International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1031

(03/2008)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Telecommunication security

Roles of end users and telecommunications networks within security architecture

Recommendation ITU-T X.1031

ITU-T X-SERIES RECOMMENDATIONS

DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

PUBLIC DATA NETWORKS	
Services and facilities	X.1–X.19
Interfaces	X.20–X.49
Transmission, signalling and switching	X.50–X.89
Network aspects	X.90–X.149
Maintenance	X.150–X.179
Administrative arrangements	X.180–X.199
OPEN SYSTEMS INTERCONNECTION	
Model and notation	X.200–X.209
Service definitions	X.210–X.219
Connection-mode protocol specifications	X.220–X.229
Connectionless-mode protocol specifications	X.230–X.239
PICS proformas	X.240–X.259
Protocol Identification	X.260–X.269
Security Protocols	X.270–X.279
Layer Managed Objects	X.280–X.289
Conformance testing	X.290–X.299
INTERWORKING BETWEEN NETWORKS	
General	X.300–X.349
Satellite data transmission systems	X.350–X.369
IP-based networks	X.370–X.379
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	
Networking	X.600–X.629
Efficiency	X.630–X.639
Quality of service	X.640–X.649
Naming, Addressing and Registration	X.650–X.679
Abstract Syntax Notation One (ASN.1)	X.680–X.699
OSI MANAGEMENT	
Systems Management framework and architecture	X.700–X.709
Management Communication Service and Protocol	X.710–X.719
Structure of Management Information	X.720–X.729
Management functions and ODMA functions	X.730–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	
Commitment, Concurrency and Recovery	X.850–X.859
Transaction processing	X.860–X.879
Remote operations	X.880–X.889
Generic applications of ASN.1	X.890–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
TELECOMMUNICATION SECURITY	**X.1000–**

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T X.1031

Roles of end users and telecommunications networks within security architecture

Summary

Recommendation ITU-T X.1031 provides guidance for applying the concepts of Recommendation ITU-T X.805 architecture to divide security controls between the telecommunication networks (including service provider's and/or application provider's networks) and the end user's equipment. The Recommendation also defines the factors to be taken into account in setting up or dividing the interaction of security controls between the telecommunication network and the users. In addition, a classification of security controls for telecommunication is given.

Source

Recommendation ITU-T X.1031 was approved on 22 March 2008 by ITU-T Study Group 17 (2005-2008) under Recommendation ITU-T A.8 procedure.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure e.g. interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

CONTENTS

Recommendation ITU-T X.1031

Roles of end users and telecommunications networks within security architecture

1 Scope

1.1 Security support in the telecommunication systems is essential for the telecommunication operators and for the users of their services. Because of this, security controls must be implemented in the telecommunication network as well as in the end-user terminals. Such controls are to support the security solutions, defined according to a security policy, in the environment of the user-to-user communication. [ITU-T X.805] defines security architecture for systems providing end-to-end communications.

This Recommendation provides guidance on applying the concepts of [ITU-T X.805] with a focus on the specifics of the use of X.805 for securing the networks and the end-user equipment.

1.2 Division of the security controls between the network and its users meets a common architectural layout of the telecommunication systems, where user premises equipment is strictly separated from the network at the infrastructure layer.

1.3 Relations between the user and the network (the communication operator) have certain regulatory and technical aspects. This Recommendation deals solely with the technical aspects.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T X.805]	Recommendation ITU-T X.805 (2003), *Security architecture for systems providing end-to-end communications*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 quality of service [b-ITU-T E.800]: The collective effect of service performance which determines the degree of satisfaction of a user of the service.

NOTE 1 – The "quality of service" is characterized by the combined aspects of service support performance, service operability performance, serveability performance, service security performance and other factors specific to each service.

NOTE 2 – The term "quality of service" is not used to express a degree of excellence in a comparative sense nor is it used in a quantitative sense for technical evaluations. In this case, a qualifying adjective (modifier) should be used.

3.1.2 security controls (based on [b-ISO/IEC TR 19791]): The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the data confidentiality, data integrity, and availability of the system and its information.

NOTE – This definition is intended to include controls that provide accountability, access control, authentication, non-repudiation, communication security, and privacy, which are sometimes considered as distinct from data confidentiality, data integrity and availability.

3.1.3 **security dimension** (based on [ITU-T X.805]): A set of security measures designed to address a particular aspect of the network security. There exist eight such sets identified to protect against all major security threats. These dimensions are not limited to the network, but extend to applications and end user information as well. The security dimensions are: (1) access control, (2) authentication, (3) non-repudiation, (4) data confidentiality, (5) communication security, (6) data integrity, (7) availability, and (8) privacy.

3.1.4 **security layers** (based on [ITU-T X.805]): A hierarchy of network equipment and facility groupings to which the security dimensions must be applied. There are three security layers identified: infrastructure security layer, services security layer, and application security layer.

3.1.5 **security plane** (based on [ITU-T X.805]): A certain type of network activity protected by security dimensions. There are three security planes identified: management plane, control plane, and end-user plane.

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

N-D	Network security controls – Dependent on UNI
N-I	Network security controls – Independent from UNI
QoS	Quality of Service
U-D	User security controls – Dependent on UNI
U-I	User security controls – Independent from UNI
UNI	User-Network Interface

5 Conventions

None.

6 Applying the X.805 concepts to the networks and end-user equipment

6.1 Three security layers in a network and in the end-user equipment

6.1.1 According to [ITU-T X.805], there are three different hierarchical security layers in a telecommunication system:

- infrastructure security layer;
- services security layer;
- applications security layer.

These security layers protect three types of telecommunication system activities:

- management plane;
- control plane;
- end-user plane.

6.1.2 The above-listed concepts of the security architecture are applicable to both, the network and the end-user equipment as illustrated by Figure 1. User-network interface is supported by the subscriber line, which may be wireline or wireless.

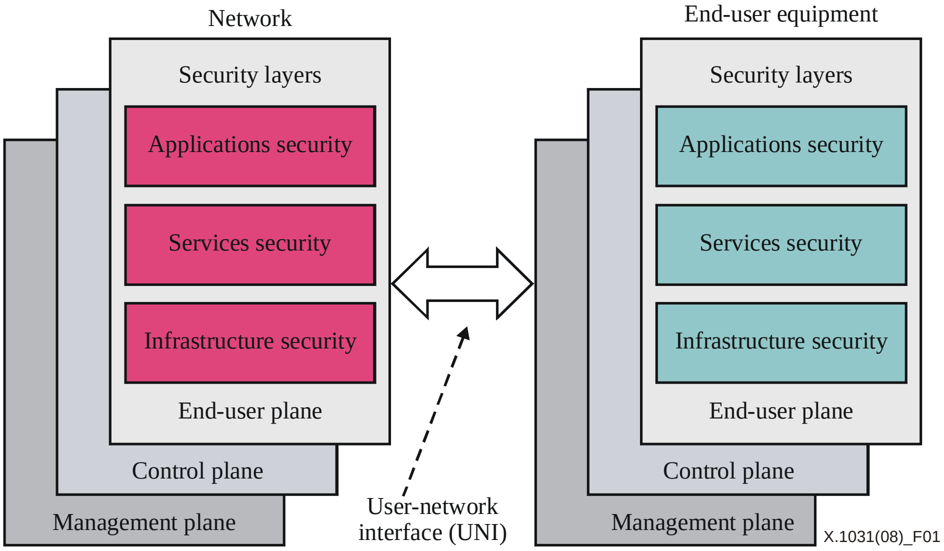

Figure 1 – Applying the concepts of X.805 to the network and to the end-user equipment

6.1.3 In line with clause 6.1.2, there are functionality layers defined for a network and for the end-user equipment as depicted in Figure 2:

– infrastructure layer;

– services layer;

– applications layer.

The following elements will correspond to these layers:

a) technical facilities of the infrastructure providers, service providers and application providers within the network;

b) technical facilities for the use of the infrastructure, services and applications at the end-user equipment.

A more detailed description of the possible technical facilities composition of network and user is offered in Annex A.

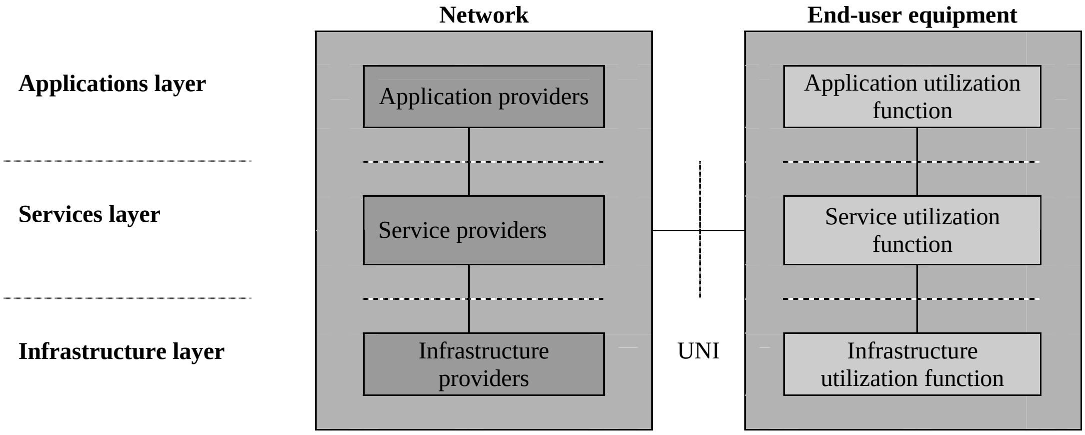

Figure 2 – Three functionality layers in network and at user end

6.1.4 The numerous users with different terminal types, requirements in term of quality of service, security requirements, etc., could be connected to the same network.

6.1.5 An important element of the system comprising the network and the end-user equipment (see Figures 1 and 2) is the user-network interface (UNI). This interface divides the user's and network's technical facilities (including the security controls), and, at the same time, it facilitates interaction between these technical facilities.

6.2 Classification of security controls in telecommunication

6.2.1 The architectural approach under consideration in this Recommendation provides for the introduction of an additional classification of the security controls in telecommunication.

6.2.2 Taking into account the location of security controls, they may be divided into three groups:

- Group N (network security controls): security controls that may be used in the network;
- Group U (user security controls): security controls that may be used by the user;
- Group NU (network and user security controls): security controls that may be used in the network and by the user.

6.2.3 Considering interrelations of both the network and user security controls with the user-network interface (UNI), Groups N, U and NU could be split further into six classes (see Figure 3), as follows:

- Class N-I (network security controls – Independent from UNI): The security controls implemented in the network and unrelated to the UNI interface;
- Class N-D (network security controls – Dependent on UNI): The security controls implemented in the network and related to the UNI interface;
- Class U-I (user security controls – Independent from UNI): The security controls realized at the user end and unrelated to the UNI interface;
- Class U-D (user security controls – Dependent on UNI): The security controls realized at the user end and related to the UNI interface;
- Class NU-I (network and user security controls – Independent from UNI): The security controls that may be used in the network and by the user and unrelated to the UNI interface;
- Class NU-D (network and user security controls – Dependent on UNI): The security controls that may be used in the network and by the user and related to the UNI interface.

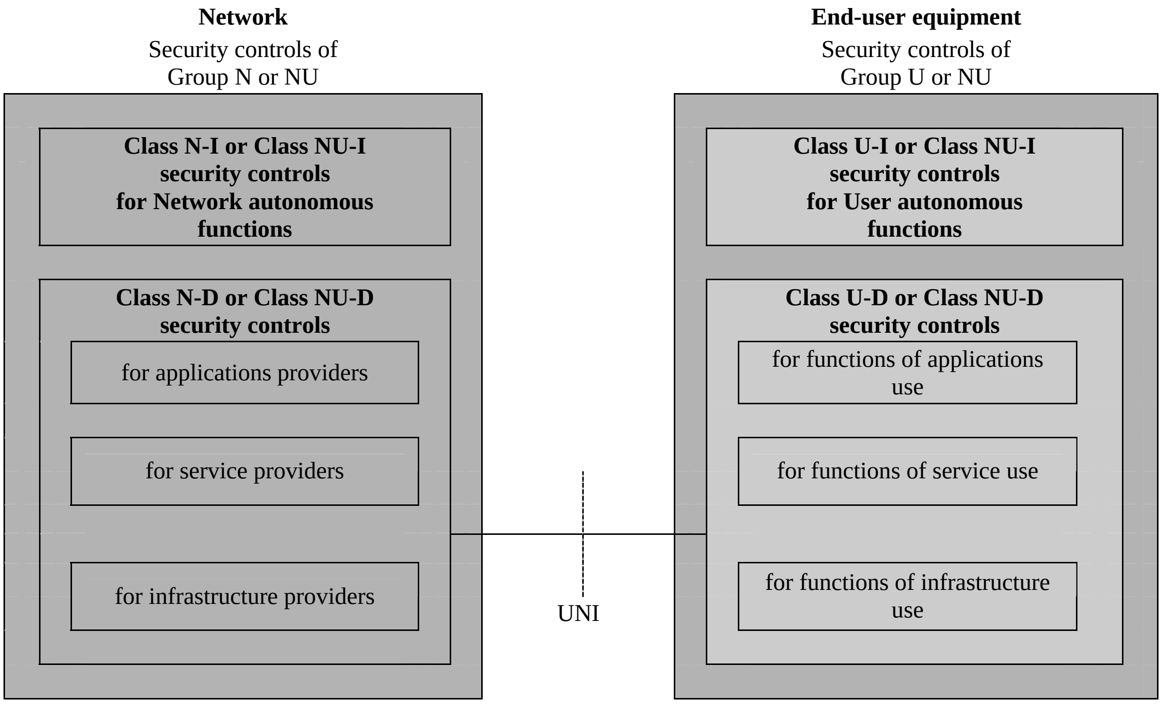
Network
Security controls of Group N or NU
Class N-I or Class NU-I security controls for Network autonomous functions
Class N-D or Class NU-D security controls
for applications providers
for service providers
for infrastructure providers
UNI
End-user equipment
Security controls of Group U or NU
Class U-I or Class NU-I security controls for User autonomous functions
Class U-D or Class NU-D security controls
for functions of applications use
for functions of service use
for functions of infrastructure use

Figure 3 – Six Classes of the security controls for Groups N, U and NU

6.2.4 Classes N-D, U-D and NU-D security controls should operate in coordination with each other through a UNI according to standardized protocols. These controls are used for performing the major tasks of security assurance in the connection between users.

6.2.5 The security controls of Classes N-I, U-I and NU-I may be selected and operated independently. These controls are orientated to the protection of autonomous functions of the network and users correspondingly.

For network, in particular, this Recommendation is to use security controls of Class N-I:

– the system of various passwords for the telecom personnel, limiting access to the network software and resources;

– the functions of a response team in reaction to any security-related incidents.

User is recommended, in particular, to adhere to the Class U-I security controls:

– utilization of a password providing access to a terminal unit;

– making sure that every incoming information-carrying medium is void of viruses and the recorded information provides integrity.

It is pointed out that such controls of network and controls of user do not need coupling through a user-network interface (UNI).

6.3 Roles of network and users

6.3.1 To divide the security controls between the network and the user, it is expedient to take into account the similarities and differences in their roles when establishing communication.

6.3.2 The main similarity between the network and the user is a formation of an inter-related chain of protocols. In addition, both fulfil the integral task of transferring the user's information. The overall security of a user-network-user chain of protocols is determined by the least secure element in that chain. Given that, the security controls providing strong protection elsewhere will be used ineffectively. For this reason, both network and user security controls must operate in the framework of an integral security system. [ITU-T X.805] describes security from an end-to-end perspective.

6.3.3 The similarity may be attributed to the fact that both the network and the user may be targets for the threat to security. On the other hand, both the network and the user may be sources of security threats.

6.3.4 The difference may be attributed to the fact that a single network is an object of collective usage, whereas a multitude of users are objects of individual usage. Due to this reason, the possibilities to realize security facilities for the network and the user are different when taking into account the regulatory requirements, and financial and operational limitations.

6.3.5 The difference may be attributed to actual applicable security policies. Specific requirements to be met by the network are defined by a single security policy (or by coordinated consistent security policies of some interoperating networks belonging to individual operators). Networks have to meet some minimal security specifications and may offer higher security degrees, as well. Specific requirements to be met by users may be defined by separate security policies of various organizations of users. Such separate policies may differ, but must be correlated with a security policy of network used.

6.3.6 The main difference between the network and the end-user equipment is that the network provides telecommunication services, whereas the end-user equipment enables to use them. According to [b-ITU-T G.1000], security is one of the important criteria of the quality of service (QoS) to user alongside with certain other criteria (speed, accuracy, availability, reliability, simplicity and flexibility).

6.3.7 Taking into account that security in telecommunication is a criterion of QoS, "security service" word-combination should not be used in new ITU-T Recommendations relating to telecommunication security to avoid expressions like "security service X for telecommunication service Y".

NOTE – The "service for security" word-combination is acceptable in case when this service is provided to security system by an external organization (service of outsourcing).

6.4 Applicability of the security architecture components to network and users

6.4.1 The security architecture for the telecommunication system depicted in [ITU-T X.805] defines the most common viewpoints on security. Namely, it defines a list of the security threats and a structure of the main elements of a telecommunication system, which altogether ensure security; it also defines interrelation among these elements. In particular, [ITU-T X.805] defines the following elements:

– security layers,

– security planes,

– security dimensions.

All of them may be applied to networks, but not all of them are likely to be applied to users. Thus, it is advisable to consider every threat and each above-mentioned element with regard to users. Clause 9 of [ITU-T X.805] states that, depending on a given network's security requirements, it might not be necessary to have all architectural elements implemented (that is to have a complete set of security dimensions, security layers, and security planes). The tables noted below show the applicability of actions taken by the service provider for the threats towards the network (service provider) and user (receiver of service) which should be specified by the security policies.

Tables 1, 2, 3 and 4 have been drawn up, taking into account the definitions of security elements provided in [ITU-T X.805]. These tables help to specify distinctions in the roles of the network and the user and to divide the security controls between the network and its users.

6.4.2 Table 1 reflects the five types of security threats described in [ITU-T X.805], and demonstrates their applicability to the networks and the end-user equipment. A threat source may be attributed to a network, the end-user equipment or an external object.

In Tables 1, 2, 3 and 4 the mark "+" implies applicability of the appropriate security element, and the mark "–" implies non-applicability of the security element.

Table 1 – Security threats

Threat	Threat description from X.805	Applicability	
		Network	End-user equipment
Destruction	Destruction of information and/or other resources	+	+
Corruption	Corruption or modification of information	+	+
Removal	Removal, theft, or loss of information and/or other resources	+	+
Disclosure	Information disclosure	+	+
Interruption	Interruption of service	+	+

6.4.3 Table 2 reflects the three security layers and also represents their applicability to the network and the end-user equipment. Referring to Table 2, the "Applications security layer" does not apply to the network, when there are no application servers in the network. The "Infrastructure security layer" does not apply to the user when the user does not use control of the infrastructure.

Table 2 – Security layers

Security layers from X.805	Applicability	
	Network	End-user equipment
Infrastructure security layer	+	+ or – (Note 1)
Services security layer	+	+
Applications security layer	+ or – (Note 2)	+
NOTE 1 – Absent when the user does not use control of the infrastructure. NOTE 2 – Absent when there are no application servers in the network or applications running on the user device.		

6.4.4 Table 3 reflects the three security planes and also represents their applicability to the network and the user. Referring to Table 3, the "Management security plane" does not apply to the user, when the user does not use the infrastructure/service/applications management in the network.

Table 3 – Security planes

Security planes from X.805	Applicability	
	Network	**End-user equipment**
Management security plane	+	+ or – (Note)
Control security plane	+	+
End-user security plane	+	+
NOTE – Absent when the network is not using the management of the user's equipment or when the user does not use the infrastructure/service/applications management in the network.		

6.4.5 Table 4 reflects the eight security dimensions. They are sets of security measures for protection of a telecommunication system from different threats. In addition, the table highlights the applicability of the security dimensions to the network and to the user. The table shows that not every security dimension may be implemented at the user end. This simplifies the division of the security controls between the network and the user.

Table 4 – Security dimensions

Security dimensions from X.805 (Note 1)	Applicability	
	Network	**End-user equipment**
Access control	+	+ or – (Note 2)
Authentication	+	+ or – (Note 2)
Non-repudiation	+	–
Data confidentiality	+	+
Communication security	+	–
Data integrity	+	+
Availability	+	–
Privacy	+	+
NOTE 1 – In compliance with the security policy, it is not that every single security dimension may be applicable. NOTE 2 – Applicable at the user end, if the network's security controls are not adequate.		

7 Capabilities for further division of the security controls

7.1 This Recommendation defines the factors influencing the division of the security controls between the main telecommunication elements: namely, between the network and the users. It should be noted that within these main elements, it is also possible to divide the security controls among their component segments (see Figure 4).

7.2 Consideration of the factors which have to be taken into account during such a division is not within the scope of this Recommendation.

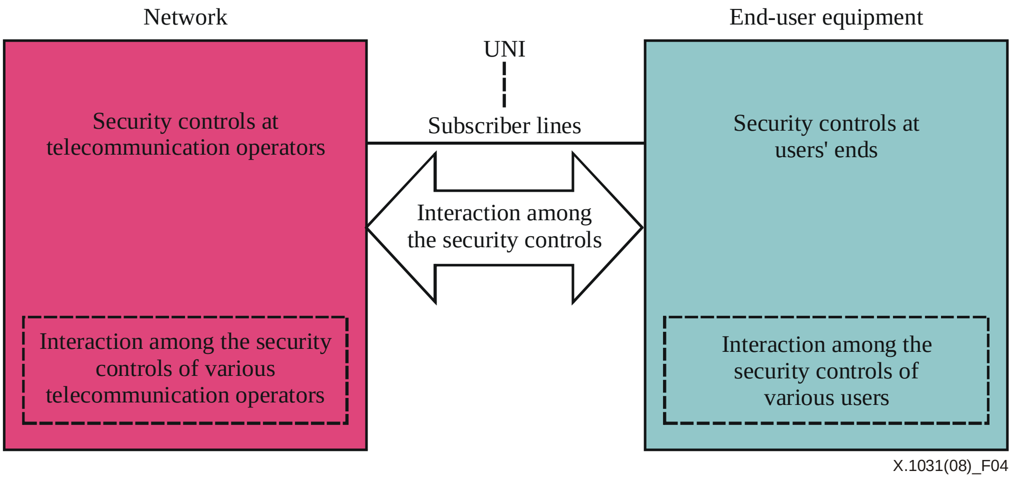
Network
End-user equipment
UNI
Subscriber lines
Security controls at telecommunication operators
Security controls at users' ends
Interaction among the security controls
Interaction among the security controls of various telecommunication operators
Interaction among the security controls of various users
X.1031(08)_F04

Figure 4 – Capabilities for further division of the security controls inside network and in end-user equipment

8 Relationship to other ITU-T Recommendations concerning security

8.1 It is recommended that any detailed ITU-T Recommendations where the aspects of the telecommunication system security are standardized should take into account the factors defined in this Recommendation. These factors would help to split/integrate the security controls located in the network and at the user ends. It is recognized that this Recommendation addresses the division of security controls across one of the many interfaces in modern telecommunications networks.

8.2 Division of security controls between the user and the network, within the end-to-end context provided by [ITU-T X.805], may be useful, for example, in the following cases:

– **separate standardization** and **design engineering** of a security control for the terminals and network devices, which are usually produced by various manufacturers;

– **division of responsibility** for service security between the telecommunication operator (an infrastructure provider and/or service provider and/or applications provider) and the end user in the operational environment;

– facilitating the issue of **notifying a law-enforcement authority** about illegal security violations from sources of different types:

a) the first source – telecommunication operators (they are few);

b) the second source – users (they are many).

8.3 Diversity of security threats and that of mechanisms of protection against them prevents the formulation of general rules for dividing the security controls between the network and the users. Specific solutions, which will take into consideration the security requirements, the type of a telecommunication network, and the protection mechanisms selected, could be formulated in detailed security Recommendations with reference to the concepts of this Recommendation.

8.4 Detailed Recommendations should specify whether a security controls solution in question is allocated:

– solely to network (to Group N); or

– solely to users (to Group U); or

– both to network and users (to Group NU).

Such an indication will make it easier to understand the location of any security controls offered within the general architecture of the telecommunication system.

It is recommended, in this case, to rely upon the security controls classification offered in clause 6.2.3 (Classes NU-I, NU-D, N-I, N-D, U-I, U-D). For Classes NU-D, N-D and U-D, it will be necessary to provide specifications of the UNI interface with respect to security.

8.5 In the event that a security control under consideration is capable of supporting more than one security degree, all the degrees should be somehow named. In case where the network is capable of supporting different security degrees to users, a supplementary service should be defined allowing the user to request a required security degree (for instance, this could be a supplementary service "security degree option").

Annex A

Possible composition of technical facilities of network and users

(This annex forms an integral part of this Recommendation)

A.1 This Recommendation uses the term "network" to cover the following facilities of the telecommunication operators:

– facilities of the infrastructure providers (i.e., network nodes, their connecting circuits, access networks, etc.);

– facilities of the service providers (i.e., service servers, etc.); a role of the service provider can be played by the infrastructure provider; otherwise, the service provider may operate within the network independently;

– facilities of the application providers (i.e., application servers, etc.); a role of the application provider can be played by the service provider; otherwise, the application provider may function within the network independently (see Note);

– a subscriber line connecting the user with the telecommunication operator (i.e., with the infrastructure/services/applications provider);

– information being transferred and stored within the facilities run by the infrastructure /service/application providers.

NOTE – The application providers may either share a part of the telecommunication operator facilities, or operate as external application service providers (ASPs). The user usually does not draw any distinction between such application providers. In any case, the user looks at them as one network-based application provider.

A.2 The term end-user equipment refers to:

– a telecommunication subscriber's terminal(s) (together with its software to perform the functions of an infrastructure user, a service user and an applications user, including execution of certain local functions – for example, message preparation and editing);

– an application server(s), if the user performs the functions of an application services provider external to the network structure;

– a corporate/local/home network (if present) in the user premises;

– a firewall/gateway (if present);

– user's information – transmitted, received and stored.

Bibliography

[b-ITU-T E.800]	Recommendation ITU-T E.800 (1994), *Terms and definitions related to quality of service and network performance including dependability*.
[b-ITU-T G.1000]	Recommendation ITU-T G.1000 (2001), *Communications quality of service – A framework and definitions*.
[b-ISO/IEC TR 19791]	ISO/IEC TR 19791:2006, *Information technology – Security techniques – Security assessment of operational systems.* <http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue-detail.htm?csnumber=33929>

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	**Data networks, open system communications and security**
Series Y	Global information infrastructure, Internet protocol aspects and next-generation networks
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2008