A Guide to Understanding Audit in Trusted Systems

NATIONAL COMPUTER SECURITY CENTER

FORT GEORGE G. MEADE, MARYLAND 20755-6000

NCSC-TG-001
VERSION-2
Library No. S-228,470

FOREWORD

This publication, "A Guide to Understanding Audit in Trusted Systems," is being issued by the National Computer Security Center (NCSC) under the authority of and in accordance with Department of Defense (DoD) Directive 5215.1. The guidelines described in this document provide a set of good practices related to the use of auditing in automatic data processing systems employed for processing classified and other sensitive information. Recommendations for revision to this guideline are encouraged and will be reviewed biannually by the National Computer Security Center through a formal review process. Address all proposals for revision through appropriate channels to:

National Computer Security Center
9800 Savage Road
Fort George G. Meade, MD 20755-6000
Attention: Chief, Computer Security Technical Guidelines

Patrick R. Gallagher, Jr.
Director
National Computer Security Center

28 July 1987

ACKNOWLEDGEMENTS

Special recognition is extended to James N. Menendez, National Computer Security Center (NCSC), as project manager of the preparation and production of this document.

Acknowledgement is also given to the NCSC Product Evaluations Team who provided the technical guidance that helped form this document and to those members of the computer security community who contributed their time and expertise by actively participating in the review of this document.

CONTENTS

PREFACE

Throughout this guideline there will be recommendations made that are not included in the Trusted Computer System Evaluation Criteria (the Criteria) as requirements. Any recommendations that are not in the Criteria will be prefaced by the word "should," whereas all requirements will be prefaced by the word "shall." It is hoped that this will help to avoid any confusion.

1 INTRODUCTION

1.1 History of the National Computer Security Center

The DoD Computer Security Center (DoDCSC) was established in January 1981 for the purpose of expanding on the work started by the DoD Security Initiative. Accordingly, the Director, National Computer Security Center, has the responsibility for establishing and publishing standards and guidelines for all areas of computer security. In 1985, DoDCSC's name was changed to the National Computer Security Center to reflect its responsibility for computer security throughout the federal government.

1.2 Goal of the National Computer Security Center

The main goal of the National Computer Security Center is to encourage the widespread availability of trusted computer systems. In support of that goal a metric was created, the DoD Trusted Computer System Evaluation Criteria (the Criteria), against which computer systems could be evaluated for security. The Criteria was originally published on 15 August 1983 as CSC-STD-001-83. In December 1985 the DoD adopted it, with a few changes, as a DoD Standard, DoD 5200.28-STD. DoD Directive 5200.28, "Security Requirements for Automatic Data Processing (ADP) Systems" has been written to, among other things, require the Department of Defense Trusted Computer System Evaluation Criteria to be used throughout the DoD. The Criteria is the standard used for evaluating the effectiveness of security controls built into ADP systems. The Criteria is divided into four divisions: D, C, B, and A, ordered in a hierarchical manner with the highest division (A) being reserved for systems providing the best available level of assurance. Within divisions C and B there are a number of subdivisions known as classes, which are also ordered in a hierarchical manner to represent different levels of security in these classes.

2 PURPOSE

For Criteria classes C2 through A1 the Criteria requires that a user's actions be open to scrutiny by means of an audit. The audit process of a secure system is the process of recording, examining, and reviewing any or all security-relevant activities on the system. This guideline is intended to discuss issues involved in implementing and evaluating an audit mechanism. The purpose of this document is twofold. It provides guidance to manufacturers on how to design and incorporate an effective audit mechanism into their system, and it provides guidance to implementors on how to make effective use of the audit capabilities provided by trusted systems. This document contains suggestions as to what information should be recorded on the audit trail, how the audit should be conducted, and what protective measures should be accorded to the audit resources. Any examples in this document are not to be construed as the only implementations that will satisfy the Criteria requirement. The examples are merely suggestions of appropriate implementations. The recommendations in this document are also not to be construed as supplementary requirements to the Criteria. The Criteria is the only metric against which systems are to be evaluated.

This guideline is part of an on-going program to provide helpful guidance on Criteria issues and the features they address.

3 SCOPE

An important security feature of Criteria classes C2 through A1 is the ability of the ADP system to audit any or all of the activities on the system. This guideline will discuss auditing and the features of audit facilities as they apply to computer systems and products that are being built with the intention of meeting the requirements of the Criteria.

4 CONTROL OBJECTIVES

The Trusted Computer System Evaluation Criteria gives the following as the Accountability Control Objective:

"Systems that are used to process or handle classified or other sensitive information must assure individual accountability whenever either a mandatory or discretionary security policy is invoked. Furthermore, to assure accountability the capability must exist for an authorized and competent agent to access and evaluate accountability information by a secure means, within a reasonable amount of time and without undue difficulty."(1)

The Accountability Control Objective as it relates to auditing leads to the following control objective for auditing:

"A trusted computer system must provide authorized personnel with the ability to audit any action that can potentially cause access to, generation of, or effect the release of classified or sensitive information. The audit data will be selectively acquired based on the auditing needs of a particular installation and/or application. However, there must be sufficient granularity in the audit data to support tracing the auditable events to a specific individual (or process) who has taken the actions or on whose behalf the actions were taken."(1)

5 OVERVIEW OF AUDITING PRINCIPLES

Audit trails are used to detect and deter penetration of a computer system and to reveal usage that identifies misuse. At the discretion of the auditor, audit trails may be limited to specific events or may encompass all of the activities on a system. Although not required by the TCSEC, it should be possible for the target of the audit mechanism to be either a subject or an object. That is to say, the audit mechanism should be capable of monitoring every time John accessed the system as well as every time the nuclear reactor file was accessed; and likewise every time John accessed the nuclear reactor file.

5.1 Purpose of the Audit Mechanism

The audit mechanism of a computer system has five important security goals. First, the audit mechanism must "allow the review of patterns of access to individual objects, access histories of specific processes and individuals, and the use of the various protection mechanisms supported by the system and their effectiveness."(2) Second, the audit mechanism must allow discovery of both users' and outsiders' repeated attempts to bypass the protection mechanisms. Third, the audit mechanism must allow discovery of any use of privileges that may occur when a user assumes a functionality with privileges greater than his or her own, i.e., programmer to administrator. In this case there may be no bypass of security controls but nevertheless a violation is made possible. Fourth, the audit mechanism must act as a deterrent against perpetrators' habitual attempts to bypass the system protection mechanisms. However, to act as a deterrent, the perpetrator must be aware of the audit mechanism's existence and its active use to detect any attempts to bypass system protection mechanisms. The fifth goal of the audit mechanism is to supply "an additional form of user assurance that attempts to bypass the protection mechanisms are recorded and discovered."(2) Even if the attempt to bypass the protection mechanism is successful, the audit trail will still provide assurance by its ability to aid in assessing the damage done by the violation, thus improving the system's ability to control the damage.

5.2 Users of the Audit Mechanism

"The users of the audit mechanism can be divided into two groups. The first group consists of the auditor, who is an individual with administrative duties, who selects the events to be audited on the system, sets up the audit flags which enable the recording of those events, and analyzes the trail of audit events."(2) In some systems the duties of the auditor may be encompassed in the duties of the system security administrator. Also, at the lower classes, the auditor role may be performed by the system administrator. This document will refer to the person responsible for auditing as the system security administrator, although it is understood that the auditing guidelines may apply to system administrators and/or system security administrators and/or a separate auditor in some ADP systems.

"The second group of users of the audit mechanism consists of the system users themselves; this group includes the administrators, the operators, the system programmers, and all other users. They are considered users of the audit mechanism not only because they, and their programs, generate audit events,"(2) but because they must understand that the audit mechanism exists and what impact it has on them. This is important because otherwise the user deterrence and user assurance goals of the audit mechanism cannot be achieved.

5.3 Aspects of Effective Auditing

5.3.1 Identification/Authentication

Logging in on a system normally requires that a user enter the specified form of identification (e.g., login ID, magnetic strip) and a password (or some other mechanism) for authentication. Whether this information is valid or invalid, the execution of the login procedure is an auditable event and the identification entered may be considered to be auditable information. It is recommended that authentication information, such as passwords, not be forwarded to the audit trail. In the event that the identification entered is not recognized as being valid, the system should also omit this information from the audit trail. The reason for this is that a user may have entered a password when the system expected a login ID. If the information had been written to the audit trail, it would compromise the password and the security of the user.

There are, however, environments where the risk involved in recording invalid identification information is reduced. In systems that support formatted terminals, the likelihood of password entry in the identification field is markedly reduced, hence the recording of identification information would pose no major threat. The benefit of recording the identification information is that break-in attempts would be easier to detect and identifying the perpetrator would also be assisted. The information gathered here may be necessary for any legal prosecution that may follow a security violation.

5.3.2 Administrative

All systems rated at class C2 or higher shall have audit capabilities and personnel designated as responsible for the audit procedures. For the C2 and B1 classes, the duties of the system operators could encompass all functions including those of the auditor. Starting at the B2 class, there is a requirement for the TCB to support separate operator and administrator functions. In addition, at the B3 class and above, there is a requirement to identify the system security administrator functions. When one assumes the system security administrator role on the system, it shall be after taking distinct auditable action, e.g., login procedure. When one with the privilege of assuming the role is on the system, the act of assuming that role shall also be an auditable event.

5.3.3 System Design

The system design should include a mechanism to invoke the audit function at the request of the system security administrator. A mechanism should also be included to determine if the event is to be selected for inclusion as an audit trail entry. If pre-selection of events is not implemented, then all auditable events should be forwarded to the audit trail. The Criteria requirement for the administrator to be able to select events based on user identity and/or object security classification must still be able to be satisfied. This requirement can be met by allowing post-selection of events through the use of queries. Whatever reduction tool is used to analyze the audit trail shall be provided by the vendor.

5.4 Security of the Audit

Audit trail software, as well as the audit trail itself, should be protected by the Trusted Computing Base and should be subject to strict access controls. The security requirements of the audit mechanism are the following:

1. The event recording mechanism shall be part of the TCB and shall be protected from unauthorized modification or circumvention.
2. The audit trail itself shall be protected by the TCB from unauthorized access (i.e., only the audit personnel may access the audit trail). The audit trail shall also be protected from unauthorized modification.
3. The audit-event enabling/disabling mechanism shall be part of the TCB and shall remain inaccessible to the unauthorized users.(2)

At a minimum, the data on the audit trail should be considered to be sensitive, and the audit trail itself shall be considered to be as sensitive as the most sensitive data contained in the system.

When the medium containing the audit trail is physically removed from the ADP system, the medium should be accorded the physical protection required for the highest sensitivity level of data contained in the system.

6 MEETING THE CRITERIA REQUIREMENTS

This section of the guideline will discuss the audit requirements in the Criteria and will present a number of additional recommendations. There are four levels of audit requirements. The first level is at the C2 Criteria class and the requirements continue evolving through the B3 Criteria class. At each of these levels, the guideline will list some of the events which should be auditable, what information should be on the audit trail, and on what basis events may be selected to be audited. All of the requirements will be prefaced by the word "shall," and any additional recommendations will be prefaced by the word "should."

6.1 The C2 Audit Requirement

6.1.1 Auditable Events

The following events shall be subject to audit at the C2 class:

- Use of identification and authentication mechanisms
- Introduction of objects into a user's address space
- Deletion of objects from a user's address space
- Actions taken by computer operators and system administrators and/or system security administrators
- All security-relevant events (as defined in Section 5 of this guideline)
- Production of printed output

6.1.2 Auditable Information

The following information shall be recorded on the audit trail at the C2 class:

- Date and time of the event
- The unique identifier on whose behalf the subject generating the event was operating
- Type of event
- Success or failure of the event

- Origin of the request (e.g., terminal ID) for identification/authentication events
- Name of object introduced, accessed, or deleted from a user's address space
- Description of modifications made by the system administrator to the user/system security databases

6.1.3 Audit Basis

At the C2 level, the ADP System Administrator shall be able to audit based on individual identity.

The ADP System Administrator should also be able to audit based on object identity.

6.2 The B1 Audit Requirement

6.2.1 Auditable Events

The Criteria specifically adds the following to the list of events that shall be auditable at the B1 class:

- Any override of human readable output markings (including overwrite of sensitivity label markings and the turning off of labelling capabilities) on paged, hard-copy output devices
- Change of designation (single-level to/from multi-level) of any communication channel or I/O device
- Change of sensitivity level(s) associated with a single-level communication channel or I/O device
- Change of range designation of any multi-level communication channel or I/O device

6.2.2 Auditable Information

The Criteria specifically adds the following to the list of information that shall be recorded on the audit trail at the B1 class:

- Security level of the object

The following information should also be recorded on the audit trail at the B1 class:

- * Subject sensitivity level

6.2.3 Audit Basis

In addition to previous selection criteria, at the B1 level the Criteria specifically requires that the ADP System Administrator shall be able to audit based on individual identity and/or object security level.

6.3 The B2 Audit Requirement

6.3.1 Auditable Events

The Criteria specifically adds the following to the list of events that shall be auditable at the B2 class:

- Events that may exercise covert storage channels

6.3.2 Auditable Information

No new requirements have been added at the B2 class.

6.3.3 Audit Basis

In addition to previous selection criteria, at the B2 level the Criteria specifically requires that the TCB shall be able to audit the identified events that may be used in the exploitation of covert storage channels." The Trusted Computing Base shall audit covert storage channels that exceed ten bits per second.(1)

The Trusted Computing Base should also provide the capability to audit the use of covert storage mechanisms with bandwidths that may exceed a rate of one bit in ten seconds.

6.4 The B3 Audit Requirement

6.4.1 Auditable Events

The Criteria specifically adds the following to the list of events that shall be auditable at the B3 class:

- Events that may indicate an imminent violation of the system's security policy (e.g., exercise covert timing channels)

6.4.2 Auditable Information

No new requirements have been added at the B3 class.

6.4.3 Audit Basis

In addition to previous selection criteria, at the B3 level the Criteria specifically requires that "the TCB shall contain a mechanism that is able to monitor the occurrence or accumulation of security auditable events that may indicate an imminent violation of security policy. This mechanism shall be able to immediately notify the system security administrator when thresholds are exceeded and, if the occurrence or accumulation of these security-relevant events continues, the system shall take the least disruptive action to terminate the event."(1)

Events that would indicate an imminent security violation would include events that utilize covert timing channels that may exceed a rate of ten bits per second and any repeated unsuccessful login attempts.

Being able to immediately notify the system security administrator when thresholds are exceeded means that the mechanism shall be able to recognize, report, and respond to a violation of the security policy more rapidly than required at lower levels of the Criteria, which usually only requires the System Security Administrator to review an audit trail at some time after the event. Notification of the violation "should be at the same priority as any other TCB message to an operator."(5)

"If the occurrence or accumulation of these security-relevant events continues, the system shall take the least disruptive action to terminate the event."(1) These actions may include locking the terminal of the user who is causing the event or terminating the suspect's process(es). In general, the least disruptive action is application dependent and there is no requirement to demonstrate that the action is the least disruptive of all possible actions. Any action which terminates the event is acceptable, but halting the system should be the last resort.

6.5 The A1 Audit Requirement

6.5.1 Auditable Events

No new requirements have been added at the A1 class.

6.5.2 Auditable Information

No new requirements have been added at the A1 class.

6.5.3 Audit Basis

No new requirements have been added at the A1 class.

7 POSSIBLE IMPLEMENTATION METHODS

The techniques for implementing the audit requirements will vary from system to system depending upon the characteristics of the software, firmware, and hardware involved and any optional features that are to be available. Technologically advanced techniques that are available should be used to the best advantage in the system design to provide the requisite security as well as cost-effectiveness and performance.

7.1 Pre/Post Selection of Auditable Events

There is a requirement at classes C2 and above that all security- relevant events be auditable. However, these events may or may not always be recorded on the audit trail. Options that may be exercised in selecting which events should be audited include a pre-selection feature and a post-selection feature. A system may choose to implement both options, a pre-selection option only, or a post-selection option only.

If a system developer chooses not to implement a general pre/post selection option, there is still a requirement to allow the administrator to selectively audit the actions of specified users for all Criteria classes. Starting at the B1 class, the administrator shall also be able to audit based on object security level.

There should be options to allow selection by either individuals or groups of users. For example, the administrator may select events related to a specified individual or select events related to individuals included in a specified group. Also, the administrator may specify that events related to the audit file be selected or, at classes B1 and above, that accesses to objects with a given sensitivity level, such as Top Secret, be selected.

7.1.1 Pre-Selection

For each auditable event the TCB should contain a mechanism to indicate if the event is to be recorded on the audit trail. The system security administrator or designee shall be the only person authorized to select the events to be recorded. Pre-selection may be by user(s) identity, and at the B1 class and above, pre-selection may also be possible by object security level. Although the system security administrator shall be authorized to select which events are to be recorded, the system security administrator should not be able to exclude himself from being audited.

Although it would not be recommended, the system security administrator may have the capability to select that no events be recorded regardless of the Criteria requirements. The intention here is to provide flexibility. The purpose of designing audit features into a system is not to impose the Criteria on users that may not want it, but merely to provide the capability to implement the requirements.

A disadvantage of pre-selection is that it is very hard to predict what events may be of security-relevant interest at a future date. There is always the possibility that events not pre-selected could one day become security-relevant, and the potential loss from not auditing these events would be impossible to determine.

The advantage of pre-selection could possibly be better performance as a result of not auditing all the events on the system.

7.1.2 Post-Selection

If the post-selection option to select only specified events from an existing audit trail is implemented, again, only authorized personnel shall be able to make this selection. Inclusion of this option requires that the system should have trusted facilities (as described in section 9.1) to accept query/retrieval requests, to expand any compressed data, and to output the requested data.

The main advantage of post-selection is that information that may prove useful in the future is already recorded on an audit trail and may be queried at any time.

The disadvantage involved in post-selection could possibly be degraded performance due to the writing and storing of what could possibly be a very large audit trail.

7.2 Data Compression

"Since a system that selects all events to be audited may generate a large amount of data, it may be necessary to encode the data to conserve space and minimize the processor time required" to record the audit records.(3) If the audit trail is encoded, a complementary mechanism must be included to decode the data when required. The decoding of the audit trail may be done as a preprocess before the audit records are accessed by the database or as a postprocess after a relevant record has been found. Such decoding is necessary to present the data in an understandable form both at the administrators terminal and on batch reports. The cost of compressing the audit trail would be the time required for the compression and expansion processes. The benefit of compressing data is the savings in storage and the savings in time to write the records to the audit trail.

7.3 Multiple Audit Trails

All events included on the audit trail may be written as part of the same audit trail, but some systems may prefer to have several distinct audit trails, e.g., one would be for "user" events, one for "operator" events, and one for "system security administrator" events. This would result in several smaller trails for subsequent analysis. In some cases, however, it may be necessary to combine the information from the trails when questionable events occur in order to obtain a composite of the sequence of events as they occurred. In cases where there are multiple audit trails, it is preferred that there be some accurate, or at least synchronized, time stamps across the multiple logs.

Although the preference for several distinct audit trails may be present, it is important to note that it is often more useful that the TCB be able to present all audit data as one comprehensive audit trail.

7.4 Physical Storage

A factor to consider in the selection of the medium to be used for the audit trail would be the expected usage of the system. The I/O volume for a system with few users executing few applications would be quite different from that of a large system with a multitude of users performing a variety of applications. In any case, however, the system should notify the system operator or administrator when the audit trail medium is approaching its storage capacity. Adequate advance notification to the operator is especially necessary if human intervention is required.

If the audit trail storage medium is saturated before it is replaced, the operating system shall detect this and take some appropriate action such as:

1. Notifying the operator that the medium is "full" and action is necessary. The system should then stop and require rebooting. Although a valid option, this action creates a severe threat of denial-of-service attacks.
2. Storing the current audit records on a temporary medium with the intention of later migration to the normal operational medium, thus allowing auditing to continue. This temporary storage medium should be afforded the same protection as the regular audit storage medium in order to prevent any attempts to tamper with it.
3. Delaying input of new actions and/or slowing down current operations to prevent any action that requires use of the audit mechanism.
4. Stopping until the administrative personnel make more space available for writing audit records.
5. Stopping auditing entirely as a result of a decision by the system security administrator.

Any action that is taken in response to storage overflow shall be audited. There is, however, a case in which the action taken may not be audited that deserves mention. It is possible to have the system security administrator's decisions embedded in the system logic. Such pre-programmed choices, embedded in the system logic, may be triggered automatically and this action may not be audited.

Still another consideration is the speed at which the medium operates. It should be able to accommodate the "worst case" condition such as when there are a large number of users on the system and all auditable events are to be recorded. This worst case rate should be estimated during the system design phase and (when possible) suitable hardware should be selected for this purpose.

Regardless of how the system handles audit trail overflow, there must be a way to archive all of the audit data.

7.5 Write-Once Device

For the lower Criteria classes (e.g., C2, B1) the audit trail may be the major tool used in detecting security compromises. Implicit in this is that the audit resources should provide the maximum protection possible. One technique that may be employed to protect the audit trail is to record it on a mechanism designed to be a write-only device. Other choices would be to set the designated device to write-once mode by disabling the read mechanism. This method could prevent an attacker from erasing or modifying the data already written on the audit trail because the attacker will not be able to go back and read or find the data that he or she wishes to modify.

If a hardware device is available that permits only the writing of data on a medium, modification of data already recorded would be quite difficult. Spurious messages could be written, but to locate and modify an already recorded message would be difficult. Use of a write-once device does not prevent a penetrator from modifying audit resources in memory, including any buffers, in the current audit trail.

If a write-once device is used to record the audit trail, the medium can later be switched to a compatible read device to allow authorized personnel to analyze the information on the audit trail in order to detect any attempts to penetrate the system. If a penetrator modified the audit software to prevent writing records on the audit trail, the absence of data during an extended period of time would indicate a possible security compromise. The disadvantage of using a write-once device is that it necessitates a delay before the audit trail is available for analysis by the administrator. This may be offset by allowing the system security administrator to review the audit trail in real-time by getting copies of all audit records on their way to the device.

7.6 Forwarding Audit Data

If the facilities are available, another method of protecting the audit trail would be to forward it to a dedicated processor. The audit trail should then be more readily available for analysis by the system security administrator.

8 OTHER TOPICS

8.1 Audit Data Reduction

Depending upon the amount of activity on a system and the audit selection process used, the audit trail size may vary. It is a safe assumption though, that the audit trail would grow to sizes that would necessitate some form of audit data reduction. The data reduction tool would most likely be a batch program that would interface to the system security administrator. This batch run could be a combination of database query language and a report generator with the input being a standardized audit file.

Although they are not necessarily part of the TCB, the audit reduction tools should be maintained under the same configuration control system as the remainder of the system.

8.2 Availability of Audit Data

In standard data processing, audit information is recorded as it occurs. Although most information is not required to be immediately available for real-time analysis, the system security administrator should have the capability to retreive audit information within minutes of its recording. The delay between recording audit information and making it available for analysis should be minimal, in the range of several minutes.

For events which do require immediate attention, at the B3 class and above, an alert shall be sent out to the system security administrator. In systems that store the audit trail in a buffer, the system security administrator should have the capability to cause the buffer to be written out. Regarding real-time alarms, where they are sent is system dependent.

8.3 Audit Data Retention

The exact period of time required for retaining the audit trail is site dependent and should be documented in the site's operating procedures manual. When trying to arrive at the optimum time for audit trail retention, any time restrictions on the storage medium should be considered. The storage medium used must be able to reliably retain the audit data for the amount of time required by the site.

The audit trail should be reviewed at least once a week. It is very possible that once a week may be too long to wait to review the audit trail. Depending on the amount of audit data expected by the system, this parameter should be adjusted accordingly. The recommended time in between audit trail reviews should be documented in the Trusted Facility Manual.

8.4 Testing

The audit resources, along with all other resources protected by the TCB, have increasing assurance requirements at each higher Criteria class. For the lower classes, an audit trail would be a major factor in detecting penetration attempts. Unfortunately, at these lower classes, the audit resources are more susceptible to penetration and corruption. "The TCB must provide some assurance that the data will still be there when the administrator tries to use it."(3) The testing requirement recognizes the vulnerability of the audit trail, and starting with the C2 class, shall include a search for obvious flaws that would corrupt or destroy the audit trail. If the audit trail is corrupted or destroyed, the existence of such flaws indicates that the system can be penetrated. Testing should also be performed to uncover any ways of circumventing the audit mechanisms. The "flaws found in testing may be neutralized in any of a number of ways. One way available to the system designer is to audit all uses of the mechanism in which the flaw is found and to log such events."(3) An attempt should be made to remove the flaw.

At class B2 and above, it is required that all detected flaws shall be corrected or else a lower rating will be given. If during testing the audit trail appears valid, analysis of this data can verify that it does or does not accurately reflect the events that should be included on the audit trail.

Even though system assurances may increase at the higher classes, the audit trail is still an effective tool during the testing phase as well as operationally in detecting actual or potential security compromises.

8.5 Documentation

Starting at the C2 class, documentation concerning the audit requirements shall be contained in the Trusted Facility Manual. The Trusted Facility Manual shall explain the procedures to record, examine, and maintain audit files. It shall detail the audit record structure for each type of audit event, and should include what each field is and what the size of the field is.

The Trusted Facility Manual shall also include a complete description of the audit mechanism interface, how it should be used, its default settings, cautions about the trade-offs involved in using various configurations and capabilities, and how to set up and run the system such that the audit data is afforded appropriate protection.

If audit events can be pre- or post-selected, the manual should also describe the tools and mechanisms available and how they are to be used.

8.6 Unavoidable Security Risks

There are certain risks contained in the audit process that exist simply because there is no way to prevent these events from ever occurring. Because there are certain unpredictable factors involved in auditing, i.e., man, nature, etc., the audit mechanism may never be one hundred per cent reliable. Preventive measures may be taken to minimize the likelihood of any of these factors adversely affecting the security provided by the audit mechanism, but no audit mechanism will ever be risk free.

8.6.1 Auditing Administrators/Insider Threat

Even with auditing mechanisms in place to detect and deter security violations, the threat of the perpetrator actually being the system security administrator or someone involved with the system security design will always be present. It is quite possible that the system security administrator of a secure system could stop the auditing of activities while entering the system and corrupting files for personal benefit. These authorized personnel, who may also have access to identification and authentication information, could also choose to enter the system disguised as another user in order to commit crimes under a false identity.

Management should be aware of this risk and should be certain to exercise discretion when selecting the system security administrator. The person who is to be selected for a trusted position, such as the system security administrator, should be subject to a background check before being granted the privileges that could one day be used against the employer.

The system security administrator could also be watched to ensure that there are no unexplained variances in normal duties. Any deviation from the norm of operations may indicate that a violation of security has occurred or is about to occur.

An additional security measure to control this insider threat is to ensure that the system administrator and the person responsible for the audit are two different people. "The separation of the auditor's functions, databases, and access privileges from those of the system administrator is an important application of the separation of privilege and least privilege principles. Should such a separation not be performed, and should the administrator be allowed to undertake auditor functions or vice-versa, the entire security function would become the responsibility of a single, unaccountable individual."(2)

Another alternative may be to employ separate auditor roles. Such a situation may give one person the authority to turn off the audit mechanism, while another person may have the authority to turn it back on. In this case no individual would be able to turn off the audit mechanism, compromise the system, and then turn it back on.

8.6.2 Data Loss

Although the audit software and hardware are reliable security mechanisms, they are not infallible. They, like the rest of the system, are dependent upon constant supplies of power and are readily subject to interruption due to mechanical or power failures. Their failure can cause the loss or destruction of valuable audit data. The system security administrator should be aware of this risk and should establish some procedure that would ensure that the audit trail is preserved somewhere. The system security administrator should duplicate the audit trail on a removable medium at certain points in time to minimize the data loss in the event of a system failure. The Trusted Facility Manual should include what the possibilities and nature of loss exposure are, and how the data may be recovered in the event that a catastrophe does occur.

If a mechanical or power failure occurs, the system security administrator should ensure that audit mechanisms still function properly after system recovery. For example, any auditing mechanism options pre-selected before the system malfunction must still be the ones in operation after the system recovery.

9 AUDIT SUMMARY

For classes C2 and above, it is required that the TCB "be able to create, maintain, and protect from modification or unauthorized access or destruction an audit trail of accesses to the objects it protects."(1) The audit trail plays a key role in performing damage assessment in the case of a corrupted system.

The audit trail shall keep track of all security-relevant events such as the use of identification and authentication mechanisms, introduction of objects into a user's address space, deletion of objects from the system, system administrator actions, and any other events that attempt to violate the security policy of the system. The option should exist that either all activities be audited or that the system security administrator select the events to be audited. If it is decided that all activities should be audited, there are overhead factors to be considered. The storage space needed for a total audit would generally require more operator maintenance to prevent any loss of data and to provide adequate protection. A requirement exists that authorized personnel shall be able to read all events recorded on the audit trail. Analysis of the total audit trail would be both a difficult and time-consuming task for the administrator. Thus, a selection option is required which may be either a pre-selection or post-selection option.

The audit trail information should be sufficient to reconstruct a complete sequence of security-relevant events and processes for a system. To do this, the audit trail shall contain the following information: date and time of the event, user, type of event, success or failure of the event, the origin of the request, the name of the object introduced into the user's address space, accessed, or deleted from the storage system, and at the B1 class and above, the sensitivity determination of the object.

It should be remembered that the audit trail shall be included in the Trusted Computing Base and shall be accorded the same protection as the TCB. The audit trail shall be subject to strict access controls.

An effective audit trail is necessary in order to detect and evaluate hostile attacks on a system.

GLOSSARY

Administrator - Any one of a group of personnel assigned to supervise all or a portion of an ADP system.

Archive - To file or store records off-line.

Audit - To conduct the independent review and examination of system records and activities.

Auditor - An authorized individual with administrative duties, whose duties include selecting the events to be audited on the system, setting up the audit flags which enable the recording of those events, and analyzing the trail of audit events.(2)

Audit Mechanism - The device used to collect, review, and/or examine system activities.

Audit Trail - A set of records that collectively provide documentary evidence of processing used to aid in tracing from original transactions forward to related records and reports, and/or backwards from records and reports to their component source transactions.(1)

Auditable Event - Any event that can be selected for inclusion in the audit trail. These events should include, in addition to security-relevant events, events taken to recover the system after failure and any events that might prove to be security-relevant at a later time.

Authenticated User - A user who has accessed an ADP system with a valid identifier and authentication combination.

Automatic Data Processing (ADP) System - An assembly of computer hardware, firmware, and software configured for the purpose of classifying, sorting, calculating, computing, summarizing, transmitting and receiving, storing, and retrieving data with a minimum of human intervention.(1)

Category - A grouping of classified or unclassified sensitive information, to which an additional restrictive label is applied (e.g., proprietary, compartmented information) to signify that personnel are granted access to the information only if they have formal approval or other appropriate authorization.(4)

Covert Channel - A communication channel that allows a process to transfer information in a manner that violates the system's security policy.(1)

Covert Storage Channel - A covert channel that involves the direct or indirect writing of a storage location by one process and the direct or indirect reading of the storage location by another process. Covert storage channels typically involve a finite resource (e.g., sectors on a disk) that is shared by two subjects at different security levels.(1)

Covert Timing Channel - A covert channel in which one process signals information to another by modulating its own use of system resources (e.g., CPU time) in such a way that this manipulation affects the real response time observed by the second process.(1)

Flaw - An error of commission, omission or oversight in a system that allows protection mechanisms to be bypassed.(1)

Object - A passive entity that contains or receives information. Access to an object potentially implies access to the information it contains. Examples of objects are: records, blocks, pages, segments, files, directories, directory trees and programs, as well as bits, bytes, words, fields, processors, video displays, keyboards, clocks, printers, network nodes, etc.(1)

Post-Selection - Selection, by authorized personnel, of specified events that had been recorded on the audit trail.

Pre-Selection - Selection, by authorized personnel, of the auditable events that are to be recorded on the audit trail.

Security Level - The combination of a hierarchical classification and a set of non-hierarchical categories that represents the sensitivity of information.(1)

Security Policy - The set of laws, rules, and practices that regulate how an organization manages, protects, and distributes sensitive information.(1)

Security-Relevant Event - Any event that attempts to change the security state of the system, (e.g., change discretionary access controls, change the security level of the subject, change user password, etc.). Also, any event that attempts to violate the security policy of the system, (e.g., too many attempts to login, attempts to violate the mandatory access control limits of a device, attempts to downgrade a file, etc.).(1)

Sensitive Information - Information that, as determined by a competent authority, must be protected because its unauthorized disclosure, alteration, loss, or destruction will at least cause perceivable damage to someone or something.(1)

Subject - An active entity, generally in the form of a person, process, or device that causes information to flow among objects or changes the system state. Technically, a process/domain pair.(1)

Subject Sensitivity Level - The sensitivity level of the objects to which the subject has both read and write access. A subject's sensitivity level must always be less than or equal to the clearance of the user the subject is associated with.(4)

System Security Administrator - The person responsible for the security of an Automated Information System and having the authority to enforce the security safeguards on all others who have access to the Automated Information System.(4)

Trusted Computing Base (TCB) - The totality of protection mechanisms within a computer system -- including hardware, firmware, and software -- the combination of which is responsible for enforcing a security policy. A TCB consists of one or more components that together enforce a unified security policy over a product or system. The ability of a TCB to correctly enforce a security policy depends solely on the mechanisms within the TCB and on the correct input by system administrative personnel of parameters (e.g., a user's clearance) related to the security policy.(1)

User - Any person who interacts directly with a computer system.(1)

REFERENCES

1. National Computer Security Center, DoD Trusted Computer System Evaluation Criteria, DoD, DoD 5200.28-STD, 1985.
2. Gligor, Virgil D., "Guidelines for Trusted Facility Management and Audit," University of Maryland, 1985.
3. Brown, Leonard R., "Guidelines for Audit Log Mechanisms in Secure Computer Systems," Technical Report TR-0086A(2770-29)-1, The Aerospace Corporation, 1986.
4. Subcommittee on Automated Information System Security, Working Group #3, "Dictionary of Computer Security Terminology," 23 November 1986.
5. National Computer Security Center, Criterion Interpretation, Report No. C1-C1-02-87, 1987.