

Understanding Insider Threat in Online Environments



Cyber Security Division 2012 Principal Investigators' Meeting

10/10/2012

Fariborz Farahmand
Research Assistant Professor
Purdue University
fariborz@purdue.edu

Outline

- **Introduction**
- Technical Approach
- Milestones, Deliverables, and Schedule
- Technology Transition Plan, and Quad Chart

Technical Topic Area and Team Members

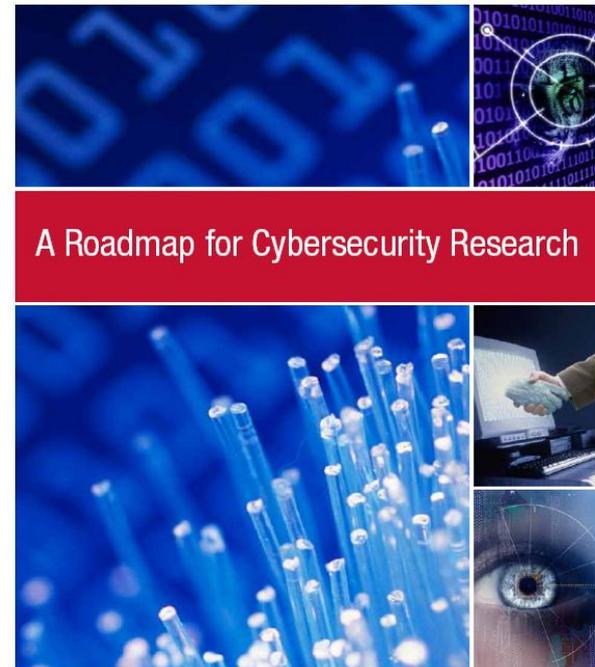
- **TTA 4**
 - Insider Threat
- **Team members**
 - Fariborz Farahmand
 - Eugene H. Spafford
 - Luo Si
 - Sonia Fahmy
 - Consultant (TBD)
 - Graduate Students and Post Doctoral Fellows (TBD)
 - Subcontractor (Applied Communication Sciences)

Outline

- Introduction
- **Technical Approach**
- Milestones, Deliverables, and Schedule
- Technology Transition Plan, and Quad Chart

Defining Insider Threat

- “An insider threat is one that is attributable to individuals who **abuse granted privileges.**”
- “The insider threat is **context dependant** in time and space.”



Insider Threat in the Banking and Finance Sector*

- Most incidents required **little technical sophistication**
- Perpetrators **planned** their actions
- **Financial gain** motivated most perpetrators
- Perpetrators did **not share a common profile**
- Incidents were usually **detected by non-security personnel**
- Incidents were usually detected through **manual procedures**

* M. R. Randazzo, M. Keeney, E. Kowalski, D. Cappelli, and A. Moore, "Insider Threat Study: Illicit cyber activity in the banking and finance sector," 2004.

Network-Based Sensors and Situation Awareness

- “Many of the insiders **do not even touch the network level.**” (M. Ben Salem, S. Hershkop, and S. J. Stolfo, 2008)
- “These sensors are our worst sensors for situational awareness. They give **no indication** of what **our adversary** is planning, sometimes they can show that we are under attack.” (D. W. Aucsmith 2011)
- “There is still a big **gap** between **human analysts’ mental model** and the capability of existing **cyber situation-awareness tools.**” (D. H. Andrews and K. T. Jabbour 2011)

Bayesian Updating

- Requires a **prior**
- **Separation** among:
 - Previous judged probabilities and evaluation of new evidence
 - Probability judgment of states and utilities that result from those states
- Predicts no effect of the **order of information arrival**

Normative Decision Theory*

- A set of potential actions (A_i) to choose between,
- A set of events or world states (E_j),
- A set of consequences (C_{ij}) obtained for each combination of action and event,
- A set of probabilities (P_{ij}) for each combination of action and event,

The expected value of a given action A_i :

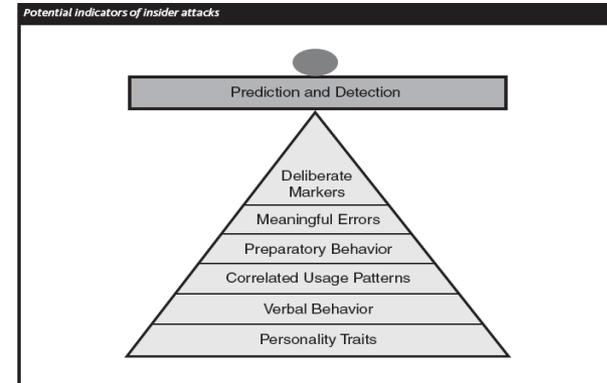
$$EV[A_i] = \sum_k P_{ik} C_{ik}$$

* J. von Neumann, and O. Morgenstern, *Theory of Games and Economic Behavior*, Princeton University Press, 1947.

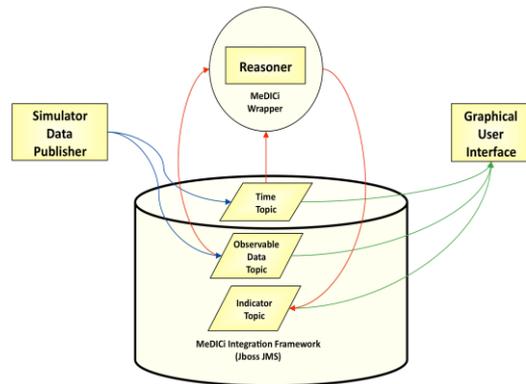
Conceptual Models



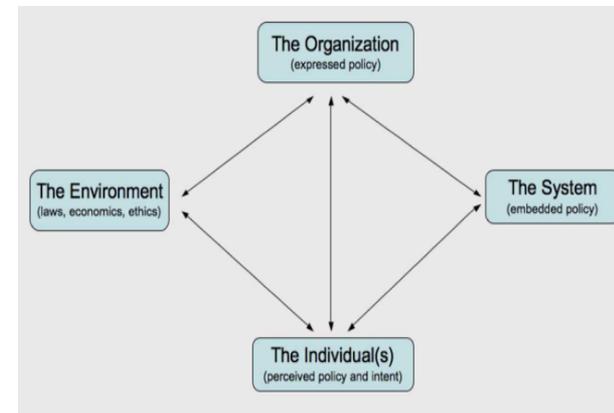
(Wells 1999)



(Schultz 2002)



(Bishop et al. 2009)



(Pfleeger et al. 2010)

Answering Fundamental Questions about Insider Threat

- How do insiders make **decisions**?
- How to **quantitatively** analyze the **context-dependent** decisions of insiders?
- How to build **realistic probabilistic models** to predict insiders' behavior?
- How to use privacy-preserving techniques to **protect users' privacy**?
- How to use **machine learning algorithms** to identify insiders?
- How to select appropriate control measures to **prevent/minimize damages** caused by insiders?

Extending and Expanding our Previous Work

Sample related publications:

- F. Farahmand, M. Atallah, and E. H. Spafford, “Incentive Alignment and Risk Perception: An Information Security Application,” *IEEE Transactions on Engineering Management*, 9 pages, to appear.
- F. Farahmand, and E. H. Spafford, “Understanding Insiders: An Analysis of Risk-Taking Behavior,” *Information Systems Frontiers*, Springer Publications, 11 pages, to appear.
- F. Farahmand, and E. H. Spafford, “Insider Behavior: An Analysis of Decision under Risk,” *First International Workshop on Managing Insider Security Threats, International Federation for Information Processing (IFIP) International Conference on Trust Management*, Jun 2009, 10 pages.
- F. Farahmand, M. J. Atallah, and B. Konsysnski, “Incentives and Perceptions of Information Security Risks,” *Twenty Ninth International Conference on Information Systems, ICIS 2008, Paris, Dec 2008*, 16 pages.

Quantitative and Cognitive Modeling

- $V_B(x, S)$: Value of option x given choice set S and background context B ,
- β_i : Weight of attribute i ,
- $v_i(x_i)$: Utility of the value x_i of option x on attribute i ,
- $R(x, y)$: Relative advantage of option x over option y ,
- θ : Weight given to the relative advantage component of the model

Componential context model:

$$V_B(x, S) = \sum_{i=1}^n \beta_i v_i(x_i) + \theta \sum_{y=S} R(x, y)^*$$

* A. Tversky, and I. Simonson, "Context-Dependent Preferences," *Management Science*, 39(10), 1993, pp. 1179-1189

Machine Learning and Privacy-Preserved Learning Methods

- Unsupervised learning
- Supervised learning
- Meta learning
- Active learning
- Protecting users' privacy

Outline

- Introduction
- Technical Approach
- **Milestones, Deliverables, and Schedule**
- Technology Transition Plan, and Quad Chart

Schedule and Milestones

| Period/Quarter | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | |
|--|-------------|---|-------|---|---|-------|-------|-------|--------|-------|-------------|-------|-------|----|--|
| Base | ←————→ | | | | | | | | | | | | | | |
| 1) Design algorithms and components for prototype | ————→ | | | | | | | | | | | | | | |
| 2) Design probabilistic models | ————→ | | | | | | | | | | | | | | |
| 3) Develop framework for detecting abnormal users | | | | | | ————→ | ————→ | | | | | | | | |
| 4) Investigate alternative modeling approaches | | | | | | ————→ | ————→ | | | | | | | | |
| 5) Design probabilistic frameworks | ————→ | | | | | | | | | | | | | | |
| 6) Design insider detection system | | | | | | ————→ | ————→ | | | | | | | | |
| 7) Develop report describe planned architecture | | | | | | ————→ | ————→ | | | | | | | | |
| 8) Determine functional requirements | | | | | | ————→ | ————→ | | | | | | | | |
| 9) Refine initial report | | | | | | | ————→ | ————→ | | | | | | | |
| 10) Implement SW prototype | | | | | | ————→ | ————→ | | | | | | | | |
| 110 Develop a human use protocol | | | ————→ | | | | | | | | | | | | |
| Option 1: Testing and Evaluation | | | | | | | | | ←————→ | | | | | | |
| 1) Provide data for algorithm refinement and prototype development | | | | | | | | | ————→ | | | | | | |
| 2) Internal functional, validation and system testing | | | | | | | | | ————→ | | | | | | |
| 3) On-site testing with a partner in the financial services | | | | | | | | | | | ————→ | | | | |
| 4) Conduct single unit and multi unit tests | | | | | | | | | | ————→ | | | | | |
| 5) Perform post-test analysis on prototype performance | | | | | | | | | | | | ————→ | | | |
| Option 2: Technology Demo. in an Operational Environment | | | | | | | | | | | | | ↔ | | |
| 1) Support a technology demonstration with a partner in financial services | | | | | | | | | | | | | ————→ | | |
| 2) Customize and adapt the software prototype | | | | | | | | | | | | | ————→ | | |
| 3) Provide on-site support staff during the technology demonstration | | | | | | | | | | | | | ————→ | | |
| Report & Documentation | - - - - - → | | | | | | | | | | | | | | |
| Deliver Software Developed | | | | | | | | | | | - - - - - → | | | | |

Deliverables

- Monthly status reports
- Architecture design documents
- System design documents
- Models of insider behavior
- Test results and analysis
- Prototype software

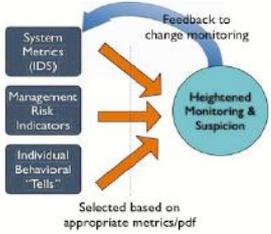
Outline

- Introduction
- Technical Approach
- Milestones, Deliverables, and Schedule
- **Technology Transition Plan, and Quad Chart**

Technology Transition Plan

- Working with a live financial partner
- Testing and Evaluation
 - Single unit testing
 - Multi unit testing
 - DETER
- Technology demonstration in operational environments

Quad Chart

| | |
|--|---|
| <p>BAA: 11-02-TTA 04-0026-I Title: Understanding Insider Behavior in Online Environments</p> | <p>Offeror Name: CERIAS, Purdue University Date : 10/10/2012</p> |
| <p>Photograph or Artist’s Concept:</p>  | <p>Operational Capability: The product will be designed to identify characteristics of insiders that can be matched with the risk models and with an observation and feedback mechanism that can be used in a continuous observational mode. It will operate in parallel with existing systems of organizations, and will provide information to the existing operational security staff.</p> |
| <p>Proposed Technical Approach: Exploring and integrating research in: 1) developing probabilistic user behavior models for accurate malicious insider detection, 2) Learning techniques coupled with active learning to reinforce or discount classification of a user as malicious, and 3) Privacy-preserving methods to protect user information collected by the system.</p> <p>We will evaluate our system via testbed experiments first via controlled experiments and then in our target domain of the financial sector, and DETER.</p> | <p>Schedule and Deliverables: This proposal involves basic research, so we are pursuing a Type I activity; Month 1– 36: Data collection and analysis, Month 1– 24: Design algorithms and components of prototype, probabilistic models, and active learning approach, Months 16-24: Design the insider detection system such that supports the privacy principles of USACM , Months 16 –24: Design and implement the software prototype, Months 25 – 36: Testing and evaluation, Months 33 – 35: Post-test analysis, Months 37-- 42: Support technology demonstration in operational environment.</p> <p>Milestones will be detailed against the preliminary development schedule detailed above. A model, technical reports, and a refined prototype system will be delivered.</p> |