attacks
Yuming Wu, Phuong Cao, Alex Withers, Zbigniew Kalbarczyk, Ravishankar Iyer
Workshop on Decentralized IoT Systems and Security, co-located with NDSS, 2020

CAUDIT: Continuous Auditing of SSH-Servers To Mitigate Brute-Force Attacks
Phuong Cao, Yuming Wu, Subho Banerjee, Alex Withers, Justin Azoff, Zbigniew Kalbarczyk, Ravishankar Iyer
USENIX Symposium on Networked Systems Design and Implementation (NSDI), 2019

SVAuth: A Single-Sign-On Integration Solution with Runtime Verification
Shuo Chen, Matt McCutchen, Phuong Cao, Shaz Qadeer, and Ravishankar Iyer
International Conference on Runtime Verification (RV), 2017

A Framework for Generation, Replay, and Analysis of Real-World Attack Variants
Phuong Cao, Eric Badger, Zbigniew Kalbarczyk, Ravishankar Iyer
ACM Symposium and Bootcamp on the Science of Security (HotSOS), 2016

Preemptive intrusion detection: theoretical framework and real-world measurements
Phuong Cao, Eric Badger, Adam Slagell, Zbigniew Kalbarczyk, Ravishankar Iyer
ACM Symposium and Bootcamp on the Science of Security (HotSOS), 2015

Security Monitoring for Virtual Machines Using Hardware Architectural Invariants
Cuong Pham, Zachary Estrada, Phuong Cao, Zbigniew Kalbarczyk, and Ravishankar Iyer
IEEE Conference on Dependable Systems and Networks (DSN), 2014

ACKNOWLEDGEMENTS NSF, NCSA