Overview of the Threat Posed by Insiders to Critical Assets

Randy Trzeciak
Technical Manager - CERT Enterprise Threat and Vulnerability Management Team & CERT Insider Threat Center

Randy is Technical Manager of CERT’s Enterprise Threat and Vulnerability Management Team and the CERT Insider Threat Center at Carnegie Mellon University's Software Engineering Institute. The team’s mission is to assist organizations in improving their security posture and incident response capability by researching technical threat areas, developing and conducting information security assessments, and providing information, solutions and training for preventing, detecting, and responding to illicit activity.

David Mundie
CERT CSIRT Development Team Member

David Mundie is a member of the CSIRT Development Team within the CERT® Program at the Software Engineering Institute (SEI), a unit of Carnegie Mellon University in Pittsburgh, PA. He has been at CERT since 2000 and has worked in a variety of areas including insider threat, malware analysis, and incident management capability metrics. From 2006 to 2009, he was a member of the Q-CERT project, which established a national information security team for the country of Qatar.
What is the CERT Insider Threat Center?

Center of insider threat expertise

Began working in this area in 2001 with the U.S. Secret Service

Our mission: *The CERT Insider Threat Center conducts empirical research and analysis to develop & transition socio-technical solutions to combat insider cyber threats.*
Goal for an Insider Threat Program

Opportunities for prevention, detection, and response for an insider incident
CERT’s Unique Approach to the Problem

Research Models

Deriving Candidate Controls and Indicators

Our lab transforms that into this...

Splunk Query Name: Last 30 Days - Possible Theft of IP

Terms: 'host=HECTOR [search host="zeus.corp.merit.lab" Message="A user account was disabled. *" | eval Account_Name=mvindex(Account_Name, -1) | fields Account_Name | strcat Account_Name "@corp.merit.lab" sender_address | fields - Account_Name] total_bytes > 50000 AND recipient_address!="*corp.merit.lab" startdaysago=30 | fields client_ip, sender_address, recipient_address, message_subject, total_bytes'
The Insider Threat

There is not one “type” of insider threat

- Threat is to an organization’s critical assets
  - People
  - Information
  - Technology
  - Facilities
- Based on the motive(s) of the insider
- Impact is to Confidentiality, Availability, Integrity

There is not one solution for addressing the insider threat

- Technology alone may not be the most effective way to prevent and/or detect an incident perpetrated by a trusted insider
Separate the “Target” from the “Impact” from the “Actor”

**Target**

**Critical Assets**
- People
- Technology
- Information
- Facilities

**Impact**

Confidentiality
Availability
Integrity

**Actor(s)**

Employees
- Current
- Former
Contractors
Subcontractors
Suppliers
Trusted Business Partners
What is a Malicious Insider Threat?

**Current or former employee, contractor, or other business partner who**

- has or had authorized access to an organization’s network, system or data and
- intentionally exceeded or misused that access in a manner that
- negatively affected the confidentiality, integrity, or availability of the organization’s information or information systems.
What is an Unintentional Insider Threat?

Current or former employee, contractor, or other business partner who

- who has or had authorized access to an organization’s network, system, or data and who, through
- their action/inaction without malicious intent
- cause harm or substantially increase the probability of future serious harm to the confidentiality, integrity, or availability of the organization’s information or information systems.
## Types of Insider Crimes

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Insider IT sabotage</strong></td>
<td>An insider’s use of IT to direct specific harm at an organization or an individual.</td>
</tr>
<tr>
<td><strong>Insider theft of intellectual property (IP)</strong></td>
<td>An insider’s use of IT to steal intellectual property from the organization. This category includes industrial espionage involving insiders.</td>
</tr>
<tr>
<td><strong>Insider fraud</strong></td>
<td>An insider’s use of IT for the unauthorized modification, addition, or deletion of an organization's data (not programs or systems) for personal gain, or theft of information which leads to fraud (identity theft, credit card fraud).</td>
</tr>
<tr>
<td><strong>National Security Espionage</strong></td>
<td>The act of stealing and delivering, or attempting to deliver, information pertaining to the national defense of the United States to agents or subjects of foreign countries, with intent or reason to believe that is to be used to the injury of the United States or to the advantage of a foreign nation.</td>
</tr>
</tbody>
</table>
IT Sabotage
TRUE STORY:

SCADA systems for an oil-exploration company is temporarily disabled…

*A contractor, who’s request for permanent employment was rejected, planted malicious code following termination*
Other Cases of IT Sabotage

Financial Institution customers lose all access to their money from Friday night through Monday

- Fired system administrator sabotages systems on his way out

A subcontractor at an energy management facility breaks the glass enclosing the emergency power button, then shuts down computers that regulate the exchange of electricity between power grids, even though his own employer had disabled his access to their own facility following a dispute.

- Impact: Internal power outage; Shutdown of electricity between the power grids in the US.

Former employee of auto dealer modified vehicle control system after being laid off

- Searched for known customers and sent out unwarranted signals to vehicle control devices disabled ignitions and set off alarms

A security guard at a U.S. hospital, after submitting resignation notice, obtained physical access to computer rooms

- Installed malicious code on hospital computers, accessed patient medical records
## Summary of Insider Threats

<table>
<thead>
<tr>
<th>Current or former employee?</th>
<th>IT Sabotage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Former</td>
<td>Technical (e.g. sys admins, programmers, or DBAs)</td>
</tr>
</tbody>
</table>

| Type of position            | Male        |

<table>
<thead>
<tr>
<th>Gender</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Male</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Target</th>
<th>Network, systems, or data</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Access used</th>
<th>Unauthorized</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>When</th>
<th>Outside normal working hours</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Where</th>
<th>Remote access</th>
</tr>
</thead>
</table>
Fraud
TRUE STORY:

An undercover agent who claims to be on the “No Fly list” buys fake drivers license from a ring of DMV employees...

The 7 person identity theft ring consisted of 7 employees who sold more than 200 fake licenses for more than $1 Million.
Other Cases of Fraud

An accounts payable clerk, over a period of 3 years, issued 127 unauthorized checks to herself and others...
  - Checks totaled over $875,000

A front desk office coordinator stole PII from hospital...
  - Over 1100 victims and over $2.8 M in fraudulent claims

A database administrator at major US Insurance Co. downloaded 60,000 employee records onto removable and solicited bids for sale over the Internet

An office manager for a trucking firm fraudulently puts her husband on the payroll for weekly payouts, and erases records of payments...
  - Over almost a year loss of over $100K
## Summary of Insider Threats

<table>
<thead>
<tr>
<th></th>
<th>IT Sabotage</th>
<th>Fraud</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Current or former employee?</strong></td>
<td>Former</td>
<td>Current</td>
</tr>
<tr>
<td><strong>Type of position</strong></td>
<td>Technical (e.g. sys admins, programmers, or DBAs)</td>
<td>Non-technical (e.g. data entry, customer service) or their managers</td>
</tr>
<tr>
<td><strong>Gender</strong></td>
<td>Male</td>
<td>Fairly equally split between male and female</td>
</tr>
<tr>
<td><strong>Target</strong></td>
<td>Network, systems, or data</td>
<td>PII or Customer Information</td>
</tr>
<tr>
<td><strong>Access used</strong></td>
<td>Unauthorized</td>
<td>Authorized</td>
</tr>
<tr>
<td><strong>When</strong></td>
<td>Outside normal working hours</td>
<td>During normal working hours</td>
</tr>
<tr>
<td><strong>Where</strong></td>
<td>Remote access</td>
<td>At work</td>
</tr>
</tbody>
</table>

© 2013 Carnegie Mellon University
Theft of Intellectual Property

WELCOME ABOARD SMITH. I'M SURE THE "KNOWLEDGE AND EXPERIENCE" YOU BRING WITH YOU WILL BE EXTREMELY VALUABLE.
TRUE STORY:

Research scientist downloads 38,000 documents containing his company’s trade secrets before going to work for a competitor…

Information was valued at $400 Million
Other Cases of Theft of IP

A technical operations associate at a pharmaceutical company downloads 65 GB of information, including 1300 confidential and proprietary documents, intending to start a competing company, in a foreign country…

- Organization spent over $500M in development costs

Simulation software for the reactor control room in a US nuclear power plant was being run from outside the US…

- A former software engineer born in that country took it with him when he left the company.
## Summary of Insider Threats

<table>
<thead>
<tr>
<th>Current or former employee?</th>
<th>IT Sabotage</th>
<th>Fraud</th>
<th>Theft of Intellectual Property</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current or former employee?</td>
<td>Former</td>
<td>Current</td>
<td>Current (within 30 days of resignation)</td>
</tr>
<tr>
<td>Type of position</td>
<td>Technical (e.g. sys admins, programmers, or DBAs)</td>
<td>Non-technical (e.g. data entry, customer service) or their managers</td>
<td>Technical (e.g. scientists, programmers, engineers) or sales</td>
</tr>
<tr>
<td>Gender</td>
<td>Male</td>
<td>Fairly equally split between male and female</td>
<td>Male</td>
</tr>
<tr>
<td>Target</td>
<td>Network, systems, or data</td>
<td>PII or Customer Information</td>
<td>IP (trade secrets) –or customer Info</td>
</tr>
<tr>
<td>Access used</td>
<td>Unauthorized</td>
<td>Authorized</td>
<td>Authorized</td>
</tr>
<tr>
<td>When</td>
<td>Outside normal working hours</td>
<td>During normal working hours</td>
<td>During normal working hours</td>
</tr>
<tr>
<td>Where</td>
<td>Remote access</td>
<td>At work</td>
<td>At work</td>
</tr>
</tbody>
</table>
Ontologies for Insider Threat Research
Vision

The most important attributes would be the construction of a common language and a set of basic concepts about which the security community can develop a shared understanding... a common language and agreed-upon experimental protocols will facilitate the testing of hypotheses and validation of concepts. –Jason Report
Medical Ontologies

**mitochondrion** (GO:0005739)
A semi-autonomous, self-replicating organelle that occurs in varying numbers, shapes, and sizes in the cytoplasm of virtually all eukaryotic cells. It is notably the site of tissue respiration.

- exact synonym: mitochondria
- subset go slim: Aspergillus GO slim
- subset go slim: Candida GO slim
- subset go slim: Generic GO slim
- subset go slim: Metagenomics GO slim
- subset go slim: PIR GO slim
- subset go slim: Plant GO slim
- subset go slim: Yeast GO slim
- xref analog: NIF_Subcellular:sao1860313010
- xref analog: Wikipedia:Mitochondrion

Child terms:
- mitochondrial derivative
- mitochondrial part
- Nebenkern
Google Knowledge Graph (cont.)

- Huge “semantic network” of over 570 million objects and 18 billion facts (500 million objects and 3.5 billion facts)

- Sources: CIA World Factbook, Wikipedia, Freebase

- Facts about: people, actors, directors, movies, cities, countries, recipes, etc.

- Available in multiple languages; localized search results

http://googleblog.blogspot.co.uk/2012/05/introducing-knowledge-graph-things-not.html
http://www.newyorker.com/online/blogs/culture/2012/05/google-knowledge-graph.html
http://venturebeat.com/2013/01/22/larry-page-on-googles-knowledge-graph-were-still-at-1-of-where-we-want-to-be/
Ontology Work at CERT

Incident Management
• Incident Management Body of Knowledge
• MAL: Ontology-based Competency Model

General
• 10-step methodology for developing ontologies
  • Terms, controlled vocabulary, static relationships, dynamic relationships

Insider Threat
• Lexicographic insider threat ontology
• Trust ontology
• Indicator ontology
• Unintentional insider threat ontology
A Lexicographic Ontology of Insider Threat
From Lexicography to Ontology
42 Definitions

• Encountered during a literature search
• Two example definitions
  – *is someone who is authorized to use computers and networks*
  – *is anyone who operated inside the security perimeter*
From Natural Language to Formal Language

• Inspired by Travis Breau
  • captured state notification laws in DL
  • Looks like this:
    • is(inside, anyone(authorized to use(computers and networks)))
    • is(inside, anyone(operating inside (security perimeter)))
From Formal Language to Structure
From Formal Language to Structure

assets

acts on, has knowledge of

individual

authorizes, trusts

organization

owns
From Formal Language to Structure

- **assets**
  - location, media type, sensitivity, owner, custodian
  - acts on, has knowledge of
  - individual
    - role, authorization, type, intention, location
  - organization
    - owns
    - sector, policy framework, size, age, maturity level
  - authorizes, trusts
Draft Ontology

- agent
  - intentional-agent
    - trustee
    - truster
    - unintentional-agent
  - asset
    - information-asset
    - physical-asset
  - attack
  - authorization
  - case
  - context
    - academic-system
    - commercial-system
    - domestic-system
    - financial-system
    - governmental-system
    - manufacturing-system
  - intention
  - materiality
  - personality-type
  - physical-location
  - policy-framework
  - professional-relationship
    - direct-supervisor
    - indirect-supervisor
  - prosecutability
  - security-location
    - outside-the-perimeter
    - within-the-perimeter
  - status
An Ontology for Insider Threat Indicators
Design Goals

• Goal #1: Focus on detection
• Goal #2: Make indicator definition simple
• Goal #3: Be agnostic and compatible with existing models
• Goal #4: Be easily extensible

• Assumption #1: The focus should be on the person
• Assumption #2: Indicators should target significant events
The Ontology in OWL
A Sample Indicator

Indicators use simple subject-verb-object (SVO) syntax borrowed from natural language.

```plaintext
if entity:securityRoleEntity:systemAdministrator
performs action:dataMovementAction:egress:printing
on object:dataObject:anyDataObject
within time:definedScheduleTime:non-work-hours
perform analysis:binaryAnalysis
```
A Sample Indicator

Indicators use simple subject-verb-object (SVO) syntax borrowed from natural language.

```plaintext
if systemAdministrator performs printing on anyDataObject within non-work-hours perform binaryAnalysis
```
CERT’s Insider Threat Services
Insider Threat Assessment (ITA)

**Objective**: To measure an organization’s level of preparedness to address insider threats to their organization.

**Method**: Document Review, Process Observation, and Onsite interviews using insider threat assessment workbooks based on all insider threat cases in the CERT case library.

**Outcome**: Confidential report of findings with findings and recommendations.

**Areas of Focus**: Information Technology/Security; Software Engineering; Data Owners; Human Resources; Physical Security; Legal / Contracting; Trusted Business Partners.
CERT Insider Threat Workshops

**Goal:** participants leave with actionable steps they can take to better manage the risk of insider threat in their organization

½ day, One day, Two days - Presentations and interactive exercises

Addresses technical, organizational, personnel, security, and process issues

Exercises

- Address portions of the insider threat assessment
- Purpose: assist participants in assessing their own organization's vulnerability to insider threat in specific areas of concern
Building an Insider Threat Program

**Goal:** CERT staff work with senior executives from across the organization to develop a strategic action plan, based on actual cases of insider threats at the participating organization and research by CERT staff, to address and mitigate the risk of insider threat at the organization.

- Key differences from standard workshop
  - Tailored course material based on actual insider incidents at the organization.
    - Cases are provided in advance by the organization, and treated with strict confidentiality.
    - Workshop is preceded by a 3-day onsite by CERT staff to work with the organization’s staff to familiarize themselves with the provided case material.
  - Second day of workshop CERT staff and executives work together to create the Organization’s strategic plan for preventing, detecting and responding to insider threats.
CERT Resources

Insider Threat Center website
(http://www.cert.org/insider_threat/)

(http://www.sei.cmu.edu/library/abstracts/reports/12tr012.cfm)

Insider threat workshops

Insider threat assessments

New controls from CERT Insider Threat Lab

Insider threat exercises

The CERT® Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes (Theft, Sabotage, Fraud) (SEI Series in Software Engineering) by Dawn M. Cappelli, Andrew P. Moore and Randall F. Trzeciak