



INTERNATIONAL TELECOMMUNICATION UNION

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

E.408

(05/2004)

SERIES E: OVERALL NETWORK OPERATION,
TELEPHONE SERVICE, SERVICE OPERATION AND
HUMAN FACTORS

Network management – International service statistics

Telecommunication networks security requirements

ITU-T Recommendation E.408

ITU-T E-SERIES RECOMMENDATIONS

OVERALL NETWORK OPERATION, TELEPHONE SERVICE, SERVICE OPERATION AND HUMAN FACTORS

INTERNATIONAL OPERATION

Definitions	E.100–E.103
General provisions concerning Administrations	E.104–E.119
General provisions concerning users	E.120–E.139
Operation of international telephone services	E.140–E.159
Numbering plan of the international telephone service	E.160–E.169
International routing plan	E.170–E.179
Tones in national signalling systems	E.180–E.189
Numbering plan of the international telephone service	E.190–E.199
Maritime mobile service and public land mobile service	E.200–E.229

OPERATIONAL PROVISIONS RELATING TO CHARGING AND ACCOUNTING IN THE INTERNATIONAL TELEPHONE SERVICE

Charging in the international telephone service	E.230–E.249
Measuring and recording call durations for accounting purposes	E.260–E.269

UTILIZATION OF THE INTERNATIONAL TELEPHONE NETWORK FOR NON-TELEPHONY APPLICATIONS

General	E.300–E.319
Phototelegraphy	E.320–E.329

ISDN PROVISIONS CONCERNING USERS

E.330–E.349

INTERNATIONAL ROUTING PLAN

E.350–E.399

NETWORK MANAGEMENT

International service statistics **E.400–E.409**

International network management	E.410–E.419
Checking the quality of the international telephone service	E.420–E.489

TRAFFIC ENGINEERING

Measurement and recording of traffic	E.490–E.505
Forecasting of traffic	E.506–E.509
Determination of the number of circuits in manual operation	E.510–E.519
Determination of the number of circuits in automatic and semi-automatic operation	E.520–E.539
Grade of service	E.540–E.599
Definitions	E.600–E.649
Traffic engineering for IP-networks	E.650–E.699
ISDN traffic engineering	E.700–E.749
Mobile network traffic engineering	E.750–E.799

QUALITY OF TELECOMMUNICATION SERVICES: CONCEPTS, MODELS, OBJECTIVES AND DEPENDABILITY PLANNING

Terms and definitions related to the quality of telecommunication services	E.800–E.809
Models for telecommunication services	E.810–E.844
Objectives for quality of service and related concepts of telecommunication services	E.845–E.859
Use of quality of service objectives for planning of telecommunication networks	E.860–E.879
Field data collection and evaluation on the performance of equipment, networks and services	E.880–E.899

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

ITU-T Recommendation E.408

Telecommunication networks security requirements

Summary

This Recommendation provides an overview of security requirements and a framework that identifies security threats to telecommunication networks in general (both fixed and mobile; both voice and data) and gives guidance for planning countermeasures that can be taken to mitigate the risks arising from the threats.

Source

ITU-T Recommendation E.408 was approved on 28 May 2004 by ITU-T Study Group 2 (2001-2004) under the WTSA Resolution 1.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications. 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, implementors are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database.

© ITU 2004

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

CONTENTS

Page

1	Introduction	1
1.1	Scope	1
1.2	References	1
1.3	Use of the term "service"	2
1.4	Rationale	2
2	System description	3
2.1	Actors and roles	4
2.2	Security domains for telecommunication networks	5
3	Generic security objectives for telecommunication networks	5
4	Legislation issues	6
5	Threats and risks	6
6	Security requirements	8
6.1	Security requirements and corresponding services	8
6.2	Requirements on the management of security	13
6.3	Security services and OSI layers	14
6.4	Security management	16
	Appendix I – Legislation issues	17
I.1	Introduction	17
I.2	Applicable legislation areas	17
I.3	Sources of legislation	17
I.4	Possible consequences for telecommunication network security standardization	18
	Appendix II – Functional classes and security profiles	19
II.1	Grouping of security measures	19
II.2	Functional classes	19
II.3	Security profiles	21

ITU-T Recommendation E.408

Telecommunication networks security requirements

1 Introduction

1.1 Scope

This Recommendation provides an overview and framework that identifies security threats to telecommunication networks in general (both fixed and mobile; both voice and data) and gives guidance for planning countermeasures that can be taken to mitigate the risks arising from the threats.

This Recommendation is generic in nature and does not identify or address requirements for specific networks.

This Recommendation does not seek to define new security services but uses existing security services defined in other ITU-T Recommendations and relevant standards from other bodies.

This Recommendation is intended to facilitate international cooperation in the following areas regarding telecommunication network security:

- Information sharing and dissemination;
- Incident coordination and crisis response;
- Recruitment and training of security professionals;
- Law enforcement coordination;
- Protection of critical infrastructure and critical services;
- Development of appropriate legislation.

To succeed in obtaining such cooperation, national implementation of the requirements of this Recommendation for the national components of the network is essential.

1.2 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 Recommendation M.3010 (2000), *Principles for a telecommunications management network*.
- ITU-T Recommendation M.3016 (1998), *TMN security overview*.
- ITU-T Recommendation M.3400 (2000), *TMN management functions*.
- ITU-T Recommendation X.509 (2000) | ISO/IEC 9594-8:2001, *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks*.
- ITU-T Recommendation X.741 (1995) | ISO/IEC 10164-9:1995, *Information technology – Open Systems Interconnection – Systems management: Objects and attributes for access control*.

- ITU-T Recommendation X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT applications*.
- ITU-T Recommendation X.802 (1995) | ISO/IEC TR 13594:1995, *Information technology – Lower layers security model*.
- ITU-T Recommendation X.803 (1994) | ISO/IEC 10745:1995, *Information technology – Open Systems Interconnection – Upper layers security model*.
- ITU-T Recommendation X.805 (2003), *Security architecture for systems providing end-to-end communications*.
- ITU-T Recommendation X.810 (1995) | ISO/IEC 10181-1:1996, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Overview*.
- ITU-T Recommendation X.812 (1995) | ISO/IEC 10181-3:1996, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Access control framework*.
- ITU-T Recommendation X.813 (1996) | ISO/IEC 10181-4:1997, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Non-repudiation framework*.
- ITU-T Recommendation X.814 (1995) | ISO/IEC 10181-5:1996, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Confidentiality framework*.
- ITU-T Recommendation X.815 (1995) | ISO/IEC 10181-6:1996, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Integrity framework*.
- ITU-T Recommendation X.816 (1995) | ISO/IEC 10181-7:1996, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Security audit and alarms framework*.
- ISO/IEC 9979:1999, *Information technology – Security techniques – Procedures for the registration of cryptographic algorithms*.
- IETF RFC 2535 (1999), *Domain Name System Security Extensions*.
- IETF RFC 2870 (2000), *Root Name Server Operational Requirements*.
- IETF RFC 3013 (2000), *Recommended Internet Service Provider Security Services and Procedures*.

1.3 Use of the term "service"

The word "service" used in this Recommendation does not refer to any defined ITU services. It is used as a generic term when discussing security issues and/or functions and should be defined in the future.

1.4 Rationale

The requirement for a generic network security framework for international telecommunications has originated from different sources:

- **Customers/subscribers** need confidence in the network and the services offered, including availability of services (especially emergency services) in case of major catastrophes, including terrorist actions.
- **The public community/authorities** demand security by directives and legislation, in order to ensure availability of services, fair competition and privacy protection.

- **Network operators/service providers** themselves need security to safeguard their operation and business interests, and to meet their obligations to the customers and the public, at the national and international level.

Telecommunication networks security requirements should preferably be based upon internationally agreed security standards as it is beneficial to reuse rather than create new ones. The provisioning and usage of security services and mechanisms can be quite expensive relatively to the value of the transactions being protected. It is, therefore, important to have the ability to customize the security provided in relation to the services being protected. The security services and mechanisms that are used should be provided in a way that allows such customization. Due to the large number of possible combinations of security features, it is desirable to have **security profiles** (see Appendix II) that cover a broad range of telecommunication network services.

Standardization will facilitate **reuse of solutions and products** meaning that security can be introduced faster and at lower cost.

Important benefits of standardized solutions for vendors and users of the systems alike are the economies of scale in product development and component interoperation within telecommunication networks with regard to security.

It is necessary to provide security services and mechanisms to protect telecommunication networks against malicious attacks such as denial of service, eavesdropping, spoofing, tampering with messages (modification, delay, deletion, insertion, replay, re-routing, misrouting, or re-ordering of messages), repudiation or forgery. Protection includes prevention, detection and recovery from attacks, as well as management of security-related information. Protection must also include measures to prevent service outages due to natural events (weather, etc.) or malicious attacks (terrorist actions). Provisions must be made to allow eavesdropping and monitoring as requested by duly authorized legal authorities.

2 System description

To effectively secure one network, it is recommended to implement layers of security; the more layers someone puts in place, the more effective its security. This technique of building layers can be analysed from the ground up:

SECURITY AUDITING
SECURITY TOOLS
SOFTWARE FOR TELECOMMUNICATIONS
MONITORING
PHYSICAL SECURITY
NETWORK ADMINISTRATOR

Figure 1/E.408 – Six layers for network security

The term "layer" as used in this Recommendation merely constitutes a description of some security considerations that are relevant to organizing network security. Layers in this Recommendation should not be considered as architectural elements and should not be confused with the security layers of ITU-T Rec. X.805.

Like the foundation of a house, the first layer, network administrators, will be an organization's most important asset in network security. Spending extra money each year on a good network administrator is more effective than buying an expensive firewall. Good network administrators understand the operating systems they work with and understand how to lock down every machine