International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1032

(12/2010)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Information and network security – Network security

Architecture of external interrelationships for a telecommunication IP-based network security system

Recommendation ITU-T X.1032

ITU-T X-SERIES RECOMMENDATIONS

DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

PUBLIC DATA NETWORKS	X.1–X.199
OPEN SYSTEMS INTERCONNECTION	X.200–X.299
INTERWORKING BETWEEN NETWORKS	X.300–X.399
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	X.600–X.699
OSI MANAGEMENT	X.700–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	X.850–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
INFORMATION AND NETWORK SECURITY	
General security aspects	X.1000–X.1029
Network security	**X.1030–X.1049**
Security management	X.1050–X.1069
Telebiometrics	X.1080–X.1099
SECURE APPLICATIONS AND SERVICES	
Multicast security	X.1100–X.1109
Home network security	X.1110–X.1119
Mobile security	X.1120–X.1139
Web security	X.1140–X.1149
Security protocols	X.1150–X.1159
Peer-to-peer security	X.1160–X.1169
Networked ID security	X.1170–X.1179
IPTV security	X.1180–X.1199
CYBERSPACE SECURITY	
Cybersecurity	X.1200–X.1229
Countering spam	X.1230–X.1249
Identity management	X.1250–X.1279
SECURE APPLICATIONS AND SERVICES	
Emergency communications	X.1300–X.1309
Ubiquitous sensor network security	X.1310–X.1339
CYBERSECURITY INFORMATION EXCHANGE	
Cyber information exchange	X.1500–X.1519
Vulnerability/state exchange	X.1520–X.1539
Event/incident/heuristics exchange	X.1540–X.1549
Exchange of policies	X.1550–X.1559
Heuristics and information request	X.1560–X.1569
Identification and discovery	X.1570–X.1579
Assured exchange	X.1580–X.1589

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

Recommendation ITU-T X.1032

Architecture of external interrelationships for a telecommunication IP-based network security system

Summary

Recommendation ITU-T X.1032 proposes four models that make possible a review of interrelationships between a telecommunication IP-based network security system (TNSS) and various groups of external objects. Each object is considered in terms of its main functions and its probable effect on TNSS construction and functioning principles. This Recommendation provides a basis for developing detailed recommendations on network security with regard to the effect on external objects.

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T X.1032	2010-12-17	17

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/.

Table of Contents

Recommendation ITU-T X.1032

Architecture of external interrelationships for a telecommunication IP-based network security system

1 Scope

1.1 A study of any object needs to take into account not only the interconnections between different components within the object, but also the object's external relationships. Through external relationships, the object performs its functions in the context of an overall system. However, these interrelationships may pose a risk due to a variety of threats that can disturb the functioning of the object.

A study of these objects is particularly important for a telecommunication IP-based network security system (TNSS), which needs to protect a telecommunication IP-based network mainly against external threats (see Figure 1).

Possible composition of technical components of a telecommunication IP-based network is presented in Appendix I.

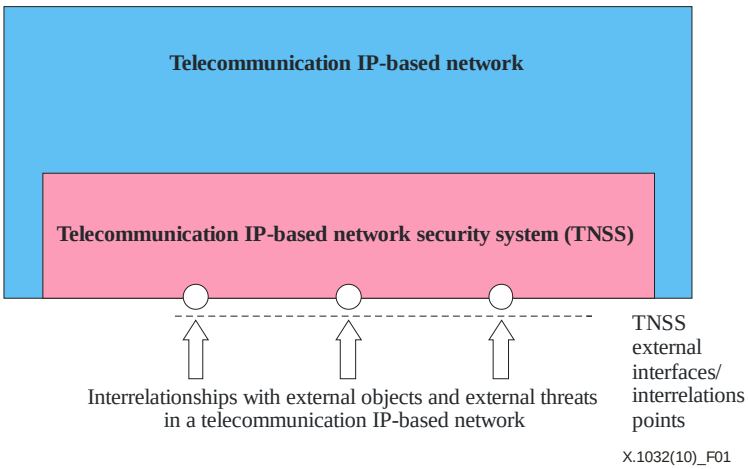

Figure 1 – Interrelationships between a telecommunication IP-based network security system and external objects

1.2 The TNSS does not function as a free-running system; it works in close interaction with a number of external systems.

Firstly, these external systems include the telecommunication IP-based network itself, which protects the TNSS. The principles that govern the construction of the transport medium and the service platforms directly determine the requirements and, therefore, the design of the TNSS.

Secondly, these external systems include the telecommunication IP-based network users whose requirements should be fulfilled by the telecommunication IP-based network and its TNSS.

Some other external organizations can also affect the TNSS construction principles. These organizations include:

– national regulatory authorities;

– trusted third parties providing services for security systems (on the "outsourcing" principle);

– organizations using telecommunication IP-based network services for the creation of information networks.

In essence, the main TNSS tasks consist of the protection of the telecommunication IP-based network and the information transmitted through this network against the various external security threats in the environment in which the TNSS functions.

The above list indicates that TNSS has interrelationships with many external objects which may be subdivided into several groups.

1.3 TNSS interrelationships with external objects can either directly or indirectly affect the TNSS requirements, the TNSS construction and the functioning principles. Therefore, these interrelationships should be taken into account in the course of TNSS development. Existing ITU-T Recommendations address certain aspects of this problem (for example, [ITU-T X.842] and [ITU-T X.843] address interrelationships with a trusted third party). However, there are many aspects of TNSS interrelationships with external objects that have not yet been considered.

1.4 This Recommendation covers a general architecture of TNSS interrelationships with external objects. This architecture can be applied to various types of telecommunication IP-based networks and to various telecommunication security systems. This Recommendation provides an overview of all external interrelationships of TNSS. This Recommendation may serve as a basis for elaborating more detailed recommendations on network security, with respect to the effect on external objects.

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.800] Recommendation ITU-T X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT applications*.

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

[ITU-T X.842] Recommendation ITU-T X.842 (2000) | ISO/IEC TR14516:2002, *Information technology – Security techniques – Guidelines for the use and management of trusted third party services*.

[ITU-T X.843] Recommendation ITU-T X.843 (2000) | ISO/IEC 15945:2002, *Information technology – Security techniques – Specification of TTP services to support the application of digital signatures*.

3 Definitions

3.1 Terms defined elsewhere

None.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 security system: A variety of interrelating elements (certain principles, organization and technical measures for security provision) that minimize vulnerability of assets and resources.

3.2.2 telecommunication IP-based network security system (TNSS): Security system used in a telecommunication IP-based network.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

ICT Information and Communication Technologies

TNSS Telecommunication IP-based Network Security System

5 Conventions

None.

6 General

6.1 Consideration of TNSS interrelationships with external objects is complicated by the great number of these objects and by various types of relationships and interfaces. Therefore, a major problem is the possibility of decomposition (division) of the set of interrelationships. This Recommendation proposes four types of external interrelationships:

– TNSS interrelationships with security systems that overlay infrastructure information systems and information structures;

– TNSS interrelationships with telecommunication system objects;

– TNSS interrelationships with other objects, e.g., external organizations;

– TNSS interrelationships with security threats in the form of either the above-named objects or new objects.

These types of interrelationships are considered below in clauses 7, 8, 9 and 10, respectively.

6.2 In addition, each of the clauses 7, 8, 9 and 10 employs the decomposition principle. First, a model of interrelationships is defined in a graphical form. This model contains external objects and their interrelationships with TNSS. The functions of each external object are then described. Finally, proceeding from these functions, brief assessments are made for:

– the possible effects of external objects on TNSS (for example, effects on requirements to TNSS, effects on principles of TNSS construction and functioning);

– the possible types of interrelationship (for example, an electrical interface, organizational requirements, external environment influences).

7 TNSS interrelationships with security systems of information systems and information structure

7.1 Model of interrelationships

Figure 2 shows TNSS interrelationships with security systems that overlay infrastructure information systems which, in turn, have interfaces with information structure security systems.

7.2 Functions of external objects and their effect on TNSS

7.2.1 Information systems employ various kinds of information technologies using telecommunications. Functions of information systems include, for instance, collection, storage and retrieval of information, organization of databases and users' sites, technical support of editing, conversion and other kinds of information processing. Information systems can perform functions of remote information transfer and distribution, using telecommunication services (i.e., from

information-telecommunication networks). Internet is one example of a public information-telecommunication network.

Traditional types of communication (for example, telephone communication and facsimile communication) can be effected both with and without the use of information-telecommunication network.

Information system security systems serve to protect the technical processes of these systems and the information stored and transferred within these systems. Information system security systems may affect TNSS in the following way, for example:

– supplement each other during protection against certain threats, for instance, against information disclosure; and

– introduce limitations for security protocols used within TNSS.

External interrelationships of TNSS with the information system security systems may be:

– hardware or software interfaces; or

– contractual agreements.

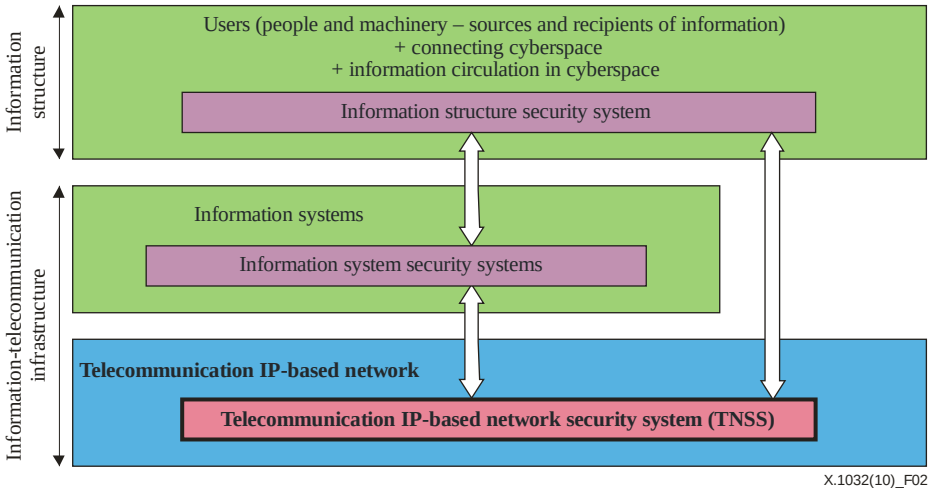

Figure 2 – Model of TNSS interrelationships with security systems of information systems and information structure

7.2.2 Information structure ensures information is used in all spheres of human activities. The information structure security system serves to protect users of cyberspace (authors, owners, sources, recipients and buyers of information) against intrusions in cyberspace which disrupt the users' work. Cyberspace users include both people and machinery (sensing elements, actuators, automatics, etc.). Examples of unwanted intrusions are viruses, "worms", spam and various maleware that exist in cyberspace. An unwanted intrusion may also include a denial of service in the information and communication infrastructure.

The information structure security system may affect TNSS directly or via information network security systems. For example, it may place requirements on TNSS such as cyberspace protection by means of technical tools which could support the implementation of legal, administrative and organizational measures used within the information structure security system. Such technical tools include the means to counter viruses and spam.

The external interrelationship of TNSS with the information structure security system may be by a contractual agreement.

8 TNSS interrelationships with telecommunication system objects

8.1 Model of TNSS interrelationships

Figure 3 shows TNSS interrelationships with its own telecommunication network objects and with security systems of other telecommunication system objects, i.e., with security systems of users' terminal equipment and neighbouring telecommunication networks.

8.2 Functions of external objects and their effect on TNSS

8.2.1 Telecommunication network internal objects (transport stratum and service stratum) determine the nomenclature of provided telecommunication services, as well as quantitative and qualitative characteristics of these services. These objects directly affect TNSS. In particular, they determine:

– The list of services subject to protection;

– The network possibilities for the realization of security mechanisms.

External interrelationships of TNSS with the transport stratum and the service stratum may be:

– hardware or software interfaces; or

– contractual agreements.

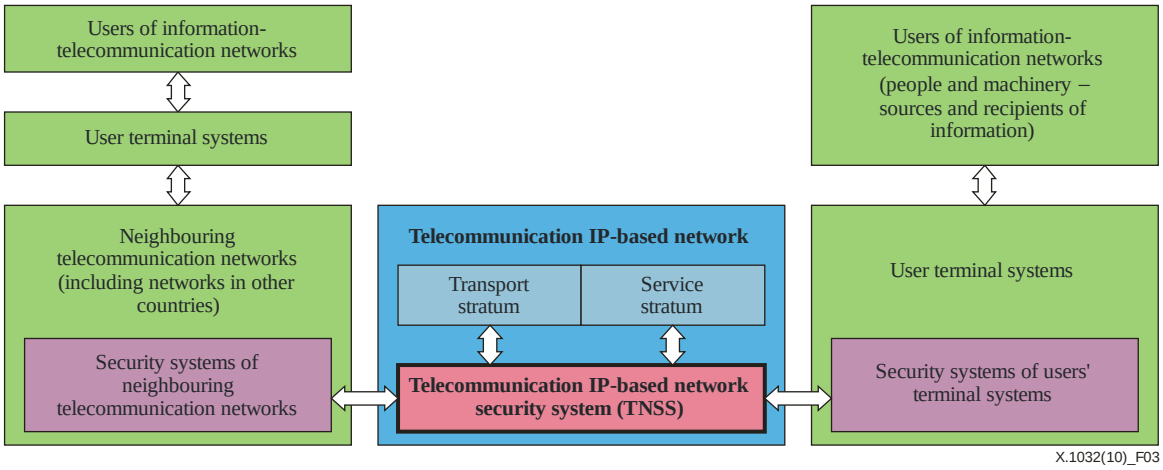

Figure 3 – Model of TNSS interrelationships with telecommunication system objects

8.2.2 Users' terminal systems may contain some terminal devices (telephone apparatus, television sets, computers and other sort of terminals) and relevant home/corporate network connections (see Appendix I for details). Security systems of users' terminal systems perform functions of protection for terminal devices and home/corporate networks against security threats. These threats may emanate either from the telecommunication network itself or from internal sources (e.g., users' terminal systems). Besides, security systems of users' terminal systems employ mechanisms to protect user information transmitted to the telecommunication network.

Security systems of users' terminal systems may affect TNSS. In particular, they may:

– support each other during protection of user information against certain threats, for example, by encrypting transmitted data;

– determine requirements for the target security level(s) to be ensured by TNSS.

External interrelationships of TNSS with the security systems of users' terminal systems may be:

– an electrical interface; or

– organizational requirements and limitations.

8.2.3 Neighbouring telecommunication networks (including networks in other countries) perform traffic exchange with the telecommunication network under consideration. Security systems of neighbouring telecommunication networks perform functions to protect these networks and the information transmitted via these networks against security threats. These systems may affect TNSS, in particular, they may:

– supplement each other during users' information protection against certain threats, for example, against corruption or modification of information; and

– introduce limitations for use of certain TNSS security mechanisms or functioning modes of these mechanisms.

External interrelationships of TNSS with security systems of neighbouring telecommunication networks may be:

– an electrical interface; or

– agreed bilateral organizational provisions.

9 TNSS interrelationships with external organizations

9.1 Model of interrelationships

Figure 4 shows TNSS interrelationships with various organizations external to the telecommunication network including:

– regulatory authorities;

– trusted third parties;

– law-enforcement authorities; and

– providers of technical tools (hardware and software).

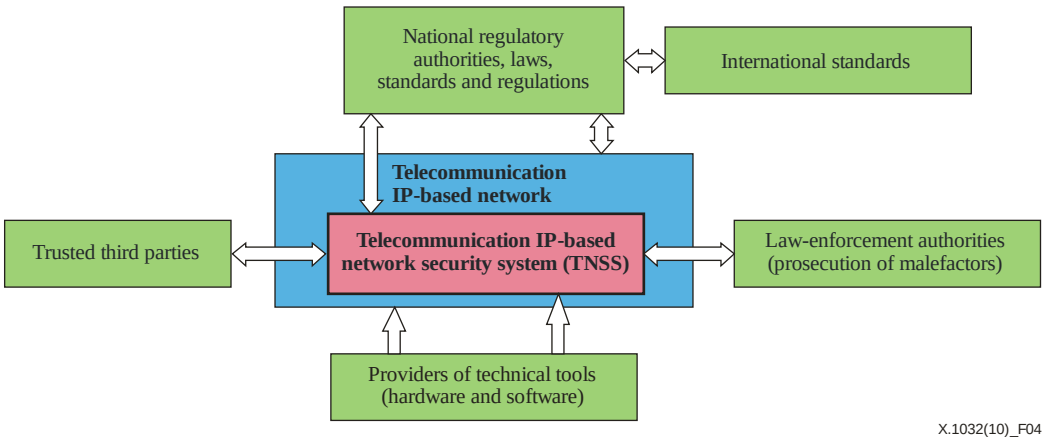

Figure 4 – Model of TNSS interrelationships with external organizations

9.2 Functions of external organizations and their effect on TNSS

9.2.1 Regulatory authorities define general policies in the telecommunication field. In particular, they support the development and application of international standards, regulations and laws, while also supporting the development of national standards.

9.2.2 In compliance with bilateral agreements with a telecommunication network operator, third parties may perform certain functions to ensure TNSS operation.

The list of these functions and principles of interaction between third parties and TNSS are determined by the operator of the infrastructure which incorporates the given TNSS.

External interrelationships of TNSS with third parties may be:

– hardware or software interfaces; or

– contractual agreements.

9.2.3 Law-enforcement authorities (prosecution of malefactors) should respond to national law violations related to the information and telecommunication network area. Specifically, they should catch malefactors responsible for such violations. The work of law-enforcement authorities and TNSS functioning supplement each other which enhances telecommunication security.

Given the importance of information and communication technologies (ICT) in all spheres of human society, as we progress towards the information society, law development is and will remain essential. Eventually, this trend will enhance the role of the relevant law-enforcement authorities.

To perform the aforesaid functions, law-enforcement authorities should receive timely data from telecommunication network operators on security incidents that constitute violations of the law. TNSS should perform acquisition, storage and analysis of information which would enable the corresponding messages to be compiled and sent to law-enforcement authorities. The possibility to transfer information on security incidents from telecommunication organizations to law enforcement authorities is indicated for example in [b-ITU-T E.409], [b-ITU-T X.1051] and [b-ITU-T X.1056].

External interrelationships of TNSS with law-enforcement authorities may be:

– electrical interface or other telecommunication services or postal services; and

– organizational provisions agreed bilaterally.

10 TNSS interrelationships with security threats sources

10.1 Model of interrelationships

Figure 5 shows a model of TNSS interrelationships with various security threat sources which include:

– users and their terminal systems connected to the subject telecommunication network;

– outsiders (non-users) and external media;

– objects and personnel of the telecommunication network;

– neighbouring telecommunication networks, including relevant users and users' terminal systems;

– connected information systems;

– trusted third parties; and

– providers of technical tools.

10.2 Functions of external objects and their effect on TNSS

Security threat sources may attack telecommunication networks. Telecommunication IP-based network security system (TNSS) is used to avert, detect and neutralize such attacks. Therefore, it is safe to say that security threats are directly related to TNSS as shown in Figure 5.

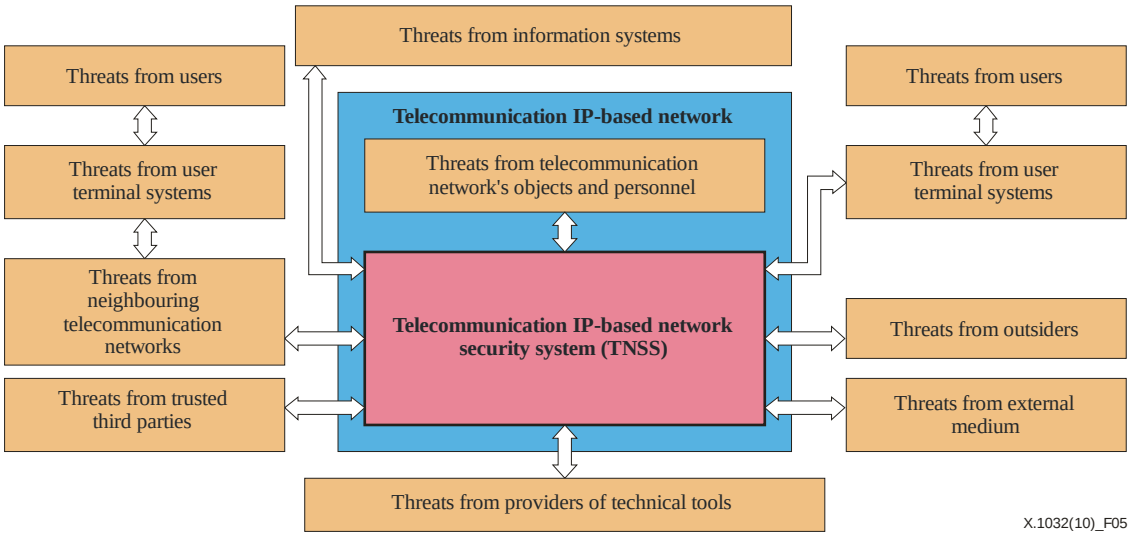

Figure 5 – Model of TNSS interrelationships with security threat sources

Threats are classified under five types as given in [ITU-T X.800] and [ITU-T X.805]:

– destruction of information and other resources;

– corruption or modification of information;

– theft, removal or loss of information and other resources;

– disclosure of information; and

– interruption of services.

Security policy in a telecommunication network may be used either to counteract all threats or to counteract some of these threats. Correspondingly, required security dimensions are selected in the course of TNSS elaboration. Mapping of security threats to security dimensions is given in Table 1 of [ITU-T X.805].

External interrelationships of TNSS with security treat sources may be:

– electrical interfaces;

– actions of people;

– attacks using technical means via the telecommunication network and external technical means;

– external environmental influences;

– technical measures for counteracting attacks; and

– organizational measures for counteracting attacks.

Appendix I

Possible composition of technical facilities of the telecommunication IP-based network

(This appendix does not form an integral part of this Recommendation)

I.1 This Recommendation uses the term "telecommunication 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;

– connection, connecting the user with the telecommunication operator (i.e., with the infrastructure/service/application provider); and

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

I.2 The telecommunication network does not include the term "user terminal systems". Such systems contain:

– a telecommunication subscriber terminal(s) (together with its software to perform the functions of an infrastructure user, a service user and an application 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);

– a firewall/gateway (if present); and

– user information – transmitted, received and stored.

Bibliography

[b-ITU-T E.409] Recommendation ITU-T E.409 (2004), *Incident organization and security incident handling: Guidelines for telecommunication organizations*.

[b-ITU-T X.1051] Recommendation ITU-T X.1051 (2008) | ISO/IEC 27011:2008, *Information technology – Security techniques – Information security management guidelines for telecommunications organizations based on ISO/IEC 27002*.

[b-ITU-T X.1056] Recommendation ITU-T X.1056 (2009), *Security incident management guidelines for telecommunications organizations*.

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	Terminals and subjective and objective assessment methods
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, 2011