Simulating Malicious Insiders in Real Host-Monitored User Data

San Diego, CA August 18, 2014
USENIX Workshop on Cyber Security Experimentation and Test (CSET'14)

Software Engineering Institute, Carnegie Mellon University
Kurt Wallnau, PhD (presenter)
Brian Lindauer, Michael Theis

Skaion Corp.
Robert Durst, Terrence Champion
Eric Renouf, Christian Petersen

Software Engineering Institute | Carnegie Mellon 1

This Presentation: Aim and Approach

Problem: Providing "red team" threat data for anomaly-based insider threat detector research under a specified protocol

Approach: Overlay synthetic threats 0btained from recorded simulated threat dramas onto real background

Where Next: Limits of what we know and speculation on what could or may follow

Software Engineering Institute | Carnegie Mellon 2

PROBLEM

Threat Data for DARPA ADAMS (1 of 2)

ADAMS: Anomaly Detection at Multiple Scales

- Detect early indicators of malicious insider threats
- Aim: Enable response to threats before suffering damage

Technology:

- Data mining, social analytics, machine learning
- Anomaly detectors, not violation (or "tripwire") detectors

Unique resource:

- Real (de-identified) host monitored user data for ~5000 industry users
- Rich collection policy (including file and communication content)
- 2.5B user events = 10^7 events per month x 25 months (29 planned)

PROBLEM

Threat Data for DARPA ADAMS (2 of 2)

ADAMS Red Team: SEI/CERT

Red team objective: Deliver threat data

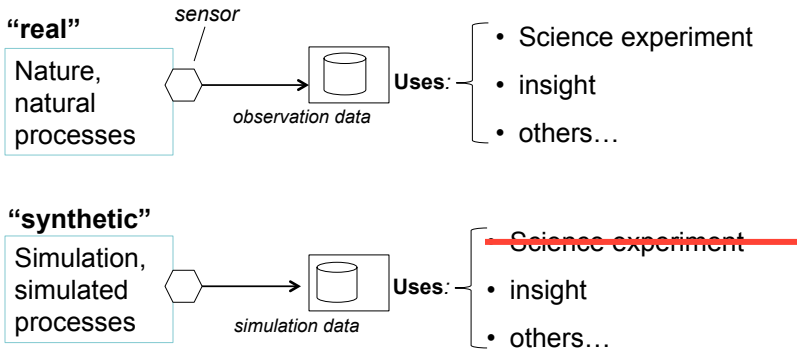
- Select representative and valid sample of the "threat domain"
- Sample expresses plausible and realistic social complexity
- Minimize risk of confusing (real v. synthetic) for (benign v. malicious)

ADAMS protocol imposes on red team ZERO VISIBILITY into

- detectors: data features observed, correlations, algorithms, what is/is not regarded as "anomalous", or threat models used in classification
- outcomes from using threat data: detection results, user classification, user ranking, explanation of results, …

APPROACH

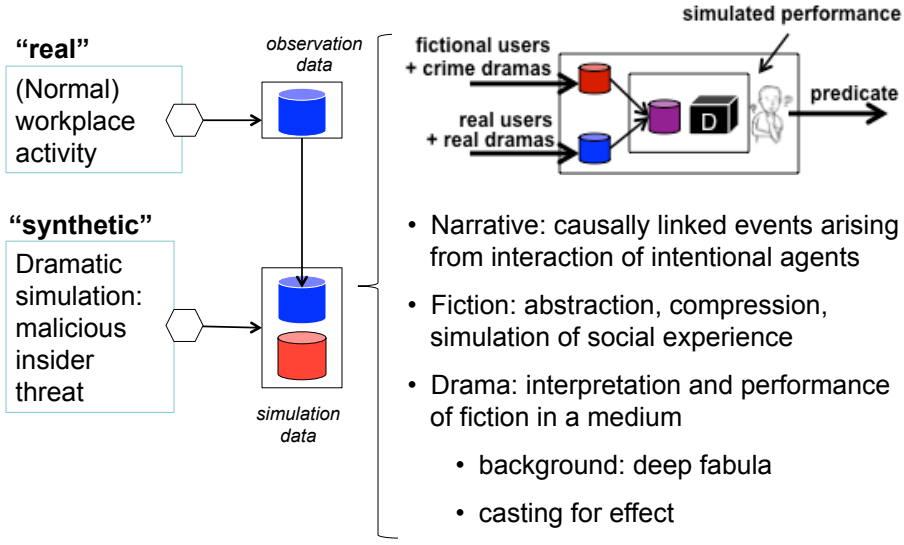
Experiments, Simulations, Fiction (1 of 2)



"*We use simulations all the time in physics, but there's no substitute for experiments.*" *Personal communication, 2013, Prof. Michael Levine, CMU, Director PSC*

APPROACH

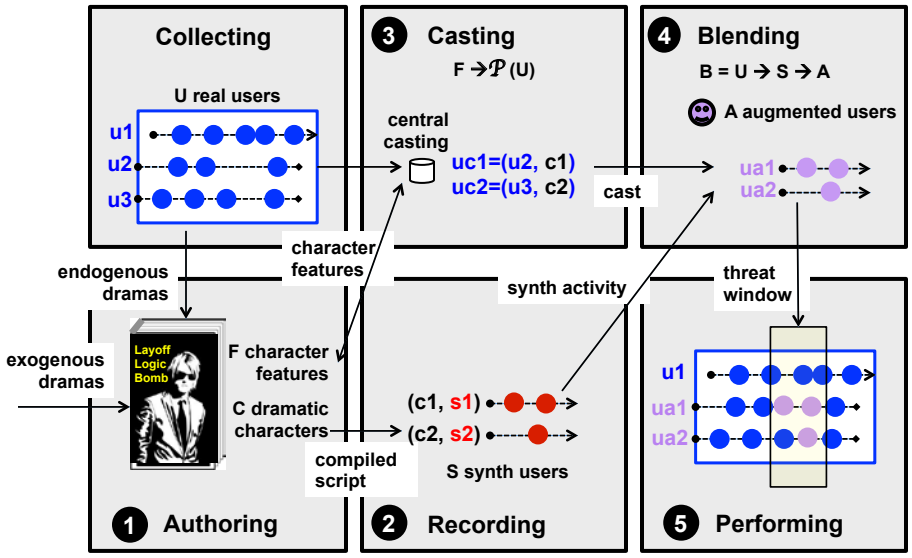
Experiments, Simulations, Fiction (2 of 2)



- Narrative: causally linked events arising from interaction of intentional agents
- Fiction: abstraction, compression, simulation of social experience
- Drama: interpretation and performance of fiction in a medium
  - background: deep fabula
  - casting for effect

APPROACH

Data from Drama (Logical)



APPROACH

Sample Treat Dramas (1 of 2)

Story	Class	Predicate	Plot Summary	Characters	
Passed Over	IT Sabotage	Subject installed malware on multiple company IT assets before resigning.	After hearing rumors to the effect, Subject learns that his/her project is being phased out in a company re-organization. Since Subject has devoted more than a decade to the project and been groomed for project leader, he/she becomes extremely disgruntled, makes demands and threats to his/her leadership, and then installs malware on several machines before submitting a resignation.	Subject	Low or mid-level employee who hears rumors that the project on which he/she has worked for a decade is being phased out.
				Coworker1	Co-worker and friend of Subject.
				Coworker2	Co-worker and friend of Subject.
				Supervisor	Superisor of Subject, CCA, CCB

APPROACH

Results 2012-Now

37 Dramas (Scenarios)
- plots for espionage, sabotage, theft, fraud
- lone wolfs, conspirators, offstage conspirators

76 Performances (Overlays)
- alternative cast of users
- variation in executions

21 Windows
- no confirmed artifacts since Aug 2012

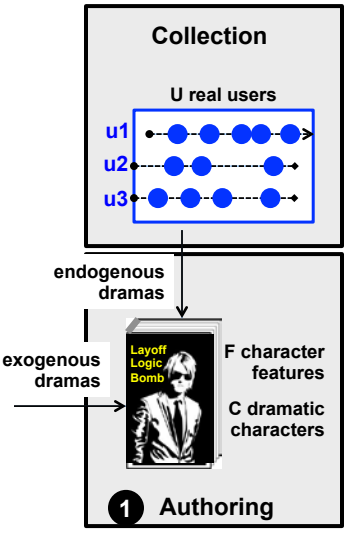
Title/Performances	
Anomalous Encryption	5
Bollywood Breakdown	1
Bona Fides	3
Breaking the Stovepipe	3
Byte Me!	2
Byte Me! Middleman	1
Circumventing Sureview	2
Conspiracy Theory	1
Credit Czech	1
Czech Mate	1
Exfil with steganography	1
Exfil Before Layoff	2
Exfil with Screenshots	5
From Belarus With Love	1
Gift Card Bonanza	1
Hiding Undue Affluence	3
Indecent RFP	1
Indecent RFP II	1

Title/Performances	
Indecent RFP 2	1
Insider Startup	6
Job Hunter	1
Layoff Logic Bomb	2
Manning Up	2
Manning Up Redux	1
Masquerading	3
Naughty by Proxy	3
Outsourcer's Apprentice	3
Panic Attack	1
Parting Shot	1
Parting Shot Deadly Aim	(1)
Passed Over	3
Selling Login Credentials	1
Snowed In	4
Stealing Login Credentials	1
Strategic Tee Time	(1)
Survivor's Burden	3
What's the Big Deal?	1

Software Engineering Institute | Carnegie Mellon 9

APPROACH

Data from Drama (Authoring)



Narrative fiction is a good way to talk about socially-manifested threats
- Insider Threat is a large construct, and threats simulate social realities within the construct
- "The Function of Fiction is the Abstraction and Simulation of Social Experience."*

Stories are authored
- Judgment sampling
- Authored by counter-intelligence and insider threat subject matter experts
- Recently
  - Contributed (not Red Team) "treatments"
  - Professional screenwriter for character development and dialog

* Mar, Raymond and Oatley, Kieth. "The Function of Fiction is the Abstraction and Simulation of Social Experience." Perspectives on Psychological Science, Vol., 3, No. 3, 2008, pp 173-192.

Software Engineering Institute | Carnegie Mellon 10

APPROACH

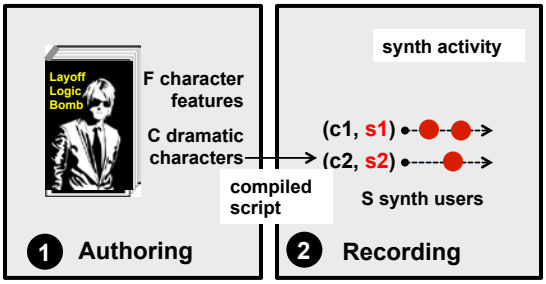
Data from Drama (Recording)

Fictional actions are simulated in a recording environment

- outside of Vegas, configured consistently with data provider sites
- "code generators" for stories, not simulations of users per se

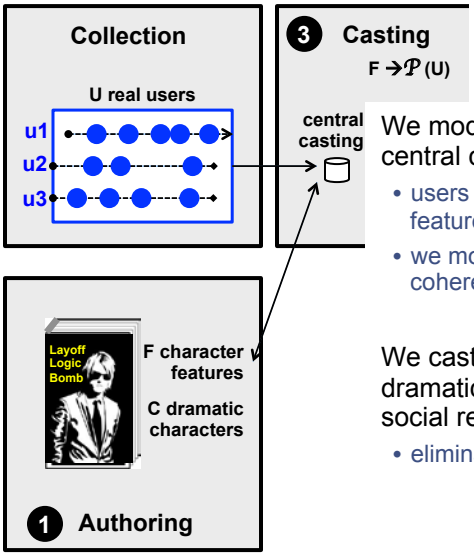
A very good heuristic: place data generating processes as close to the user in the user->automation stack as possible

- let the collector produce the data (including noise and other flaws)



APPROACH

Data from Drama (Casting)



We model the data collection as a central casting service

- users indexed by personal and social features found in background data
- we model features for narrative coherence not threat constructs

We cast users who are "closest to" dramatic characters in their job roles, social relationships activity patterns…

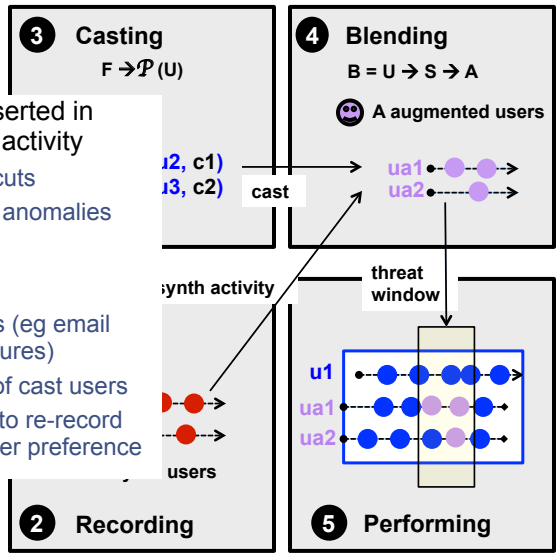
- eliminates a big source of anomaly

APPROACH

Data from Drama (Performing)

Synthetic activity is inserted in temporal gaps in user activity
- similar to editing film cuts
- we verify no temporal anomalies

Other blending
- communication details (eg email salutations and signatures)
- tool use preferences of cast users
  - source of 'rewrite!' to re-record stories to match user preference



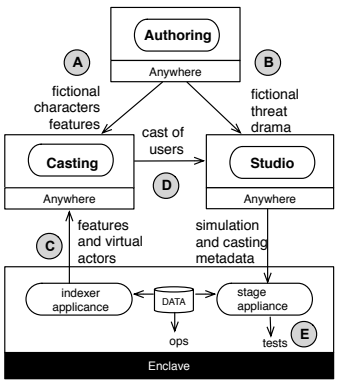
APPROACH

Limitations and Speculations

We have a practical (heuristic) demonstration of fiction to "simulate, abstract, compress social threats"
- The idea works and has many promising (speculative) extensions

We must learn the craft of telling threat stories and performing threat dramas
- What makes a good story? How are "psycho-socio" indicators reflected in character actions?
- What makes a good production? How should dramas be presented (sequence, window, real-time)?

Measurable production goals
- Testing, training, research, assessment, sharing, improving, ..
- Realism, plausibility, challenge level…



Fully abstract threats from collection policy & detectors?

Contact Information Slide Format

Kurt C Wallnau
Principal Researcher
Networked Survivable Systems
Telephone: +1 412-268-3265
Email: kcw@sei.cmu.edu
kcw@cert.org

U.S. Mail
Software Engineering Institute
Customer Relations
4500 Fifth Avenue
Pittsburgh, PA 15213-2612
USA

Web
www.sei.cmu.edu
www.sei.cmu.edu/contact.cfm

Customer Relations
Email: info@sei.cmu.edu
Telephone: +1 412-268-5800
SEI Phone: +1 412-268-5800
SEI Fax: +1 412-268-6257

Software Engineering Institute | Carnegie Mellon 15

Software Engineering Institute | Carnegie Mellon 16