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 obtained from recorded simulated threat dramas onto real background

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

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, …
“We use simulations all the time in physics, but there’s no substitute for experiments.”  Personal communication, 2013, Prof. Michael Levine, CMU, Director PSC

“We use simulations all the time in physics, but there’s no substitute for experiments.”  Personal communication, 2013, Prof. Michael Levine, CMU, Director PSC
Sample Treat Dramas (1 of 2)

<table>
<thead>
<tr>
<th>Story</th>
<th>Class</th>
<th>Predicate</th>
<th>Plot Summary</th>
<th>Characters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Passed Over</td>
<td>IT Sabotage</td>
<td>Subject installed malware on multiple company IT assets before resigning.</td>
<td>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.</td>
<td>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: Supervisor of Subject, CCA, CCB.</td>
</tr>
</tbody>
</table>
## Results 2012-Now

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

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

21 Windows
- no confirmed artifacts since Aug 2012

<table>
<thead>
<tr>
<th>Title/Performances</th>
<th>Title/Performances</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anomalous Encryption</td>
<td>Indecent RFP I</td>
</tr>
<tr>
<td>Bollywood Breakdown</td>
<td>Insider Startup</td>
</tr>
<tr>
<td>Bona Fides</td>
<td>Job Hunter</td>
</tr>
<tr>
<td>Breaking the Stovepipe</td>
<td>Layoff Logic Bomb</td>
</tr>
<tr>
<td>Byte Me!</td>
<td>Manning Up</td>
</tr>
<tr>
<td>Byte Me! Middleman</td>
<td>Manning Up Redux</td>
</tr>
<tr>
<td>Circumventing Sureview</td>
<td>Naughtly by Proxy</td>
</tr>
<tr>
<td>Conspiracy Theory</td>
<td>Outsourcer's Apprentice</td>
</tr>
<tr>
<td>Credit Czech</td>
<td>Panic Attack</td>
</tr>
<tr>
<td>Czech Mate</td>
<td>Parting Shot</td>
</tr>
<tr>
<td>Exfil with steganography</td>
<td>Parting Shot Deadly Aim(1)</td>
</tr>
<tr>
<td>Exfil Before Layoff</td>
<td>Passed Over</td>
</tr>
<tr>
<td>Exfil with Screenshots</td>
<td>Snowed In</td>
</tr>
<tr>
<td>From Belarus With Love</td>
<td>Stealing Login Credentials</td>
</tr>
<tr>
<td>Gift Card Bonanza</td>
<td>Selling Login Credentials</td>
</tr>
<tr>
<td>Hiding Undue Affluence</td>
<td>Strategic Tee Time (1)</td>
</tr>
<tr>
<td>Indecent RFP</td>
<td>Survivor's Burden</td>
</tr>
<tr>
<td>Indecent RFP II</td>
<td>What's the Big Deal?</td>
</tr>
</tbody>
</table>

## 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

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)

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
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 (e.g., email salutations and signatures)
- tool use preferences of cast users
  - source of 'rewrite!' to re-record stories to match user preference

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…
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

Copyright 2014 Carnegie Mellon University.
This material is based upon work supported by the Department of Defense under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the United States Department of Defense.

NO WARRANTY

THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

This material has been approved for public release and unlimited distribution except as restricted below.

Internal use: Permission to reproduce this material and to prepare derivative works from this material for internal use is granted, provided the copyright and "No Warranty" statements are included with all reproductions and derivative works.

External use: This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other external and/or commercial use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

*These restrictions do not apply to U.S. government entities.