Design and Implementation of a Comprehensive Insider Threat Ontology

James D. Lee

George Mason University
Design and Implementation of a Comprehensive Insider Threat Ontology

17th Annual Conference on Systems Engineering Research (CSER) 2019
Washington, D.C., April 3-4, 2019

Paper Session 13 (11:00 – 11:20 AM)

Dr. Frank L. Greitzer
James D. Lee (Presenter)
Justin Purl
Dr. Abbas K. Zaidi
Overview

• Background
  – Insider threat detection
  – Problem statement

• Sociotechnical and Organizational Factors for Insider Threat (SOFIT)

• Ontology Implementation

• Applications

• Conclusion
Background

- In 2016, 874 insider threat incidents across 54 organizations averaged $4.3M damage/organization [1]
- Organizations’ response to mitigate insider threat risk varies widely from reactive to proactive and predictive
- Best practices employ a predictive approach that monitors a variety of technical and behavioral data:
  - Data processed to observables
  - Collection of observables infer indicators
  - Indicators infer target (threat) behavior
Problem Statement

Challenges:
• Making inferences based on incomplete and uncertain data
• Lack of completeness and accuracy of a single source knowledge base that informs such inferences
• Non-optimal data – data that are the most available may not always be the most useful for particular types of threat
• Lack of ground truth required for testing mitigation approaches
• Need for better understanding of:
  – Indicators that infer target (threat) behavior
  – Collection of observables that infer indicators
  – Necessary data given the observables of interest
• Adoption of comprehensive Insider Threat factor knowledge base as an ontology
  – To provide a common structure of the knowledge of the domain
  – To facilitate sharing of the knowledge base
  – To enable knowledge base to be applied to a variety of missions
Why Ontology?

• Formal description of concepts within domain
• Formal semantics and constraints provide computational properties
• Ability to draw inferences from asserted facts
### Related Work

This work derives from a large base of published research and case studies (especially CERT reports and publications, e.g. [2] and [3]; and research by Greitzer and colleagues [4]).

Development of SOFIT is documented in [5]-[7].

<table>
<thead>
<tr>
<th>Ontology/Reference</th>
<th>Domain/Scope</th>
<th>Technical/ Cyber</th>
<th>Human/ Behavioral</th>
<th>Organizational</th>
</tr>
</thead>
<tbody>
<tr>
<td>CERT ITIO</td>
<td>Insider Threat</td>
<td>✓</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>MITRE (STIX)</td>
<td>Cyber Security</td>
<td>✓</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>MITRE (CAPEC)</td>
<td>Cyber Security - Attack Patterns</td>
<td>✓</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>MITRE (CWE)</td>
<td>Cyber Security - Weaknesses</td>
<td>✓</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>MAEC</td>
<td>Cyber Security - Malware</td>
<td>✓</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>CRATELO</td>
<td>Cyber Security</td>
<td>✓</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>HUFO</td>
<td>Cyber Security - Trust</td>
<td>✓</td>
<td>✓</td>
<td>-</td>
</tr>
<tr>
<td>SOFIT</td>
<td>Insider Threat</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>
Design Objectives

• Use Case 1. Ontology capturing expert knowledge on insider threat factors that may be shared with research/operational communities.

• Use Case 2. Support development of a tool to evaluate the coverage of an organization’s insider threat mitigation program compared to ‘best practices’.

• Use Case 3. Support development of tools to assess insider threat risk for individuals in an organization.
Ontology Overview

- Actor has Factor and Intention
- Intention is manifested as Threat Type
- Factor is associated with Threat Type and plays a role (Factor Role) in process of insider threat exploit
Taxonomy of Factors

<table>
<thead>
<tr>
<th>ID</th>
<th>Factor Label</th>
<th>Description</th>
<th>Abbreviated Citation</th>
<th>Risk Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Individual Factor</td>
<td>Characteristic relevant to assessment of insider threat. Individual human factors pertaining to human characteristics or behaviors in insider threat domain.</td>
<td>Band et al. (2008); Kremer et al. (2005)</td>
<td></td>
</tr>
<tr>
<td>1.1</td>
<td>Boundary Violation</td>
<td>Action by a person that is outside of normal or accepted behaviors. This may include violating up to the level of organizational policy violations.</td>
<td>Bulling et al. (2008)</td>
<td></td>
</tr>
<tr>
<td>1.1.1</td>
<td>Concerning Work Habits</td>
<td>Work habits and patterns that are potentially of concern for an enterprise.</td>
<td>Bulling et al. (2008)</td>
<td></td>
</tr>
<tr>
<td>1.1.1.1</td>
<td>Working At Unusual Hours</td>
<td>Working at hours markedly different from peers.</td>
<td>Bulling et al. (2008)</td>
<td>43</td>
</tr>
<tr>
<td>1.1.1.1.1</td>
<td>Odd Hours Work Machine</td>
<td>Using work-owned machine outside of normal work hours.</td>
<td>IARPA SCIE Program</td>
<td>35</td>
</tr>
<tr>
<td>1.1.1.1.2</td>
<td>Odd Hours Work Week</td>
<td>Changes times at which she/ he regularly works during work week.</td>
<td>IARPA SCIE Program</td>
<td>30</td>
</tr>
<tr>
<td>1.1.1.1.3</td>
<td>Odd Hours Work Week Offsite</td>
<td>Changes periodicity of work done at home or remote sites during work week.</td>
<td>IARPA SCIE Program</td>
<td>32</td>
</tr>
<tr>
<td>1.1.1.2</td>
<td>Change Work Performed Offsite During Week</td>
<td>Changes amount of work done at home or at remote sites during work week.</td>
<td>IARPA SCIE Program</td>
<td>30</td>
</tr>
</tbody>
</table>

![Diagram of Taxonomy Factors]

Annotations: LargeDataTransfer

- rdfs:label: LargeDataTransfer
- rdfs:abbreviatedCitation: SET (2015)
- rdfs:description: Firewall log entries that indicate transfer large amounts of data.
- rdfs:issue: 1.1.3.4.3
- rdfs:risks: 80
Threat Type and Factor Role
Use Case 1: Knowledge Base to Inform Research and Operational Communities

SOFIT is a comprehensive knowledge base for insider threat technical and behavioral indicators

- Implemented as an ontology with over 320 constructs (factors), including
  - **Individual (Human) Factor** branch contains more than 270 technical and behavioral factors
  - **Organizational Factor** branch includes roughly 50 contributing factors
- Current work focuses on applying the ontology to support modeling and inferences about insider threat.
Use Case 2: Foundation for Tools to Assess an Organization’s Insider Threat Monitoring Program

Compare the indicators detectable by the organization’s system against indicators identified in SOFIT and/or best practices.

Conceptual Illustration
Use Case 3: Foundation for Qualitative and Quantitative Insider Threat Assessment Tool

Ongoing research to estimate quantitative threat/risk values for individual indicators that can inform threat assessment models...

**Qualitative Assessment**

<table>
<thead>
<tr>
<th>Case #1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Depression</td>
</tr>
<tr>
<td>Misses or late for meetings</td>
</tr>
<tr>
<td>Recent change in marital status</td>
</tr>
<tr>
<td>Receiving large email attachments</td>
</tr>
<tr>
<td>Requires excessive oversight</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Case #2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Terminated</td>
</tr>
<tr>
<td>Extreme discontent</td>
</tr>
<tr>
<td>Establish backdoor</td>
</tr>
<tr>
<td>Transfer large amount of data</td>
</tr>
<tr>
<td>Strong reaction to organizational sanctions</td>
</tr>
</tbody>
</table>

**Quantitative Assessment**

"additive" model example

<table>
<thead>
<tr>
<th>Indicator</th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Case #1</td>
<td></td>
</tr>
<tr>
<td>Depression</td>
<td>52</td>
</tr>
<tr>
<td>Misses or late for meetings</td>
<td>38</td>
</tr>
<tr>
<td>Recent change in marital status</td>
<td>35</td>
</tr>
<tr>
<td>Receiving large email attachments</td>
<td>55</td>
</tr>
<tr>
<td>Requires excessive oversight</td>
<td>39</td>
</tr>
</tbody>
</table>

**Threat Value for Case #1:** 219

**Characterization of Case #1**
- Precipitating Event
  - Recent change in marital status
- Behavioral Precursor
  - Misses or late for meetings
- Contextual Variable
  - Depression
  - Receiving large email attachments
  - Requires excessive oversight

**Characterization of Case #2**
- Precipitating Event
  - Terminated
- Behavioral Precursor
  - Extreme discontent
- Strong reaction to organizational sanctions
- Technical Precursor
  - Establish backdoor
  - Transfer large amount of data

**Indicator | Score**

<table>
<thead>
<tr>
<th>Case #2</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Terminated</td>
<td>69</td>
</tr>
<tr>
<td>Extreme discontent</td>
<td>66</td>
</tr>
<tr>
<td>Establish backdoor</td>
<td>90</td>
</tr>
<tr>
<td>Transfer large amount of data</td>
<td>80</td>
</tr>
<tr>
<td>Strong reaction to organizational sanctions</td>
<td>69</td>
</tr>
</tbody>
</table>

**Threat Value for Case #2:** 374
Over the last 2 years we have conducted several expert knowledge elicitation surveys to support our objectives for Use Cases 1, 2 and 3:

• Helped to populate the ontology with expert judgments of threat/risk level for individual indicators
• Helped to test various quantitative models that describe how experts assess collections of observed indicators to determine overall threat/risk of insider threat cases

Because there was no access to operational test data with ground truth, these studies used expert judgments as “proxies” in evaluating models.
Conclusion

Contributions:
• Development of a comprehensive insider threat ontology that may be shared with operational and research communities
• Foundation for development of applications for
  – Assessing an organization’s insider threat program
  – Individual insider threat assessment tools (qualitative & quantitative)
• Empirical studies obtained expert judgments to inform the ontology and to test proposed models of individual threat assessment

Limitations:
• While the knowledge base has been informed by expert judgments, the ontology and associated threat models have not been validated against operational data with ground truth.


Contact Information

• For more information, please contact:

Frank L. Greitzer, PsyberAnalytix
Frank@PsyberAnalytix.com

• Acknowledgments:

SOFIT: SOCIOTECHNICAL AND ORGANIZATIONAL FACTORS FOR INSIDER THREAT

Development Team/Knowledge Base Design:
Frank L. Greitzer, PsyberAnalytix
Justin Purl, Human Resources Research Organization
Yung Mei Leong, Independent Contractor
D.E. (Sunny) Bedker, Human Resources Research Organization
Paul J. Sticha, Human Resources Research Organization

Ontology Implementation:
James Lee, George Mason University
Abbas Zaidi, George Mason University
Kathryn Laskey, George Mason University

This research was supported under IARPA contract 2016-16031400006. The content is solely the responsibility of the authors and does not necessarily represent the official views of the U.S. Government.