INTERNATIONAL STANDARD

ISO/IEC 10181-7

First edition
1996-08-01

Information technology — Open Systems Interconnection — Security frameworks for open systems: Security audit and alarms framework

Technologies de l'information — Interconnexion de systèmes ouverts (OSI) — Cadres pour la sécurité dans les systèmes ouverts: Cadre pour l'audit de sécurité et les alarmes

Reference number
ISO/IEC 10181-7:1996(E)

CONTENTS

ISO/IEC Copyright Office • Case postale 56 • CH-1211 Genève 20 • Switzerland

Printed in Switzerland

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

International Standard ISO/IEC 10181-7 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 21, *Open systems interconnection, data management and open distributed processing*, in collaboration with ITU-T. The identical text is published as ITU-T Recommendation X.816.

ISO/IEC 10181 consists of the following parts, under the general title *Information technology — Open Systems Interconnection — Security frameworks for open systems*:

—*Part 1: Overview*

—*Part 2: Authentication framework*

—*Part 3: Access control framework*

—*Part 4: Non-repudiation framework*

—*Part 5: Confidentiality framework*

—*Part 6: Integrity framework*

—*Part 7: Security audit and alarms framework*

Annexes A to D of this part of ISO/IEC 10181 are for information only.

Introduction

This Recommendation | International Standard refines the concept of security audit described in ITU-T Rec. X.810 | ISO/IEC 10181-1. This includes event detection and actions resulting from these events. The framework, therefore, addresses both security audit and security alarms.

A security audit is an independent review and examination of system records and activities. The purposes of a security audit include:

- assisting in the identification and analysis of unauthorized actions or attacks;
- helping ensure that actions can be attributed to the entities responsible for those actions;
- contributing to the development of improved damage control procedures;
- confirming compliance with established security policy;
- reporting information that may indicate inadequacies in system controls; and
- identifying possible required changes in controls, policy and procedures.

In this framework, a security audit consists of the detection, collection and recording of various security-related events in a security audit trail and analysis of those events.

Both audit and accountability require that information be recorded. A security audit ensures that sufficient information is recorded about both routine and exceptional events so that later investigations can determine if security violations have occurred and, if so, what information or other resources have been compromised. Accountability ensures that relevant information is recorded about actions performed by users, or processes acting on their behalf, so that the consequences of those actions can later be linked to the user(s) in question, and the user(s) can be held accountable for his or her actions. Provision of a security audit service can contribute to the provision of accountability.

A security alarm is a warning issued to an individual or process to indicate that a situation has arisen that may require timely action. The purposes of a security alarm service include:

- to report real or apparent attempts to violate security;
- to report various security-related events, including “normal” events; and
- to report events triggered by threshold limits being reached.

INTERNATIONAL STANDARD

ITU-T RECOMMENDATION

INFORMATION TECHNOLOGY – OPEN SYSTEMS INTERCONNECTION – SECURITY FRAMEWORKS FOR OPEN SYSTEMS: SECURITY AUDIT AND ALARMS FRAMEWORK

1 Scope

This Recommendation | International Standard addresses the application of security services in an Open Systems environment, where the term "Open Systems" is taken to include areas such as Database, Distributed Applications, Open Distributed Processing and OSI. The Security Frameworks are concerned with defining the means of providing protection for systems and objects within systems, and with the interactions between systems. The Security Frameworks are not concerned with the methodology for constructing systems or mechanisms.

The Security Frameworks address both data elements and sequences of operations (but not protocol elements) which are used to obtain specific security services. These security services may apply to the communicating entities of systems as well as to data exchanged between systems, and to data managed by systems.

The purpose of security audit and alarms as described in this Recommendation | International Standard is to ensure that open system-security-related events are handled in accordance with the security policy of the applicable security authority.

In particular, this framework:

a) defines the basic concepts of security audit and alarms;

b) provides a general model for security audit and alarms; and

c) identifies the relationship of the Security Audit and Alarms service with other security services.

As with other security services, a security audit can only be provided within the context of a defined security policy.

The Security Audit and Alarms model provided in clause 6 supports a variety of goals not all of which may be necessary or desired in a particular environment. The security audit service provides an audit authority with the ability to specify the events which need to be recorded within a security audit trail.

A number of different types of standard can use this framework including:

1) standards that incorporate the concept of audit and alarms;

2) standards that specify abstract services that include audit and alarms;

3) standards that specify uses of audit and alarms;

4) standards that specify the means of providing audit and alarms within an open system architecture; and

5) standards that specify audit and alarms mechanisms.

Such standards can use this framework as follows:

- standard types 1), 2), 3), 4) and 5) can use the terminology of this framework;
- standard types 2), 3), 4) and 5) can use the facilities defined in clause 8; and
- standard types 5) can be based upon the characteristics of mechanisms defined in clause 9.

2 Normative references

The following Recommendations and International Standards contain provisions, which through reference in this text, constitute provisions of this Recommendation | International Standard. At the time of publication, the editions indicated were valid. All Recommendations and Standards are subject to revision, and parties to agreements based on this

Recommendation | International Standard are encouraged to investigate the possibility of applying the most recent edition of the Recommendations and Standards indicated below. Members of IEC and ISO maintain registers of currently valid International Standards. The Telecommunication Standardization Bureau of the ITU maintains a list of currently valid ITU-T Recommendations.

2.1 Identical Recommendations | International Standards

- ITU-T Recommendation X.200 (1994) | ISO/IEC 7498-1:1994, *Information technology – Open Systems Interconnection – Basic Reference Model: The Basic Model.*
- CCITT Recommendation X.734 (1992) | ISO/IEC 10164-5:1993, *Information technology – Open Systems Interconnection – Systems management: Event report management function.*
- CCITT Recommendation X.735 (1992) | ISO/IEC 10164-6:1993, *Information technology – Open Systems Interconnection – Systems management: Log control function.*
- CCITT Recommendation X.736 (1992) | ISO/IEC 10164-7:1992, *Information technology – Open Systems Interconnection – Systems management: Security alarm reporting function.*
- CCITT Recommendation X.740 (1992) | ISO/IEC 10164-8:1993, *Information technology – Open Systems Interconnection – Systems management: Security audit trail function.*
- ITU-T Recommendation X.810 (1995) | ISO/IEC 10181-1:1996, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Overview.*

2.2 Paired Recommendations | International Standards equivalent in technical content

- CCITT Recommendation X.700 (1992), *Management framework for Open Systems Interconnection (OSI) for CCITT applications.*

  ISO/IEC 7498-4:1989, *Information processing systems – Open Systems Interconnection – Basic Reference Model – Part 4: Management framework.*

- CCITT Recommendation X.800 (1991), *Security Architecture for Open Systems Interconnection for CCITT applications.*

  ISO 7498-2:1989, *Information processing systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture.*

3 Definitions

For the purposes of this Recommendation | International Standard, the following definitions apply.

3.1 Basic Reference Model definitions

This Recommendation | International Standard makes use of the following terms defined in ITU-T Rec. X.200 | ISO/IEC 7498-1.

a) entity;

b) facility;

c) function;

d) service.

3.2 Security architecture definitions

This Recommendation | International Standard makes use of the following terms defined in CCITT Rec. X.800 | ISO/IEC 7498-2.

a) Accountability;

b) Availability;

c) Security Audit;

d) Security Audit Trail;

e) Security Policy.

3.3 Management framework definitions

This Recommendation | International Standard makes use of the following terms defined in CCITT Rec. X.700 | ISO/IEC 7498-4:

- Managed Object.

3.4 Security framework overview definitions

This Recommendation | International Standard makes use of the following terms defined in ITU-T Rec. X.810 | ISO/IEC 10181-1.

- Security Domain.

3.5 Additional definitions

For the purposes of this Recommendation | International Standard, the following definitions apply.

3.5.1 alarm processor: A function which generates an appropriate action in response to a security alarm and generates a security audit message.

3.5.2 audit authority: The manager responsible for defining those aspects of a security policy applicable to conducting a security audit.

3.5.3 audit analyser: A function that checks a security audit trail in order to produce, if appropriate, security alarms and security audit messages.

3.5.4 audit archiver: A function that archives a part of the security audit trail.

3.5.5 audit dispatcher: A function which transfers parts, or the whole, of a distributed security audit trail to the audit trail collector function.

3.5.6 audit trail examiner: A function that builds security reports out of one or more security audit trails.

3.5.7 audit recorder: A function that generates security audit records and stores them in a security audit trail.

3.5.8 audit provider: A function that provides security audit trail records according to some criteria.

3.5.9 audit trail collector: A function that gathers records from a distributed audit trail into a security audit trail.

3.5.10 event discriminator: A function which provides initial analysis of a security-related event and, if appropriate, generates a security audit and/or an alarm.

3.5.11 security alarm: A message generated when a security-related event that is defined by security policy as being an alarm condition has been detected. A security alarm is intended to come to the attention of appropriate entities in a timely manner.

3.5.12 security alarm administrator: An individual or process that determines the disposition of security alarms.

3.5.13 security-related event: Any event that has been defined by security policy to be a potential breach of security, or to have possible security relevance. Reaching a pre-defined threshold value is an example of a security-related event.

3.5.14 security audit message: A message generated as a result of an auditable security-related event.

3.5.15 security audit record: A single record in a security audit trail.

3.5.16 security auditor: An individual or a process allowed to have access to the security audit trail and to build audit reports.

3.5.17 security report: A report that results from the analysis of the security audit trail and that can be used to determine whether a breach of security has occurred.

4 Abbreviations

OSI Open Systems Interconnection

5 Notation

The terms "service" and "mechanism", where not otherwise qualified, are used to refer to "security audit service" and "security audit mechanism" respectively. The term "audit", where not otherwise qualified, refers to a "security audit". The term "alarm", where not otherwise qualified, refers to a "security alarm".

6 General discussion of security audit and alarms

This clause describes a model for handling security alarms and for conducting a security audit for open systems.

A security audit allows the adequacy of the security policy to be evaluated, aids in the detection of security violations, facilitates making individuals accountable for their actions (or for actions by entities acting on their behalf), assists in the detection of misuse of resources, and acts as a deterrent to individuals who might attempt to damage the system. Security audit mechanisms are not involved directly in the prevention of security violations: they are concerned with the detection, recording and analysis of events. This allows changes to operational procedures to be implemented in response to abnormal events such as security violations.

A security alarm is generated following detection of any security-related event that has been defined by security policy to be an alarm condition. This could include the case of a pre-defined threshold being reached. Some of these events may require immediate recovery action while others may require further investigation to determine what, if any, action is required.

An implementation of the security audit and alarms model may need to use other security services to support the security audit and alarms service and to ensure its correct and assured operation. This subject is considered further in clause 10.

Although security audit trails and security audits have special characteristics, other (non-security) audit trails and audits may make use of the facilities and mechanisms described in this framework.

As with other aspects of security, maximum effectiveness is achieved by ensuring that specific security audit requirements are designed into the system. Systems developers should, therefore, take account of the need for auditability (i.e. ready examination and analysis) of both the design process and the system under development.

NOTE – The security audit and alarms model does not show how other system management and operational facilities relate to this model.

6.1 Model and functions

The model presented below illustrates the functions used in the provision of a security audit and alarms service.

6.1.1 Security audit and alarms functions

Various functions are necessary to support a security audit and alarm service. These are:

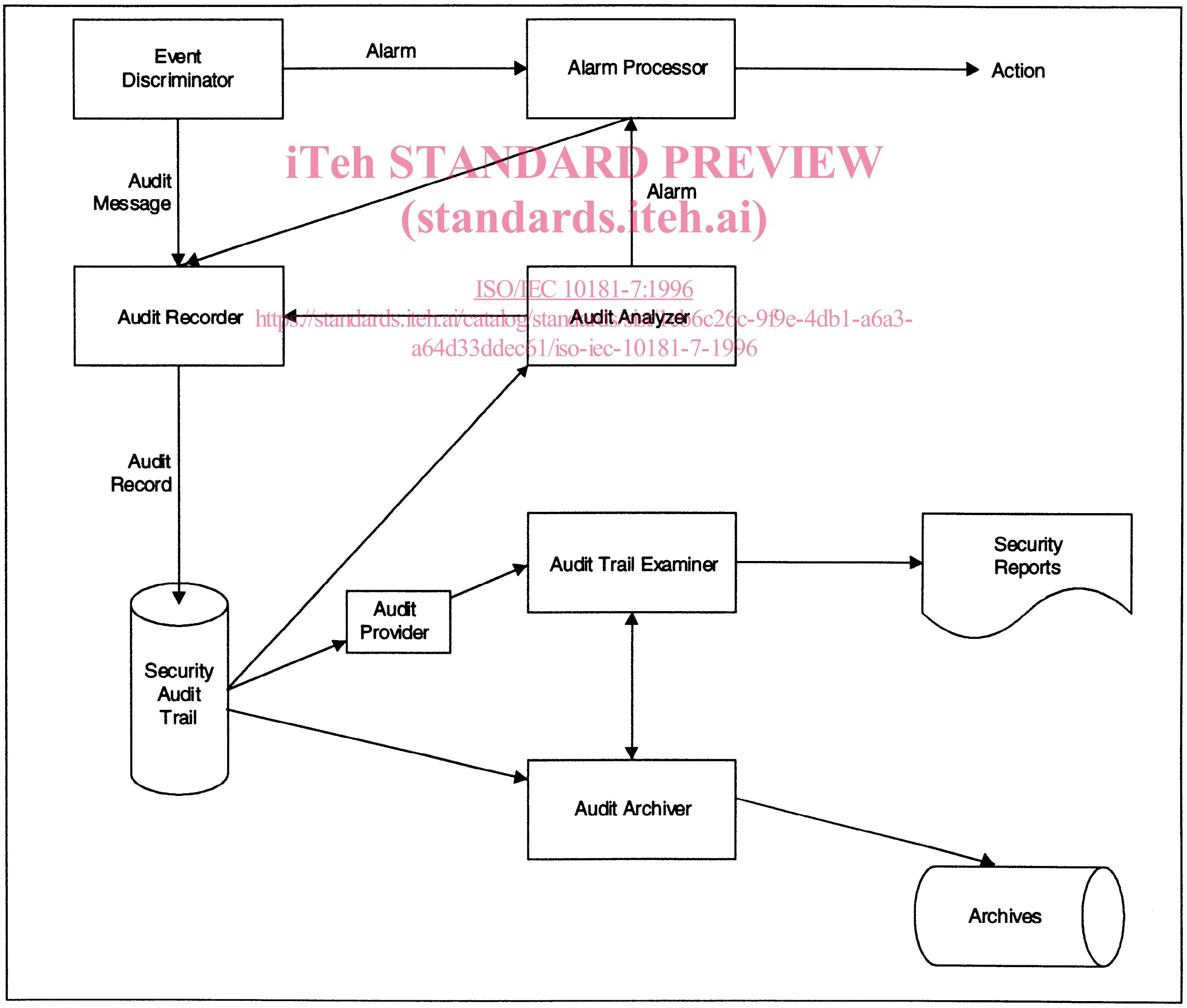
- the **event discriminator** which provides initial analysis of the event and determines whether to forward the event to the audit recorder or the alarm processor;
- the **audit recorder** which generates audit records from the messages received and stores the records in a security audit trail;
- the **alarm processor** which generates both an audit message and an appropriate action in response to a security alarm;
- the **audit analyser** which checks a security audit trail and, if appropriate, produces security alarms and security audit messages;
- the **audit trail examiner** which builds security reports out of one or more security audit trails;
- the **audit provider** which provides audit records according to some criteria; and
- the **audit archiver** which archives part of a security audit trail.

Additional functions may be necessary to support distributed security audit trails and alarms. These include:

- the **audit trail collector** that gathers records from a distributed audit trail into a security audit trail; and
- the **audit dispatcher** which transfers parts, or the whole, of a distributed security audit trail to the audit trail collector function.

6.1.2 Security audit and alarms model

The security audit and alarms model depicted below involves several phases. Following detection of an event, a determination must be made as to whether the event is security-relevant or not. The *event discriminator* assesses the event to determine whether a security audit message and/or a security alarms message should be generated. Security audit messages are forwarded to the *audit recorder*: security alarms are forwarded to the *alarm processor* for evaluation and further action. Security audit messages are then formatted and transformed into security audit records to be included in the security audit trail. The older parts of the security audit trail may be archived and both the security audit trail and the security audit trail archives may be used to construct audit reports by selecting particular security audit trail records according to specified criteria. That is, the security audit trail may be analysed and security audit reports and/or security alarms generated. The security audit and alarms model is shown in Figure 1.



TISO6430-95/d01

Figure 1 – Security audit and alarms model

6.1.3 Grouping of security audit and alarm functions

The functions depicted in the model may be colocated in one component of a system or distributed among several components of the system. These functions may also be located in different end systems and they may be duplicated. In some cases, such as for performance considerations, it will be advantageous for the functions to be grouped. In particular, an *audit recorder*, an *audit dispatcher*, an *audit provider* and an *audit analyser* all working on the same security audit trail may form a part of an unattended end-system.

Another grouping could be an *audit trail examiner*, and an *audit analyser* which may be useful for a security auditor.

There may be a chain of functions arranged in a hierarchical manner, particularly in a distributed security audit trail (see Figure 2). Here an *audit trail collector* of one component collects audit messages from the *audit dispatcher* of another component. This chain ends when a component does not support an *audit dispatcher*: in this case the component must support an *audit archiver* to be able to archive its security audit trail.

The decision of what, if any, functions to group is an implementation issue. The above examples are given as illustrations only.

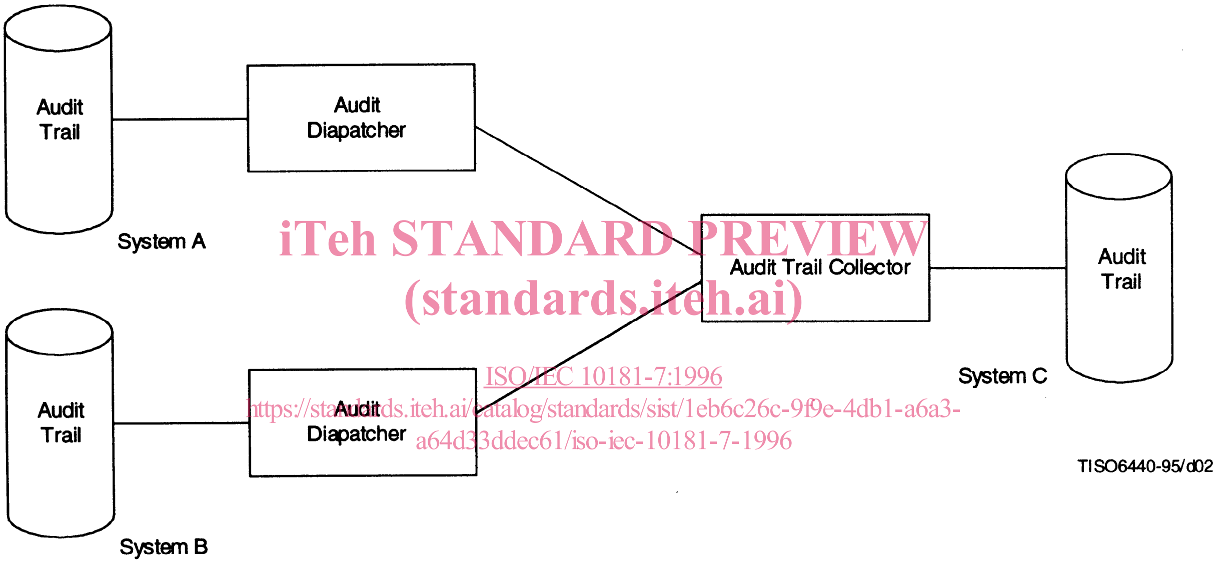


Figure 2 – Distributed audit trail model

6.2 Phases of security audit and alarms procedures

The security audit service provides an audit authority with the ability to specify and select the events which need to be detected and to be recorded within a security audit trail, and the events which need to trigger a security alarm and security audit messages.

The following phases may occur in audit procedures:

- detection phase, in which a security-related event is detected;
- discrimination phase, in which an initial determination is made as to whether it is necessary to record the event in the security audit trail or to raise an alarm;
- alarm processing phase, in which a security alarm or security audit message may be issued;
- analysis phase, in which a security-related event is evaluated together with, and in the context of, previously detected events as logged in the audit trail, and a course of action determined;

- aggregation phase, in which distributed security audit trail records are collected into a single security audit trail;
- report generation phase, in which audit reports are built from security audit trail records; and
- archiving phase, in which records from the security audit trail are transferred to the security audit trail archive.

The phases described here are not necessarily distinct in time, i.e. they may overlap.

6.2.1 Detection phase

The detection phase involves determining that an event that may be security-related has occurred. Actual determination of what, if any, action should be taken in response to this event is the task of the *event discriminator* (see 6.2.2) but, in some cases, as determined by security policy, an immediate alarm may be raised.

6.2.2 Discrimination phase

When a security-related event has been detected, the event discriminator will determine the appropriate initial course of action. The action will be one of:

a) take no action;

b) generate a security audit message; or

c) generate both a security alarm and a security audit message.

The decision as to which of these courses of action should be taken for each event is dependent on the security policy in effect.

6.2.3 Alarm processing phase

In the alarm processing phase, the alarm processor analyses the alarm to determine the correct course of action. The action will be one of:

a) take no action;

b) initiate recovery action; or

c) initiate recovery action and generate a security audit message.

The decision as to which of these courses of action should be taken for each event is dependent upon the security policy in operation.

NOTE – b) and c) might involve bringing the event to the attention of a person such as a security officer or audit administrator.

6.2.4 Analysis phase

In the analysis phase, a security-related event is processed to determine the appropriate course of action. This processing can also make use of information about earlier security-related events, as recorded in the security audit trail. The action will be one of the following:

a) take no action;

b) generate a security alarm;

c) generate a security audit record; or

d) generate both a security alarm and a security audit record.

The decision as to which of these four courses of action should be taken for each event is dependent upon the security policy in effect.

As part of the analysis process, reference may be made to previous events by examining records in the security audit trail and the security audit trail archive.

6.2.5 Aggregation phase

Individual security audit records from a distributed audit trail must periodically be collected into a single audit trail. This process, which includes use of an *audit trail collector* (at the collection point) and the use of an *audit dispatcher* function (at the remote systems), is called aggregation. (As noted in 6.1.3, this process could be hierarchical.)