Best Practices and Controls for Mitigating Insider Threats

George Silowash  
Team Member, Technical Solutions  
- Digital Forensic Investigations & Incident Response  
- Information Assurance Risk Management  
- Open Source Solutions

Alex Nicoll  
Team Lead, Technical Solutions  
- Information Assurance  
- Operating System Design  
- High Assurance Systems (MLS)
**Title:** Best Practices and Controls for Mitigating Insider Threats

**Performing Organization:** Carnegie Mellon University, Software Engineering Institute, Pittsburgh, PA, 15213

**Distribution/Availability Statement:** Approved for public release; distribution unlimited

**Security Classification:** Unclassified

**Abstract:**

Insider threats are a significant concern for organizations, as they can exploit their access to sensitive information. Effective controls and practices are essential to mitigate these threats. This report outlines best practices and controls that organizations can implement to safeguard against insider threats. These strategies include awareness training, access controls, monitoring, and incident response protocols. By adopting these measures, organizations can enhance their security posture and reduce the risk of unauthorized access and data breaches.

**Number of Pages:** 53
Agenda

• Introduction

• Common Sense Guide to Mitigating Insider Threats, 4th Edition
  • 19 Best Practices

• Technical Demonstration(s)
CERT Insider Threat Center—Mission

Assist organizations in identifying indications and warnings of insider threat by

- performing vulnerability assessments
- assisting in the design and implementation of policies, practices, and technical solutions

based on our ongoing research of hundreds of actual cases of insider IT sabotage, theft of intellectual property, fraud, and espionage
Definition of Insider Threat

The CERT Program’s definition of a malicious insider is a current or former employee, contractor, or business partner who meets the following criteria:

- has or had authorized access to an organization’s network, system, or data
- has intentionally exceeded or intentionally used that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization’s information or information systems
Methods

• Research
• Empirical Evidence
• Control Hypothesis
• Control Implementation and Testing
• Control Pilot
• Revisions
• Release
Who does the CSG apply to?

- Information Technology / IT Security
- Physical Security
- Software Engineering
- Data Owners
- Legal
- Human Resources
- …..everyone across the organization
New Features

- Mappings to other best practices / standards
  - NIST 800-53
  - ISO 27002
  - CERT RMM
- Quick wins & High Impact Solutions
- Quick reference guide
### Practices you are familiar with

<table>
<thead>
<tr>
<th>Consider threats from insiders and business partners in enterprise-wide risk assessments.</th>
<th>Consider insider threats in the software development life cycle.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clearly document and consistently enforce policies and controls.</td>
<td>Use extra caution with system administrators and technical or privileged users.</td>
</tr>
<tr>
<td>Institute periodic security awareness training for all employees.</td>
<td>Implement system change controls.</td>
</tr>
<tr>
<td>Monitor and respond to suspicious or disruptive behavior, beginning with the hiring process.</td>
<td>Log, monitor, and audit employee online actions.</td>
</tr>
<tr>
<td>Anticipate and manage negative workplace issues.</td>
<td>Use layered defense against remote attacks.</td>
</tr>
<tr>
<td>Track and secure the physical environment.</td>
<td>Deactivate computer access following termination.</td>
</tr>
<tr>
<td>Implement strict password and account management policies and practices.</td>
<td>Implement secure backup and recovery processes.</td>
</tr>
<tr>
<td>Enforce separation of duties and least privilege.</td>
<td>Develop an insider incident response plan.</td>
</tr>
</tbody>
</table>
New Best Practices

- Practice 9: Define explicit security agreements for any cloud services, especially access restrictions and monitoring capabilities.
- Practice 16: Develop a formalized insider threat program.
- Practice 17: Establish a baseline of normal network device behavior.
- Practice 18: Be especially vigilant of emerging social media trends.
- Practice 19: Close the doors to unauthorized data exfiltration.
Practice 9

Define explicit security agreements for any cloud services, especially access restrictions and monitoring capabilities.

- Conduct a Risk Assessment before entering into any agreement.
- Chose a cloud service provider that meets or exceeds the organization’s own levels of security.
- Understand how the cloud provider protect data and other assets.
Practice 16

Develop a formalized insider threat program.

- Work with Legal Counsel.
- Requires involvement from various departments across the organization.
- Share information.
Practice 17

Establish a baseline of normal network device behavior.

- Know what is normal and abnormal for a given system.
- Excessive traffic, Insufficient traffic
- Store logs for 60 days or longer
Practice 18

Be especially vigilant regarding social media.

- Train users to be aware of what they post
- Small disclosures of information can create bigger problems
- Develop a social media policy
Practice 19

Close the doors to unauthorized data exfiltration.

• Understand how data can leave the organization.
• Control removable media.
• Watch for “old school” methods: printers, copiers, etc.
Technical Controls: Preventing Data Exfiltration
The Problem

• Organizations need to use web based services on a daily basis for business needs. However, services that offer the ability to upload attachments present an opportunity for sensitive data to leave the organization.

• Communications that are secured with SSL encryption are difficult to inspect and therefore it is difficult to detect and prevent sensitive data from leaving the organization.
Data Loss Through the Web

Difficult problem

Perfect exfiltration channel

- Encrypted
- Appears “normal”
- Send many files at once
- Possibly essential to operations
What can be done to prevent this?

Options:

1. Implement policies regarding how sensitive information is disseminated
2. Full packet capture of all Internet traffic for further analysis
3. White listing
4. Block all webmail services
5. Allow all webmail services and cross your fingers
6. Or…
CERT’s Solution

- Allow proxied Internet access to any website
- Inspect encrypted communication sessions for sensitive documents
- Block sensitive attachments from being uploaded to the Internet
Blocking Documents

Documents can be stopped based on three methods:

1. Block all attachments
2. Keywords
3. Tags
The Proxy Server
Man-in-the-Middle (MITM) Proxy

MERIT CORP
The Proxy Server Main Components

- Ubuntu Linux Version 10.04 LTS
- Squid Version 3.1.19
- C-ICAP
- Clam Antivirus (ClamAV)
Client Configuration

- The Organization's Certificate needs installed in the Trusted Root Certificate Store on each client
- Internet Explorer needs to be configured to use the proxy on port 3128 for HTTP/S traffic

Both of these settings can be configured using Group Policy
Here's the documents you wanted. Now hire me!

Sincerely,

Joe User
<table>
<thead>
<tr>
<th>URL</th>
<th>Status</th>
<th>Domain</th>
<th>Size</th>
<th>Remote IP</th>
<th>Timeline</th>
</tr>
</thead>
<tbody>
<tr>
<td>POST ServiceLoginAuth</td>
<td>302 Moved Temporarily</td>
<td>accounts.google.com</td>
<td>649 B</td>
<td>10.64.22.15:8080</td>
<td>145ms</td>
</tr>
<tr>
<td>GET SetSID?ssdc=1&amp;sid...DrOl71t5NtKDNvBz</td>
<td>302 Moved Temporarily</td>
<td>accounts.youtube.com</td>
<td>212 B</td>
<td>10.64.22.15:8080</td>
<td>112ms</td>
</tr>
<tr>
<td>GET ?auth=DQAAAIAAAAAF...DrOl71t5NtKDNvBz</td>
<td>302 Moved Temporarily</td>
<td>mal.google.com</td>
<td>0</td>
<td>10.64.22.15:8080</td>
<td>152ms</td>
</tr>
<tr>
<td>GET ?shva=1</td>
<td>200 OK</td>
<td>mal.google.com</td>
<td>21.8 KB</td>
<td>10.64.22.15:8080</td>
<td>432ms</td>
</tr>
<tr>
<td>GET ?ui=2&amp;view=js&amp;name...k1HFMewXo6MJX</td>
<td>200 OK</td>
<td>mal.google.com</td>
<td>343 KB</td>
<td></td>
<td>37ms</td>
</tr>
<tr>
<td>GET ?ui=2&amp;view=bsp&amp;ver=ohhl4rw8mnb4</td>
<td>200 OK</td>
<td>mal.google.com</td>
<td>62 B</td>
<td>10.64.22.15:8080</td>
<td>35ms</td>
</tr>
<tr>
<td>GET ?ui=2&amp;view=bsp&amp;ver=ohhl4rw8mnb4</td>
<td>200 OK</td>
<td>mal.google.com</td>
<td>62 B</td>
<td>10.64.22.15:8080</td>
<td>238ms</td>
</tr>
<tr>
<td>GET ?ui=2&amp;view=bsp&amp;ver=ohhl4rw8mnb4</td>
<td>200 OK</td>
<td>mal.google.com</td>
<td>62 B</td>
<td>10.64.22.15:8080</td>
<td>239ms</td>
</tr>
<tr>
<td>GET ?ui=2&amp;view=ss&amp;mset...MewXo6MJQhTjE</td>
<td>200 OK</td>
<td>mal.google.com</td>
<td>55.2 KB</td>
<td>10.64.22.15:8080</td>
<td>134ms</td>
</tr>
<tr>
<td>GET ?ui=2&amp;view=jsm&amp;nam...k1HFMewXo6MJ</td>
<td>200 OK</td>
<td>mal.google.com</td>
<td>5.4 KB</td>
<td>10.64.22.15:8080</td>
<td>766ms</td>
</tr>
<tr>
<td>GET ?ui=2&amp;view=ss&amp;mset...MewXo6MJQhTjE</td>
<td>200 OK</td>
<td>mal.google.com</td>
<td>55.2 KB</td>
<td>10.64.22.15:8080</td>
<td>688ms</td>
</tr>
<tr>
<td>GET sem_8e56e5be46cb600be9ba1b375de5d</td>
<td>200 OK</td>
<td>cs1.gstatic.com</td>
<td>12.1 KB</td>
<td>10.64.22.15:8080</td>
<td>598ms</td>
</tr>
<tr>
<td>POST ?ui=2&amp;ik=19011efaa...&amp;rt=j&amp;search=i</td>
<td>200 OK</td>
<td>mal.google.com</td>
<td>1.7 KB</td>
<td>10.64.22.15:8080</td>
<td>852ms</td>
</tr>
<tr>
<td>GET cleardotgif?zx=1qnihw87jnu</td>
<td>200 OK</td>
<td>mal-attachment.googleusercontent.com</td>
<td>43 B</td>
<td>10.64.22.15:8080</td>
<td>44ms</td>
</tr>
<tr>
<td>GET setgmail?zx=pc36swyhBrif</td>
<td>204 No Content</td>
<td>google.com</td>
<td>0</td>
<td>10.64.22.15:8080</td>
<td>70ms</td>
</tr>
<tr>
<td>GET ?s=gmail&amp;a=viewinfo...s&amp;zx=1md35xr0y</td>
<td>200 OK</td>
<td>clients2.google.com</td>
<td>35 B</td>
<td>10.64.22.15:8080</td>
<td>475ms</td>
</tr>
<tr>
<td>GET ?ui=2&amp;ik=19011efaa...k=W1UH0X3tnf9k</td>
<td>200 OK</td>
<td>mal.google.com</td>
<td>890 B</td>
<td>10.64.22.15:8080</td>
<td>153ms</td>
</tr>
</tbody>
</table>
Man-in-the-Middle (MITM) Proxy

POST https://mail.google.com/mail/ota?zx=24i9nkail4gs
Squid’s HTTP Request Logging

image/gif

<table>
<thead>
<tr>
<th>Time</th>
<th>IP Address</th>
<th>Binary</th>
<th>Type</th>
<th>Destination URL</th>
<th>Referrer URL</th>
<th>Content Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>131070438.915</td>
<td>10.0.3.100</td>
<td>TCP_MISS/200</td>
<td>GET</td>
<td><a href="https://mail.google.com/mail/images/c.gif">https://mail.google.com/mail/images/c.gif</a></td>
<td>-</td>
<td>image/gif</td>
</tr>
<tr>
<td>131070432.096</td>
<td>10.0.3.100</td>
<td>TCP_MISS/200</td>
<td>POST</td>
<td><a href="https://mail.google.com/mail/ota">https://mail.google.com/mail/ota</a>? -</td>
<td>DIRECT/74.125.225.86</td>
<td>text/plain</td>
</tr>
<tr>
<td>131070432.894</td>
<td>10.0.3.100</td>
<td>TCP_MISS/200</td>
<td>GET</td>
<td><a href="https://mail.google.com/mail/channel/test">https://mail.google.com/mail/channel/test</a>? -</td>
<td>DIRECT/74.125.225.86</td>
<td>text/plain</td>
</tr>
<tr>
<td>131070433.281</td>
<td>10.0.3.100</td>
<td>TCP_MISS/200</td>
<td>POST</td>
<td><a href="https://mail.google.com/mail/channel/bind">https://mail.google.com/mail/channel/bind</a>? -</td>
<td>DIRECT/74.125.225.86</td>
<td>text/plain</td>
</tr>
<tr>
<td>131070433.948</td>
<td>10.0.3.100</td>
<td>TCP_MISS/200</td>
<td>GET</td>
<td><a href="https://mail.google.com/mail/channel/bind">https://mail.google.com/mail/channel/bind</a>? -</td>
<td>DIRECT/74.125.225.86</td>
<td>text/plain</td>
</tr>
<tr>
<td>131070433.950</td>
<td>10.0.3.100</td>
<td>TCP_MISS/200</td>
<td>POST</td>
<td><a href="https://mail.google.com/mail/channel/bind">https://mail.google.com/mail/channel/bind</a>? -</td>
<td>DIRECT/74.125.225.86</td>
<td>text/plain</td>
</tr>
<tr>
<td>131070433.958</td>
<td>10.0.3.100</td>
<td>TCP_MISS/200</td>
<td>GET</td>
<td><a href="https://mail.google.com/mail/channel/bind">https://mail.google.com/mail/channel/bind</a>? -</td>
<td>DIRECT/74.125.225.86</td>
<td>text/plain</td>
</tr>
<tr>
<td>131070434.181</td>
<td>10.0.3.100</td>
<td>TCP_MISS/200</td>
<td>POST</td>
<td><a href="https://mail.google.com/mail/channel/bind">https://mail.google.com/mail/channel/bind</a>? -</td>
<td>DIRECT/74.125.225.86</td>
<td>text/plain</td>
</tr>
<tr>
<td>131070434.224</td>
<td>10.0.3.100</td>
<td>TCP_MISS/200</td>
<td>POST</td>
<td><a href="https://mail.google.com/mail/channel/bind">https://mail.google.com/mail/channel/bind</a>? -</td>
<td>DIRECT/74.125.225.86</td>
<td>text/plain</td>
</tr>
<tr>
<td>131070436.859</td>
<td>10.0.3.100</td>
<td>TCP_MISS/200</td>
<td>POST</td>
<td><a href="https://mail.google.com/mail/channel/bind">https://mail.google.com/mail/channel/bind</a>? -</td>
<td>DIRECT/74.125.225.86</td>
<td>text/plain</td>
</tr>
<tr>
<td>131070436.694</td>
<td>10.0.3.100</td>
<td>TCP_MISS/200</td>
<td>POST</td>
<td><a href="https://mail.google.com/mail/channel/bind">https://mail.google.com/mail/channel/bind</a>? -</td>
<td>DIRECT/74.125.225.86</td>
<td>text/plain</td>
</tr>
<tr>
<td>131070438.611</td>
<td>10.0.3.100</td>
<td>TCP_MISS/200</td>
<td>POST</td>
<td><a href="https://mail.google.com/mail/channel/bind">https://mail.google.com/mail/channel/bind</a>? -</td>
<td>DIRECT/74.125.225.86</td>
<td>text/plain</td>
</tr>
<tr>
<td>131070440.587</td>
<td>10.0.3.100</td>
<td>TCP_MISS/200</td>
<td>POST</td>
<td><a href="https://mail.google.com/mail/channel/bind">https://mail.google.com/mail/channel/bind</a>? -</td>
<td>DIRECT/74.125.225.86</td>
<td>text/plain</td>
</tr>
<tr>
<td>131070450.621</td>
<td>10.0.3.100</td>
<td>TCP_MISS/200</td>
<td>POST</td>
<td><a href="https://mail.google.com/mail/channel/bind">https://mail.google.com/mail/channel/bind</a>? -</td>
<td>DIRECT/74.125.225.86</td>
<td>text/plain</td>
</tr>
<tr>
<td>131070450.695</td>
<td>10.0.3.100</td>
<td>TCP_MISS/200</td>
<td>POST</td>
<td><a href="https://mail.google.com/mail/channel/bind">https://mail.google.com/mail/channel/bind</a>? -</td>
<td>DIRECT/74.125.225.86</td>
<td>text/plain</td>
</tr>
<tr>
<td>131070477.220</td>
<td>10.0.3.100</td>
<td>TCP_MISS/200</td>
<td>POST</td>
<td><a href="https://mail.google.com/mail/channel/bind">https://mail.google.com/mail/channel/bind</a>? -</td>
<td>DIRECT/74.125.225.86</td>
<td>text/plain</td>
</tr>
<tr>
<td>131070485.568</td>
<td>10.0.3.100</td>
<td>TCP_MISS/200</td>
<td>POST</td>
<td><a href="https://mail.google.com/mail/channel/bind">https://mail.google.com/mail/channel/bind</a>? -</td>
<td>DIRECT/74.125.225.86</td>
<td>text/plain</td>
</tr>
<tr>
<td>131070502.412</td>
<td>10.0.3.100</td>
<td>TCP_MISS/200</td>
<td>POST</td>
<td><a href="https://mail.google.com/mail/channel/bind">https://mail.google.com/mail/channel/bind</a>? -</td>
<td>DIRECT/74.125.225.86</td>
<td>text/plain</td>
</tr>
<tr>
<td>131070538.693</td>
<td>10.0.3.100</td>
<td>TCP_MISS/200</td>
<td>POST</td>
<td><a href="https://mail.google.com/mail/channel/bind">https://mail.google.com/mail/channel/bind</a>? -</td>
<td>DIRECT/74.125.225.86</td>
<td>text/plain</td>
</tr>
<tr>
<td>131070543.425</td>
<td>10.0.3.100</td>
<td>TCP_MISS/200</td>
<td>POST</td>
<td><a href="https://mail.google.com/mail/channel/bind">https://mail.google.com/mail/channel/bind</a>? -</td>
<td>DIRECT/74.125.225.86</td>
<td>text/plain</td>
</tr>
<tr>
<td>131070557.655</td>
<td>10.0.3.100</td>
<td>TCP_MISS/200</td>
<td>GET</td>
<td><a href="https://mail.google.com/mail/channel/bind">https://mail.google.com/mail/channel/bind</a>? -</td>
<td>DIRECT/74.125.225.86</td>
<td>text/plain</td>
</tr>
<tr>
<td>131070583.442</td>
<td>10.0.3.100</td>
<td>TCP_MISS/200</td>
<td>GET</td>
<td><a href="https://mail.google.com/mail/channel/bind">https://mail.google.com/mail/channel/bind</a>? -</td>
<td>DIRECT/74.125.225.86</td>
<td>text/plain</td>
</tr>
<tr>
<td>131070603.661</td>
<td>10.0.3.100</td>
<td>TCP_MISS/200</td>
<td>GET</td>
<td><a href="https://mail.google.com/mail/channel/bind">https://mail.google.com/mail/channel/bind</a>? -</td>
<td>DIRECT/74.125.225.86</td>
<td>text/plain</td>
</tr>
<tr>
<td>131070608.375</td>
<td>10.0.3.100</td>
<td>TCP_MISS/200</td>
<td>GET</td>
<td><a href="https://mail.google.com/mail/channel/bind">https://mail.google.com/mail/channel/bind</a>? -</td>
<td>DIRECT/74.125.225.86</td>
<td>text/plain</td>
</tr>
<tr>
<td>131070633.368</td>
<td>10.0.3.100</td>
<td>TCP_MISS/200</td>
<td>GET</td>
<td><a href="https://mail.google.com/mail/channel/bind">https://mail.google.com/mail/channel/bind</a>? -</td>
<td>DIRECT/74.125.225.86</td>
<td>text/plain</td>
</tr>
<tr>
<td>131070659.669</td>
<td>10.0.3.100</td>
<td>TCP_MISS/200</td>
<td>GET</td>
<td><a href="https://mail.google.com/mail/channel/bind">https://mail.google.com/mail/channel/bind</a>? -</td>
<td>DIRECT/74.125.225.86</td>
<td>text/plain</td>
</tr>
<tr>
<td>131070655.453</td>
<td>10.0.3.100</td>
<td>TCP_MISS/200</td>
<td>GET</td>
<td><a href="https://mail.google.com/mail/channel/bind">https://mail.google.com/mail/channel/bind</a>? -</td>
<td>DIRECT/74.125.225.86</td>
<td>text/plain</td>
</tr>
<tr>
<td>131070682.258</td>
<td>10.0.3.100</td>
<td>TCP_MISS/200</td>
<td>GET</td>
<td><a href="https://mail.google.com/mail/channel/bind">https://mail.google.com/mail/channel/bind</a>? -</td>
<td>DIRECT/74.125.225.86</td>
<td>text/plain</td>
</tr>
<tr>
<td>131070888.769</td>
<td>10.0.3.100</td>
<td>TCP_MISS/200</td>
<td>GET</td>
<td><a href="https://mail.google.com/mail/channel/bind">https://mail.google.com/mail/channel/bind</a>? -</td>
<td>DIRECT/74.125.225.86</td>
<td>text/plain</td>
</tr>
</tbody>
</table>

Managing The Insider Threat:
What Every Organization Should Know
Twitter #CERTinsiderthreat
© 2013 Carnegie Mellon University
Man-in-the-Middle (MITM) Proxy

POST https://mail.google.com/mail/ota?zx=24i9nkai14gs
Man-in-the-Middle (MITM) Proxy

RegEx: mail.google.com/mail/ota*

POST https://mail.google.com/mail/ota?zx=24i9nkail4gs
Success!

Here's the documents you wanted. Now hire me!

Sincerely,
Joe User
Shortcomings

• Not very granular
• Doesn’t account for the scenario where text is copied and pasted into an email
Detection using ClamAV
Detection using ClamAV
Detection using ClamAV
Plagiarism Detection & DLP
Solution:

• What if we could inspect all text flowing through the network?

• Rather than look for ‘tags’ or keywords, look for similarity

• How do we test document similarity?

• **Cosine similarity algorithms**
  
  • Laymen’s terms: Plagiarism Detection
  
  • Even though we’re not checking for plagiarism in academic papers, the process is virtually identical
The Plagiarism Detection Method

- Rather than asking
  - “Does any text in this document sufficiently match anything within its cited references?”
- We’re asking
  - “Does any text in this outgoing network traffic sufficiently match anything within our repository of intellectual property?”
  - If not – send it through
  - If so – create an alert and/or actively block the traffic from leaving the organization’s perimeter
Plagiarism Detection

Text

Software

Sources

Text Index

Not similar

Similar
Plagiarism Detection in DLP

Outgoing Web Request → Proxy → Data Repository

Text Index

Internet

Not similar → Alert!

Similar
Open Source Tools

- Squid proxy server
- Apache Lucene
- Apache Tika
- GreasySpoon ICAP server
Apache Lucene

- Powerful open-source text indexer and search engine
- Used in IBM’s famous Watson AI system
- Scalable, fast, and mature
- Perfect for our needs
Order of Events

1. User sends a webmail message
2. Proxy receives the webmail message
3. Proxy forwards the webmail message to GreasySpoon ICAP server
4. GreasySpoon ICAP server forwards the webmail message to Apache Lucene indexer
5. Apache Lucene indexer ‘scores’ the outgoing text against all indexed documents containing intellectual property
6. If any computed score exceeds the organization’s defined threshold (ex: 50%), either create an alert and/or block the outgoing webmail message
Shortcomings

- Tuning the threshold is difficult
- Does not detect encodings other than ASCII or Unicode
- Processing intensive
- Large index (lots of duplicated data)
- Index contains sensitive information
Future Work

- Create an efficient open-source DLP framework for correlating any given input data with any set of data, regardless of their type (i.e. text, image, raw)
- Tagging network traffic with usernames and other attribution information
- Improving our “Tagger” tool to automatically store file usage information within documents when they are created/accessed/modified
Upcoming Control Topics

- Two Man Control For Operating Systems
  - Why is it so hard?
- Better Forensics for Insider Threat Indicators
  - How to use what we know more effectively
Point of Contact

Randy Trzeciak
Technical Manager, CERT Insider Threat

CERT Division
Software Engineering Institute
Carnegie Mellon University
4500 Fifth Avenue
Pittsburgh, PA 15213-3890
+1 412 268-7040 – Phone
rft@cert.org – Email

http://www.cert.org/insider_threat/