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

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.*