TECHNICAL REPORT

ISO/IEC TR 13594

First edition
1995-12-15

Information technology — Lower layers security

Technologies de l'information — Modèle de sécurité pour les couches inférieures

Reference number
ISO/IEC TR 13594:1995(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.

The main task of technical committees is to prepare International Standards, but in exceptional circumstances a technical committee may propose the publication of a Technical Report of one of the following types:

— type 1, when the required support cannot be obtained for the publication of an International Standard, despite repeated efforts;

— type 2, when the subject is still under technical development or where for any other reason there is the future but not immediate possibility of an agreement on an International Standard;

— type 3, when a technical committee has collected data of a different kind from that which is normally published as an International Standard ("state of the art", for example).

Technical reports of types 1 and 2 are subject to review within three years of publication, to decide whether they can be transformed into International Standards. Technical Reports of type 3 do not necessarily have to be reviewed until the data they provide are considered to be no longer valid or useful.

ISO/IEC TR 13594, which is a Technical Report of type 3, was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, in collaboration with ITU-T. The identical text is published as ITU-T Recommendation X.802.

Introduction

This Recommendation | International Standard describes the cross layer aspects of the revision of security services in the lower layers of the OSI Reference Model (Transport, Network, Data Link, Physical). It describes the architectural concepts common to these layers, the basis for interactions relating to security between layers and the placement of security protocols in the lower layers.

TECHNICAL REPORT

ITU-T RECOMMENDATION

INFORMATION TECHNOLOGY – LOWER LAYERS SECURITY MODEL

1 Scope

This Recommendation | Technical Report describes the cross layer aspects of the provision of security services in the lower layers of the OSI Reference Model (Transport, Network, Data Link and Physical layers).

This Recommendation | Technical Report describes:

a) architectural concepts common to the lower layers based on those defined in CCITT Rec. X.800 | ISO 7498-2;

b) the basis for interactions relating to security between protocols in the lower layers;

c) the basis for any interactions relating to security between the lower layers and upper layers of OSI;

d) the placement of security protocols in relation to other lower layer security protocols and the relative role of such placements.

There should be no conflict between the security protocols for the lower layers and the model described in this Recommendation | Technical Report.

CCITT Rec. X.500 | ISO/IEC 9594-1 identifies the security services relevant to each of the lower layers of the OSI Reference Model.

2 References

The following Recommendations and International Standards contain provisions which, through reference in this text, constitute provisions of this Recommendation | Technical Report. At time of publication, the editions indicated were valid. All Recommendations and Standards are subject to revision, and parties to agreements based on this Recommendation | Technical Report 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 OSI connectionless-mode Network service: Protocol specification.*
- ITU-T Recommendation X.234 (1994) | ISO/IEC 8602:1995, *Information technology – Protocol for providing the OSI connectionless-mode Transport service.*
- 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.803 (1994) | ISO/IEC 10745:1995, *Information technology – Open Systems Interconnection – Upper layers security model.*

- ITU-T Recommendation X.810[1)] | ISO/IEC 10181-1...[1)], *Information technology – Open Systems Interconnection – Security frameworks in open systems: Security frameworks overview.*
- ITU-T Recommendation X.812[1)] | ISO/IEC 10181-3...[1)], *Information technology – Open Systems Interconnection – Security frameworks in 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.*
- 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.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 One (ASN.1).*

  ISO/IEC 8825:1990, *Information technology – Open Systems Interconnection – Specification of Basic Encoding Rules for Abstract Syntax Notation One (ASN.1).*

2.3 Additional references

- ISO/IEC 8208:1995, *Information technology – Data communications – X.25 Packet Layer Protocol For Data Terminal Equipment.*
- ITU-T Recommendation X.25 (1993), *Interface between Data Terminal Equipment (DTE) and Data Circuit-Terminating Equipment (DCE) for terminals operating in packet mode and connected to public data networks by dedicated circuits.*
- ISO 8648:1988, *Information processing systems – Open Systems Interconnection – Internal organization of the Network Layer.*
- ISO 9542:1988[2)], *Information processing systems – Telecommunications and information exchange between systems – End system to intermediate system routeing exchange protocol for use in conjunction with the Protocol for providing the connectionless-mode network service (ISO 8473).*
- ISO/IEC 10589:1992, *Information technology – Telecommunications and information exchange between systems – Intermediate system to intermediate system intra-domain-routeing routine information exchange protocol for use in conjunction with the protocol for providing the connectionless-mode Network service (ISO 8473).*
- ISO/IEC 10747:1994, *Information technology – Telecommunications and information exchange between systems – Protocol for exchange of inter-domain routeing information among intermediate systems to support forwarding of ISO 8473 PDUs.*

3 Definitions

3.1 OSI Reference Model definitions

This Recommendation | Technical Report makes use of the following terms as defined in ITU-T Rec. X.200 | ISO/IEC 7498-1:

- Quality of Service

---

1) Presently at the stage of draft.

2) Currently under revision.

3.2 Open System Security Frameworks definitions

This Recommendation | Technical Report makes use of the following terms as defined in ITU-T Rec. X.810 | ISO/IEC 10181-1:

– security domain

3.3 Internal Organization of the Network Layer definitions

This Recommendation | Technical Report makes use of the following terms as defined in ISO 8648:

a) subnetwork access protocol;

b) end system;

c) intermediate system.

3.4 Additional definitions

For the purposes of this Recommendation | Technical Report, the following definitions apply:

3.4.1 reflection protection: A protection mechanism to detect when a protocol data unit has been sent back to the originator.

3.4.2 security association attributes: The collection of information required to control the security of communications between an entity and its remote peer(s).

3.4.3 security association: The relationship between lower layer communicating entities for which there exists corresponding security association attributes.

3.4.4 security rules: Local information which, given the security services selected specify the underlying security mechanisms to be employed, including all parameters needed for the operation of the mechanism.

NOTE – Security rules are a form of secure interaction rules as defined in the Upper Layers Security Model (ITU-T Rec. X.803 | ISO/IEC 10745).

4 Abbreviations

ISN	Integrity Sequence Number
SSAA	Set of SA-Attributes
NLSP	Network Layer Security Protocol
NLSP-CO	NLSP Connection mode
NLSP-CL	NLSP Connectionless mode
QOS	Quality of Service (as defined in CCITT Rec. X.200 | ISO/IEC 7498-1)
SA	Security Association
SA-ID	Security Association Identifier
SNAcP	Subnetwork Access Protocol (as defined in ISO 8648)
SNISP	Subnetwork Independent Security Protocol
TLSP	Transport Layer Security Protocol

5 Security associations

5.1 General overview

5.1.1 Any security protocol makes use of a number of security mechanisms to provide security services to the layer above. The security services required by the higher layer may be indicated to the lower layers through use of local security management functions. The security protocol and each of its security mechanisms require information, in addition to that which is encoded in the PDUs, to enable secure communication. Examples of such additional

information are the specification of the mechanisms to be used by the protocol and, for each mechanism, specific information such as the key required by an encipherment mechanism. Each piece of additional information is known as a Security Association Attribute.

5.1.2 Security Association Attributes may be placed in a protocol entity using a number of mechanisms. Some examples of placement mechanisms are:

a) placement during manufacture of a device;

b) placement during initialisation of a device;

c) placement via a manual interface, e.g. front panel controls;

d) placement by OSI Systems Security Management;

e) placement by OSI Layer Security Management;

f) placement by OSI Operations Security Management.

5.1.3 SA-Attributes may be placed at any time prior to the communication to which they relate. When compatible Sets of SA-Attributes (SSAA) are in place in each protocol entity, a Security Association is said to exist between the protocol entities.

5.1.4 SSAAs (and Security Associations) may exist with different granularity. Sometimes it is useful to be able to refer to SSAAs with different granularity. For instance, the SSAA defined by an Agreed Set of Security Rules (ASSR) could be denoted by SSAA ASSR. Or a pairwise key may be established between two protocol entities for use over a number of instances of common Source-Destination Address Pair. Similarly the SSAA for an instance of communication could be referred to by SSAA-Instance of Communication. Likewise the SSAA for a connection oriented PDU could be referred to by SSAA CO PDU.

5.1.5 In general, SA-Attributes must be placed in the Protocol Entity by secure means in order to maintain security. This implies that the SA-Attributes are either placed using a physically secure means or they may be placed making use of an existing Security Association which has been pre-placed for this purpose.

5.1.6 The SSAA which are part of a security association are often referred to by an identifier which has local significance and is known as an SA-ID. At any instant, some members of the Set of SA-Attributes may be undefined. Typically during the initialisation of a secure communication, the SSAA will not be fully populated and the initial exchanges will be used to completely populate the SSAA before user data is exchanged.

5.1.7 In order to provide Replay Protection, constraints must be applied to the use of SA-IDs, their referenced SSAAs and SA-Attributes.

a) SA-IDs may not be re-used with the same encipherment key.

b) After any SA-Attribute has been populated in a SSAA which is referred to by an SA-ID, that SA-Attribute may never be changed unless the security protocol has a means for signalling the change between the communicating entities. This implies that to enable key roll-over a new SA-ID must be used with copies of the old SA-Attributes and a new key unless the security protocol has an alternative means of signalling the key change (e.g. as supported by NLSP-CO CSC PDU).

5.1.8 Removal of any SA-Attribute from the SSAA effectively closes the Security Association

5.1.9 Some SA-Attributes have significance for an instance of communication (a connectionless PDU or a connection). Other SA-Attributes have significance for a single PDU on a connection. Examples of such SA-Attributes are Integrity Sequence Numbers and Security Labels. It may appear that the changing of these SA-Attributes violates the constraint in b) in 5.1.7 above. However, logically the Security Association, including these SA-Attributes, is only valid for the lifetime of a single PDU. The ISN acts as a logical extension to the SA-ID, hence changing the effective SA-ID. The label is only valid for this instance of the extended SA-ID. Thus, the constraints are maintained. Such SA-Attributes are sometimes termed 'Dynamic' SA-Attributes.

5.1.10 Part of a security policy will constrain the operation of the protocol entity. This part of the security policy is termed the Set of Security Rules for the Protocol Entity. The Set of Security Rules for a protocol entity may constrain such things as the security mechanisms to be used and the values and placement mechanisms for the SA-Attributes. The Set of Security Rules will also define the mapping of the security services selected into Security mechanisms used by the Security Protocol. The Set of Security Rules is a form of Secure Interaction Rules.

5.1.11 When used for operation within or between domains, a unique identifier for such Sets of Security Rules needs to be established and is known as an Agreed Set of Security Rules. The ASSR identifier may be exchanged as part of Security Association establishment to define or constrain the SSAA ASSR which are defined in that Set of Security Rules. The remaining SA-Attributes, if any, must be established using other means such as those listed in 5.1.2 above.

5.2 Establishing a security association for the lower layers

5.2.1 In order to protect an instance of communication (a connectionless SDU or a connection) a security association has to be established between the communicating entities.

5.2.2 The information forming an SA is either static information, which may be "negotiated" when the SA is established and then remains fixed for the duration of the association, or dynamic information which may be updated in an instance of communication.

5.2.3 An SA may be established as a OSI layer 1 to 4 protocol through the exchange of security association protocol data units (PDUs), or through mechanisms outside the scope of the lower layers of OSI.

5.2.4 Prior to establishing an SA each entity must have pre-established a common, mutually agreed and uniquely identified, set of security rules as well as the security services that may be selected.

5.2.5 If the SA is to be established through the exchange of security association PDUs, then the following must also be pre-established:

a) An initial selection of security services, and hence the security mechanisms, to be applied in establishing an SA.

b) Basic keying information needed to establish an SA.

5.2.6 On SA establishment, an entity establishes the following shared information with its remote peer which must remain unchanged (i.e. static) for the lifetime of the association:

a) Local and remote SA-IDs.

b) The Security Services Selected for use between the associated entities for instances of communication.

NOTE – The security services to be used may be selected among the pre-established security services.

c) The mechanisms and their properties to be used as implied through the Security Services Selected.

d) Initial shared keys for integrity, encipherment mechanisms and authentication of an instance of communication;

e) The set of security labels and addresses that may be used on this association for access control.

5.2.7 The SA-IDs and shared keys [items a) and d) above] must be established on a per association basis. The other information may be pre-established. In addition, as part of establishing a SA the identity of the remote peer must be authenticated to provide peer entity authentication.

5.2.8 The following information can be dynamically updated for an instance of communication:

a) Integrity sequence number(s) as needed for normal and expedited data in each direction.

b) A security label which is selected dynamically from the static set of security labels.

c) Re-key information for the encipherment/integrity mechanisms in security protocols supporting re-keying within an association (e.g. the connection-mode Network Layer Security Protocol).

5.2.9 To achieve peer entity or data origin authentication, authentication mechanisms need to be applied to each instance of communication.

5.2.10 The different SA-Attributes that may be established at the different stages of a security association are shown diagrammatically as in Figure 1. The terms pre-established, static and dynamic are used in relation to a security association as described in the preceding subclauses. The terms used and the form of authentication are as described in the preceding subclauses.

Pre-established	Static	Dynamic
Agreed Set of Security Rules Possible Security Services Initial Security Services Basic key information	SA-IDs Initial Keys Authentication	ISN Security Label Re-key information Authentication
Selected level of Protection QOS Selected mechanism Security label / Address set		

Figure 1 – Illustration of Attributes of a Security Association

5.2.11 An entity should identify necessary SA-Attributes using the SA-ID.

5.2.12 The SA shall be established prior to protecting an instance of communication.

5.3 Security association close

An SA indicated by an SA-ID is closed when the SA is no longer valid.

A security association can be closed by the following methods:

a) as a OSI layer 1 to 4 protocol through the exchange of security association protocol data units (PDUs);

b) using external mechanisms outside the scope of the lower layers of OSI;

c) implicitly by closing a connection (this is applicable only to connection mode);

d) implicitly when a key within the SA expires.

NOTE – Care should be taken in using this approach d) with the lifetime of a key defined by the number of packets sent/received between peer entities since significantly different values may result in each peer.

Before using method c) above, an attribute of the security association must indicate that the association is to be closed on closing a connection using that association.

5.4 Modification of attributes in a connection

For each instance of communication (a connectionless PDU or a connection), only one SA can be established.

During the existence of a connection the security services and mechanisms used on that connection cannot be modified (note this does not preclude changing keys).

Indication of use of new keys shall be described by the security protocol.

6 Influence on existing protocols

6.1 General principle

In principle the influence of security protocols on existing protocols should be minimal.

6.2 Connectionless SDU size

During data transfer, depending on the security mechanisms selected, security has the following impact on the (N)-layer protocol:

a) the (N)-user-data, and in some cases parts of the (N)-protocol-control-information, is operated on by cryptographic transformations before and after transmission. This may change the length of the (N)-user-data.

b) protocol control information related to (N)-user-data (e.g. security association identifier, cryptographic check code) may need to be carried by the (N)-protocol.

NOTE – This will have impact on the maximum User Data size as defined in CCITT Rec. X.213 | ISO/IEC 8348, subclause 15.2.3 and CCITT Rec. X.214 | ISO/IEC 8072.

6.3 Concatenation of PDUs

Only PDUs which are to be protected under the same security association may be concatenated.

6.4 Algorithm and mechanism independence

Lower layer security protocols are specified to be independent of the algorithm. Furthermore, NLSP has taken the approach of separating mechanism dependent and mechanism independent parts of the security protocol. It is anticipated that future lower layer security protocols may achieve this using generic abstract services for security common to the upper and lower layers of OSI.

7 Common security PDU structure

7.1 A common general PDU structure is to be used for protected data PDUs in the lower layer security protocols. Although the general PDU structure is the same for all lower layer security protocols they are not, of course, identical for a variety of reasons, the most obvious of which is the format restrictions imposed by a particular protocol layer.

7.2 Common aspects of the PDU structures in the lower layer security protocols may be:

a) an Integrity Check Value (ICV) at the end of the PDU (except for any encipherment padding, see below);

b) padding for traffic flow confidentiality, integrity and encipherment mechanisms may be placed in separate fields;

c) a variable length number used for sequence integrity;

d) a flexible approach to the encoding of fields using type/length/value to allow easy extendibility and place minimal restrictions on the ordering of fields;

e) reflection protection provided by a protected SA initiator to responder direction flag.

8 Determination of security services and mechanisms

The security services to be applied by a security protocol are determined as described in clause 9. The security mechanisms to be applied are determined, given Security Services Selected, through use of security rules as described in clause 10.

9 Protection QOS

Protection QOS is the degree to which a service provider attempts to counter security threats using security services applied in the lower layers.

The handling of protection QOS service parameters is a local matter controlled according to the security policy in force. Protection QOS is not negotiated between the service users. For an instance of communication a service user may indicate its protection QOS requirements to the service provider. A service provider may indicate the protection QOS provided on an instance of communication to the service user. The protection QOS provided by the service provider need not be the same as that requested by the service user.

Any lower layer protocol exchanges between open systems (referred to as "in band" protocol exchanges) to convey information on the security services to be selected are carried in a security association protocol which is independent of an instance of communication. This may be carried implicitly by a security label or explicitly by other means.

10 Security rules

Security rules, given the security services selected, specify the security mechanisms to be used including all parameters needed for the operation of the mechanisms. An illustrative example of security rules which may be registered as agreed for use by a community is given in Annex A.

In the case of the security services selected being implied by a security label, the security rules also specify the mapping from a security label to the implied protection requirements.

NOTE – Currently, ITU-T | ISO/IEC are not standardising security rules.

11 Placement of security in the lower layers

Security Protocols are currently defined for use in the transport layer and the network layer [Transport Layer Security Protocol (TLSP) and Network Layer Security Protocol (NLSP)].

For connection mode communications TLSP operates in conjunction with ITU-T Rec. X.224 | ISO/IEC 8073 (see Figure 2). For connectionless mode communications TLSP operates in conjunction with ITU-T Rec. X.234 | ISO/IEC 8602 (see Figure 3).