Global Information Assurance Certification Paper

The Internal Threat:
Espionage and Sensitive Information Leaks

Introduction:

Information is the currency of the modern economy. All enterprises process information in the course of performing business. Among this is information and data that must be protected from competitors and the public for financial, legal, or competitive reasons. Espionage, originally a military endeavor, has found a new calling in the private sector. Furthermore, accidental disclosure of sensitive information can also have a detrimental impact on organizations. Enterprises must establish procedures to guard against the accidental or deliberate disclosure of potentially damaging knowledge.
Much of this information resides on computers and networks. It is up to the managers and administrators of these systems to implement the managerial and technical details of protecting their systems and the valuable information they contain. While the majority of the work in Incident Response and Handling has concentrated on external attempts to break into a system, history has shown that sensitive information leaks usually require trusted insiders. This paper shall demonstrate how to apply the steps of incident response to internal threats attempting to get information to the "outside". For any examples I shall use the Microsoft NT operating system.

Preparation

Of the six steps of Incident Handling (IH), preparation is the most important. Preparation is the sum of all actions taken before an incident and is crucial to the success of all the other steps. Preparation itself can be broken down into the following areas:

Policy

Before we can begin any other preparation, an enterprise wide policy for sensitive information must be established. This policy may be part of a larger policy defining user's rights and responsibilities. It must address the most basic issues, such as:

What is sensitive? Examples may include trade secrets, confidential agreements, private records, or classified information. Sensitive information can also include information that isn't owned by the organization, such as information from partnership, associations, and any other information trusted to the organization by a third party. Are there differing levels of sensitivity, each level with its own set of rules and policies? Should work be derived from sensitive information, shall it be considered sensitive itself?

Who may access this information? Under what conditions may they access it; how can this privilege be revoked? Does the information have an owner who is directly responsible for it? Should this information be disclosed who is held liable for any damage to the enterprise?

Where can this information reside? If the information is placed on a network, what are the logical and physical controls on its transmission? What are the rules for viewing, printing, or otherwise working with the information?

When is information considered sensitive and when does it lose this status?

How is sensitive information recognized? What are the corporate policies for marking and identifying it? How should it be transmitted or transported?

Example: The US Government has very strict regulations defining Secret, Top Secret, and other levels of information. Each level has its own set of rules, usually building upon the ruleset of the next lowest level. No one is allowed to work with or handle classified information without signing an agreement, receiving initial handling and transport training, and having passed an appropriate background check.

People

As defined in the policy, people may handle sensitive information, according to their role:

Users: Users are the organization's members entrusted to utilize sensitive information in their work. Before they are allow to handle it they should clearly understand the policies in place, the rules and procedures for working with it, and the conditions under which their privileges may be revoked. It is strongly encouraged they receive initial and periodic training as a condition of handling this type of information.

Owner: This is typically a user who has special administrative authority over information. It may include broad privileges over the life of the information, from its creation to its disclosure or destruction.

Support personnel: This category includes all who don't directly work with sensitive information, but are involved in its administration, transmission, storage, or destruction. Examples of support personnel include system administrators and network managers.

Examples: In the government, an intelligence analysis shop may own classified information regarding a geographical region, the Office of the President of the United States would be a user of this information in determining national objectives, and the Intelink or NIPRNET administrators would act as support personnel.

Hardware

Management and system administrators must determine what networks, servers, and clients are cleared to handle sensitive information, and how would they relate to other networks in the enterprise's control. The most extreme example would be the Department of Defense's classified network, SIPRNET, which is rigorously separated by an "air-gap" from any other network. No logical or physical connections are allowed to any other network. Such a solution is effective, yet it also consumes extremely large amounts of manpower, resources, space, and finances. For a medium or small company such a solution would be overkill. Instead, they may dedicate a subnet to sensitive

information. This subnet would logically reside behind a second firewall and a modified intrusion detection system monitoring what's *leaving*. Client access to this subnet may be allowed from a handful of workstations located in certain pre-approved areas. No home or internet access would be allowed to or from the subnet or clients.
As a special consideration one must take into account is removable media on clients and servers. "SneakerNet" can negate any carefully designed physical or logical protection scheme. 3.5" floppies, CD-ROM burners, flash memory, and even removable and external hard drives must be taken into account when tracking an incident. If possible, remove or restrict these devices on your protected networks
Finally, if you permit modems on your sensitive systems, or any other uncontrolled external access, you're asking for a world of trouble.

Software

Properly loaded and operating software can provide assistance in handling incidents. Intrusion Detection Systems (IDS), Network Management Systems (NMS), logging, sanitizers, and application specific utilities are particularly helpful in controlling leaks.

IDS can be broadly defined as a system that monitors access from one network into another. In their usual usage, they track access from an external, untrusted network. Given the broader definition, however, they are also useful for tracking data flowing from confidential networks or subnets. For instance, they can be set-up to track when someone attempts to establish an FTP connection from the sensitive network to an external site.

NMS are software suites that automate the network management process. They provide some very helpful tools to the Incident Handler. First, they provide a real-time map of the network, which may be useful in tracking the path of a leak. Second, they give an assessment of the health of the network, Which includes what systems are down or acting suspiciously (ie, high traffic load from a classified server). Third, these programs can provide near real-time alarms, with preset trigger points. This feature can be used in conjunction with an IDS to pinpoint systems and drastically reduce response time. Fourth, they provide independent data on clients and servers that may be compared against a system's logs. For instance, NMS might determine that a sensitive client was down for 10 minutes, yet that client's logs shows "normal" activity during that time.

On your confidential networks what should you log? The short answer is "everything". For example, in NT security events are defined through the User Manager. The ones helpful for tracking leaks and espionage include 'File and Object Access', which tracks events that deal with access to restricted objects such as printers, files, and directories; and 'Process Tracking', which tracks process actions including process creation and indirect access to objects. Auditing these events provides valuable clues to leaks.
For example, through 'File and Object Access' an administrator may notice a user opened the file TopSecret.doc and created a new file Temp.doc. Process Tracking then recorded the user opening Internet Explorer, and the IDS logged an attempted connection to hotmail.com.

A sanitizer program is valuable for shutting down leaks. These programs go beyond the simple delete command in the operating system. This command usually doesn't really delete the file, rather it just alters its pointer in the directory. The actual file is still physically located on the hard-drive. Most deleted files can be simply recovered using common utilities. In more extreme cases, deleted information can be recovered using physical scans of the hard-drive's surface. A sanitizer program operates by overwriting the affected sectors multiple times with predetermined or random data, fully removing directory pointers, and clearing temporary memory areas, such as swapfiles [1]. There are many excellent commercial, freeware, and shareware sanitizers available. Later in this paper I will illustrate an example using Eraser 4.1, a shareware program written by Sami Tolvanen [2]. For more severe cleanings, degaussing provides the ultimate in removing information.

Other tools include protocol and application specific programs. For example, in cases involving Microsoft Exchange, the Message Store Sanitizer [3] is a command line program that deletes or locates messages in mailboxes. Messages are identified by conversation index, which is a unique number assigned at the start of a conversation and carried through each reply and forward message. As each reply or forward occurs, the conversation index grows, but the first 22 bytes of the index remain the same. All messages starting with the same sequence belong to the same conversation. Messages can be located by sender, recipient, subject line, or conversation index.

Communications and Transportation

In handling a leak or suspected espionage, the Incident Handling Team must share information to accomplish their tasks. In doing so, however, they should take care to prevent the exposure of more sensitive information. Especially in an espionage case, the team must assume that their actions are being watched by the "bad guy", and in such a situation even indirect observations may be useful to their goals of obtaining even more information. As a minimum all transmissions must be encrypted, carried according to predefined rules, and handled in an appropriately cleared facility.

Examples: In the DoD we have access to STU III's and STE's, which are telephones that encrypt voice or fax transmissions. As policy, no conversations or faxes are sent in the clear, and any information regard a leak is handled at the same classification level as the original. Any related email must be sent via DMS, the DoD's secure email system. Under no circumstances is the Incident Handling Team to discuss the clean-up effort over cell-phones.
Companies that don't have access to such specialized systems may incorporate commercially available encryption packages, such as PGP, to secure their communications

Space

When handling sensitive or classified information, an appropriately cleared work-area is necessary to perform the tasks. Ideally it should be located near the scene of the incident with enough space to accommodate all team members, and have sufficient telephone and network access. It should be cleared to contain the information being worked on, and controlled access devices such as peepholes and cipher-locks, use in conjunction with procedures to track entry and exit from the work area
In many workplaces having a room dedicated solely for Incident Handling would be an excessive burden. In our case we have a conference room that we convert to a command center. We have an agreement with the room's management that we're given primary access to the room whenever there is an incident, even if there are meetings scheduled in the room (for this reason they never schedule important meetings there)

Documentation

In tracking a leak or espionage, documentation surrounding the incident must be controlled. Anything not to be kept as evidence at the end of the case should be destroyed. Paper shredders are you friends. For evidence, raw files such as IDS logs, server/client logs, and NMS maps should be stored, as well as derived works, such as timelines, theories, working notes and official reports.

Identification

When it comes to identification, there are ultimately two means:

Reactive

Reactive identification is when somebody else tells you your information has been leaked. This could include the media, upper management, competitors, or contact from thieves (i.e.: blackmail). Reactive Identification should be avoided if at all possible.

Proactive

Proactive identification occurs when you identify an information leak before it gets beyond your control. It can be triggered by automated means, such as by an IDS or NMS alarm or a log checker. In many occasions, users themselves have proven to be the best detection system for leaks. All users should be taught what to do should they encounter misplaced sensitive information. In the course of their daily work, users may inadvertently disclose controlled information. Policies should encourage self-reporting of leaks; the point is to safeguard sensitive information, not punishing users for their mistakes. When determining if there has been a leak, contact the information owner as soon as possible. Their collaboration will prove crucial in this and all further steps. Based on the evidence on hand, and consulting with the owner, an initial determination should be made if this is a deliberate or accidental leak. If espionage is suspected, and your policy allows it, this is the point to notify law enforcement. Furthermore, assume the spy may have otherwise compromised systems (installed backdoors, trojanized programs, etc), and proceed using normal IH techniques for systems break-ins. If the

information has already left your control, upper management should be notified to begin damage control, if possible. If you can't determine whether a leak was intentional or a mistake, treat it as if it were deliberate. If further evidence shows it was accidental, then you may downgrade the initial assessment.

Containment

The first step in containment is to determine the path of the leak. Begin with a network map and the logs of the suspected server or client. Check to see what files were opened, created, renamed, printed, or copied to another host. Take special note of printouts or writes to removable media. Determine what protocol was used to move information off the host (email, FTP, HTTP, etc) and use any special identification fields from the protocol.

Suppose for example, a file was email through your exchange server. On all of our exchange servers we have the Message Store Sanitizer (MSS) pre-installed.
Opening a command line interface, issue the command

C:\Exchange>MSS /INIFILE=MSS.INI

MSS operates with an initialization file. An example of the mss.ini file: {with parameter descriptions in parenthesis}

[General]
{The general section contains required run and general operation parameters of MSS.}

Server=mail1
{The server name is used to direct the export of mailboxes from the Exchange server to a file. The server name is also used as a filter on mailboxes when the "scope=server" option is selected.}

/o=Users/ou=Site/cn=Recipeints;/o=Users/ou=Site/cn=Others
{The Exchange container parameters for mailboxes to use. Specifies containers using Exchange X500 format.}

mss_profile
{This is the profile is used by MSS to log on to Exchange, just as a typical Outlook user does. However, the mailbox and account must be a privileged user capable of logging on to all mailboxes being searched by MSS. MSS will log on to each mailbox it searches.}

Scope=Server
{Scope=Server: only mailboxes homed on the server specified with the server parameter will be processed. The typical scenario is that you search a server, specifying a container on that server, and only mailboxes on that server are processed.
Scope=All: allows all mailboxes in the container to be processed. However, the performance of searches performed on any mailbox not on this server is greatly affected.}

Delete Flag = 0
{Delete Flag = 0: MSS will only perform a search operation and will not delete messages it finds (Unless overridden by the command line /DELETIONS flag).
Delete Flag = 1: MSS will first alert the user to be sure that a delete operation will occur. It will then delete messages that match the search criteria. This option may be later used in the eradication phase}

Export=False
{This option is useful for passing in a file of mailboxes to MSS. The default behavior of MSS to export to file mailboxes.txt and then read mailboxes.txt to add mailboxes to be processed. By setting Export=False or Export=0, the Export from Exchange step is skipped and the mailboxes.txt file is read immediately. This can also be used to save execution time to run MSS repeatedly on the same set of mailboxes}

[Criteria]
{The Criteria section contains the property values to search on.}

MatchType=1
{The MatchType parameter allows control over different kinds of searches.
MatchType=2: all values that start with the given criteria with match.
MatchType=0: all messages that match exactly the given the search string will be found.
MatchType=1: any message that contains the value somewhere in the field will match.
For any value other than 0, 1, or 2; any message is assumed to be a match.}

PR_SUBJECT="Secret information"
{This is most important parameter, used as the criteria to search against. MSS can process standard exchange property names like PR_SUBJECT, PR_BODY, and PR_CONVERSATION_INDEX. It can be a string or binary. Criteria can be concantenated with 'OR'.}

[Report]
{This section controls generation and location of report file}.

Report File Name=mss.txt
{Specifies the name of the report file. The file generated is a tab-delimited file. The first line provides column headings. Succeeding lines provide values for the column headings. Each line is a message found in a mailbox. If saved with a .cvs extension, can be opened in Excel.}

Report Flag=1
{Report Flag= 0: suppresses report file. Otherwise a report is generated.

Many of the parameters specified in the initialization file can also be overridden on the command line. For example, if the initialization file contains "Delete Flag=FALSE", MSS can be made to delete by specifying /DELETIONS on the command line.

MSS operates in four phases. The first phase examines the configuration data and logs on to Exchange as a client program. The second phase exports the configured containers to a file. The third phase processes the export file, creating a list of mailboxes. Finally, the mailboxes are searched using the configured criteria, and generates a report. For each mailbox processed, a user message is generated giving the number of folders processed, the number of messages found, and the time it took to process the mailbox. All MSS entries are logged in the Application Event Log.

For each system in the leak's path, determine if the information should be allowed to continue to reside on the system or should it be eradicated. Determine if the system should be taken offline or whether affected user's accounts should be suspended until eradication is completed. This is especially important if the host or users have access to public networks beyond your control (i.e., the Internet). Repeat these steps with every system identified until you have a complete map.
Before eradication is to begin, should you desire to keep any evidence, this would be the time to perform a full backup, using disk imaging or cloning. In the next phase the leaked information will be deliberately, irreversibly lost

Eradication

In the containment stage decisions were made to identify which hosts the information should be eradicated from. This eradication can take several forms:

Sanitizing: This is best used for specific, known files that do not consume massive quantities of hard-drive space. You simply load the sanitizing software, configure it, feed it the name of the file, and let it do it's job. When configuring the software, we typically use the maximum settings. This includes 35 write passes, scanning file slack space, checking swap space, and performing a full sweep at shut-down

For example, I shall illustrate an incident using Eraser 4.1. Suppose we've isolated the file TopSecret.doc on an unauthorized client. While in administrative mode we load the program (it comes with its own setup program). After installation, We set virtual memory to zero by opening Control Panel, System, Performance, Virtual Memory. After the required reboot, we open a command line interface and enter the commands

```
C:\> del \temp\*.*
C:\> eraser1 -file TopSecret.doc -results
C:\> eraser1 -recycled -results
C:\> eraser1 -disk c:\ -results
```

The first command ensures that no copy of the file is remaining in the Temp file.
The second command eradicates the indicated file and
The third and fourth commands are an insurance policy, combined with the zeroing of the swapfile, that ensures no copy remains in the recycle bin or where the swap file used to exist.

Once these steps are completed, be sure to reset the Virtual Memory!

Other useful parameters include:

-folder: The data to erase is files on a folder
-subfolders: Erase all data in subfolders as well (only with -file or with -folder)
-keepfolder: Do not delete the folder (only with -folder)
-disk: The data to erase in unused space on a drive or all local hard drives (all)
-recycled: Erase all data on the Recycle Bin
-silent: Do not show any windows
-results: Show results after the operation
-resultsonerror: Show results only in case of error
-queue: Wait until previous instances have finished
-options: Ignore all other valid parameters and show the options window. By default, Eraser does a full Gutmann scan (minimum 35 passes). Overwrite and other options may be changed in this window.

Self Sanitizing: This option is best used on heavily used servers that can not be brought down due to their mission critical status (ie, email servers). Furthermore, these servers should be located in an area not readily accessible to others. Once the information is deleted, the heavy usage may naturally degrade the deleted sensitive information. A note should be made to fully sanitize the server when it is taken down for service.

Backup and Degauss. This is the most extreme, yet effective solution. The system is taken offline. A backup is then make of the hard-drive(s). Unlike all other incident response cases, the point here is to permanently lose information, not recover lost data. Therefore disk imaging or cloning *won't* be used, instead a simple, full, file back up that doesn't store empty sectors or sector slack space shall be used.

I shall illustrate making a backup using the NTBackup.exe utility, which is included in the standard NT installation.
1. If it hasn't already been done, install a tape drive to the host using the Add/Remove Hardware utility in the Control Panel

2. Open a command line interface, install a blank tape, and format it:

C:\>ntbackup /nopoll

3. Begin the actual backup:

c:\>ntbackup backup c:;d: /v /b /d "emergency full backup {date}" /hc: off /t normal /l "{date}.log" /tape: 5

An explanation of the parameters:
Backup - specifies the operation, can be backup or eject.

c:;d: - Defines the paths of the directories to be backed up.
/b - Backs up the local registry.
/v - Verifies the operation.
/d "emergency full backup {date}" - Labels the backup contents.
/hc:off - Specifies that hardware compression is off.
/t normal - Specifies the backup type. Can be one of the following: normal, copy, incremental, differential, daily
/l "{date}.log" - Specifies the filename for the backup log.
/tape: 5 - Specifies the tape drive to which the files should be backed up. 5 corresponds to the number the drive was assigned when the tape drive was installed.

Once the backup is made and verified, the hard-drive is removed and degaussed. Degaussing is a physical level operation, performed in a specialized device. The hard drive is exposed to a series of alternating magnetic fields which gradually decreasing in strength. This reduces the magnetic flux in the magnetized medium to near zero. To properly degauss a hard-drive, treat it as if you were cooking a microwave dinner:
Place the hard-drive in the degausser and perform the first pass.
2nd Pass: Turn it clockwise and perform the next pass.
3rd Pass: Turn it over and pass again
4th Pass: Turn it counter-clockwise and complete the final pass.

Once you've completed degaussing the drive, reinstall it in to the system and reformat it. Copy the backed-up data onto the drive and continue with other systems to eradicate.

Recovery

For leaks and espionage recovery is typically a short phase where the systems disconnected during the Identification and Eradication phases are reconnected to the network. Follow normal IH procedures:
Validate the system to ensure the restoration was successful.
Consult with the system owner when to reconnect operations.
Monitor the system to ensure it's operations weren't degraded by the eradication.

Follow-up

Usually the information owner will have to prepare a separate report, detailing the impact of the disclosure. Offer to prepare a report with the technical details of the process. Include the incident map, an incident timeline, your analysis of what occurred, and supporting raw data (logs) as appendices. After a leak has been closed, schedule a follow-up meeting with the involved parties and the information owner. Invite critiques of how the process was handled, including:
Were we prepared to handle this leak? What preparations were overlooked?
Was the leak reactively or proactively detected?
What operational difficulties were encountered?
Was the leak properly contained?
Were the eradication steps taken appropriate for the information?

Were there any problems with the recovery?
What was the value of the data exposed?

Analyze the cost of the incident in terms of customer downtime, management and administrative hours consumed, impact to the network and enterprise.

References

[1] More information on sanitizing and overwriting can be found in Peter Gutmann's paper "Secure Deletion of Data from Magnetic and Solid-State Memory", available at http://www.cs.auckland.ac.nz/~pgut001/secure_del.html

[2] Eraser 4.1 is available at the Eraser Home Page:
http://www.tolvanen.com/eraser/

[3] The MSS utility is available from the Microsoft FTP site:
ftp://ftp.microsoft.com/transfer/outgoing/bussys/premier/Melissa/MSS/