INTERNATIONAL STANDARD

ISO/IEC 10164-7

First edition
1992-05-15

Information technology — Open Systems Interconnection — Systems Management: Security alarm reporting function

Technologies de l'information — Interconnexion de systèmes ouverts — Gestion-système: Fonction de compte rendu d'alarme de sécurité

Reference number
ISO/IEC 10164-7:1992(E)

Contents

Page

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 10164-7 was prepared by the Joint Technical Committee ISO/IEC JTC 1, *Information technology*, in collaboration with the CCITT. The identical text is published as CCITT Recommendation X.736.

ISO/IEC 10164 consists of the following parts, under the general title *Information technology - Open Systems Interconnection - Systems Management:*

— Part 1: *Object management function*

— Part 2: *State management function*

— Part 3: *Attributes for representing relationships*

— Part 4: *Alarm reporting function*

— Part 5: *Event report management function*

— Part 6: *Log control function*

— Part 7: *Security alarm reporting function*

— Part 8: *Security audit trail function*

— Part 9: *Objects and attributes for access control*

— Part 10: *Accounting meter function*

— Part 11: *Workload monitoring function*

— Part 12: *Test management function*

— Part 13: *Summarization function*

— Part 14: *Confidence and diagnostic test categories*

Introduction

ISO/IEC 10164 is a multipart standard developed according to ISO 7498 and ISO/IEC 7498-4. ISO/IEC 10164 is related to the following International Standards

— ISO/IEC 9595 : 1990, *Information technology — Open Systems Interconnection — Common management information service definition*;

— ISO/IEC 9596 : 1990, *Information technology — Open Systems Interconnection — Common management information protocol*;

— ISO/IEC 10040 : 1992, *Information technology — Open Systems Interconnection — Systems management overview*;

— ISO/IEC 10165 : 1992, *Information technology — Open Systems Interconnection — Structure of management information.*

INTERNATIONAL STANDARD

CCITT RECOMMENDATION

Information technology — Open Systems Interconnection — Systems Management: Security alarm reporting function

1 Scope

This Recommendation | International Standard defines the security alarm reporting function. The security alarm reporting function is a systems management function which may be used by an application process in a centralized or decentralized management environment to exchange information for the purpose of systems management, as defined by CCITT Rec. X.700 | ISO/IEC 7498-4. This Recommendation | International Standard is positioned in the application layer of CCITT Rec. X.200 | ISO 7498 and is defined according to the model provided by ISO/IEC 9545. The role of systems management functions is described by CCITT Rec. X.701 | ISO/IEC 10040. The security alarm notifications defined by this systems management function provide information regarding operational condition and quality of service, pertaining to security.

Security-related events are of relevance to the provision of security. The security policy determines the actions to be undertaken whenever a security-related event has occured. The security policy may, for example, specify that a security alarm report be generated, a record of the event be made in a security audit trail, a threshold counter be incremented, the event be ignored, or a combination of these actions be taken. This Recommendation | International Standard is only concerned with security alarm reporting.

This Recommendation | International Standard

- establishes user requirements for the service definition needed to support the security alarm reporting function;
- defines the service provided by the security alarm reporting function;
- specifies the protocol that is necessary in order to provide the service;
- defines the relationship between the service and management notifications;
- defines relationships with other systems management functions;
- specifies conformance requirements.

This Recommendation | International Standard does not

- define the nature of any implementation intended to provide the security alarm reporting function;
- specify the manner in which management is accomplished by the user of the security alarm reporting function;
- define the nature of any interactions which result in the use of the security alarm reporting function;
- specify the services necessary for the establishment, normal and abnormal release of a management association;
- define any other notifications, defined by other Recommendations | International Standards, which may be of interest to a security administrator.

2 Normative references

The following CCITT 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 editions of the Recommendations and Standards listed below. Members of IEC and ISO maintain registers of currently valid International Standards. The CCITT Secretariat maintains a list of the currently valid CCITT Recommendations.

2.1 Identical CCITT Recommendations | International Standards

- CCITT Recommendation X.701 (1992) | ISO/IEC 10040 : 1992, *Information technology - Open Systems Interconnection - Systems management overview.*
- CCITT Recommendation X.721 (1992) | ISO/IEC 10165-2 : 1992, *Information technology - Open Systems Interconnection - Structure of management information: Definition of management information.*
- CCITT Recommendation X.722 (1992) | ISO/IEC 10165-4 : 1992, *Information technology - Open Systems Interconnection - Structure of management information: Guidelines for the definition of managed objects.*
- CCITT Recommendation X.733 (1992) | ISO/IEC 10164-4 : 1992, *Information technology - Open Systems Interconnection - Systems Management: Alarm reporting function.*
- CCITT Recommendation X.734[1)] | ISO/IEC 10164-5 : 1992, *Information technology - Open Systems Interconnection - Systems Management: Event report management function.*
- CCITT Recommendation X.735[1)] | ISO/IEC 10164-6 : 1992, *Information technology - Open Systems Interconnection - Systems Management: Log control function.*

2.2 Paired CCITT Recommendations | International Standards equivalent in technical content

- CCITT Recommendation X.200 (1988), *Reference model of Open Systems Interconnection for CCITT applications.*

  ISO 7498 : 1984, *Information processing systems - Open Systems Interconnection - Basic Reference Model.*
- CCITT Recommendation X.208 (1988), *Specification of abstract syntax notation one (ASN.1).*

  ISO/IEC 8824 : 1990, *Information technology - Open Systems Interconnection - Specification of Abstract Syntax Notation One (ASN.1).*
- CCITT Recommendation X.209 (1988), *Specification of Basic Encoding Rules for abstract syntax notation.*

  ISO/IEC 8825 : 1990, *Information technology - Open Systems Interconnection - Specification of Basic Encoding Rules for Abstract Syntax Notation One (ASN.1).*
- CCITT Recommendation X.210 (1988), *Open Systems Interconnection layer service definition conventions.*

  ISO/TR 8509 : 1987, *Information processing systems - Open Systems Interconnection - Service conventions.*
- CCITT Recommendation X.290 (1992), *OSI conformance testing methodology and framework for protocol Recommendations for CCITT applications - General concepts.*

  ISO/IEC 9646-1 : 1991, *Information technology - Open Systems Interconnection - Conformance testing methodology and framework - Part 1: General concepts.*
- CCITT Recommendation X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT applications.*

  ISO 7498-2 : 1988, *Information processing systems - Open Systems Interconnection - Basic Reference Model - Part 2: Security Architecture.*

---

1) Presently at state of draft Recommendation.

— CCITT Recommendation X.700[1], *Management framework definition for Open Systems Interconnection for CCITT applications.*

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

— CCITT Recommendation X.710 (1991), *Common management information service definition for CCITT applications.*

ISO/IEC 9595 : 1991, *Information technology - Open Systems Interconnection - Common management information service definition.*

2.3 Additional references

— ISO/IEC 9545 : 1989, *Information technology - Open Systems Interconnection - Application Layer structure.*

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 term defined in CCITT Rec. X.200 | ISO 7498:

open system

3.2 Security architecture definitions

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

a) authentication;

b) confidentiality;

c) integrity;

d) non-repudiation;

e) security policy;

f) security service.

3.3 Management framework definitions

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

managed object

3.4 Systems management overview definitions

This Recommendation | International Standard makes use of the following terms defined in CCITT Rec. X.701 | ISO/IEC 10040:

a) agent role;

b) dependent conformance;

c) general conformance;

d) manager role;

---

[1] Presently at state of draft Recommendation.

e) notification;

f) systems management functional unit.

3.5 Event report management function definitions

This Recommendation | International Standard makes use of the following term defined in CCITT Rec. X.734 | ISO/IEC 10164-5:

discriminator

3.6 Service conventions definitions

This Recommendation | International Standard makes use of the following terms defined in CCITT Rec. X.210 | ISO/TR 8509:

a) service-user;

b) service-provider.

3.7 OSI conformance testing definitions

This Recommendation | International Standard makes use of the following term defined in CCITT Rec. X.290 | ISO/IEC 9646-1:

system conformance statement

3.8 Additional definitions

3.8.1 **security alarm**: A security-related event that has been identified by a security policy as a potential breach of security;

3.8.2 **security-related event**: An event which is considered to have relevance to security.

4 Abbreviations

ASN.1	Abstract Syntax Notation One
CMIS	Common Management Information Services
Conf	Confirmation
Ind	Indication
MAPDU	Management Application Protocol Data Unit
OSI	Open Systems Interconnection
Req	Request
Rsp	Response
SMAPM	Systems Management Application Protocol Machine

5 Conventions

This Recommendation | International Standard defines services for the security alarm reporting function using the descriptive conventions defined in CCITT Rec. X.210 | ISO/TR 8509. In clause 9, the definition of each service includes a table that lists the parameters of its primitives. For a given primitive, the presence of each parameter is described by one of the following values

M the parameter is mandatory

(=) the value of the parameter is equal to the value of the parameter in the column to the left

U the use of the parameter is a service-user option

— the parameter is not present in the interaction described by the primitive concerned

C the parameter is conditional. The condition(s) are defined by the text which describes the parameter

P subject to the constraints imposed on the parameter by CCITT Rec. X.710 | ISO/IEC 9595

NOTE — The parameters that are marked "P" in Table 2 of this Recommendation | International Standard are mapped directly onto the corresponding parameters of the CMIS service primitive, without changing the semantics or syntax of the parameters. The remaining parameters are used to construct an MAPDU.

6 Requirements

The security management user needs to be alerted whenever an event indicating an attack or potential attack on system security has been detected. A security attack may be detected by a security service, a security mechanism, or another process.

A security alarm notification may be generated by either of the communicating end users, or by any intermediate system or process between the end users. The security alarm report shall identify the cause of the security alarm, the source of the detection of the security-related event, the appropriate end users, and of the perceived severity of any misoperation, attack or breach of security, as specified by the security policy.

This Recommendation | International Standard describes the use of services and techniques to satisfy these requirements.

7 Model

The model for security alarm reporting is defined in CCITT Rec. X.734 | ISO/IEC 10164-5. The information may be logged in accordance with CCITT Rec. X.735 | ISO/IEC 10164-6.

8 Generic definitions

8.1 Generic notifications

This Recommendation | International Standard defines a set of generic security alarm notifications and their applicable parameters and semantics.

The set of generic notifications, parameters and semantics defined by this Recommendation | International Standard provide the detail for the following parameters of the M-EVENT-REPORT service as defined by CCITT Rec. X.710 | ISO/IEC 9595

— event type;

— event information;

— event reply.

All notifications are potential entries in a systems management log and this Recommendation | International Standard defines a managed object class for this purpose. CCITT Rec. X.721 | ISO/IEC 10165-2 defines a generic log record object class from which all entries are derived, the additional information being specified by the event information and event reply parameters.

8.1.1 Event type

This parameter defines the type of the security alarm report. The following event types are defined in this Recommendation | International Standard

— integrity violation: an indication that information may have been illegally modified, inserted or deleted;

— operational violation: an indication that the provision of the requested service was not possible due to the unavailability, malfunction or incorrect invocation of the service;

— physical violation: an indication that a physical resource has been violated in a way that suggests a security attack;

— security service or mechanism violation: an indication that a security attack has been detected by a security service or mechanism;

— time domain violation: an indication that an event has occurred at an unexpected or prohibited time.

8.1.2 Event information

The following parameters constitute the notification specific event information.

8.1.2.1 Security alarm cause

This parameter defines further qualification as to the probable cause of the security alarm. The value of this parameter in combination with the value of event type, determines which parameters constitute the balance of the security alarm event report, and what the possible values of those parameters may be.

Security alarm cause values for notifications shall be indicated in the behaviour clause of the object class definition. This Recommendation | International Standard defines, for use within the systems management application context defined in CCITT Rec. X.701 | ISO/IEC 10040, security alarm causes that have wide applicability across managed object classes. These values are registered in CCITT Rec. X.721 | ISO/IEC 10165-2. The syntax of security alarm causes shall be the ASN.1 type object identifier. Additional security alarm causes, for use within the systems management application context defined in CCITT Rec. X.701 | ISO/IEC 10040, may be added to this Recommendation | International Standard and registered using the registration procedures defined for ASN.1 object identifier values in CCITT Rec. X.208 | ISO/IEC 8824.

Other security alarm causes, for use within the systems management application context defined in CCITT Rec. X.701 | ISO/IEC 10040, may be defined outside of this Recommendation | International Standard and registered using the registration procedures defined for ASN.1 object identifier values in CCITT Rec. X.208 | ISO/IEC 8824.

Table 1 identifies the security alarm causes for the event types specified in this Recommendation | International Standard.

Table 1 — Security alarm causes

Event type	Security alarm causes
integrity violation	duplicate information information missing information modification detected information out of sequence unexpected information
operational violation	denial of service out of service procedural error unspecified reason
physical violation	cable tamper intrusion detection unspecified reason
security service or mechanism violation	authentication failure breach of confidentiality non-repudiation failure unauthorized access attempt unspecified reason
time domain violation	delayed information key expired out of hours activity

This Recommendation | International Standard defines the following security alarm causes

- authentication failure: an indication that an attempt to authenticate a user was unsuccessful;
- breach of confidentiality: an indication that information may have been read by an unauthorized user;
- cable tamper: an indication that a physical violation of a communications medium has occurred;
- delayed information: an indication that information has been received later than expected;

- denial of service: an indication that a valid request for service has been prevented or disallowed;
- duplicate information: an indication that an item of information has been received more than once, and therefore may be a replay attack;
- information missing: an indication that expected information has not been received;
- information modification detected: an indication, for example by a data integrity mechanism, that information has been modified;
- information out of sequence: an indication that information has been received in an incorrect sequence;
- intrusion detection: an indication that either the site on which the identified equipment is located may have been illegally entered, or the equipment itself has been violated;
- key expired: an indication that an out of date encipherment key has been presented or used;
- non-repudiation failure: an indication that communication has been prevented or halted due to the failure or unavailability of a non-repudiation service;
- out of hours activity: an indication that resource utilization has occurred at an unexpected time;
- out of service: an indication that a valid request for service could not be satisfied due to the unavailability of the service provider;
- procedural error: an indication that an incorrect procedure has been used in invoking a service;
- unauthorized access attempt: an indication that an access control mechanism has detected an illegal attempt to access a resource;
- unexpected information: an indication that information that was not expected has been received;
- unspecified reason: an indication that an unspecified security-related event has occurred.

The managed object class definer should choose the most specific security alarm cause applicable.

8.1.2.2 Security alarm severity

This parameter defines the significance of the security alarm as perceived by the managed object. The following levels of severity are defined

- indeterminate: a security attack has been detected. The integrity of the system is unknown;
- critical: a breach of security has occurred that has compromised the system. The system may no longer be assumed to be operating correctly in support of the security policy. Critical severity may involve the modification of security information without the correct authorization, leakage of information vital to the security of the system (such as passwords, private encryption keys etc), or breaches of physical security;
- major: a breach of security has been detected and significant information or mechanisms have been compromised;
- minor: a breach of security has been detected and less significant information or mechanisms have been compromised;
- warning: a security attack has been detected. The security of the system is not believed to be compromised.

8.1.2.3 Security alarm detector

This parameter identifies the detector of the security alarm.

8.1.2.4 Service user

This parameter identifies the service-user whose request for service led to the generation of the security alarm.

8.1.2.5 Service provider

This parameter identifies the intended service-provider of the service that led to the generation of the security alarm.