

Profiling Users: Insider Threat Detection and Prevention

Veronica Young
 University of California, Merced
 Research Alliance in Math and Science
 Computational Sciences and Engineering Division, Oak Ridge National Laboratory
 Mentor: Dr. Robert K. Abercrombie
http://wiki.ornl.gov/sites/rams09/v_young/Pages/default.aspx

Insider sourced espionage, sabotage, and fraud are now considered as the top cyber threat. Cost estimates approach \$250 billion/year from modification of data, security mechanism, unauthorized network connections, covert channels, and physical damage and destruction including information extrusion/exfiltration. Insiders have access privileges enable them to easily bypass many countermeasures such as firewalls. Methods developed to counter this attack currently utilize machine learning techniques and sensors. This project studied characteristics activities and relationships among cyber assets and players by developing a heuristic anomaly detector.

Research Objectives

- Survey current anomaly detectors
- Select a set of criteria appropriate methods for Heuristic Identification and Tracking of Insider Threat (HIT-IT)

Definitions

- **Insider** - an individual who has a trust relationship with an organization that is manifested by that organization's granting the person some level of privileges [3].
- **Malicious Insider** - an insider that betrays or takes advantage of the given trust.

Malicious Insiders

- Estimated \$250 B/year lost due to malicious insiders

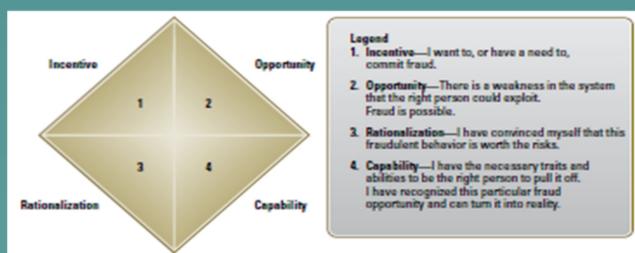


Figure 1. The Fraud Diamond (Gabrielson, et al. 2008)

- Commit espionage, exfiltration, fraud, sabotage, intellectual and identity theft
- Display certain behaviors before attack

Anomaly Detector (AD) Methods

- **Honeypots, Honeynets and Honeytokens** - utilized to identify malicious users
- **Support Vector Machines** - classifies users via machine learning
- **Finite State Automata (FSA)** - monitors system call sequences
- **Hidden Markov Models (HMM)** - probabilistic historical behavioral analysis

Insider Threat Scenario Model

- Petri Net implements AD methods to detect malicious threat

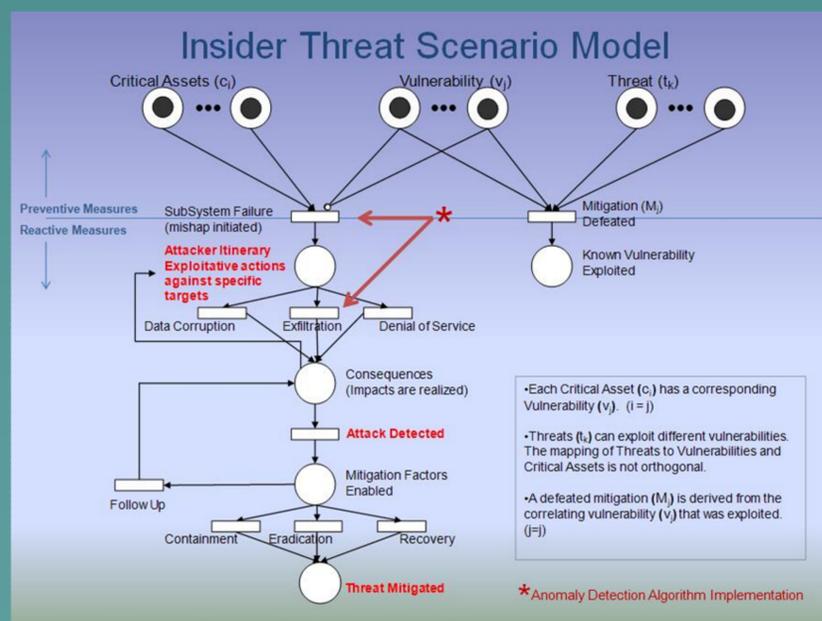


Figure 2. Petri Net: Insider threat scenario model.

Theoretical Results

- Displays SVM results in Figure 3 below
- Projects accurate with low false positives and negatives

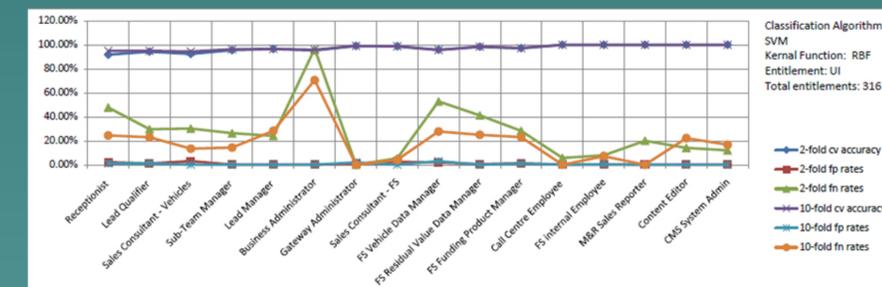


Figure 3. SVM results (Ni, et al. 2009).

Future Research

- Utilize selected AD methods in HIT-IT software implementation
- Establish metrics and set up experiments to test and evaluate selected methods

References

- [1] Ni, Q., J. Lobo, et al. (2009). Automating role-based provisioning by learning from examples. *Proceedings of the 14th ACM symposium on Access control models and technologies*. Stresa, Italy, ACM.
- [2] Seo, Y.-W. and K. Sycara (2008). Addressing Insider Threat through Cost-Sensitive Document Classification. *Terrorism Informatics*. E. R. Hsinchun Chen, Joshua Sinai, Andrew Silke, and Boaz Ganor, Springer US. 18: 451-472.
- [3] Gabrielson, B., K. M. Goertzel, et al. (2008). "The Insider Threat to Information Systems: A State-of-the-Art Report." *State-of-the-Art Report*.