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

		Page
1	Scope	1
2	References	1
	2.1 Identical Recommendations | International Standards	1
	2.2 Paired Recommendations | International Standards equivalent in technical content	2
	2.3 Additional references	2
3	Definitions	2
	3.1 OSI Reference Model definitions	2
	3.2 Open System Security Frameworks definitions	3
	3.3 Internal Organization of the Network Layer definitions	3
	3.4 Additional definitions	3
4	Abbreviations	3
5	Security associations	3
	5.1 General overview	3
	5.2 Establishing a security association for the lower layers	5
	5.3 Security association close	6
	5.4 Modification of attributes in a connection	6
6	Influence on existing protocols	6
	6.1 General principle	6
	6.2 Connectionless SDU size	6
	6.3 Concatenation of PDUs	6
	6.4 Algorithm and mechanism independence	6
7	Common security PDU structure	7
8	Determination of security services and mechanisms	7
9	Protection QOS	7
10	Security rules	7
11	Placement of security in the lower layers	7
12	Use of (N-1)-layer(s) to enhance (N)-layer security	13
13	Security labelling	13
14	Security domains	13
15	Security of routeing	13
16	Security Management	14
	16.1 Security policy	14
	16.2 Security association management	14
	16.3 Key management	14
	16.4 Security Audit	14
17	Traffic flow confidentiality	14
18	Guidelines for the definition of SA-Attributes	15
19	Error handling	15
Annex A – Illustrative example of an Agreed Set of Security Rules		16

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.

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.*

---

[1] Presently at the stage of draft.

[2] Currently under revision.