Cyber Security and Insider Threat: Research and Challenges

Dr. Deanna D. Caputo

The MITRE Corporation

Usability, Security, and Privacy of Computer Systems: A Workshop
July 21 & 22, 2009
Washington DC

MITRE

© 2009 The MITRE Corporation. All rights reserved.

Problem: Trusted Insiders

- Malicious insiders leverage their assigned privileges to gather sensitive or proprietary information.
- Malicious (or even inadvertent) insiders usually do not need to engage in rule breaking behavior

- What should practitioners be looking at to spot a “lawful” but suspicious user?
- How do we make detection mechanisms usable to security analysts?
- How do we balance this security with the privacy of employees?

© 2009 The MITRE Corporation. All rights reserved.

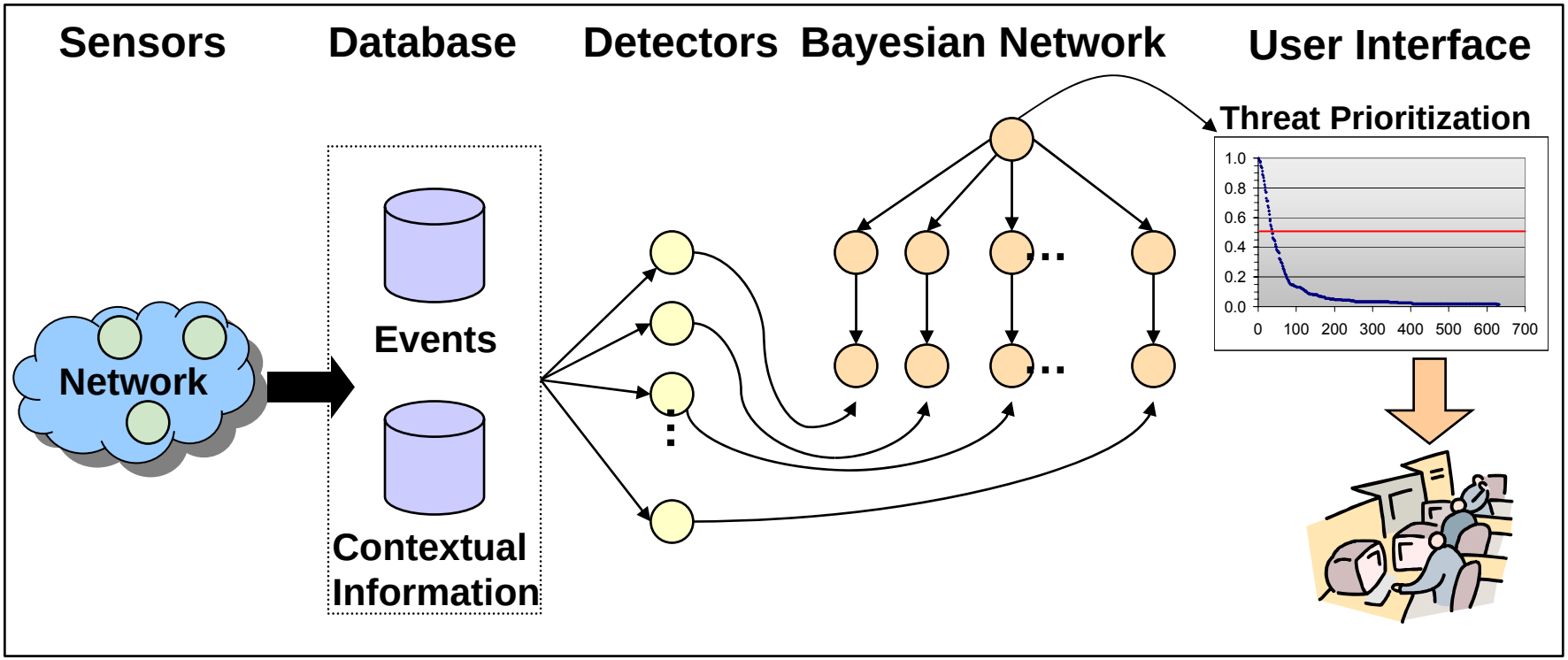
MITRE's Research Focus:

- **Create a Detection System**
  - Developed and successfully tested novel detection technique and prototype (ELICIT)
  - Piloting within Federal Government
- **Generating Good Data**
  - Design an experiment which generates malicious insider data
  - Include control set data to build a baseline (benign user)
  - Integrate human behavior and computer audit
  - Develop framework which can be used in future studies
- **Put Together Practical Guidance**
  - Focus on both network and endpoint cyber events
  - Develop indicators or groups of indicators that highlight suspicious users
  - Report interesting data which may generate ideas for future human behavior and cyber security studies

© 2009 The MITRE Corporation. All rights reserved.

The ELICIT System

Exploit Latent Information to Counter Insider Threats



Detection Performance

- Successfully detected red teams 16 of 19 days
- Flagged ~23 users/day for further scrutiny (approx. 4 hrs analyst time)

MITRE

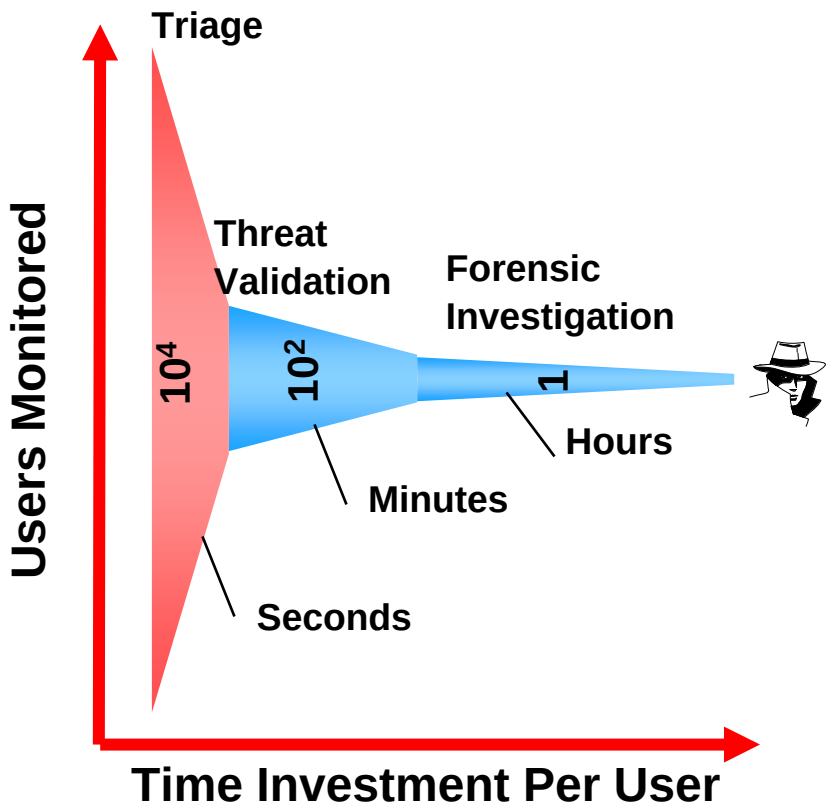
© 2009 The MITRE Corporation. All rights reserved.

MITRE's ELICIT Breakthroughs

Greg Stephens and Mark Maloof

1. **Focus on how trusted insiders use information**
   - Previous approaches focused on lower-level, machine behavior
2. **Use context to differentiate malicious from legitimate**
   - User context
   - Information context
3. **Help analysts prioritize their investigations**

The Analysis Funnel



© 2009 The MITRE Corporation. All rights reserved.

Problem Focus for Further Research: Research Data Set Availability

- Insider post-mortem case studies do not contain enough detail regarding *computer usage* by the insider
- Pilfered organizations are not eager to announce their losses by offering to share their audit data
- Privacy concerns

© 2009 The MITRE Corporation. All rights reserved.

MITRE's Experimental Design

Deanna Caputo, Greg Stephens, and Brad Stephenson

- **Double Blind Procedures**
  - Cover story related to anti-keylogging software testing
- **Conditions (random assignment)**
  - Benign user (control group) – 25 participants
  - Malicious user (experimental group) – 26 participants
- **Variables**

Experimental Variable	Value	Same/Different
Information Scope	Topic (Biosecurity)	Same
Environmental Constraints	None	Same
Time Constraints	One Week	Same
Intent	**Benign or Malicious**	**Different**

- **Manipulate intent using scenarios**
- **Participant stratification by cumulative job experience**
- **Funnel debriefing**

© 2009 The MITRE Corporation. All rights reserved.

RAND's Research Focus

Shari Lawrence Pfleeger and Joel Predd

- **A Framework for the Insider Threat Problem**
  - **Five question emerge from the framework:**
    - Does X have legitimate access to the IT system?
    - Has X violated security policy?
    - Are policies deficient?
    - Are the policies implemented effectively on the system?
    - What are the intent and motivation of the insider?
- **A Taxonomy for Insider Action**
  - Provides a system for categorizing insider actions
  - Requires experts to explicitly consider a range of important factors.
  - Provides a basis for answering the unanswered questions:
    - What is an insider?
    - What kinds of insider actions are inappropriate?
- **Next Steps: A Framework for Response**

© 2009 The MITRE Corporation. All rights reserved.

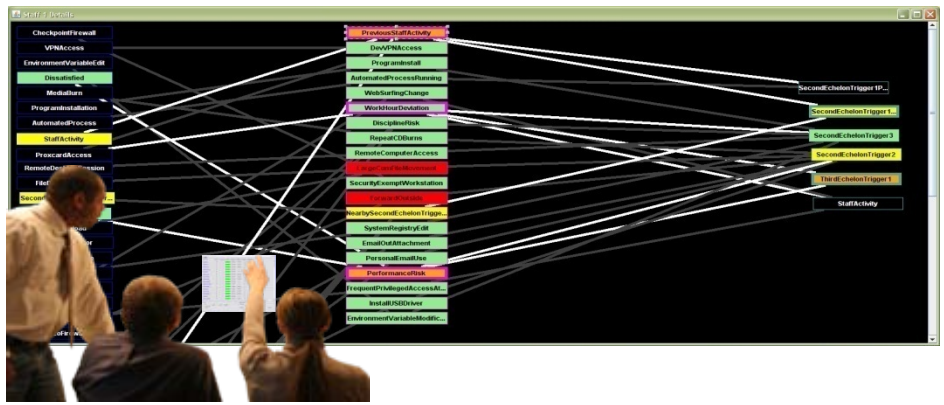
PNNL's Research Focus

Frank L. Greitzer, PhD

- ***PACMAN: IT***
  - ***Key idea: Use of behavioral as well as IT/cyber data within a predictive modeling and analysis framework will improve the security analyst's situation awareness and filter/focus attention on possible higher-risk exploits by insiders.***
- The ***Psyber Sleuth™*** prototype system under development seeks to extend the cyber security analyst's time horizon for proactive defense/mitigation.

- Visual analytics enhancements to improve situation awareness and facilitate coordination among stakeholders

- Multi-layered user interface from high level status displays to detailed monitoring displays.



© 2009 The MITRE Corporation. All rights reserved.

Defense Against the Insider Threat

- **Make your employees the first line of defense**
  - Educating them on spotting suspicious behavior; Treat them fairly
- **Pay attention to your employees behavior**
  - Look for signs of vulnerability, unexplained wealth, etc.
- **Prioritize your assets**
  - Concentrate monitoring resources where it matters
- **Know your network**
  - Baseline normal behaviors on network; look for anomalies
  - Enumerate trust relationships with other orgs; their insiders can become your insiders
- **Divide responsibilities**
  - Separate duties for key functions
- **Grant least privileges**
  - Audit for privilege over-entitlement
- **Prepare for recovery (e.g., COOP, data back up plan)**

http://www.thei3p.org/research/mitremi.html

© 2009 The MITRE Corporation. All rights reserved.

Data from Security Mechanisms Question

Effect of Security Mechanisms on User Behavior (Survey)

For each of these security mechanisms, how would they have affected your behavior as you were gathering information?

Scale: Please rate each (1=No Effect, 5=Great Effect)

Document headers/footers identifying pages as proprietary or sensitive

Pop-up warnings indicating that you were being monitored

Awareness that there is monitoring software on your computer

Signing of company confidentiality agreement

Being in a public environment while using the laptop

Security Policy

Corporate ethics and code of conduct

Knowledge of recent employee information use violations

Mandatory training on safeguarding of proprietary information

© 2009 The MITRE Corporation. All rights reserved.

Advanced Research Questions and Issues

- **Insider Threat Monitoring:**
  - What are the tradeoffs between the individual's right to privacy and the organization's need to protect its assets?
- **Predictive Modeling:**
  - Would pre-intervention violate employee trust or legal guidelines?
  - What about the possibilities of misuse? False accusations can affect the career of the accused.
  - Collection/monitoring of certain types of data may affect employee morale.
- **Impact of "Profiling:"**
  - Understanding the risks (i.e., biases) associated with the collection , access, and assessment of psychological and social information.
  - What are the ethical and legal issues surrounding this approach?
- **Data and Analysis**
  - Need good operational data samples

© 2009 The MITRE Corporation. All rights reserved.

References

Publications

Caputo, D.D., Maloof, M.A., & Stephens, G.D (in press). Detecting the Theft of Trade Secrets by Insiders: A Summary of MITRE Insider Threat Research, *IEEE Security & Privacy, Fall 2009.*

Caputo, D.D, Stephens, G.D., Stephenson, B., Cormier, M. & Kim, M (2008). An Empirical Approach to Identify Information Misuse by Insiders," *Recent Advances in Intrusion Detection, Lecture Notes in Computer Science,* Volume 5230, Springer, pp. 402–403.

Maloof, M.A., & Stephens, G.D. (2007). ELICIT: A System for Detecting Insiders Who Violate Need-to-Know," *Recent Advances in Intrusion Detection, Lecture Notes in Computer Science,* Volume 4637, Springer, pp. 146–166.

Presentations

"An Empirical Approach to Identify Information Misuse by Insiders." Presented at *The Malicious Exploitation of Information Systems: Preventing the Rise of the Insider Threat. University College London. Nov. 6, 2008.*

© 2009 The MITRE Corporation. All rights reserved.

Research often creates more questions than answers!

Backup Slide

© 2009 The MITRE Corporation. All rights reserved.