# Preemptive Intrusion Detection

Phuong Cao, Key-whan Chung, Adam Slagell, Zbigniew Kalbarczyk, Ravishankar Iyer • {pcao3,kchung10,slagell,kalbarcz,iyer}@illinois.edu

Coordinated Science Laboratory & National Center for Supercomputing Applications • University of Illinois at Urbana-Champaign

## Background

### National Center for Supercomputing Applications

151 security incidents in a six-year period are studied (2008-2013).

Attackers enter the target system with known credentials (about 20% of them).

Detection often happens after attack payloads have been executed.

| *ID* | *Raw log* | *Event* | *User state* | *Attack state* |
|---|---|---|---|---|
| *1* | `sshd: Accepted password for user from <remote-host> ssh2` | remote_login | benign | no_attack |
| *2* | `HTTP GET /..0/vm.c (200 "OK" server6.bad-domain.com)` | download_sensitive | suspicious | prepare_exploit |
| *3* | `HTTP GET /..0/vm64.c (200 "OK" server6.bad-domain.com)` | download_sensitive | **malicious** | prepare_exploit |
| *4* | `HTTP GET /..0/sudo.tgz (200 "OK" server6.bad-domain.com)` | download | malicious | execute_payload |
| *5* | `sshd: Received SIGHUP; restarting.` | restart_system_service | malicious | execute_payload |

Table 1: This table illustrates events in a November 2008 incident with raw logs and events. AttackTagger tags the events with user states and attack states *automatically* to show user intention and attack semantics.

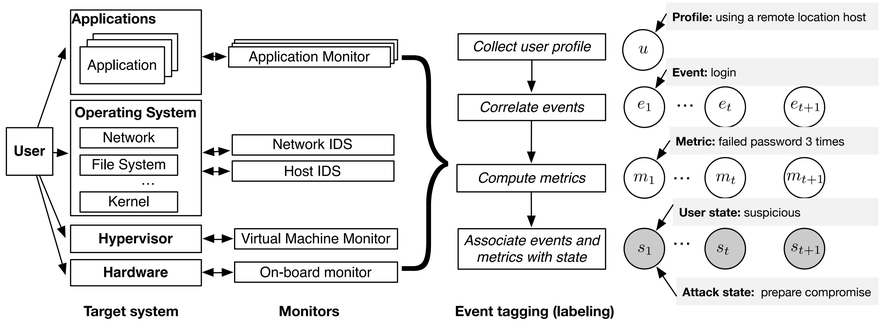
### Challenges

Interpreting semantics of events

Understanding user intention and attack progress

Incorporating security metrics and prior knowledge

## System Workflow




Workflow of the preemptive intrusion detection system. Events collected from monitors are examined to identify user state and attack state.

## Experiment

### Dataset

**Format:** written incident report, syslog, Bro log, netflows.

**Statistics:**

24 over 151 incidents are credential stealing incidents, ~ 13,700 events per incident.

5027 users, 32 compromised users, ~ 65 events per user.

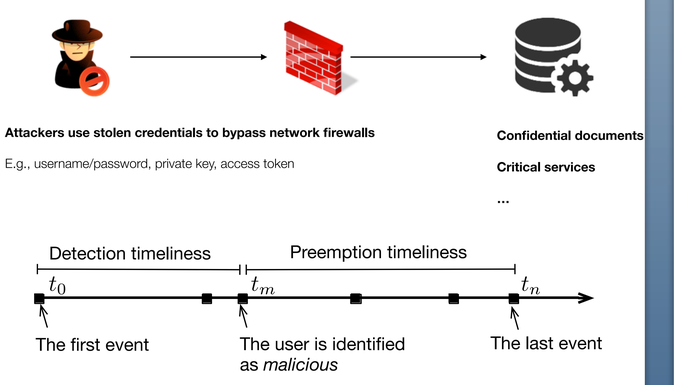
**Ground truth:** NCSA provides ground truth of compromised users.

### Evaluation metrics

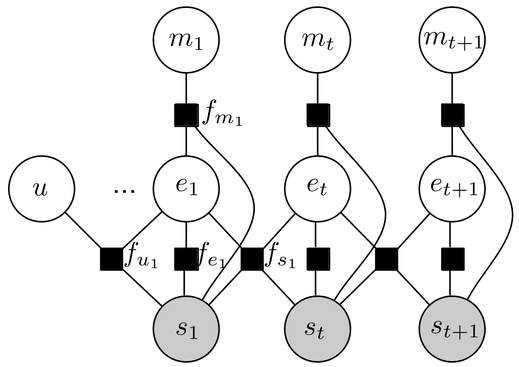
**Detection timeliness:** the time interval from the first observed event of a user to the time where the user is identified as malicious.

**Preemption timeliness:** the time interval from the time where the user is identified as malicious to the last observed event.

## Threat Model




## Probabilistic Model




Probabilistic model that captures relationships between user, event, metrics, and states.

| Variable nodes | Factor nodes |
|---|---|
| User u | User-state |
| Event e | Event-state |
| Metric m | Metric-state |
| State s | Event-event-state |

**The joint distribution**

$$P(u,E,M,S) = \frac{1}{Z}\prod_{f\in F} f(u,E,M,S)$$

**Observed variables**

$$X = \{u,E,M\}$$

**Hidden states**

$$Y = \{S\}$$

**Estimating hidden states**

$$P(Y|X) = \frac{1}{Z}\prod_{f\in F, x\in X, y\in Y} f(x,y)$$

## Problem Statement

### Problem

Detecting compromised users in advance: given an event sequence of a user, identify the state of the user and the attack.

### Assumptions

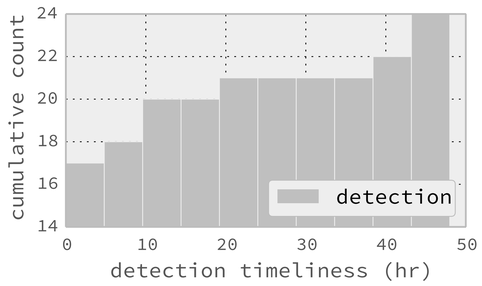
A monitoring system captures a target system operation.

The attacker does not contaminate monitors.

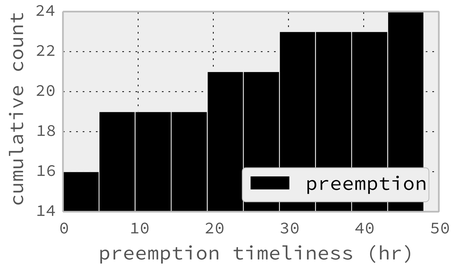
### Approach

Using probabilistic graphical model to capture relationships between observed events and the user/attack state.

## Result




Detection timeliness experimented with 24 incidents




Preemption timeliness experimented with 24 incidents

## Conclusion

A probability based framework to identify user intentions and progress of ongoing attacks.

Experiments are performed using 24 real security incidents dataset happened during the past 6 years at NCSA

Experimental results show that attacks can be prevented from minutes to tens of hours before attack payloads are executed

## Acknowledgements

This work was supported in part by NSF grant CNS 10-18503 CISE and 1314891, by the Army Research Office under Award No. W911NF-13-1-0086, the National Security Agency (NSA) under Award No. H98230-14-C-0141, Air Force Research Laboratory and the Air Force Office of Scientific Research, under agreement No. FA8750-11-2-0084.

## References

[1] Bilton, N. Adobe breach inadvertently tied to other accounts, Nov. 2013.

[2] Hammersley, J. M., and Clifford, P. Markov fields on finite graphs and lattices.

[3] Pearl, J. *Reverend Bayes on inference engines: A distributed hierarchical approach.* UCLA, 1982.

[4] Sharma, A., Kalbarczyk, Z., Barlow, J., and Iyer, R. Analysis of security data from a large computing organization. In *Dependable Systems & Networks (DSN), 2011* (2011).