INTERNATIONAL
STANDARD

ISO/IEC
10181-6

First edition
1996-09-15

Information technology — Open Systems Interconnection — Security frameworks for open systems: Integrity framework

Technologies de l'information — Interconnexion de systèmes ouverts (OSI) — Cadres généraux pour la sécurité des systèmes ouverts: Cadre général d'intégrité

Reference number
ISO/IEC 10181-6:1996(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 10181-6 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.815.

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 framework*

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

Introduction

Many open systems applications have security requirements which depend upon the integrity of data. Such requirements may include the protection of data used in the provision of other security services such as authentication, access control, confidentiality, audit and non-repudiation, that, if an attacker could modify them, could reduce or nullify the effectiveness of those services.

The property that data has not been altered or destroyed in an unauthorized manner is called integrity. This Recommendation | International Standard defines a general framework for the provision of integrity services.

INTERNATIONAL STANDARD

ITU-T RECOMMENDATION

INFORMATION TECHNOLOGY – OPEN SYSTEMS INTERCONNECTION – SECURITY FRAMEWORKS FOR OPEN SYSTEMS: INTEGRITY FRAMEWORK

1 Scope

The Recommendation | International Standard on Security Frameworks for Open Systems addresses the application of security services in an Open Systems environment, where the term "Open System" 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 may be 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.

This Recommendation | International Standard addresses the integrity of data in information retrieval, transfer, and management:

1) defines the basic concept of data integrity;
2) identifies possible classes of integrity mechanism;
3) identifies facilities for each class of integrity mechanisms;
4) identifies management required to support the class of integrity mechanism;
5) addresses the interaction of integrity mechanism and the supporting services with other security services and mechanisms.

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

1) standards that incorporate the concept of integrity;
2) standards that specify abstract services that include integrity;
3) standards that specify uses of an integrity service;
4) standards that specify means of providing integrity within an open system architecture; and
5) standards that specify integrity mechanisms.

Such standards can use this framework as follows:

- standards of type 1), 2), 3), 4) and 5) can use the terminology of this framework;
- standards of type 2), 3), 4) and 5) can use the facilities identified in clause 7;
- standards of type 5) can be based upon the classes of mechanisms identified in clause 8.

Some of the procedures described in this security framework achieve integrity by the application of cryptographic techniques. This framework is not dependent on the use of particular cryptographic or other algorithms, although certain classes of integrity mechanisms may depend on particular algorithm properties.

NOTE – Although ISO does not standardize cryptographic algorithms, it does standardize the procedures used to register them in ISO/IEC 9979.

The integrity addressed by this Recommendation | International Standard is that defined by the constancy of a data value. This notion (constancy of a data value) encompasses all instances in which different representations of a data value are deemed equivalent (such as different ASN.1 encodings of the same value). Other forms of invariance are excluded.

The usage of the term data in this Recommendation | International Standard includes all types of data structures (such as sets or collections of data, sequences of data, file-systems and databases).

This framework addresses the provision of integrity to data that are deemed to be write-accessible to potential attackers. Therefore, it focusses on the provision of integrity through mechanisms, both cryptographic and non-cryptographic that do not rely exclusively on regulating access.

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 listed 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.*
- ITU-T Recommendation X.273 (1994) | ISO/IEC 11577:1995, *Information technology – Open Systems Interconnection – Network layer security protocol.*
- ITU-T Recommendation X.274 (1994) | ISO/IEC 10736:1995, *Information technology – Telecommunications and information exchange between systems – Transport layer security protocol.*
- ITU-T Recommendation X.810 (1995) | ISO/IEC 10181-1:1996, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Overview.*
- ITU-T Recommendation X.811 (1995) | ISO/IEC 10181-2:1996, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Authentication framework.*
- ITU-T Recommendation X.812 (1995) | ISO/IEC 10181-3:1996, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Access control framework.*

2.2 Paired Recommendations | International Standards equivalent in technical content

- ITU-T Recommendation X.224 (1993), *Protocol for providing the OSI connection-mode transport service.*

  ISO/IEC 8073:1992, *Information technology – Telecommunications and information exchange between systems – Open Systems Interconnection – Protocol for providing the connection-mode transport service.*
- 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 9979:1991, *Data cryptographic techniques – Procedures for the registration of cryptographic algorithms.*