Preparing to Detect Signs of Intrusion

John Kochmar
Julia Allen
Christopher Alberts
Cory Cohen
Gary Ford
Barbara Fraser
Suresh Konda
Klaus-Peter Kossakowski
Derek Simmel

June 1998

SECURITY IMPROVEMENT MODULE
CMU/SEI-SIM-005

Carnegie Mellon
Software Engineering Institute
Pittsburgh, PA 15213-3890

Preparing To Detect Signs of Intrusion

CMU/SEI-SIM-005

John Kochmar
Julia Allen
Christopher Alberts
Cory Cohen
Gary Ford
Barbara Fraser
Suresh Konda
Klaus-Peter Kossakowski
Derek Simmel

June 1998

Program Affiliation

Unlimited distribution subject to the copyright.

This report was prepared for the

SEI Joint Program Office
HQ ESC/AXS
5 Eglin Street
Hanscom AFB, MA 01731-2116

The ideas and findings in this report should not be construed as an official DoD position. It is published in the interest of scientific and technical information exchange.

FOR THE COMMANDER

(signature on file)

Mario Moya, Maj, USAF
SEI Joint Program Office

This work is sponsored by the U.S. Department of Defense.

Copyright © 1998 by Carnegie Mellon University.

Requests for permission to reproduce this document or to prepare derivative works of this document should be addressed to the SEI Licensing Agent.

NO WARRANTY

THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN “AS-IS” BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

This work was created in the performance of Federal Government Contract Number F19628-95-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center. The Government of the United States has a royalty-free government-purpose license to use, duplicate, or disclose the work, in whole or in part and in any manner, and to have or permit others to do so, for government purposes pursuant to the copyright license under the clause at 52.227-7013.

Use of any trademarks in this report is not intended in any way to infringe on the rights of the trademark holder.

This document is available through Asset Source for Software Engineering Technology (ASSET): 1350 Earl L. Core Road; PO Box 3305; Morgantown, West Virginia 26505 / Phone: (304) 284-9000 or toll-free in the U.S. 1-800-547-8306 / FAX: (304) 284-9001 World Wide Web: http://www.asset.com / e-mail: sei@asset.com

Copies of this document are available through the National Technical Information Service (NTIS). For information on ordering, please contact NTIS directly: National Technical Information Service, U.S. Department of Commerce, Springfield, VA 22161. Phone: (703) 487-4600.

This document is also available through the Defense Technical Information Center (DTIC). DTIC provides access to and transfer of scientific and technical information for DoD personnel, DoD contractors and potential contractors, and other U.S. Government agency personnel and their contractors. To obtain a copy, please contact DTIC directly: Defense Technical Information Center / Attn: BRR / 8725 John J. Kingman Road / Suite 0944 / Ft. Belvoir, VA 22060-6218 / Phone: (703) 767-8274 or toll-free in the U.S.: 1-800 225-3842.

Table of Contents

Preface iii

Preparing to Detect Signs of Intrusion **1**

1. Establish a policy and set of procedures that prepare your organization to detect signs of intrusion. 5
2. Identify and enable system and network logging mechanisms. 11
3. Identify and install tools that aid in detecting signs of intrusion. 17
4. Generate information required to verify the integrity of your systems and data. 21

Preface

This document is one of a new series of publications of the Software Engineering Institute at Carnegie Mellon University—*security improvement modules*. They are intended to provide concrete, practical guidance that will help organizations improve the security of their networked computer systems.

Module structure

Each module addresses an important but relatively narrowly defined problem in network security. The first section of the module describes the problem and outlines a set of *security improvement practices* to help solve it. Each practice is a recommended way of performing common tasks related to the secure operation of networked computer systems.

The remaining sections of the module are detailed descriptions of the practices. Each includes a rationale for the recommended actions and a step-by-step description of how to perform them.

Intended audience

The practices are written for system and network administrators within an organization. These are the people whose day to day activities include installation, configuration, and maintenance of the computers and networks.

Revised versions

Network technologies continue to evolve rapidly, leading to both new solutions and new problems in security. We expect that modules and practices will need to be revised from time to time. To permit more timely publication of the most up-to-date versions, the modules and practices are also being published on the World Wide Web. At the end of each section of this document is the URL of its Web version.

Implementation details

How an organization adopts and implements the practices often depends on the specific networking and computing technologies it uses. For some practices, technology-specific implementation details have been written and are being published on the World Wide Web. The Web version of each practice contains links to the implementation details.

Preparing to Detect Signs of Intrusion

It is essential that those responsible for your organization's information systems and networks be adequately prepared to detect evidence of breaches in security when they occur. Without advance preparation, it will be difficult, if not impossible, to determine if an intruder has been present and the extent of the damage caused by the intrusion. Thorough preparation will permit you to detect an intrusion or an intrusion attempt during or soon after it occurs. Preparation involves consideration of your security policy and supporting procedures, your critical business information, your systems, your networks, your user community (internal and external), and the tools to be employed in detecting intrusions.

A general security goal is to prevent intrusions. Even if you have sophisticated prevention measures in place, your strategy for detecting intrusions must include preparation. This module is a companion to CMU/SEI-SIM-001 *Detecting Signs of Intrusion*.

The practices contained in this module identify advance preparations you must make to enable you to obtain evidence of an intrusion or an intrusion attempt. They are designed to help you prepare by configuring your data, systems, networks, workstations, tools, and user environments to capture the necessary information for detecting signs of intrusion.

Who should read these practices

These practices are intended primarily for system and network administrators, managers of information systems, and security personnel responsible for networked information resources.

These practices are applicable to your organization if its networked systems infrastructure includes:

- host systems providing services to multiple users (file servers, timesharing systems, database servers, Internet servers, and so forth)
- local-area or wide-area networks
- direct connections, gateways, or modem access to and from external networks, such as the Internet

What these practices do not cover

These practices do not cover:

- prevention of intrusions, detecting signs of intrusion, analyzing the information required to characterize an intrusion, or responding to an intrusion
- establishing initial configurations of applications, operating systems, networks, or workstations

Security issues

Intruders are always looking for ways to break into systems. For example, they may attempt to breach your network's perimeter defenses from external locations or physically infiltrate your organization to gain internal access to its information resources. Intruders seek and take advantage of both old, unpatched vulnerabilities and newly discovered vulnerabilities in operating systems, network services, and protocols. They actively develop and use sophisticated programs to rapidly penetrate systems. As a result, intrusions and the damage they cause can occur in a matter of seconds.

If you are not adequately prepared to detect the signs of an intrusion, it is difficult, if not impossible, to later determine if your systems have been compromised. If the information necessary to detect an intrusion is not being collected and reviewed, you are unable to determine which of your sensitive data, systems, and networks are being attacked and what breaches in confidentiality, integrity, or availability have occurred. Specifically, as a result of insufficient preparation:

1. You will be unable to detect signs of an intrusion in a timely manner due to the absence of necessary warning mechanisms.
2. You will be unable to identify intrusions due to the absence of expected state information with which to compare your current operational state. Differences between this expected configuration and your current state can provide an indication that an intrusion has occurred.
3. You will be unable to determine the full extent and damage of the intrusion and whether or not you have completely removed the intruder from your systems and networks. This will significantly increase your time to recover.
4. Your organization may be subject to legal action. Intruders often attempt to hide their tracks by making use of systems they have compromised to launch attacks against others. If one of your systems is used in this way, you may be held liable for inadequate due care with respect to security.
5. Your organization may experience lost business opportunities.

In all cases, adequate preparation can lead to your staff and systems being able to detect signs of an intrusion or an intrusion attempt in a timely manner. As a result, you are then able to mitigate your exposure to the intrusion and the possible damage caused to your data or systems.

Security improvement approach

These practices assume that:

- You have performed security planning that addresses your organization's business objectives.

- You have performed trade-off analyses to determine the cost of protecting versus the cost of reconstituting critical assets (data, systems, networks, workstations, tools) in the event of an intrusion. Protecting an asset includes consideration of the loss of confidentiality and customer confidence if the asset is disclosed (e.g., confidential, competitive information).
- You have documented a disaster recovery policy and procedures that include determining what assets are critical to protect and with what priority. The policy identifies who has responsibility for and authority to access each asset that needs to be recovered, under what conditions, and by what means.

To prepare to detect signs of intrusion, we recommend a two-step approach, incorporating practices in which:

1. You define the required level of preparedness necessary to meet your business objectives
2. You implement selected steps that prepare your staff and systems to detect signs of intrusion.

Summary of recommended practices

Area	Recommended Practice
Define level of preparedness	1. Establish a policy and set of procedures that prepare your organization to detect signs of intrusion.
Implement preparation steps	2. Identify and enable system and network logging mechanisms. 3. Identify and install tools that aid in detecting signs of intrusion. 4. Generate information required to verify the integrity of your systems and data.

Abbreviations used in these practices

ACL	access control list
IRC	Internet relay chat

References and sources

[Maximum 97] *Maximum Security: A Hacker's Guide to Protecting Your Internet Site and Network*. Indianapolis, IN: Sams.net Publishing, 1997.

[Firth 97] Firth, Robert, et al. *Detecting Signs of Intrusion*. (CMU/SEI-SIM-001). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 1997. Available online at http://www.cert.org/security-improvement/modules/m01.html

[Garfinkel 96] Garfinkel, S., Spafford, G. *Practical UNIX and Internet Security, Second Edition*. Sebastopol, CA: O'Reilly & Associates, Inc., 1996.

[Guttman 97] Guttman, B., Bagwill, R. *Internet Security Policy: A Technical Guide - Draft*. Gaithersburg, MD: NIST Special Publication 800-XX, 1997.

[IETF 97]	Internet Engineering Task Force Network Working Group. RFC 2196 Site Security Handbook. Edited by Barbara Fraser. Available online at http://ds.internic.net/rfc/rfc2196.txt (1997)
[Summers 97]	Summers, Rita C. *Secure Computing*. New York, NY: McGraw-Hill, 1997.

CERT Coordination Center Web and FTP sites:
http://www.cert.org, ftp://info.cert.org;
specifically ftp://info.cert.org/pub/tech_tips/intruder_detection_checklist

Computer Operations, Audit, and Security Web site:
http://www.cs.purdue.edu/coast

Where to find updates

The latest version of this module is available on the Web at URL

http://www.cert.org/security-improvement/modules/m05.html

1 *Establish a policy and set of procedures that prepare your organization to detect signs of intrusion.*

A security policy defines the rules that regulate how your organization manages and protects its information and computing resources to achieve security objectives. One of the policy's primary purposes in preparing to detect signs of intrusion is to define the range of threats that your organization chooses to guard against and how these threats are dealt with when they occur.

Preparation procedures include the actions necessary to observe systems and networks for signs of intrusion. Observation can take the form of monitoring, inspecting, and auditing. [Monitoring is the observation of data streams for specific events. Inspection is the examination of a data resource or process. Auditing is the systematic examination of data against documented expectations of form or behavior.] From these procedures, all concerned parties are able to determine what operational steps they need to take to comply with your policy and, thereby, uphold the security of your organization's information and networked systems.

Security policies and procedures that are documented, well known, and visibly enforced establish expected user behavior and serve to inform users of their obligations for protecting computing assets. Users include all those who access, administer, and manage your data, systems, and networks. Users play a vital role in detecting signs of intrusion.

This practice describes the topics your policy and procedures should address. They need to be tailored to reflect the specific business objectives and security requirements of your organization and its computing environment.

Why this is important

Having policy language and procedures in place that prepare you to detect signs of intrusion provides the ability to exercise your procedures in a timely, managed, controlled manner and eliminate potential errors or omissions in advance of an attack. You do not want to be caught trying to determine what actions to take, what data to gather and preserve, and how to protect your data, systems, and networks from further damage while under attack or after the fact.

With advanced planning, documentation, and education, trained staff members are able to more effectively and efficiently coordinate their activities when detecting an intrusion or intrusion attempt. Without the necessary knowledge and skills, users may inadvertently expose parts of the organization to security threats.

How to do it

➤ *Include language in your organization's networked systems security policy that prepares you to detect signs of intrusion.*

Document the activities that indicate possible signs of intrusion and for which you intend to take action. These activities include:

- attempts (either failed or successful) to gain unauthorized access to a system or its data
- unintended and unauthorized disclosure of information
- unwanted disruption or denial of service
- the unauthorized use of a system for the processing or storage of data
- changes to system hardware, firmware, or software characteristics without your knowledge or consent

Recognize that there are threats that are difficult to protect against if your systems are connected to the Internet. You need to determine what actions you will take if these occur. Activities of this type include:

- denial of service, including e-mail bombing (sending a large volume of electronic messages to a targeted recipient until the system fails) and flood attacks (e.g., filling a channel with garbage, thereby denying others the ability to communicate across that channel or to the receiving host)
- programmed threats such as new viruses not yet detected and eliminated by virus checking tools and malicious applets (ActiveX, Java)
- intruders probing your systems with the intent of using any vulnerabilities they discover for future intrusion attempts

Document the requirement to establish and maintain secure, reliable configuration information for all data, systems, and networks that represents your known, expected state. This includes the tagging and inventory of all physical computing resources. This information is periodically compared with your current state to determine if anything has been altered in an unexpected way.

Document the roles, responsibilities, and authority of system administrators, security personnel, and users regarding use and administration of all data, systems, and networks when detecting signs of intrusion.

Document the roles, responsibilities, authority, and conditions for the testing of intrusion detection tools and procedures as well as the examination of data, systems, and networks suspected of having been compromised. We strongly recommend that your policy require all such activity to be conducted in a test environment isolated from production systems and networks.

➤ *Document procedures and take actions that implement your intrusion preparation policy.*

Document the procedure(s) by which regular inspection and auditing of recorded data (e.g., logs) are performed to identify evidence of intrusions or intrusion attempts.

Document the procedure by which physical audits of installed hardware and software are performed.

Document the procedure(s) by which monitoring is performed, i.e., the observation of data streams for specific events. This procedure specifies:

- the operational activities necessary to alert appropriate personnel to act upon the suspected intrusion
- how monitoring tools are acquired and securely maintained
- the frequency with which monitoring is performed
- roles and responsibilities for all procedure steps

Install all tools necessary to implement your monitoring, inspection, and auditing procedures.

Document the procedure by which integrity checking is performed, i.e., where your current operational state is compared with a previously generated, secure, reliable, known state. Specify:

- what files are to be checked
- how integrity information is securely generated, maintained, and tested
- how integrity checking tools are acquired and securely maintained
- frequency with which integrity checking is performed
- roles and responsibilities for all procedure steps

Document the procedure by which correlation of intrusions is performed, i.e., determining when intrusion activity occurring in one part of your systems may be related to activity in another part. Doing some level of correlation analysis during the intrusion detection process will assist you in determining the full extent of any compromise and its characteristics.

For each procedure, document the roles, responsibilities, and authority of system administrators, security personnel, and users. Identify who performs each procedure activity, when, and under what conditions.

➤ *Conduct a legal review of your policy and procedures.*

This should be performed by your organization's legal counsel. It is intended to ensure that your policy and procedures:

- are legally defensible and enforceable
- comply with overall company policies and procedures
- reflect known industry best practices demonstrating the exercise of due care
- conform to federal, state, and local laws and regulations
- protect your organization from being held legally responsible in the event of compromise

➤ *Train users (includes all those who access your data, systems, and networks).*

During the training process, users should learn:

- what is expected of them
- how to identify suspicious behavior and who to notify
- what behaviors can reduce the exposure of data, systems, and networks to possible compromise (e.g., protecting passwords and sensitive data, knowing how to respond to social engineering attempts)

- what types of information are being gathered as part of routine security procedures and the degree to which this information gathering may affect them.

Create and conduct periodic training on your intrusion preparation and detection policy and procedures. This training should be mandatory for all new employees and should cover aspects that are relevant to the employee's knowledge and responsibilities.

Test the effectiveness of the training and each employee's readiness. Conduct practice drills (e.g., detecting break-ins and viruses) that test procedures and execute operational activities, making sure all staff members are aware of their roles and responsibilities. Conduct post-mortem meetings with trainees. Provide remedial training as required.

Regularly conduct mandatory security awareness refresher training. Highlight recent changes to policy or procedures and summarize recent incidents and intrusions. Make this subject a recurring topic at executive and management level staff meetings to maintain awareness.

Due to the rapid rate of technology change, ensure that system and network administration staff have time set aside to maintain their knowledge, skills, and currency in technical topics required to implement your policy and procedures.

➤ *Keep intrusion preparation policy, intrusion detection policy, and all related procedures and training current.*

Periodically review your policy, procedures, and training, taking into account public and vendor information sources. These sources regularly report current intruder trends, new attack scenarios, security vulnerabilities, methods for their detection, and guidance to address them.

If your organization suffers an intrusion, review your policy, procedures, and training to determine if revisions are necessary to ensure that future intrusion attempts of the same type can be more readily detected and controlled, if not prevented.

Other information

The system and information assets that you want to consider when documenting intrusion detection policy language and procedures include:

- data (system and user)
- systems (hardware, software)
- networks (hardware, software)
- applications
- tools
- user file systems and environments

See also Firth, Robert, et al. *Detecting Signs of Intrusion*. (CMU/SEI-SIM-001). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 1997. Available online at http://www.cert.org/security-improvement/modules/m01.html

Where to find updates

The latest version of this practice, plus implementation details for selected technologies, is available on the Web at URL

http://www.cert.org/security-improvement/practices/p040.html

2 Identify and enable system and network logging mechanisms.

Collecting data generated by system, network, application, and user activities is essential for analyzing the security of these assets and detecting signs of intrusion. Log files contain information about what activities have occurred over time. Different systems provide different types of logging information; some systems do not collect adequate information as their default condition. You should identify the types of logs and logging mechanisms available for each system asset (file access logs, process logs, network logs, application-specific logs, etc.), identify the data recorded within each log, and then enable the collection of the desired data.

Why this is important

Log files are often the only record of suspicious behavior. Failure to enable the necessary mechanisms to record this information and use it to initiate alert mechanisms will greatly weaken and possibly even eliminate your ability to determine whether or not an intrusion has been attempted and has indeed succeeded. This also applies to having the necessary procedures and tools in place to process and analyze your log files.

You may need your logs to:

- alert you that an intrusion is occurring
- help recover your systems
- conduct an investigation
- give testimony
- file insurance claims

How to do it

➤ *Identify the information to be logged.*

You must first identify the types of information you can log, the mechanisms for such logging, where the logging is performed, and the locations where the log files are stored.

A table of log categories and types of log information within each category is described below. This table contains the types of information you likely want to log although not all systems are able to log all of this information. Logging selections should be tailored to meet your site's specific needs.

Log Category	Types of Information to Log
Users	• Login/logout information: failed attempts, location, time, attempted logins to privileged accounts • Changes in authentication status, such as enabling privileges
Processes	• Real and effective user executing the process • Process start-up time, arguments • Process exit status, time, duration, resources consumed
Systems	• Actions requiring special privileges • Status/errors reported by hardware and software subsystems • Changes in system status, including shutdowns and restarts
Networks	• Service initiation requests • The name of the user/host requesting the service • Network traffic • New connections • Connection duration
File Systems	• Changes to access control lists and file protections • File accesses (opening, creating, executing, deleting)
Applications	• Applications- and services-specific information, e.g., mail logs, ftp logs, Web server logs, modem logs, firewall logs

Do not log passwords, even incorrect ones. Logging correct passwords creates an enormous potential vulnerability if the audit records are improperly accessed. Recording incorrect passwords is also risky as they often differ from valid passwords by only a single character or transposition. Turning off password logging may require resetting a system default. The data you may want to log regarding password use includes number of failed attempts, accesses to specific accounts, etc.

➤ *Determine if the logging mechanisms provided with your systems and networks sufficiently capture the required information.*

Determine what logging mechanisms are available for the specific platforms that you have at your site, how the log files are named, and where they are located. The names of these log files can differ even among versions of the same operating system delivered by a single vendor, so it is important that you verify this each time you upgrade your systems.

Identify what types of information each logging mechanism can capture. The combination of mechanisms should capture the information identified in the table categories noted above. There may be differences in the log file contents provided by different vendors, even for similar types of systems.

If your vendor-provided logging mechanisms are insufficient to capture the data you require, supplement these mechanisms with tools that capture the additional information.

➤ *Enable logging.*

Using the vendor-provided logging mechanisms and supplemental tools, enable all logging that you have selected from the previous step. You need to refer to the administration documentation for your systems to determine the exact method of enabling each of the logging mechanisms, along with any tool-specific documentation for setup. This documentation provides guidance as to whether these mechanisms need to be enabled only once, each time the system is rebooted, or at regular intervals during the system's normal operation. Some logging mechanisms provide for selection of various levels of logging detail.

Pay specific attention to the location of the log data: some tools allow you to specify a file or directory where the data is logged, while others write their data to a predefined default location. Make sure that you have sufficient space for the data that is generated. Pay special attention to ensure that the logged data is protected correctly, based on previously determined ACLs (access control lists).

Be aware that multiple logging mechanisms may contribute log records to a single log file (e.g., in Unix systems, syslog).

➤ *Protect logs to ensure they are reliable.*

Log files often contain sensitive information that you would not want an intruder to have. Ensure that log files are protected so that they cannot be accessed or modified by unauthorized users. Confirm that only authorized users can access utilities that reconfigure logging mechanisms and turn them on and off as well as write to, modify, and read log data.

It is important to collect and archive log files so that they cannot be accessed by an intruder to remove or alter signs of an intrusion or add erroneous information. The following methods can be used to ensure log files are not modified:

- Log data to a file on a separate host, preferably one in a physically secure location that is not easily accessible from the network. For example, capturing log data using a machine via a dedicated serial line provides a way of storing the log files more securely than if they were written on the logging host's disks.
- Log selected data to a write-once/read-many device (e.g., a CD-ROM or a specially configured tape drive) to eliminate the possibility of the data being modified once it is written, or to a write-only device (e.g., a printer).
- If supported by your systems, set selected log file attributes that enable only new information to be appended to the log files (i.e., new records can be added, those already recorded cannot be modified).

- Encrypt log files, particularly those that contain sensitive data or are being transmitted across a network.

Logging directly to disk on the local host is easiest to configure, allows instant access to file records for analysis, but is also the least reliable. Collecting log files on a write-once device is slightly more effort to configure but is more secure. However data is not as easily accessible and you need to maintain a supply of storage media. Logging to a hardcopy device, such as a printer, is useful where permanent and immediate log files are required, but it is difficult to search and does require manual analysis and a potentially large storage space.

In cases where the host generating the logging data is different from the host recording the logging data, it is important to secure the path between them. For environments where short distances separate the generating host from the recording host, this can be accomplished by directly attaching the generating and recording hosts with single point-to-point cable(s). For environments where this approach is not practical, you need to minimize the number of networks and routers that are used to make the connection or encrypt sensitive log data as it is generated.

You need to prepare systems that perform logging to ensure that they do not stop functioning in the event of a logging denial of service attack. A Unix example would be an intruder launching such an attack that fills up the syslog files so that when the logging partition is full, logging ceases. Two means of preparation are creating separate file partitions for different log information and filtering network messages to decrease the likelihood of such attacks.

➤ *Document your management plan for handling log files.*

Address the following topics:

Handle the total volume of logged information. We recommend that you log as much as possible for your systems and networks. While log files can consume a great deal of storage very quickly, it is difficult to anticipate which logs will be critical in the event of an intrusion. Based on your log collection and storage approach, you may want to compress log files to allow them to remain accessible online for easier review and to conserve space.

Determine what logging data is most useful to collect. You need to balance the importance of recording system, network, and user activities with the resources available to store, process, review and secure them. Some questions you need to ask to aid in determining logging data utility include:

- What is the host's sole or primary purpose? For example, if it is acting as a Web server, you want to capture Web logs.
- How many users are assigned to the host or system and how important is it for you to know who is logged on? This assists you in determining how much login/logout information you need to capture.
- How important is it to be able to use your logs to recover a compromised system? This helps determine the priority of capturing, e.g., data and file transaction logs.

- What are the range of services that can be performed on this host or system? Process accounting information is useful to detect unauthorized services.
- What is your organizational ability and capacity to process and analyze all collected logs to obtain useful information in a timely manner?

Rotate log files. This means:

- making a copy of the active (online) log files at regular intervals (anywhere from daily to once a week)
- renaming the files so that the information contained in the file is not further augmented
- resetting file contents
- verifying that logging still works

This action allows you to limit the volume of log data you have to examine at any given time and to keep log files open for a limited duration so that damage is bounded if an active log file is compromised. In this way, you create a collection of log files that contain well-defined time intervals of recorded data. You are then able to consolidate logs from different systems by matching time intervals so as to gain a network-wide perspective on what is occurring. To perform this consolidation, you will likely need to merge log files from different systems into a central log file, adjusting the timestamps used in each to a master clock.

Back up and archive log files. Moving your log files to permanent storage or capturing them as part of your regular backup procedure allows them to be retrieved at a later time if the need arises. You need to document your approach for access to archived log files. Backups should be made before you execute any automated tools that truncate and reset the log files so that minimal logging data is lost.

Encrypt log files. We recommend encrypting log files that contain sensitive data. Encryption can be performed as the log data is being recorded. In addition, you need to protect the encryption software and place a copy of your encryption keys on a floppy disk or writable CD-ROM in a safe location from which they can be retrieved (e.g., safe, safety deposit box). If the keys are lost, the log files cannot be used. If possible, use public key encryption. The logs can be encrypted using the public key (which can be safely stored online) and the corresponding private key (stored offline) can then be used to decrypt the logs.

Ensure that you have the system and personnel resources necessary to analyze logs on a regular basis and on demand (i.e., in some cases, daily, and as alert events occur).

Dispose of log files. Ensure that all media containing log file data are disposed of in a secure manner (e.g., shredding hardcopy output, sanitizing disks, destroying CD-ROMs).

Policy considerations

Your organization’s networked systems security policy should require that you document a management plan for handling log files. This plan should include what to log, when and why to log, where to log, and who is responsible for all aspects of the plan.

Other information

See also Firth, Robert, et al. *Detecting Signs of Intrusion*. (CMU/SEI-SIM-001). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 1997. Available online at http://www.cert.org/security-improvement/modules/m01.html

Where to find updates

The latest version of this practice, plus implementation details for selected technologies, is available on the Web at

http://www.cert.org/security-improvement/practices/p041.html

3 Identify and install tools that aid in detecting signs of intrusion.

It is important to supplement your system and network logs with additional tools that watch for signs of intrusions or intrusion attempts as well as alert responsible parties when such events occur. Included are tools that monitor and inspect system resource use, network traffic and connections, and user account and file access; tools to scan for viruses; tools to verify file and data integrity; tools to probe for system and network vulnerabilities; and tools to reduce, scan, monitor, and inspect your log files.

Monitoring is the observation of data streams for specific events, whereas logging systematically records specified events in the order that they occur. Inspection is the examination of a data resource or process. Monitoring is often preferable where there are large quantities of data, such as network traffic. In most circumstances, it isn't feasible to store every network packet, but monitoring the network traffic for specific types of events is very desirable.

It is possible that some of this information may already be captured by the logging features or the tools provided as part of your systems. In these cases, you need to determine whether or not to enable these features based on your site's security needs.

Why this is important

It is possible that the logging mechanisms and monitoring tools provided with your systems may not produce all of the information necessary to detect signs of an intrusion in a timely manner. Even if adequate information is provided, the volume of data may be so overwhelming that its reduction to a manageable subset is required before you can examine it for signs of intrusive activity. In either case, you will need to add tools to your systems to adequately detect signs of intrusion.

How to do it

➤ *Determine what additional information and alert mechanisms you require.*

In each of the tool types described below, a series of events, mechanisms, and desired data are provided that will aid you in deciding whether or not you require a tool of this type to implement your intrusion detection policy and procedures. It is difficult to provide specific guidance on tool selection as the criteria by which to select varies broadly based on each organization's needs. This is made more complex due to the lack of uniformity in characterizations of common security tools. Further guidance on this topic is provided in **Other information** below.

In most cases, you need to perform manual analysis in concert with the automated data collection and reporting performed by the tool.

➤ *Identify tools that report system events.*

Tools that monitor and inspect for use of system resources (e.g., process being executed, changes to file systems) can aid in the detection of the following intruder activities:

- password cracking
- execution of unauthorized programs
- installation of tools that may be used to break into other systems

Tools that monitor and inspect for unusual or unexpected open files can identify the presence of sniffer logs resulting from intruder use of sniffer programs.

Tools that monitor and inspect for successful and failed administrative logins can aid in the detection of intruder use or attempted use of administrative accounts.

Tools that monitor and inspect for unexpected shutdowns and restarts can aid in the detection of trojan horse programs that require a shutdown or restart of a system or service.

Tools that monitor and inspect for unusual modem activities can identify intruder access through overlooked entry points (ports).

Tools that perform real-time intrusion detection, including log file monitoring, can detect possible intrusions or access violations as they are occurring. Real-time intrusion detection occurs while an intruder is attempting to break in or is still present on your system. This is contrasted with offline intrusion detection which is performed after the intrusion has occurred, usually through inspecting various system and network log files and performing data and system integrity tests.

➤ *Identify tools that report network events.*

Tools that monitor and inspect network traffic and connections (e.g., what kinds of connections, from where, and when) can identify:

- use of Internet Relay Chat (IRC), a common means of communication used by intruders
- intruder use of unexpected or unrecognized hosts
- intruder access during non-business hours
- intruder file transfers of tools to be used in launching subsequent attacks

This monitoring and inspection is performed for attempted connections that failed as well as for established connections and to aid in detecting traffic that is contrary to your firewall setup.

Tools that detect whether or not your network interface card is in promiscuous mode can aid in determining if intruders are using this mode to run network sniffers for capturing passwords.

Tools that detect the presence of new or unexpected services can aid in determining if intruders are running IRC servers, Web servers, FTP servers, etc., to allow them to distribute tools and information to other compromised hosts.

Tools that check for unauthorized network probes can detect failed attempts to connect to unsupported services and systematic port scans.

➤ *Identify tools that report user-related events.*

Tools that check account configurations (e.g., authentication and authorization information) can aid in detecting creation of files in user home directories that can be later used for backdoor access.

Tools that monitor and inspect user activity can aid in detecting repeated, failed login attempts, logins from unusual locations, logins at unusual times, changes in user identity, and unauthorized attempts to access restricted information.

➤ *Identify tools that verify data, file, and software integrity.*

Tools that inspect operating systems and tool configurations can aid in detecting possible signs of intrusion (e.g., improperly set access control lists on system tools). Intruders have been known to review and execute security tools that were installed by the authorized system administrator.

Tools that detect unexpected changes to the contents or protections of files and directories can be used to identify the possible presence of trojan horses, often used to hide intruder activity.

Tools that scan for viruses and trojan horses can aid in the elimination of these programs before they damage your systems and data.

➤ *Identify tools to examine your systems in detail periodically or as events warrant.*

- Tools that reduce and scan log files can enhance the immediate detection of unusual activity. Regular use of log filtering tools improves the efficiency with which you are able to examine your logs.
- Tools that check log file consistency for possible tampering can aid in detecting whether or not an intruder removed references to their activities from specific log files.
- Tools that check for known vulnerabilities and vulnerability patch logging can aid in identifying a pattern where an intruder exploits more that one vulnerability before gaining access. For example, a failed logged attempt to probe for an old vulnerability could be followed by a successful probe for a new vulnerability that is not logged.

➤ *Protect the tools and the output of the tools to ensure they are reliable.*

When obtaining tools, ensure that you do so from a reliable source and that you verify the integrity of the software through such means as digital signatures, cryptographic checksums, or use of trusted copies from secure media. Intruders have been known to modify tools installed by authorized administrators so that the tools, when used, do not identify the presence of the intruder.

Once you have verified the software, you need to configure it for use at your site. The installation should be performed on a secure system to eliminate the possibility of the tool being tampered with before you have had a chance to deploy it. You should make a cryptographic checksum of these tools. Using this information, you can then verify that your original configuration has not been compromised. You need to protect these tools by ensuring that they have the appropriate access control lists set to allow use and modification only by authorized users. The output produced by these tools also needs to be protected so that it is only viewable by authorized users.

Policy considerations

Your organization's networked systems security policy should identify approved sources for acquiring tool software (Internet, shareware, purchased from vendor, etc.) and acceptable use practices related to tools.

Other information

Tool selection:

You may find it useful to categorize and select tools using a set of specific activities associated with common approaches for detecting signs of intrusion. Such a set of activities would include:

filtering	examining a data stream and removing from it items that are deemed undesirable or inappropriate
probing	attempting connections or queries
scanning	iteratively probing a collection of systems or data
monitoring	observing a data stream for specified events
inspecting	examining a data resource or process
auditing	systematically examining system data against documented expectations of form or behavior
integrity checking	verifying that the contents of a data resource are exactly as created, stored, or transmitted
notifying	alerting a designated recipient to the occurrence of a specific event

See also Firth, Robert, et al. *Detecting Signs of Intrusion*. (CMU/SEI-SIM-001). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 1997. Available online at http://www.cert.org/security-improvement/modules/m01.html

---

Where to find updates

The latest version of this practice, plus implementation details for selected technologies, is available on the Web at

http://www.cert.org/security-improvement/practices/p042.html

4 Generate information required to verify the integrity of your systems and data.

Capturing an accurate, reliable, and complete record of your systems and data when they are first created, and as they evolve, establishes the expected state against which to compare your current systems and data. The information to be captured includes a known, expected state for all assets—your data (system and user), systems (hardware, software), networks (hardware and software), workstations (hardware and software), applications, and user environments. It should also include information that characterizes past process and user behavior derived from system and network transaction logs, once you have been operational for some period of time. This information is periodically compared with your current systems and data to determine if anything has been altered in an unexpected way.

Why this is important

Approaches to detecting signs of intrusion are usually based on identifying differences between your current operational state and a previously captured expected state.

You need to know where each asset is located and what information you expect to find in each location. You need to be able to verify the correct or expected state of every asset. Without this information, you cannot adequately determine if anything has been added, deleted, modified, lost, or stolen. You may not be able to rebuild a critical component that has been compromised. Creating up-to-date records that are reliable and secure is the only way to address these requirements.

How to do it

➤ *Generate an inventory of your system hardware.*

If you have not already done so, create an inventory of all of your computing hardware assets. This is most likely accomplished as a physical audit. Utilize a tool (e.g., a database management system or spreadsheet) to record the initial inventory and keep it up to date. Select a tool that will easily allow you to perform comparisons with subsequent inventories.

Ensure that procedures are in place to update your hardware inventory whenever the physical location of equipment changes, when its hardware configuration is upgraded (e.g., memory is added), and when equipment is added to or removed from your systems.

Produce and maintain complete, up-to-date network infrastructure information that captures the architecture, connectivity, and identity of all network devices. This includes:

- the layout or topology of all network devices
- network architecture
- network and device connectivity
- network and device configuration
- administrative domains
- physical location of all network devices
- intermediate public networks, if any

Identify network and management monitoring mechanisms to keep this information up to date and to alert you to anomalies.

Use automated tools to detect installed hardware and compare the results with your physical inventory. For PC-based systems, the Windows95 or NT operating systems provide a complete hardware inventory capability as part of system properties. There are also a variety of vendor tools available. For UNIX-based systems, tools such as daemon dialers, strobe, and fremont can help determine what modems and other devices are connected to your telephone lines, systems, and networks.

➤ *Generate an authoritative copy of all critical files and directories.*

This is also known as generating authoritative reference data. For each file and directory, the authoritative reference data you capture should provide enough information for you to be able to identify changes to:

- file type
- location in the file system
- alternate paths to any file or directory, via links, aliases, or shortcuts
- contents of files, entries in directories
- exact size
- time and date indicating when the file or directory was created and last modified
- ownership and access control settings

Capture a cryptographic checksum for all files. For example, for UNIX-based systems, Tripwire will generate this as well as inform you of the state of the collection of files on your system (added or deleted), changes in state (protection changes), and the fact that changes to file contents have or have not occurred (but not what the actual changes are).

Critical files and directories include:

- operating systems
- access control lists
- applications
- security tools and data such as those used for integrity checking and detecting signs of intrusion
- organizational data such as financial reports and employee information

- user data
- public information such as Web pages

➤ *Capture and characterize expected process and user behavior.*

Document the procedure by which you intend to verify that the processes executing on your systems are attributed only to authorized activities of users, administrators, and system functions, and are operating only as expected.

See also Firth, Robert, et al. *Detecting Signs of Intrusion*. (CMU/SEI-SIM-001). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 1997, specifically the practice “Inspect processes for unexpected behavior.”

➤ *Protect your system inventory and authoritative reference data to ensure their integrity.*

Keep authoritative copies of files and checksums on write-protected or read-only media stored in a physically secure location.

If you transmit authoritative reference data over unsecured network connections, make sure to verify the data upon arrival at the destination host (e.g., by using MD5). Consider encrypting the reference data at the source host to reduce the likelihood of the information being compromised.

➤ *Encrypt your system inventory if your organization’s security requirements demand this level of protection.*

➤ *Make paper copies of critical files in the event you are unable to recover uncorrupted electronic versions.*

Policy considerations

Your organization’s networked systems security policy should require that your system administrators create an accurate, reliable, complete record of your systems and critical data when they are first created and at well-defined events when you modify, add to, and replace elements of your systems and data.

Other information

See also Firth, Robert, et al. *Detecting Signs of Intrusion*. (CMU/SEI-SIM-001). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 1997. Available online at http://www.cert.org/security-improvement/modules/m01.html

Where to find updates

The latest version of this practice, plus implementation details for selected technologies, is available on the Web at

http://www.cert.org/security-improvement/practices/p043.html

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503.

1. **AGENCY USE ONLY** (leave blank)	2. **REPORT DATE** June 1998	3. **REPORT TYPE AND DATES COVERED** Final

4. **TITLE AND SUBTITLE**

Preparing to Detect Signs of Intrusion

5. **FUNDING NUMBERS**

C — F19628-95-C-0003

6. **AUTHOR(S)**

John Kochmar, Julia Allen, Christopher Alberts, Cory Cohen, Gary Ford, Barbara Fraser, Suresh Konda, Klaus-Peter Kossakowski, Derek Simmel

7. **PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)**

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

8. **PERFORMING ORGANIZATION REPORT NUMBER**

CMU/SEI-SIM-005

9. **SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)**

HQ ESC/DIB
5 Eglin Street
Hanscom AFB, MA 01731-2116

10. **SPONSORING/MONITORING AGENCY REPORT NUMBER**

11. **SUPPLEMENTARY NOTES**

12.a **DISTRIBUTION/AVAILABILITY STATEMENT**

Unclassified/Unlimited, DTIC, NTIS

12.b **DISTRIBUTION CODE**

13. **ABSTRACT** (maximum 200 words)

It is essential that those responsible for your organization’s information systems and networks be adequately prepared to detect evidence of breaches in security when they occur. Without advance preparation, it will be difficult, if not impossible, to determine if an intruder has been present and the extent of the damage caused by the intrusion. Thorough preparation will permit you to detect an intrusion or an intrusion attempt during or soon after it occurs. Preparation involves consideration of your security policy and supporting procedures, your critical business information, your systems, your networks, your user community (internal and external), and the tools to be employed in detecting intrusions.

A general security goal is to prevent intrusions. Even if you have sophisticated prevention measures in place, your strategy for detecting intrusions must include preparation. This module is a companion to CMU/SEI-SIM-001 *Detecting Signs of Intrusion*.

The practices contained in this module identify advance preparations you must make to enable you to obtain evidence of an intrusion or an intrusion attempt. They are designed to help you prepare by configuring your data, systems, networks, workstations, tools, and user environments to capture the necessary information for detecting signs of intrusion.

14. **SUBJECT TERMS**

network security, World Wide Web, web servers

15. **NUMBER OF PAGES**

32

16. **PRICE CODE**

17. **SECURITY CLASSIFICATION OF REPORT** UNCLASSIFIED	18. **SECURITY CLASSIFICATION OF THIS PAGE** UNCLASSIFIED	19. **SECURITY CLASSIFICATION OF ABSTRACT** UNCLASSIFIED	20. **LIMITATION OF ABSTRACT** UL