Carnegie Mellon University
Software Engineering Institute

Detecting Signs of Intrusion

Robert Firth
Gary Ford
Barbara Fraser
John Kochmar
Suresh Konda
John Richael
Derek Simmel
Networked Systems Survivability Program

Lisa Cunningham
Computer Sciences Corporation

August 1997

DISTRIBUTION STATEMENT A
Approved for public release;
Distribution Unlimited

Security Improvement Module
CMU/SEI-SIM-001

19971002 067

Carnegie Mellon University does not discriminate and Carnegie Mellon University is required not to discriminate in admission, employment, or administration of its programs or activities on the basis of race, color, national origin, sex or handicap in violation of Title VI of the Civil Rights Act of 1964, Title IX of the Educational Amendments of 1972 and Section 504 of the Rehabilitation Act of 1973 or other federal, state, or local laws or executive orders.

In addition, Carnegie Mellon University does not discriminate in admission, employment or administration of its programs on the basis of religion, creed, ancestry, belief, age, veteran status, sexual orientation or in violation of federal, state, or local laws or executive orders. However, in the judgment of the Carnegie Mellon Human Relations Commission, the Department of Defense policy of, "Don't ask, don't tell, don't pursue," excludes openly gay, lesbian and bisexual students from receiving ROTC scholarships or serving in the military. Nevertheless, all ROTC classes at Carnegie Mellon University are available to all students.

Inquiries concerning application of these statements should be directed to the Provost, Carnegie Mellon University, 5000 Forbes Avenue, Pittsburgh, PA 15213, telephone (412) 268-6684 or the Vice President for Enrollment, Carnegie Mellon University, 5000 Forbes Avenue, Pittsburgh, PA 15213, telephone (412) 268-2056.

Obtain general information about Carnegie Mellon University by calling (412) 268-2000.

Security Improvement Module

CMU/SEI-SIM-001

August 1997

Detecting Signs of Intrusion

Robert Firth

Gary Ford

Barbara Fraser

John Kochmar

Suresh Konda

John Richael

Derek Simmel

Networked Systems Survivability Program

Lisa Cunningham

Computer Sciences Corporation

Unlimited distribution subject to the copyright.

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, Pennsylvania 15213

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

Thomas R. Miller, Lt Col, USAF
SEI Joint Program Office

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

Copyright © 1997 by Carnegie Mellon University.

Permission to reproduce this document and to prepare derivative works from this document for internal use is granted, provided the copyright and "No Warranty" statements are included with all reproductions and derivative works.

Requests for permission to reproduce this document or to prepare derivative works of this document for external and commercial use 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.

This document is available through SAIC/ASSET: 1350 Earl L. Core Road; PO Box 3305; Morgantown, West Virginia 26505 / Phone: (304) 284-9000 / FAX: (304) 284-9001 / World Wide Web: http://www.saic.com/contact.html / e-mail: webmaster@cpqm.saic.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).

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

Table of Contents

Preface iii

Detecting Signs of Intrusion **1**

1. Ensure that the software used to examine systems has not been compromised. 5
2. Look for unexpected changes to directories and files. 9
3. Inspect your system and network logs. 13
4. Review notifications from system and network monitoring mechanisms. 17
5. Inspect processes for unexpected behavior. 19
6. Investigate unauthorized hardware attached to your organization's network. 23
7. Look for signs of unauthorized access to physical resources. 27
8. Review reports by users and external contacts about suspicious system and network events and behavior. 29

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.

Detecting Signs of Intrusion

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

This means that even if your organization has implemented comprehensive information security measures, it is essential that your information resources, and transactions involving them, be watched closely for signs of intrusion. Doing so may be complicated, since intruders often cover their tracks by changing the systems they break into to hide their activities. In other words, an intrusion may have already taken place but you may not have noticed anything wrong because everything *seems* to be operating normally.

A general security goal is to prevent intrusions. But because no prevention measures are perfect, you also need a strategy for handling intrusions that includes *preparation*, *detection*, and *response*. This module focuses on detection. The practices recommended below are designed to help you detect intrusions by looking for the "fingerprints" of known intrusion methods.

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 your networked systems infrastructure includes:

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

Approach

The general approach to detecting intrusions is

1. Observe your systems, networks, and user activities for anything unusual.
2. Investigate anything you find to be unusual.
3. If your investigation finds something that isn't explained by authorized activity, immediately initiate your intrusion response procedures.

While this process sounds simple enough, implementing it is a resource-intensive activity that requires continuous, automated support and daily administrative effort. Furthermore, the scale of intrusion-detection practices may need to change as threats, system configurations, or security requirements change. In all cases, however, there are five areas that must be addressed:

- Integrity of the software you use to detect intrusions
- Integrity of your file systems and the program and data files they contain
- Operations of your systems and the traffic on your networks
- Physical forms of intrusion to your computer systems, offline data storage media, and output devices
- Investigation of reports by users and other reliable sources (such as incident response teams) of unusual activities associated with your networked information resources

As you look for signs of intrusion, keep in mind that information from one source may not appear suspicious by itself. Inconsistencies among several sources can sometimes be the best indication of suspicious activities or intrusions.

Summary of recommended practices

Area	Recommended Practices
Integrity of intrusion-detection software	1. Ensure that the software used to examine systems has not been compromised.
Integrity of file systems and sensitive data	2. Look for unexpected changes to directories and files.
System and network activities	3. Inspect your system and network logs. 4. Review notifications from system and network monitoring mechanisms. 5. Inspect processes for unexpected behavior.
Physical forms of intrusion	6. Investigate unauthorized hardware attached to your organization's network. 7. Look for signs of unauthorized access to physical resources.
Other sources of information	8. Review reports by users and external contacts about suspicious system and network events and behavior.

Where to find updates The latest version of this module is available on the Web at URL

`http://www.cert.org/security-improvement/modules/m01.html`

1 Ensure that the software used to examine systems has not been compromised.

When looking for signs of intrusions on your systems, and when examining your systems in general, you should use a verified, reference set of software—one that contains only genuine copies of software that have not been modified. In addition to executable programs, the verified set of software must include all the system libraries, configuration and data files, and system utilities on which the programs depend. You should avoid relying on software that resides on systems being inspected (unless you can verify that the software and its supporting libraries, configuration files, and data files have not been modified).

Why this is important

Intrusion detection depends heavily on the reliability of the information you gather about the state and behavior of your systems, networks, data, and user activities. Therefore, it is essential that you use only software that you know to be genuine and accurate in its reporting of such information.

Intruders often replace software that would reveal their presence with substitutes that obscure or remove such information. Intruders are known to have replaced programs, libraries, and other utilities called by the programs. If a program used in detecting intrusions has been tampered with or substituted, you cannot rely on its output.

Ensuring that you are using only verified software may be very difficult. Modifications that intruders make to systems can be extremely devious and make things appear to be normal when in fact they are not. For example, the `ps` command on a UNIX system may be replaced with one that does not display the intruder's process, or an editor can be replaced with one that will read a file different from the one specified (the intruder may have hidden the original file and replaced it with another version). Intruders also have been known to modify software that is executed at system boot and shutdown, complicating your ability to safely take a system down for more detailed analysis.

How to do it

The guiding principle for this practice is that you maintain a certain amount of suspicion. Question everything you see, and try to answer the question, "What software is producing this output?"

There are five general ways to achieve the goal of using a verified set of software, and each way has advantages and disadvantages. You should choose a method appropriate to your current circumstances.

In all cases, the verified software should be located on physically write-protected media (e.g., CD-ROM or write-protected disk), so that it cannot be modified by a user or software running on the system being examined.

- *Move the disk from the suspect system to a write-protected, verified system and examine the disk's contents using the software of the protected system.*

This method has the advantage that you need not rely on the validity of any part of the operating system or the hardware on the suspect system.

The method is effective and reasonable when you suspect that a particular system has been compromised and want to analyze it. However, it may not be practical for automated procedures or for checking a large number of systems.

Be careful when shutting down the suspect system since the mere act of doing so may result in hiding the evidence you are seeking. Before shutting down the suspect system, look at any programs that will run at shutdown for signs that they've been modified (for example in some UNIX operating systems, the `/etc/shutdown` program should be examined). But be aware that just looking at the file may be misleading since you are relying on the software on the suspect system. So, to be completely safe, you may want to execute verified copies of shutdown programs and their data files (taking care to save the original files for later analysis). Other alternatives are to execute the shutdown from external media, force the system to halt immediately (e.g., `L1,A` on a UNIX system), or just pull the plug.

- *Attach to the suspect system a write-protected, verified system disk that contains the operating system and all needed software, and then reboot the system using the verified operating system.*

This method has similar advantages and disadvantages to those of the method above, but relies on the trustworthiness of the hardware of the suspect system.

- *Generate an image of the suspect system disk, mount it on a verified system, and examine it there.*

This method is acceptable if you have a verified system that you can use for this purpose. An advantage of this approach is that you won't affect the operational environment of the suspect system because you're looking at an image of it on another system.

- *Use external media containing a verified set of software to examine the suspect system.*

To use this method, you need a CD-ROM or write-protected diskette containing verified software to be used when checking the suspect system.

A significant concern with this approach is that you will still be using the operating system of the suspect system (e.g., the UNIX kernel), and it may be difficult, if not impossible, to ensure that you have provided every needed program, utility, and library.

➤ *Verify the software on the suspect system first, then use it to examine the system.*

This method will require that you compare the software on the suspect system with a reference copy (either complete files or cryptographic checksums). However, care must be taken to use a verified comparison program or cryptographic checksumming program. The program used to verify the software should be located on a hardware write-protected medium.

Policy considerations

Your organization's networked systems security policy should:

- Specify the level of verification that is required when examining each class of data and service provided by the organization.

Other information

Some operating systems provide the capability to make files *immutable*, meaning unchangeable by *any* process on the system, including system and administrative processes. All operating system files that don't need to be modified when a system is running can be made immutable.

When you are examining your system through a remote access connection, you need to be sure that you have established a secure channel to the system so that only authorized personnel use the channel and nothing is changed in transit.

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/p001.html`

2 Look for unexpected changes to directories and files.

The file systems in your network environment contain a variety of software and data files. Unexpected changes in directories and files, especially those to which access is normally restricted, may be an indication that an intrusion has occurred. Changes may include modifying, creating, or deleting directories and files. What makes such changes *unexpected* may depend on who changed them and where, when, and how the changes were made.

Why this is important

Intruders often substitute, modify, and damage files on systems to which they have gained access. To hide their presence on your systems, it is common for intruders to replace system programs with substitutes that perform the same functions but exclude information that could reveal their illicit activities. They also often modify system log files to remove traces of their activities. By masking their presence on a compromised system, intruders prolong the time they have to use that system for their purposes. In several notable cases, the presence of intruders on compromised systems was not discovered until many months after the initial intrusion occurred.

Intruders may also create new files on your systems. For example, they may install *backdoor* programs or tools used to gain privileged access on the system. Intruders also make use of the disk space on compromised systems to store their tools and contraband.

Private data files and files containing mission-critical information are common targets of modification or corruption by intruders. Information about your organization that is accessible to the public or to subscribers via public networks and the Internet is also a common target. Several documented cases exist of prominent organizations that have had their Web sites modified to include offensive content and other erroneous information.

How to do it

➤ *Establish priorities and schedules.*

Examine the files on your system and prioritize the frequency with which they should be checked. The more mission- or security-critical the file, the more frequent the checking should be.

➤ *Maintain authoritative reference data for critical files and directories.*

For each file and directory, the authoritative reference data you maintain should provide enough information for you to be able to identify changes to

- location in the file system
- alternate paths to it, via links, aliases, or shortcuts
- contents of files, entries in directories
- exact size, and if possible, file system units allocated
- time and date indicating when the file or directory was created and last modified
- ownership and access permission settings, including execution privilege settings for software

Use robust cryptographic checksum technologies to generate a checksum for each file. Keep authoritative copies of files and checksums on write-protected or read-only media stored in a physically secure location.

➤ *Verify the integrity of directories and files according to your established schedule.*

Compare the attributes and contents of files and directories to the authoritative reference (either complete copies or cryptographic checksums). Identify any files and directories whose contents or other attributes have changed.

Always access authoritative reference information directly from its secured, read-only media. Never transmit authoritative reference information over unsecured network connections.

➤ *Identify any missing files or directories.*

➤ *Identify any new files and directories.*

Pay special attention to any new program files and their associated execution privilege settings.

➤ *Investigate any unexpected changes among those you have identified.*

If any changes cannot be attributed to authorized activity, initiate your intrusion-response procedures immediately.

Report the incident to your organization's designated security point of contact.

Policy considerations

Your organization's networked systems security policy should

- Define the responsibilities and authority of systems administrators and security personnel to examine file systems on a regular basis for unexpected changes. Users should be told about such authority and examination.
- Require users to report any unexpected changes to their software and data files to system administrators or your organization's designated security point of contact.

Other information

As authorized and expected changes are made to files and directories, you will need to perform your organization's procedures for securely updating your authoritative reference data.

Some kinds of important files are expected to change frequently (perhaps several times per second); these include system log files, transaction log files, and database tables. In general, the techniques described above will not be particularly useful in distinguishing normal changes to such files from those that might have been caused by intruders. Techniques based on transaction auditing are more useful in these cases.

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/p002.html`

3 Inspect your system and network logs.

Frequently, intruders leave traces of their actions in system log files. Hence, checking system and network log files periodically is one way to detect intrusions.

Why this is important

Logs may contain evidence of unusual and unexpected activities that have occurred on the system or network. Such log entries may indicate that someone has compromised or tried to compromise the system. By looking at log files on a regular basis, you may be able to identify attempted or successful intrusions soon after they occur and initiate the proper damage-prevention or containment procedures.

Background information

Log files vary depending on the operating system, application software running on the system, and logging configuration you have chosen. Multiuser operating systems often provide more extensive logging capabilities than do single-user operating systems. Table 1 describes information typically contained in logs.

Type of Log	Information Contained in the Log
user activity	• login activity • changes in user identity • file accesses by the user • authorization information • authentication information
process activity	• commands run by users • running-process information including program name, user, start and stop times, and execution parameters
system activity	• restarts and shutdowns of the system • administrative logins
network connections	• details (when, where, what kind) of connections attempted or established with the system • details of connections established from the system
network traffic monitoring	• records of all network traffic transactions
program-specific log files	• details of the specific program's behavior

How to do it

➤ *Periodically inspect each type of log file.*

We recommend that each log file be inspected at least daily.

Look for evidence of unusual or unexpected activity. One benefit of periodic inspections is that, over time, you will become increasingly familiar with the signs of *usual* and *expected* activity. This will make it easier to recognize the unusual and unexpected.

The table below summarizes unusual or unexpected activities that may be reported in each log type. For operating systems that support different levels of user privilege, be sure to look for unusual activity by users at all levels.

Type of Log	Unusual or Unexpected Activities
user activity	• repeated failed login attempts • logins from unexpected locations • logins at unusual times of day • unusual attempts to change user identity • unusual processes run by users • unauthorized attempts to access restricted files
process activity	• processes that are run at unexpected times • processes that have terminated prematurely • unusual processes (i.e., those not due to normal, authorized activities)
system activity	• unexpected shutdowns • unexpected reboots
network connections	• connections to or from unusual locations • repeated failed connection attempts and their origination and destination addresses and ports • connections made at unusual times • unexpected network traffic (i.e., contrary to your firewall configuration or unexpected traffic volume)
network traffic monitoring	• sweeps of your network address space for various services, indicating attempts to identify hosts on your network and the services they run • repeated half-open connections (may signify IP spoofing attempts, or denial of service activity) • successive attempts to connect to unusual services on your network's hosts • transactions originating outside your network with destinations also outside your network (signifying traffic that should not be traversing your network) • sequential (attempted) connections to specific services signifying someone trying to run network-probing tools against your networked systems

Type of Log	Unusual or Unexpected Activities
program-specific log files	The presence and content of program-specific logs depend entirely on the program. The following are only examples of the kinds of logging that may occur: • unusual uses of outgoing modems • excessive or unusual file transfers • unusual entries from mail utilities • excessive mailings • unusual database transactions

➤ *Document any unusual entries that you discover.*

Over time, you may see recurring kinds of unusual log file entries. Maintaining records of such entries and what you determined to be their causes will help you and others to understand new occurrences more quickly and accurately.

➤ *Investigate each documented abnormality.*

Ask yourself questions such as

- Can it be explained by the activities of an authorized user? (e.g., the user really was in Cairo last week and connected to the network)
- Can it be explained by known system activity? (e.g., there was a power outage that caused the system to reboot)
- Can it be explained by authorized changes to programs? (e.g., the mail log showed abnormal behavior because the system programmer made a mistake when the software was modified)

➤ *Report all confirmed evidences of intrusion (or attempted intrusion) to your organization's internal security point of contact.*

➤ *Read security bulletins from trustworthy sources (e.g., CERT®[1] advisories and summaries[2]) and other security publications regularly.*

This can increase your understanding of current intruder activities and methods, and you can use this information to improve what you look for in log files.

Policy considerations

Your organization's networked systems security policy should:

- Specify that log files be inspected on a regular basis by authorized personnel, and that anomalies be recorded and reported to your organization's designated security point of contact.

Other information

If your site has large networks of systems with many log files to inspect, consider using tools that collect and consolidate log file information. Over time, you will learn what is normal for your environment. You should integrate this knowledge into your site's specific procedures for inspecting log files.

---

[1] Registered in the U.S. Patent and Trademark Office.

[2] See http://www.cert.org and ftp://info.cert.org/pub/cert_advisories/ .

Also, as you acquire, modify, or retire systems, your log review procedures may need to change. Make sure that your site's procedures are appropriate for your current technology.

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/p003.html`

4

Review notifications from system and network monitoring mechanisms.

If you have intrusion detection mechanisms monitoring your systems, you should investigate any warnings they sound. Although monitors are not foolproof, they can be part of an effective early warning system against certain types of attacks.

Why this is important

The monitoring of processes provides the capability to identify intrusive activity at the time it is occurring or soon after. By catching suspect activity as early as possible, you can immediately begin to investigate the activity and minimize the damage.

How to do it

➤ *Notify users that process monitoring is being done.*

In most cultures today, monitoring users' activities may be considered an unwarranted invasion of privacy. Be sure to inform authorized users of your networked systems about the scope and kind of monitoring you will be doing.

➤ *When a notification is generated, examine it to see if it is caused by authorized activity.*

If it is not, notify your organization's designated security point of contact.

➤ *Update monitoring configurations when information on new attack methods is published.*

Policy considerations

Your organization's networked systems security policy should

- Require the notification of users regarding the monitoring that will be done.
- Specify which data streams will be monitored and for what purposes.
- Define the responsibilities of system administrators for handling notifications generated by monitoring software.

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/p004.html`

5 Inspect processes for unexpected behavior.

Programs executing on your networked systems typically include a variety of operating system and network services, user-initiated programs, and special-purpose applications such as database servers. Every program executing on a system is represented by one or more processes. Each process executes in an environment with specific privileges that govern what system resources, programs, and data files it can access, and what it is permitted to do with them.

The execution behavior of a process is represented by the operations it performs while running, the manner in which those operations execute, and the system resources it uses while executing. Operations include computations, transactions with files, devices, and other processes, and communications with processes on other systems via your network.

Why this is important

The goal is 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 would be expected.

A process that exhibits unexpected behavior may indicate that an intrusion into a system has occurred. Intruders may have disrupted the execution of a program or service, causing it to fail, or to operate in a way other than the user or administrator intended. For example, if intruders were to successfully disrupt the execution of access-control processes running on a firewall system, they may be able to gain access to your organization's internal network in ways that would normally be blocked by the firewall. Unexpected processes may also indicate that an intruder is using the system covertly for unauthorized purposes, including attempts to attack other systems within and external to your network, or running network sniffer programs.

How to do it

➤ *Notify users that process inspection is being done.*

In most cultures today, monitoring users' activities may be considered an unwarranted invasion of privacy. Be sure to inform authorized users of your networked systems about the scope and kind of process inspections you will be doing.

➤ *To the extent that you are able, continuously monitor processes, network socket status, open files, and device activity on your networked systems.*

The examination of processes is complex, time consuming, and resource intensive. The degree to which you will be able to identify suspicious processes will depend on your knowledge of what processes you would normally expect to be executing on a given system and how they should behave.

As a general guideline, you should look for

- missing processes
- extra processes
- unusual process behavior or resource utilization
- processes that have unusual user identification associated with them

Due to the large number of processes and their rapidly changing natures, it is impractical for you to monitor them continually yourself. In addition, the amount and value of information that you can gather from a snapshot of currently executing processes may be very limited. This means that you must employ a variety of information-gathering and monitoring mechanisms to help you collect and analyze data associated with processes, and to alert you to suspicious activity.

One common approach with multiuser systems is to set up consoles (or terminal windows on graphical workstations) that display the current status of processes and are updated at short intervals. Ideally, these consoles should be hard-wired to the systems for which they are displaying information. With strategic placement of these displays, you can take advantage of the experience of system administrators and operators to notice unexpected activity that may not be picked up by your automated system and network monitoring mechanisms.

More generally, there are several sources of information that will help you to analyze the behavior of processes:

- logs from programs that collect and record information about
  - process accounting (i.e. who executed what programs when, where, how long the processes took, and what resources they accessed)
  - login and network connection attempts
  - attempts to access restricted resources and data
  - transactions with specific network services (e.g., Web servers)
- output from programs that tell you about
  - the state of current processes on your systems
  - the configuration of resources and devices on your systems
  - which resources and devices are currently being used by processes and how
  - files currently open by processes on your system
  - the states and activities associated with network sockets currently open on your system
- system- and network-monitoring programs that alert you when they find
  - unexpected volume or types of resource usage on a system
  - attempts to log into systems with privileged (e.g., administrator) access
  - attempts to access sensitive system data files or restricted resources
  - unexpected volume and types of network traffic
  - network interfaces operating in promiscuous mode
  - other unexpected changes to hardware configuration settings

➤ *As events give you reason to believe that intrusive activity may be taking place, examine any suspect processes.*

There are typically several questions that you may need to answer when analyzing processes to determine if they are authorized and behaving normally. We recommend that you adopt or develop a checklist of such questions to enable a structured and repeatable analysis procedure.

When examining suspect processes, bear in mind the recommendations in the practice "Ensure that the software used to examine systems has not been compromised.".

➤ *If you notice unusual activity associated with particular users, initiate supplemental logging and monitoring mechanisms to gather detailed information about those users' activities on your systems and networks.*

Many multiuser systems provide facilities to audit all processes associated with a particular user. Since process accounting logs tend to generate a great deal of information rapidly, you will need to dedicate sufficient resources to store the data collected. Similarly, detailed network logging of all activity associated with all the systems accessed by a specific user can be voluminous, and you will need to allocate resources accordingly. Review the newly collected data often (at least daily) to minimize the amount of information that you have to analyze at any given time.

Policy considerations

Your organization's networked systems security policy should

- Require notification of users regarding the process inspections that will be done.
- Specify the responsibilities and authority of designated systems administrators and security personnel to examine processes for unexpected behavior.
- Specify what forms of unexpected behavior users should watch for. Require users to report any such behavior to their designated security officials and system administrators.
- Specify what software and data users and administrators are permitted to install, collect, and use, with explicit procedures and conditions for doing so.
- Specify what programs users and administrators are permitted to execute and under which conditions.

Other information

One common activity of intruders is to gather information from the traffic on your networks to find user account names, passwords, and other information that may facilitate their ability to gain access to your systems. They do this by breaking into one system on your network and executing on it a *packet sniffer* program. This program collects information about connections established between systems from network data packets as they arrive at or pass by the compromised system. To hide this illicit activity on compromised systems, intruders typically modify log files and replace programs that would reveal the presence of the sniffer program with "Trojan horse" versions. The substitute programs appear to perform the same functions but exclude information associated with the intruders and their activities. In many documented cases of this type of intrusion, the intruders' activities went unnoticed for a considerable amount of time, during which they collected enough information to gain privileged access to several other systems.

This underscores the importance of using verified software to examine your systems and the need to verify the integrity of your files, as described in other practices. Unfortunately, there are several sophisticated collections of programs that intruders can use to rapidly gain access to systems and "set up shop" to install and execute a packet sniffer. This means that the only means you may have to catch such activity is to use verified software to examine processes on your systems for unexpected behavior. Processes associated with a packet sniffer will typically have transactions with a network interface that has been placed in *promiscuous mode*[1], as well as a file or network connection to which the information gathered from network packets is being sent.

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/p005.html`

---

[1] Network interfaces on most systems normally operate in *non-promiscuous* mode, which means that they ignore network packets not explicitly addressed to them. In *promiscuous* mode, no packets are ignored, that is, all packets that traverse the network segment to which the system is attached are read by its network interface and are accessible to processes executing on that system.

6 Investigate unauthorized hardware attached to your organization's network.

Unauthorized hardware may include computers connected to network segments or hubs, and peripheral communication or input/output equipment such as modems, terminals, printers, and disk or tape drives.

Why this is important

Intruders actively attempt to circumvent network perimeter defenses. If they can gain physical access to your organization's internal network, they can install their own equipment and software. Alternatively, intruders may learn of insecure (unauthorized) equipment added by users that they can use to gain access to the organization's network. For example, users might install modems for the purpose of remote access to their office computers from home. Intruders often use automated tools to identify such modems attached to public telephone lines. If the configuration of the dial-up access, and the traffic through it, is not secured, intruders may use such *back doors* to gain access to the internal network, bypassing preventative measures that may have been put in place to restrict external connections to the organization's network. They may then capture network traffic, infiltrate other systems, disrupt operations, and steal sensitive, private information.

Access to other peripheral equipment may also facilitate intrusions. Unsecured output and removable media devices, such as printers and diskette drives, may give intruders the opportunity to generate copies of sensitive information that can be physically removed from your organization's premises.

How to do it

➤ *Perform a monthly "walkabout" audit of all systems and peripherals attached to the network infrastructure.*

Visits to physically examine equipment attached to the network should not be announced, so that unauthorized equipment cannot be hidden before the auditors arrive.

Using your documented hardware inventory, identify any missing hardware, hardware that is not in its expected location, and any unexpected, extra hardware.

➤ *On a daily basis, probe for unauthorized modems attached to your organization's telephone lines.*

You can do this using "demon dialer" tools. Because this process will cause all telephones in your organization to ring, we recommend that it be done during nonworking hours.

➤ *On a daily basis, probe all internal network segments to identify devices attached to them. You can do this using a variety of commercial network management software packages.*

Identify any missing hardware, hardware that is not in its expected location, and any unexpected, extra hardware.

➤ *On a daily basis, look for unexpected routes between the organization's network and external networks.*

Examine the network traffic logs for connections that originate outside your network and are destined for addresses outside your network. Such transit traffic may indicate that an unauthorized computer is connecting to one of your hosts. Although in this case, the extra hardware will probably not be located at your site, you should be able to establish which of the organization's hosts is involved.

Examine the network traffic logs for traffic to or from external networks other than through authorized, secured connections and gateways. For example, if a user has added a modem to his desktop workstation and is using it to dial up to an external Internet service provider, the traffic generated will bypass his organization's firewalled Internet connection.

➤ *Resolve all instances of hardware anomalies.*

Investigate each instance of new, missing, or mislocated hardware to determine if the changes were authorized.

Report any confirmed unauthorized hardware additions, removals, or changes to the organization's security contact for further handling.

Update hardware inventories to reflect identified changes that you found to be authorized.

Policy considerations

Your organization's networked systems security policy should

- Require the maintenance of documented hardware inventories.
- Require the maintenance of a documented network topology.
- Specify the authority and responsibility of designated security personnel to perform physical audits of installed hardware and software.
- Specify what kinds of hardware and software users are permitted to install themselves on their desktop machines.

Other information	In addition to the periodic inspections of hardware recommended above, you may need to conduct inspections in response to suspected intrusions. Watch for evidence of activities that indicate unusual access to your network.
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/p006.html`

7 Look for signs of unauthorized access to physical resources.

Although we tend to think of the information in networked computer systems as being in electronic form, we should remember that that information is held on physical media—tapes, disks, paper—and these media are physical objects subject to physical compromise by theft, destruction, corruption, or unauthorized duplication. To ensure the security of your network, you should also ensure the physical security of its components by periodically inspecting them for possible compromise.

In many organizations, there will be personnel responsible for the physical security of the premises. However, as a system or network administrator, you are often in a unique position to notice signs of physical access to computing and network resources.

Why this is important

If a document or electronic storage medium is stolen, the confidentiality and availability of the information it contained is lost. Even if the item is recovered, you won't know the extent to which its contents have been copied and disseminated. Also, you won't know whether the information it contains has been damagingly corrupted or altered. Furthermore, if the compromised information is security critical, for example, user passwords, internal network addresses, or system configuration data, your entire network is under threat from further, deeper, and more damaging intrusions.

Therefore, it is just as important for you to keep track of physical resources and to promptly detect attempts at physical intrusion and access as it is for you to track and protect your electronic resources.

How to do it

➤ *Daily, check all physical means of entrance or exit for signs of tampering, trespass, or attempted trespass.*

Keep in mind that intruders have many strategies for obtaining confidential or security-critical documents. For example, they may steal discarded copies of reports, console logs, system printouts, or other sensitive data. They search through trash containers or dumpsters to find carelessly discarded physical copies. They may also attempt to steal backup or archive tapes, whose disappearance may not be noticed for some time.

- ➤ *Daily, check physical resources for signs of tampering.*

  For example, inspect locks or seals on hardware cabinets, review console logs, and monitor paper usage.

- ➤ *Weekly or monthly, perform a physical audit of all movable media.*

  Ensure that write-disabled media continue to be so.

  Note that, as a complementary practice, you should also audit the contents of the media for electronic integrity.

- ➤ *Report all signs of unauthorized physical access to your organization's internal security point of contact.*

Policy considerations

Your organization's networked systems security policy should

- Require the tagging and inventory of all physical computing resources.
- Specify how to respond when a physical intrusion has been detected.

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/p007.html`

8

Review reports by users and external contacts about suspicious system and network events and behavior.

In security-conscious organizations, users of networked systems will report suspicious events and behaviors. You, as a system or network administrator, should use those reports along with information you gather yourself to help identify possible intrusions. In addition, you should use external sources of information, such as the reports from incident response teams, where appropriate to help you plan your system monitoring and incident analysis efforts.

Why this is important

Recruiting users and external contacts to assist you in security monitoring greatly extends your ability to detect intrusions. Not only do they represent extra eyes, they can often be more aware of the "normal" behavior of their personal computing environments than you are. Many intrusions are not discovered until someone with day-to-day experience using a particular system notices something unusual.

Intruders often compromise multiple systems when they attack a target site. At each compromised system, there may be telltale signs of intrusive activities that users of the system discover. Although a single user report may not be sufficient evidence of an intrusion, analysis of several reports may reveal a pattern of attack underway. By consolidating users' reports of suspicious system behaviors, you may also be able to determine how widespread attacks against your networked systems are.

As intrusions into networked systems at other organizations occur, administrators at those organizations may contact your organization if they have reason to believe that the intrusion may also involve or affect your organization. Reports you receive from incident response teams, such as the CERT Coordination Center, should always be investigated thoroughly to determine if in fact an intrusion has occurred at your site. If your network environment supports connections to external networks, it is possible that your systems may be involved in a large-scale attack against several sites.

How to do it

➤ *Perform "triage" upon receipt of a report.*

Immediately gather as much information as necessary to make an initial assessment of whether there is a probable intrusion and, if so, how severe it seems to be. You may need to make direct contact with the user to get a description of what was observed. Also acquire any records or data from logging, monitoring, or other facilities that illustrate the problem. If the information clearly indicates an intrusion attempt, investigate it immediately.

➤ *Evaluate, correlate, and prioritize reports.*

On a regular basis (daily, if possible), review all user and external reports. These include new reports, reports currently under investigation, and any that remain unresolved after investigation. Look for correlations or patterns among the reports. Prioritize and schedule investigations of all reports based on your assessment of their severity. If a reported suspicion is unfounded, close the report and reassure the user who reported the problem.

➤ *Investigate each report or set of related reports.*

Based on the nature of the report, you may need to contact other users to document their observations. You may also need to verify the integrity of directories and files, examine your system and network logs, examine processes on affected systems, and install additional monitoring mechanisms to identify the cause of the anomalous behavior.

➤ *If an intrusion has been discovered, initiate your intrusion response procedures immediately.*

➤ *Document and report your findings.*

Regardless of your investigation's outcome, record and report your findings to the users who submitted the reports, system and network administrators, and security personnel in your organization, and other appropriate individuals as specified in your organization's policies.

Policy considerations

Your organization's networked systems security policy should

- Require users to report any unexpected or suspicious system behavior immediately to their designated security officials and system administrators.
- Require users to report any physical intrusions to networked systems or offline data storage facilities immediately to their designated security officials and system administrators.
- Require system administrators to investigate each reported suspicious activity to determine whether it represents an intrusion.
- Require system administrators to notify users in advance of any changes that will be made to the systems they use, including software configurations, data storage and access, and revised procedures for using systems as a result of the changes.

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/p008.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** August 1997	3. **REPORT TYPE AND DATES COVERED** Final
4. **TITLE AND SUBTITLE** Detecting Signs of Intrusion		5. **FUNDING NUMBERS** C — F19628-95-C-0003
6. **AUTHOR(S)** Robert Firth, Gary Ford, Barbara Fraser, John Kochmar, Suresh Konda, John Richael, Derek Simmel, Lisa Cunningham		
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-001
9. **SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)** HQ ESC/AXS 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)

The module provides concrete, practical guidance to help organizations improve the security of their networked computer systems. It describes a set of practices that can help detect intrusions by looking for the "fingerprints" of known intrusion methods.

14. **SUBJECT TERMS** breakin, intrusion detection, network security			15. **NUMBER OF PAGES** 30 pp.
			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