INTERNATIONAL STANDARD

ISO/IEC 10181-5

First edition
1996-09-15

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

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

Reference number
ISO/IEC 10181-5:1996(E)

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 10181-5 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.814.

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 E of this part of ISO/IEC 10181 are for information only.

Introduction

Many Open Systems applications have security requirements which depend upon the prevention of disclosure of information. Such requirements may include the protection of information used in the provision of other security services such as authentication, access controls or integrity, that, if known by an attacker, could reduce or nullify the effectiveness of those services.

Confidentiality is the property that information is not made available or disclosed to unauthorized individuals, entities, or processes.

This Recommendation | International Standard defines a general framework for the provision of confidentiality services.

This page intentionally left blank

INTERNATIONAL STANDARD

ITU-T RECOMMENDATION

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

1 Scope

This 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 confidentiality of information in retrieval, transfer and management. It:

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

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

1) standards that incorporate the concept of confidentiality;
2) standards that specify abstract services that include confidentiality;
3) standards that specify uses of a confidentiality service;
4) standards that specify means of providing confidentiality within an open system architecture; and
5) standards that specify confidentiality 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 defined in clause 7 of this framework;
- standards of type 5) can be based upon the classes of mechanism defined in clause 8 of this framework.

As with other security services, confidentiality can only be provided within the context of a defined security policy for a particular application. The definitions of specific security policies are outside the scope of this Recommendation | International Standard.

It is not a matter for this Recommendation | International Standard to specify details of the protocol exchanges which need to be performed in order to achieve confidentiality.

This Recommendation | International Standard does not specify particular mechanisms to support these confidentiality services nor the full details of security management services and protocols. Generic mechanisms to support confidentiality are described in clause 8.

Some of the procedures described in this security framework achieve confidentiality by the application of cryptographic techniques. This framework is not dependent on the use of particular cryptographic or other algorithms, although certain classes of confidentiality 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 9979:1991, Procedures for the registration of criptographic algorithms.

This framework addresses the provision of confidentiality when the information is represented by data that are read-accessible to potential attackers. Its scope includes traffic flow confidentiality.

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.233 (1993) | ISO/IEC 8473-1:1994, *Information technology – Protocol for providing the connectionless-mode Network service: Protocol specification.*
- 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 – Telecommunication 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.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

- 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 general security-related terms defined in ITU-T Rec. X.200 | ISO/IEC 7498-1:

a) (N)-connection;

b) (N)-entity;

c) (N)-facility;

d) (N)-layer;

e) (N)-PDU;

f) (N)-SDU;

g) (N)-service;

h) (N)-unitdata;

i) (N)-userdata;

j) segmenting.

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) active threat;

b) confidentiality;

c) decipherment;

d) decryption;

e) encipherment;

f) encryption;

g) identity-based security policy;

h) key;

i) passive threat;

j) routing control;

k) rule-based security policy;

l) sensitivity;

m) traffic analysis;

n) traffic padding.

3.3 Security frameworks overview definitions

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

a) secret key;

b) private key;

c) public key.

3.4 Additional definitions

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

3.4.1 confidentiality-protected-environment: An environment which prevents unauthorized information disclosure either by preventing unauthorized data inspection or by preventing unauthorized derivation of sensitive information through data inspection. Sensitive information may include some or all of the data attributes (e.g. value, size, or existence).

3.4.2 confidentiality-protected-data: Data within a confidentiality-protected-environment.

NOTE – A confidentiality-protected environment may also protect some (or all) of the attributes of the confidentiality-protected data.

3.4.3 confidentiality-protected-information: Information all of whose concrete encodings (i.e. data) are confidentiality protected.

3.4.4 hide: An operation that applies confidentiality protection to unprotected data or additional confidentiality protection to already protected data.

3.4.5 reveal: An operation that removes some or all of previously applied confidentiality protection.

3.4.6 hiding confidentiality information: Information that is used to perform the **hide** operation.

3.4.7 revealing confidentiality information: Information that is used to perform the reveal operation.

3.4.8 direct attack: An attack on a system based on deficiencies in the underlying algorithms, principles, or properties of a security mechanism.

3.4.9 indirect attack: An attack on a system which is not based on the deficiencies of a particular security mechanism (e.g. attacks which bypass the mechanism, or attacks which depend on the system using the mechanism incorrectly).

4 Abbreviations

For the purposes of this Recommendation | International Standard, the following abbreviations apply:

HCI	Hiding Confidentiality Information
PDU	Protocol Data Unit
RCI	Revealing Confidentiality Information
SDU	Service Data Unit

5 General discussion of confidentiality

5.1 Basic concepts

The purpose of the confidentiality service is to ensure that information is available only to those authorized. Insofar as information is represented through data and insofar as data may result in contextual changes (e.g. file manipulations may result in directory changes or in changes in the number of available storage locations), information can be derived from data in a number of different ways:

1) by understanding the semantics of the data (e.g. the value of the data);
2) by using the associated attributes of the data (such as existence, date of creation, size, date of last update, etc.) to permit inferencing; and
3) by considering the context of the data, i.e. those other data objects that are associated with it; and
4) by observing the dynamic variations of the representation.

The information can be protected either by ensuring that the data is limited to those authorized or by representing the data in such a way that their semantics remain accessible only to those who possess some critical information. Effective confidentiality protection requires that the necessary control information (such as keys and other RCI) be protected. This protection may be provided by mechanisms that are different from those used to protect the data (e.g. cryptographic keys may be protected by physical means).

The notions of protected environments and of overlapped protected environments are used in this framework. Data within protected environments are protected by the application of a particular security mechanism (or mechanisms). All data within a protected environment are thus similarly protected. When two or more environments overlap, the data in the overlap are multiply protected. It may be deduced that the continuous protection of data that are moved from one environment into another must involve overlapped protected environments.

5.1.1 Protection of information

Communication or storage of information is realized by representing the information as data items. Confidentiality mechanisms protect against the disclosure of information by protecting some or all of the items listed in 5.1 above.

Ways to achieve confidentiality include:

1) prevention of the knowledge of the existence of data or of characteristics of data (such as data size or data creation date);
2) prevention of read-access to data; and
3) prevention of the knowledge of the semantics of data.

Confidentiality mechanisms protect against the disclosure of information by either:

1) protecting the representation of the information item from disclosure; or by

2) protecting the representation rules from disclosure.

In the second case, protection against disclosure of the existence or other attributes of a data item can be achieved by combining several data items into a composite data item and by protecting the representation rules of the composite object from disclosure.

5.1.2 Hide and reveal operations

The **hide** operation can be modeled as a movement of information from an environment A to the overlap (B) of A with another environment C. The reveal operation can be seen as the inverse of a hide operation. This is depicted in Annex B.

When information is moved from an environment protected by one confidentiality mechanism to an environment protected by another confidentiality mechanism:

1) if the **hide** operation of the second mechanism precedes the **reveal** operation of the first, the information is continually protected; and

2) if the **reveal** operation of the first mechanism precedes the **hide** operation of the second mechanism, the information is not continually protected.

For 1) above to be possible, some form of commutativity must exist between the **reveal** of the old mechanism and the **hide** of the new. An example in which **hide** and **reveal** operate with commutative properties occurs when one environment is protected through Access Control or physical means and the other is protected through cryptographic transformations.

Confidentiality impacts information retrieval, transfer, and management as follows:

1) confidentiality in information transfer using OSI is provided when the **hide** operation, transfer using an (N-1)-facility, and the **reveal** operation are combined to form the transmission part of an (N)-service;

2) confidentiality in data storage retrieval is provided when the **hide** operation, storage and retrieval, and the **reveal** operation are combined to form a higher level storage and retrieval service;

3) other forms of confidentiality may be provided by combining **hide** and **reveal** with other operations (e.g. those used for the purposes of data management).

With some confidentiality mechanisms, the **hide** facility makes part of the confidentiality-protected data available to the service user before the facility has completed the processing of all of the data. Similarly, with some mechanisms the **reveal** facility is able to start work on processing part of a confidentiality-protected data item before all of it is available. Thus, a data item may consist simultaneously of parts that are not yet **hidden**, parts that are **hidden**, and parts that have been **revealed**.

5.2 Classes of confidentiality services

Confidentiality services may be classified by the type of information protection they support. The types of information protection are:

1) protection of data semantics;

2) protection of data semantics and of associated attributes;

3) protection of data semantics, of their attributes, and of any information that may be derived from the data in question.

In addition, the service may be classified by the type of threats that exist in the environment in which it operates and against which the information is protected. By this criterion, services can be classified as follows:

1) *Protection against external threats*

Such services assume that those with legitimate access to the information will not divulge it to those unauthorized. Such services do not protect the information divulged to authorized parties and do not constrain the behaviour of such parties while they possess information previously protected.

Example: Sensitive files in A are protected through encryption. But processes that possess the required decryption keys may read the protected files and subsequently write to unprotected files.

2) *Protection against internal threats*

Such services assume that those authorized to have access to critical information and data may, willingly or not, carry out activities that eventually compromise the confidentiality of the information to be protected.

Example: Security labels and clearances are attached to the resources that are protected and to the entities that can access them. Accesses are restricted according to a well defined and understood flow control model.

Services that provide confidentiality protection against internal threats must either disallow covert channels (see Annex D) or restrict their information transfer rate within acceptable levels. In addition, they must disallow unauthorized inferences that may come about from the unexpected usage of legitimate information channels [such as inferences based on carefully constructed database queries – each of which is individually legitimate – or inferences based on the (in)ability of a system utility to carry out a command].

5.3 Types of confidentiality mechanisms

The objective of confidentiality mechanisms is to prevent unauthorized information disclosure. To this end, a confidentiality mechanism may:

1) Prevent access to the data (such as physical protection of a channel).

Access Control mechanisms (as described in ITU-T Rec. X.812 | ISO/IEC 10181-3) may be used to enable only authorized entities to have access to the data.

Techniques for physical protection are outside the scope of this Recommendation | International Standard. They are nevertheless included in other standards such as ISO 10202 (Security Architecture of Integrated Circuit Cards) and ANSI X9.17 / ISO 8734 (Financial Institution Key Management – Wholesale).

2) Use mapping techniques that render the information to be protected relatively inaccessible to all but those who possess some critical information about the mapping technique. Such techniques include:

a) encipherment;

b) data padding;

c) spread spectrum.

Confidentiality mechanisms of either type can be used in conjunction with other mechanisms of the same or of different types.

Confidentiality mechanisms can achieve different kinds of protection:

- protection of data semantics;
- protection of data attributes (including the existence of data); or
- protection against inferences.

Examples of these classes of mechanisms include:

1) Encipherment to conceal the data.
2) Encipherment in conjunction with segmenting and padding to conceal the length of PDUs (see 8.2).
3) Spread-spectrum techniques to conceal the existence of a communications channel.

5.4 Threats to confidentiality

There is a single, generic threat to confidentiality-protected information, namely, disclosure of the protected information. There are several threats to confidentiality-protected data, corresponding to the different ways in which confidentiality-protected information can be derived from the data. The following subclauses describe some of the threats to confidentiality-protected data in different environments.

5.4.1 Threats when confidentiality is provided through access prevention

Such threats include:

1) Penetration of the Access prevention mechanism, such as:

a) Exploiting weaknesses in physically protected channels.

b) Masquerading or using certificates inappropriately.

c) Exploiting weaknesses in the implementation of the prevention mechanism (e.g. a user might be able to request access to a file A, be granted access to A, and then modify the file name submitted so as to gain access to another file, B).

d) Embedding Trojan horses within trusted software.

2) Penetration of the services the prevention mechanism relies upon (e.g. masquerading when access is based on identity authentication, improper use of certificates, or penetration of the integrity mechanism used to protect certificates).

3) Exploitation of system utilities that may disclose, directly or indirectly, information about the system.

4) Covert channels.

5.4.2 Threats when confidentiality is provided through information hiding

Such threats include:

1) penetration of the cryptographic mechanism (be it through cryptanalysis, through purloined keys, chosen plaintext attacks, or through other means);

2) traffic analysis;

3) analysis of PDU headers;

4) covert channels.

5.5 Types of confidentiality attacks

To each of the threats enumerated above correspond one or more attacks, i.e. instantiations of the threat in question.

It is possible to distinguish between active and passive attacks, i.e. confidentiality attacks that result in system change and attacks that do not result in system change.

NOTE – Whether an attack is passive or active may be determined both by the characteristics of system under attack and by the actions carried out by the attacker.

Examples of passive attacks are:

1) eavesdropping and wiretapping;

2) traffic analysis;

3) analysis of PDU headers for purposes that are not legitimate;

4) copying of PDU data to systems other than the intended destinations.

5) cryptanalysis.

Examples of active attacks are:

1) Trojan horses (code whose undocumented features facilitate security breaches);

2) covert channels;

3) penetration of the mechanisms that support confidentiality; such as penetration of the authentication mechanism (e.g. successfully masquerading as an authorized entity), penetration of the Access Control Mechanism, and key interception;

4) spurious invocations of the cryptographic mechanisms, such as chosen plaintext attacks.

6 Confidentiality policies

A confidentiality policy is the part of a security policy which deals with the provision and use of the confidentiality service.

Data representing information whose confidentiality is protected is subject to control over which entities may read it. A confidentiality policy must therefore identify the information that is subject to controls and indicate which entities are intended to be allowed to read it.