

I n t e r n a t i o n a l T e l e c o m m u n i c a t i o n U n i o n

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Series X

Supplement 3

(04/2008)

SERIES X: DATA NETWORKS, OPEN SYSTEM
COMMUNICATIONS AND SECURITY

**ITU-T X.800-X.849 series – Supplement on
guidelines for implementing system and
network security**

ITU-T X-series Recommendations – Supplement 3



International
Telecommunication
Union

Document Sharing Hub

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

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

Supplement 3 to ITU-T X-series Recommendations

ITU-T X.800-X.849 series – Supplement on guidelines for implementing system and network security

Summary

Network security is designed around a strong security framework, available tools, and standardized protocols. In complex multi-vendor environments, standards-based security solutions can ensure interoperability and operational efficiencies in realizing end-to-end security. Network providers depend upon security information available to them to help plan, design and implement and maintain their networks in order to meet the security objectives. Standards-based systematic methodology and guidelines identify and address critical security challenges of network and information security.

This supplement establishes guidelines for implementing system and network security with a focus on telecommunications networks. This supplement provides security guidelines for critical activities during the network life-cycle. These guidelines address four areas: 1) technical security policy, 2) asset identification, 3) threats, vulnerabilities and mitigations, and 4) security assessment. The guidelines and associated templates help in systematically addressing the security of networks.

Source

Supplement 3 to ITU-T X-series Recommendations was agreed on 18 April 2008 by ITU-T Study Group 17 (2005-2008).

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

Compliance with this publication is voluntary. However, the publication may contain certain mandatory provisions (to ensure e.g., interoperability or applicability) and compliance with the publication 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 publication is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this publication 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 publication development process.

As of the date of approval of this publication, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this publication. 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/>.

© ITU 2009

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

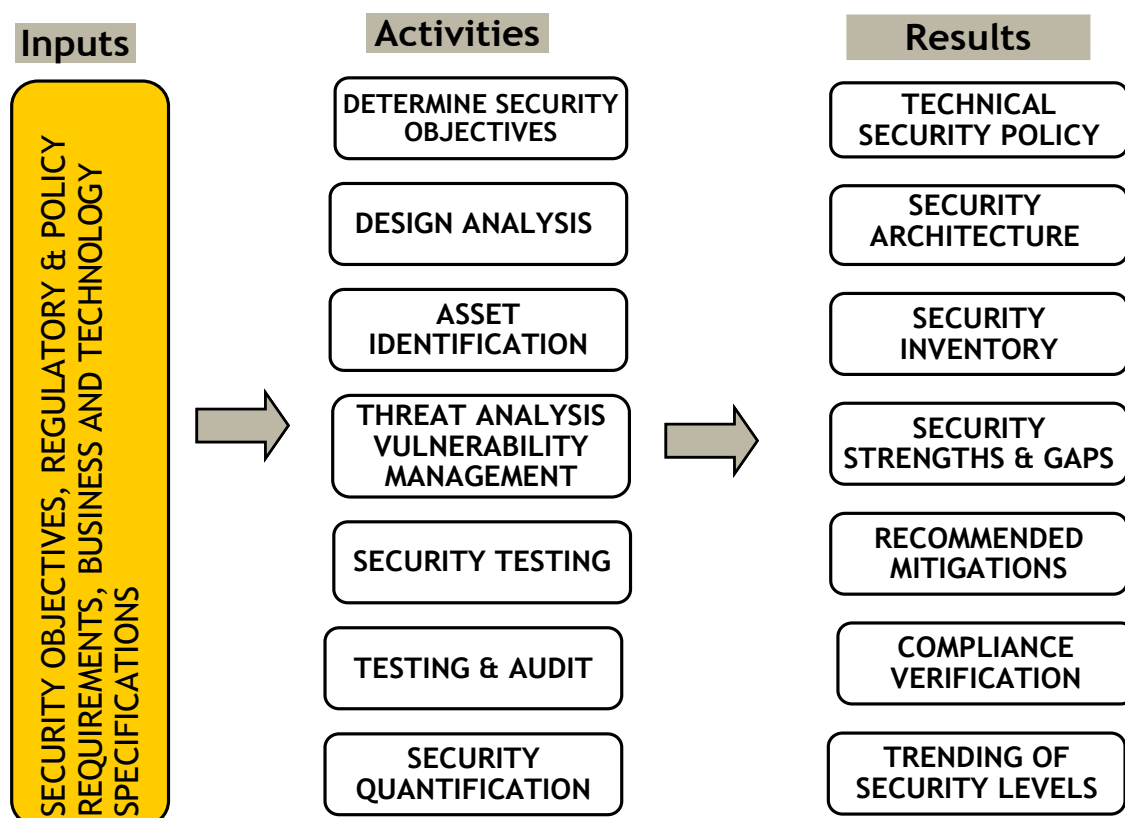
CONTENTS

Page

1	Scope	1
1.1	Guidance to organizations on technical security policies.....	1
1.2	Guidance on hierarchical-asset identification	1
1.3	Guidance on understanding threats, vulnerabilities and mitigations.....	1
1.4	Guidance on security assessments.....	1
2	References.....	1
3	Definitions	2
4	Abbreviations and acronyms	2
5	Conventions	2
6	Guidelines phases	2
6.1	Security integration into product and systems life-cycle	2
6.2	Guidance to organizations on technical security policies.....	4
6.3	Guidance on hierarchical-asset identification	8
6.4	Guidance for understanding threats, vulnerabilities and mitigations	9
6.5	Guidance on security assessments.....	14
	Bibliography.....	22

Introduction

Network security is designed around a strong security framework, the available tools, and standardized protocols. In complex multi-vendor environments, standards-based security solutions can ensure interoperability and operational efficiencies in realizing end-to-end security. Network operators depend upon key security information to plan/design, implement and maintain secure networks to meet the organization's business and technical goals. The figure below shows the key security activities and associated results needed during the security life-cycle. Standards-based systematic methodology and guidelines help in identifying and addressing critical security information challenges of systems and networks. A systematic assessment can provide a baseline of the current level of security and mitigations that are required to support the security life-cycle.



This supplement establishes guidelines for implementing system and network security with a focus on telecommunications networks. This supplement provides security guidelines for critical activities during the network security life-cycle. These guidelines address four areas: 1) technical security policy, 2) hierarchical-asset identification, 3) threats, vulnerabilities and mitigations based on hierarchical assets, and 4) security assessment. The guidelines and associated templates will help in systematically addressing the security of networks.

1) *Guidance to organizations on technical security policies*

This clause describes the value of a security policy and provides guidance on the components of a technical security policy. Recommendation ITU-T X.1051| ISO/IEC 27011 provides details of ISMS security policy. This supplement leverages existing standards on security policy to build and manage the technical policy. The guidelines in this supplement show key components required to build and continuously manage the technical policy.

2) *Guidance on hierarchical-asset identification*

Guidelines are provided on how to comprehensively identify assets that need to be protected. These guidelines can be used to identify critical security assets regardless of the technology or industry vertical.

3) *Guidance on understanding threats, vulnerabilities and mitigations*

Guidelines on how to identify potential threats to the assets are provided. As part of the threat analysis, guidelines on recognizing the potential vulnerabilities within the hierarchical-assets and the resulting impact of potential threat materialization are provided in this clause. It is important to also recognize the mitigations needed and their implementation priority.

4) *Guidance on security assessments*

Guidelines are provided on network security assessment in the three stages of the security life-cycle that are shown in Figure 1. Securing activities related to management, control and users for the network infrastructure, services and applications is the focus of this clause. The assessment guidelines cover plan/design, implementation and maintenance phases of a system or network life-cycle. It leverages the guidelines and results from technical policy, hierarchical-asset identification, and threat/vulnerability mitigation guidelines to secure a network.

Benefits of system and network security implementation guidance:

The industry needs a uniform set of security guidelines that can be consistently applied to relevant phases of system and network life-cycle to realize the following benefits:

- A common approach leads to shared understanding and interoperability in multi-supplier networks.
- An identification of hierarchical assets and what is needed to protect them.
- A consistent way to look at threats, vulnerabilities for products, regardless of technology.
- A systematic analysis assures efficient coverage of network security.

Supplement 3 to ITU-T X-series Recommendations

ITU-T X.800-X.849 series – Supplement on guidelines for implementing system and network security

1 Scope

This supplement provides system and network security implementation guidelines. These guidelines can be utilized to realize a network security program. The guidelines are applicable to management, control, and user activities to secure assets belonging to infrastructure elements, network services and applications. These guidelines are independent of the underlying technology and focus on telecommunications networks security. This supplement focuses on four different areas as described in the paragraphs below:

1.1 Guidance to organizations on technical security policies

This clause shares the need and value of a security policy and then provides guidance on the components needed for a technical security policy. [b-ITU-T X.1051] provides details of ISMS security policy. This supplement leverages existing standards on security policy to build and manage the technical policy. The guidelines in this supplement show key components required to build and continuously manage the technical policy.

1.2 Guidance on hierarchical-asset identification

Guidelines are provided on how to comprehensively identify assets that require protection. These guidelines can be used to identify critical security assets, regardless of the technology or industry vertical.

1.3 Guidance on understanding threats, vulnerabilities and mitigations

Guidelines on identifying potential threats to the assets, recognizing the potential vulnerabilities within the assets, and the resulting impact and mitigations of potential threat materialization are provided in this clause. These guidelines leverage the policy and hierarchical-asset identification.

1.4 Guidance on security assessments

Guidelines are provided on network security assessment for three stages of the life-cycle, which include the planning and definition, design and implementation and maintenance phases. Securing activities related to management, control and users for the network infrastructure, services and applications is the focus of this clause. In this clause, the assessment addresses the implementation of policy, hierarchical-asset identification, and threat/vulnerability guidelines and baselines of the security of the system or network.

The selection of protocols for specific technologies is not within the scope of this supplement. Protocol details are covered by other Recommendations and standards. This supplement does not cover all aspects of the security life-cycle, including product end-of-life. Security domain experts, depending on the operating environment and objectives, will have to select the relevant Recommendations and standards. The guidelines in this supplement, together with the domain expertise, will help in achieving comprehensive security.

2 References

None.

3 Definitions

This supplement uses the following terms defined elsewhere:

3.1 attack [b-ITU-T H.235.0]: The activities undertaken to bypass or exploit deficiencies in a system's security mechanisms. By a direct attack on a system they exploit deficiencies in the underlying algorithms, principles, or properties of a security mechanism. Indirect attacks are performed when they bypass the mechanism, or when they make the system use the mechanism incorrectly.

3.2 information asset [b-ISO/IEC 13335-1]: An information asset is defined as a physical or logical (tangible or intangible) entity that is of value to an organization or institution and characterized by the following: Anything that has value to the organization.

3.3 threat [b-ISO/IEC 13335-1]: A potential cause of an unwanted incident that may result in harm to a system or organization.

3.4 vulnerability [b-ISO/IEC 13335-1]: A vulnerability is any weakness that could be exploited to violate a system or the information it contains.

4 Abbreviations and acronyms

This supplement uses the following abbreviations and acronyms:

DMZ	Demilitarized Zone
EDI	Electronic Data Exchange
IDS	Intrusion Detection System
OAM&P	Operations, Administration, Maintenance and Provisioning
TSSR	Technology Specific Security Requirements

5 Conventions

None.

6 Guidelines phases

This clause describes the guidelines and how they can be built and leveraged from one phase to another phase of the security life-cycle.

6.1 Security integration into product and systems life-cycle

A complete and cost-effective security solution can be achieved by a comprehensive approach to security, where security is implemented in every step of the product life-cycle: from concept to development to ongoing maintenance. Figure 1 shows the key steps in the security life-cycle and the activities.