INTERNATIONAL STANDARD

ISO/IEC 10164-8

First edition
1993-06-15

Information technology — Open Systems Interconnection — Systems Management: Security audit trail function

Technologies de l'information — Interconnexion de systèmes ouverts — Gestion-système: Fonction de sécurité de l'expertise de l'historique

Reference number
ISO/IEC 10164-8:1993(E)

Contents

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 10164-8 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, in collaboration with the CCITT. The identical text is published as CCITT Recommendation X.740.

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*

Annexes A, B, C, D and E form an integral part of this part of ISO/IEC 10164. Annex F is for information only.

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 : 1991, *Information technology - Open Systems Interconnection - Common management information service definition;*
- ISO/IEC 9596 : 1991, *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 AUDIT TRAIL FUNCTION

1 Scope

This Recommendation | International Standard defines the security audit trail function. The security audit trail function is a systems management function which may be used by an application process in a centralized or decentralized management environment to exchange information and commands for the purpose of systems management, as defined by CCITT Rec. X.700 | ISO 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.

This Recommendation | International Standard

- establishes user requirements for the service definition needed to support the security audit trail reporting function;
- defines the service provided by the security audit trail 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

- a security audit, nor how to perform one. A security audit may be used to assist in assessing the effectiveness of a security policy. The security policy identifies the categories of security-related events that require auditing, and the location of the security audit trail log in which they are to be recorded;
- the nature of any implementation intended to provide the security audit trail function;
- the occasions where the use of the security audit trail function is appropriate;
- the services necessary for the establishment, normal and abnormal release of a management association;
- 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 currently valid CCITT Recommendations.

2.1 Identical 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.724[1)] | ISO/IEC 10165-6[1)], *Information technology – Open Systems Interconnection – Structure of management information: Requirements and guidelines for implementation conformance statement proformas associated with management information.*
- CCITT Recommendation X.733 (1992) | ISO/IEC 10164-4:1992, *Information technology – Open Systems Interconnection – Systems management: Alarm reporting function.*
- 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.*

2.2 Paired 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 (ASN.1).*

  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.291 (1992), *OSI conformance testing methodology and framework for protocol Recommendations for CCITT applications – Abstract test suite specification.*

  ISO/IEC 9646-2 : 1991, *Information technology – Open Systems Interconnection – Conformance testing methodology and framework – Part 2: Abstract test suite specification.*
- CCITT Recommendation X.700 (1992), 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.*

---

1) Presently at the stage of draft.

- 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.*

- 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.*

2.3 Additional references

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

- ISO/IEC 10181-7[1)], *Information technology – Open Systems Interconnection – Security frameworks – Part 7: Security audit framework.*

1) Presently at the stage of draft.