

International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1205

(04/2008)

SERIES X: DATA NETWORKS, OPEN SYSTEM
COMMUNICATIONS AND SECURITY

Telecommunication security

Overview of cybersecurity

Recommendation ITU-T X.1205

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.1205

Overview of cybersecurity

Summary

Recommendation ITU-T X.1205 provides a definition for cybersecurity. This Recommendation provides a taxonomy of the security threats from an organization point of view. Cybersecurity threats and vulnerabilities including the most common hacker's tools of the trade are presented. Threats are discussed at various network layers.

Various cybersecurity technologies that are available to remedy the threats are discussed, including: routers, firewalls, antivirus protection, intrusion detection systems, intrusion protection systems, secure computing and audit and monitoring. Network protection principles, such as defence in depth, access management with application to cybersecurity are discussed. Risk management strategies and techniques are discussed including the value of training and education in protecting the network. Examples for securing various networks, based on the discussed technologies, are also discussed.

Source

Recommendation ITU-T X.1205 was approved on 18 April 2008 by ITU-T Study Group 17 (2005-2008) under the WTSA Resolution 1 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/>.

© 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
2	References.....	1
3	Definitions	2
3.1	Terms defined elsewhere	2
3.2	Terms defined in this Recommendation.....	2
4	Abbreviations.....	3
5	Conventions	5
6	Introduction	5
7	Cybersecurity	6
7.1	What is cybersecurity?	6
7.2	Nature of enterprise cybersecurity environment	7
7.3	Threats to cybersecurity and a methodology to address them.....	9
7.4	End-to-end communications security	9
8	Possible network protection strategies.....	12
8.1	Closed loop policy management	12
8.2	Uniform access management.....	13
8.3	Secure communications.....	14
8.4	Variable depth security	15
8.5	Securing management	16
8.6	Layered security across the application, network and network management.....	18
8.7	Network survivability even under attack.....	19
	Appendix I – Attackers techniques	20
I.1	Taxonomy of security threats	20
I.2	Security threats	23
	Appendix II – Fields of cybersecurity technologies	26
II.1	Cryptography.....	27
II.2	Access control technologies	28
II.3	Antivirus and system integrity.....	33
II.4	Audit and monitoring	33
II.5	Management	34
	Appendix III – Example of network security.....	37
III.1	Securing remote access.....	37
III.2	Securing IP telephony.....	39
III.3	Securing the remote office.....	43
III.4	Securing WLAN.....	45
	Bibliography.....	53

Recommendation ITU-T X.1205

Overview of cybersecurity

1 Scope

This Recommendation develops a definition of cybersecurity in clause 7. This Recommendation provides a taxonomy of security threats from an organization point of view.

NOTE – The use of the term "identity" in this Recommendation does not indicate its absolute meaning. In particular, it does not constitute any positive validation.

Clause 7 discusses the nature of enterprise cybersecurity environment, cybersecurity risks and end-to-end communications security. Clause 8 discusses possible network protection strategies, including: closed loop policy management, uniform access management. Clause 8 also discusses secure communications techniques, variable depth security, securing the management plane, layered security and network survivability even under attack.

Appendix I discusses taxonomy of security threats, hackers tools of the trade and security threats.

Appendix II provides a review of the fields of cybersecurity technologies, including: cryptograph, access control technologies, perimeter protection techniques, antivirus and system integrity, audit and monitoring, and management.

Appendix III provides examples of network security. Examples include: securing remote access, securing IP telephony, securing VoIP clients, securing the remote office and securing WLANs.

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), <i>Security architecture for Open Systems Interconnection for CCITT applications</i> . |
| [ITU-T X.805] | Recommendation ITU-T X.805 (2003), <i>Security architecture for systems providing end-to-end communications</i> . |
| [ITU-T X.811] | Recommendation ITU-T X.811 (1995) ISO/IEC 10181-2:1996, <i>Information technology – Open Systems Interconnection – Security frameworks for open systems: Authentication framework</i> . |
| [ITU-T X.812] | Recommendation ITU-T X.812 (1995) ISO/IEC 10181-3:1996, <i>Information technology – Open Systems Interconnection – Security frameworks for open systems: Access control framework</i> . |
| [IETF RFC 1918] | IETF RFC 1918 (1996), <i>Address Allocation for Private Internets</i>
< http://www.ietf.org/rfc/rfc1918.txt?number=1918 >. |
| [IETF RFC 2396] | IETF RFC 2396 (1998), <i>Uniform Resource Identifiers (URI): Generic Syntax</i>
< http://www.ietf.org/rfc/rfc2396.txt?number=2396 >. |

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 This Recommendation uses the following terms defined in [ITU-T X.800]:

- a) Authorization;
- b) Security architecture;
- c) Security policy;
- d) User.

3.1.2 This Recommendation uses the following terms defined in [ITU-T X.805]:

- a) Security dimension;
- b) Security service.

3.1.3 This Recommendation uses the following terms defined in [ITU-T X.811]:

- a) Authentication;
- b) Principle.

3.1.4 This Recommendation uses the following terms defined in [ITU-T X.812]:

- a) Access control information;
- b) Access;
- c) Access control;
- d) User.

3.1.5 This Recommendation uses the following terms defined in [IETF RFC 2396]:

- a) Uniform resource identifier (URI);
- b) URI reference.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 access point: IEEE 802.11 wireless hub, a special kind of station (STA) operating as an access point.

3.2.2 basic service set (BSS): Coverage area served by one access point (AP).

3.2.3 cryptographic algorithm: A cryptographic algorithm is the means by which data are altered and disguised in encryption.

3.2.4 cyber environment: This includes users, networks, devices, all software, processes, information in storage or transit, applications, services, and systems that can be connected directly or indirectly to networks.

3.2.5 cybersecurity: Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment. The general security objectives comprise the following:

- Availability
- Integrity, which may include authenticity and non-repudiation
- Confidentiality.

3.2.6 distributed system: A non-standardized medium for interconnecting BSSs within an ESS.

3.2.7 extensible authentication protocol: This PPP extension providing support for additional authentication methods is part of the [b-IEEE 802.1X] specification.

3.2.8 extended service set: A single wireless LAN with BSSs within a single IP subnet.

3.2.9 firewall: A system or combination of systems that enforces a boundary between two or more networks. A gateway that limits access between networks in accordance with local security policy.

3.2.10 foreign agent: The visited/host network's router that services the mobile node while it is visiting the host network. This foreign agent handles the tunnelling and delivery between the mobile node and others, and between the mobile's home network and the host network.

3.2.11 honeyspot: A software program that emulates a network so as to attract (and maybe confuse) intruders and track their actions. The output of these systems can be used to infer the intruder's intentions and evidence gathering.

3.2.12 home agent: A router that services the mobile node while it is visiting other networks, maintaining current location information on that mobile node.

3.2.13 hot spots: Public places that host mobile IEEE 802.11 users to connect to the Internet.

3.2.14 IP mobility: A mechanism which enables more transparent connectivity for mobile nodes that "visit" different IP sub-networks while travelling. This is a mechanism for mobile management for mobile nodes on both wired networks and wireless networks.

4 Abbreviations

This Recommendation uses the following abbreviations:

3DES	Triple Data Encryption Standard
AAA	Authentication, Authorization and Accounting
ACL	Access Control List
AES	Advanced Encryption Standard
AP	Access Point
ASP	Application Service Provider
BSS	Basic Service Set
CA	Certification Authority
CMP	Certificate Management Protocol
COPS	Common Open Policy Service
CRL	Certificate Revocation List
DISA	Direct Inward System Access
DNS	Domain Name System
EAP	Extensible Authentication Protocol
EMS	Element Management System



ESS	Extended Service Set
ESSID	Extended Service Set Identifier
FTP	File Transfer Protocol
HMAC	Hash function based MACs
HTTP	HyperText Transfer Protocol
IDS	Intrusion Detection System
IKE	Internet Key Exchange
IP	Internet Protocol
IPSec	Internet Protocol Security
ISP	Internet Service Provider
L2TP	Layer 2 Tunnelling Protocol
LAN	Local Area Network
MAC	Message Authentication Code
MD5	Message Digest algorithm 5
MIC	Message Integrity Check
MIME	Multipurpose Internet Mail Extensions
MPLS	MultiProtocol Label Switching
MU	Mobile Unit
NAT	Network Address Translation
NGN	Next Generation Network
NIC	Network Interface Card
NOC	Network Operations Centre
OAM&P	Operations, Administration, Maintenance & Provisioning
OCSP	Online Certificate Status Protocol
OS	Operating System
OSI	Open Systems Interconnection
PDP	Policy Decision Point
PEAP	Protected EAP protocol
PEP	Policy Enforcement Point
PGP	Pretty Good Privacy
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure X.509
PoP	Proof of Possession
PPP	Point-to-Point Protocol
PSTN	Public Switched Telephone Network
RADIUS	Remote Authentication Dial-in User Service
RSA	Rivest Shamir Adleman public key algorithm

SHA-1	Secure Hash Algorithm 1
SIP	Session Initiation Protocol
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SP	Service Provider
SSH	Secure Shell
SSID	Service Set Identification
SSO	Single Sign On
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security Protocol
UE	User Equipment
URI	Uniform Resource Identifier
UTC	Coordinated Universal Time
VAR	Value-Added Reseller
VLAN	Virtual LAN
VoIP	Voice-over-IP
VPLS	Virtual Private LAN Service
VPN	Virtual Private Network
VPWS	Virtual Private Wire Service
WAN	Wide Area Network
WEP	Wired Equivalent Privacy
WLAN	Wireless LAN
WPA	Wi-fi Protected Access
XML	eXtensible Markup Language

5 Conventions

User equipment (UE) within this Recommendation is understood in a broad sense to encompass all sorts of devices, (hardware- or software based-) entities, mobile and/or stationary, personal computer (PC)s, (multimedia-enabled) terminals, phones, etc., all in the user premises, often out of control of an operator or service provider.

6 Introduction

The use of networks to connect heterogeneous IT systems can result in productivity gains to organizations and new capabilities that are enabled by the networked systems. Nowadays it is relatively easy to obtain information, to communicate, to monitor and control IT systems across vast distances. As such, today's networks play a key role in many nations' critical infrastructure that include: electronic commerce, voice and data communications, utility, financial, health, transportation, and defence.

Network connectivity and ubiquitous access is central to today's IT systems. However, widespread access and the loose coupling of interconnected IT systems can be a primary source of widespread vulnerability. Threats to networked systems such as: denial of service attacks, theft of financial and personal data, network failures and disruption of voice and data telecommunications are increasing.

The network protocols that are in use today were developed in an environment of trust. Most new investments and development are dedicated to building new functionality and not on securing that functionality.

Cybersecurity threats are growing rapidly. Viruses, worms, Trojan horses, spoofing attacks, "identity theft"¹, spam, and cyber attacks are on the rise. An understanding of cybersecurity is needed in order to build a foundation of knowledge that can aid securing the networks of tomorrow.

Corporations and government agencies are encouraged to view security as a process or way of thinking on how to protect systems, networks, applications, and resources. The underlying thinking is that connected networks have inherent risks. However, security should not be an obstacle to business. The objective is on how to offer the necessary services in a secure way.

In today's business environment, the concept of perimeter is disappearing. The boundaries between inside and outside networks are becoming thinner. Applications run on top of networks in a layered fashion. It is assumed that security exists between each of these layers. A layered approach to security enables organizations to create multiple levels of defence against threats.

7 Cybersecurity

Organizations need to devise a comprehensive plan for addressing its security needs. Organizations are encouraged to view security as a process or way of thinking on how to protect systems, networks, applications, and resources.

7.1 What is cybersecurity?

In this Recommendation, the term cybersecurity is defined in clause 3.2.5.

Cybersecurity techniques can be used to ensure system availability, integrity, authenticity, confidentiality, and non-repudiation. Cybersecurity can be used to ensure that user privacy is respected. Cybersecurity techniques can be used to establish the user's trustworthiness.

Technologies, such as wireless networks and voice-over-IP (VoIP), extend the reach and scale of the Internet. In this regard, the cyber environment includes users, the Internet, the computing devices that are connected to it and all applications, services and systems that can be connected directly or indirectly to the Internet, and to the next generation network (NGN) environment, the latter with public and private incarnations. Thus, with VoIP technology, a desk telephone is part of the cyber environment. However, even isolated devices can also be part of cyber environment if they can share information with connected computing devices through removable media.

The cyber environment include the software that runs on computing devices, the stored (also transmitted) information on these devices or information that are generated by these devices. Installations and buildings that house the devices are also part of the cyber environment. Cybersecurity needs to take such elements into consideration.

¹ The term "identity theft" refers only to the unauthorized use of the set identifiers and other information which, together, characterize the identity of a specific user. In contrast to the normal concept of theft, where the target item is physically removed from the victim, identity theft generally involves capturing or copying identity details such that the legitimate owner may not even be aware of the theft.

Cybersecurity aims at securing the cyber environment, a system that may involve stakeholders that belong to many public and private organizations, using diverse components and different approaches to security. As such, it is beneficial to think of cybersecurity in the following sense:

- The collection of policies and actions that are used to protect connected networks (including, computers, devices, hardware, stored information and information in transit) from unauthorized access, modification, theft, disruption, interruption or other threats.
- An ongoing evaluation and monitoring of the above policies and actions in order to ensure the continued quality of security in face of the changing nature of threats.

[b-ITU-T Y.2201] places requirements on NGN networks that can be used for enhancing the cybersecurity of these networks. The work calls for the support for authentication with the possibility of authenticating devices and users separately. In NGN, multi-factor bilateral authentication with support of authorization on a service-by-service level reduces the risks of user targeted attacks.

7.2 Nature of enterprise cybersecurity environment

Organizations need to devise a comprehensive plan for addressing its security needs. Security is not one size fit all (see [ITU-T X.805]). Security cannot be achieved by a collection of modules that are interconnected together. Organizations are encouraged to view security as a process or way of thinking on how to protect systems, networks, applications, and network services.

Security has to be comprehensive across all network layers. Adopting a layered approach to security that, when combined with strong policy management and enforcement, provides security professionals a choice of security solutions that could be modular, flexible, and scalable.

Security is difficult to test, predict and implement. Security is not a 'one size fits all' situation. The security needs and the recommended security strategy of each organization is unique and different. For example, an enterprise, a telecommunication provider, a network operator, or service providers each can have a unique set of business needs and may have evolved their networking environment to meet these needs.

A closed enterprise, for example, uses logical (e.g., frame relay) or physical private lines between sites, remote access provided selectively for employees needing access into the Internet. Web presence is achieved through an Internet data centre provided by a service provider (who is responsible for establishing a secure environment). The organization also provides conventional dial access for remote employees (e.g., working from a hotel). The company uses private e-mail among employees with no external access. Wireless LANs are also used.

An extended enterprise or a telecomm provider, network operator or service provider, through various business models, can provide support for remote employee and remote office access over IP VPNs over the Internet, or deliver higher speed, lower cost connectivity including general-purpose access into the Internet, such as interworking between internal e-mail systems and the rest of the world.

In an open enterprise, the business model can leverage the Internet by allowing partner, supplier and customer to have access to a enterprise-managed Internet data centre, even allowing selective access to internal databases and applications (e.g., as part of a supply chain management system). Internal and external users access the enterprise network from home, remote offices or other networks using wired or mobile devices. As such, the security requirement for such an enterprise is different from other enterprises.

A summary of enterprise types is given in Figure 7-1.

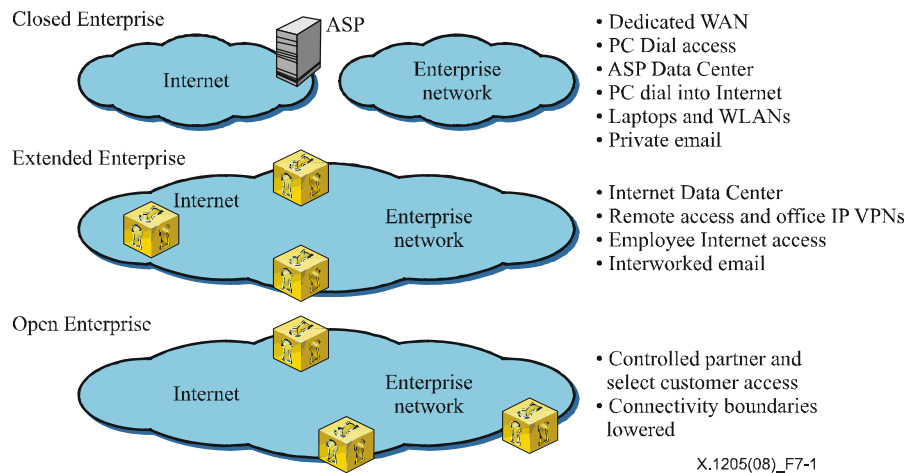


Figure 7-1 – Generic enterprise types

Cybersecurity requires risk management. This process involves the task of identifying the collective set of components that need to be protected. In order to facilitate the risk analysis, it is beneficial to consider attacks as belonging to the following categories:

- 1) **Service interruption attacks:** These types of attacks disable user access to the targeted services either temporary or permanently. Examples include lack of access to a web site, or the inability to conduct a financial transaction, or the ability to initiate a voice call. Several types of attacks can lead to service disruption. For example, denial of service (DoS), distributed denial of service attacks (DDoS), or damaging of buildings that host critical infrastructure could result in preventing users from accessing a service.
- 2) **Assets compromise:** These types of attacks involve theft or misuse of infrastructure. Attacks of this type can have an impact on cybersecurity if carried on a large scale.
- 3) **Component hijacking:** These types of attacks involve taking control of some devices and then using them to launch new attacks against other components of the cyber environment.

Any element of the cyber environment can be viewed as a security risk, which is generally thought of as a combined assessment of threat. Threat analysis includes the task of describing the type of possible attacks, potential attackers and their methods of attack and the consequences of successful attacks. On the other hand, vulnerability in this Recommendation refers to a weakness that could be exploited by an attacker. Risk assessment combined with threat analysis allows an organization to evaluate potential risk to their network.

Attacks can originate in the cyber environment, such as via worms or other malware, by direct attack on critical infrastructure, such as telecommunications cables, or through the actions of a trusted insider. A combination of these attacks is also possible. Risks are often characterized as high, medium, or low. The level of risk varies among different components of the cyber environment.

Security is all about risk management. In order to manage risks, many techniques can be used. For example, the development of a defence strategy that specifies countermeasures to possible attacks may be used; detection, which includes identifying an attack in progress or afterward; formulating a response to an attack that specifies the collection of countermeasures to an attack to either stop it or reduce its impact; formulating a recovery strategy that enables the network to resume operation from a known state.

7.3 Threats to cybersecurity and a methodology to address them

From an X.800 viewpoint, threats to a data communication system include the following:

- a) destruction of information and/or other resources;
- b) corruption or modification of information;
- c) theft, removal or loss of information and/or other resources;
- d) disclosure of information; and
- e) interruption of services.

According to [ITU-T X.800] threats can be classified as accidental or intentional and may be active or passive. Accidental threats are those that exist with no premeditated intent. Examples of realized accidental threats include system malfunctions, operational blunders and software bugs. Intentional threats may range from casual examination, using easily available monitoring tools, to sophisticated attacks using special system knowledge. An intentional threat, if realized, may be considered to be an "attack". Passive threats are those which, if realized, would not result in any modification to any information contained in the system(s), and where neither the operation nor the state of the system is changed. The use of passive wire tapping to observe information being transmitted over a communications line is a realization of a passive threat. Active threats to a system involve the alteration of information contained in the system, or changes to the state or operation of the system. A malicious change to the routing tables of a system by an unauthorized user is an example of an active threat. Appendix I provides a brief summary of some specific types of attacks.

The X.800 security threats equally apply to the cyber environment. According to [ITU-T X.800], security features usually increase the cost of a system and may make it harder to use. Before designing a secure system, therefore, a recommended practice is to identify the specific threats against which protection is needed. This is known as threat assessment. A system is vulnerable in many ways, but only some of them are exploitable because the attacker lacks the opportunity, or because the result does not justify the effort and risk of detection. Although detailed issues of threat assessment are beyond the scope of this Recommendation, in broad outline they include:

Threats are against assets, so the first step is to list out the assets that require protection. The next step of the assessment is a threat analysis, then a vulnerability analysis (including impact assessment), countermeasures and security mechanisms.

- a) identifying the vulnerabilities of the system;
- b) analysing the likelihood of threats aimed at exploiting these vulnerabilities;
- c) assessing the consequences if each threat were to be successfully carried out;
- d) estimating the cost of each attack;
- e) costing out potential countermeasures; and
- f) selecting the security mechanisms that are justified (possibly by using cost benefit analysis).

In some cases, non-technical measures, such as insurance coverage, may be a cost effective alternative to technical security measures. In general, perfect technical security is not possible. The objective, therefore, should be to make the cost of an attack high enough to reduce the risk to acceptable levels.

7.4 End-to-end communications security

[ITU-T X.805] defines a network security framework for addressing end-to-end network security. [ITU-T X.805] is applicable to various types of networks where the end-to-end security is a concern. The architecture is independent of a network underlying technology.

The security architecture addresses the global security challenges of service providers, enterprises, and consumers and is applicable to wireless, optical and wireline voice, data and converged networks. The architecture addresses security concerns for the management, control, and use of network infrastructure, services and applications. [ITU-T X.805] enables proactive detection and mitigation of security vulnerabilities for the known threats. The security architecture logically divides a complex set of end-to-end network security-related features into separate architectural components. This separation allows for a systematic approach to end-to-end security that can be used for planning of new security solutions, as well as for assessing the security of the existing networks.

In [ITU-T X.805], a security dimension is a set of security measures designed to address a particular aspect of network security. [ITU-T X.805] defines eight dimensions that protect against all major security threats. These dimensions are not limited to the network, but also extend to applications and end user information. The security dimensions apply to service providers or enterprises offering security services to their customers. 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.

In order to provide an end-to-end security solution, the security dimensions are applied to a hierarchy of network equipment and facility groupings, which are referred to as security layers. The following three security layers are addressed:

- 1) the infrastructure security layer;
- 2) the services security layer; and
- 3) the applications security layer.

The security layers identify where security is addressed in products and solutions by providing a sequential perspective of network security. For example, first security vulnerabilities are addressed for the infrastructure layer, then for the services layer and security vulnerabilities are addressed for the applications layer. Figure 7.4-1 depicts how the security dimensions are applied to security layers in order to reduce vulnerabilities that exist at each layer.

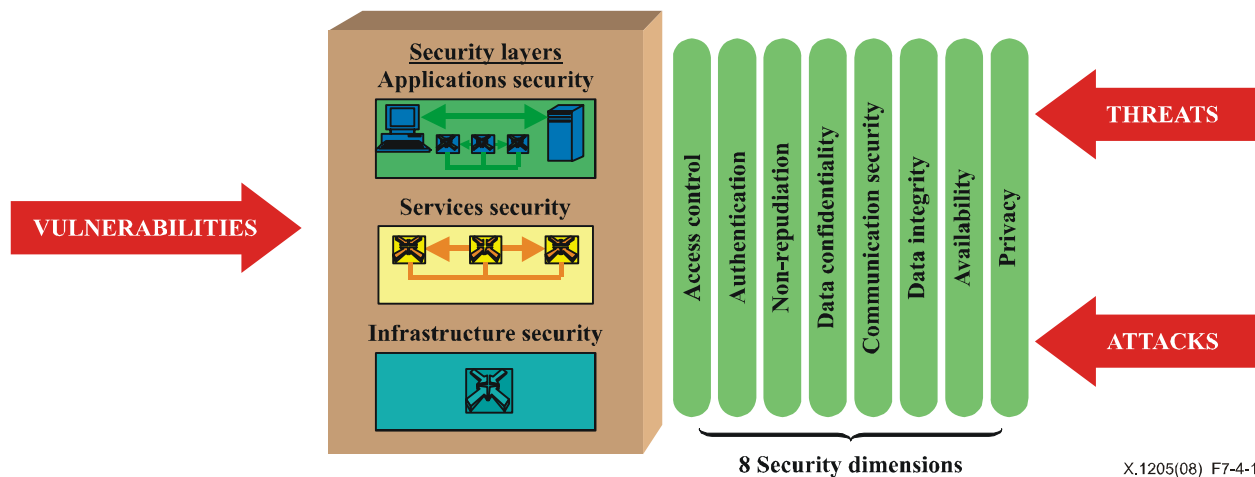


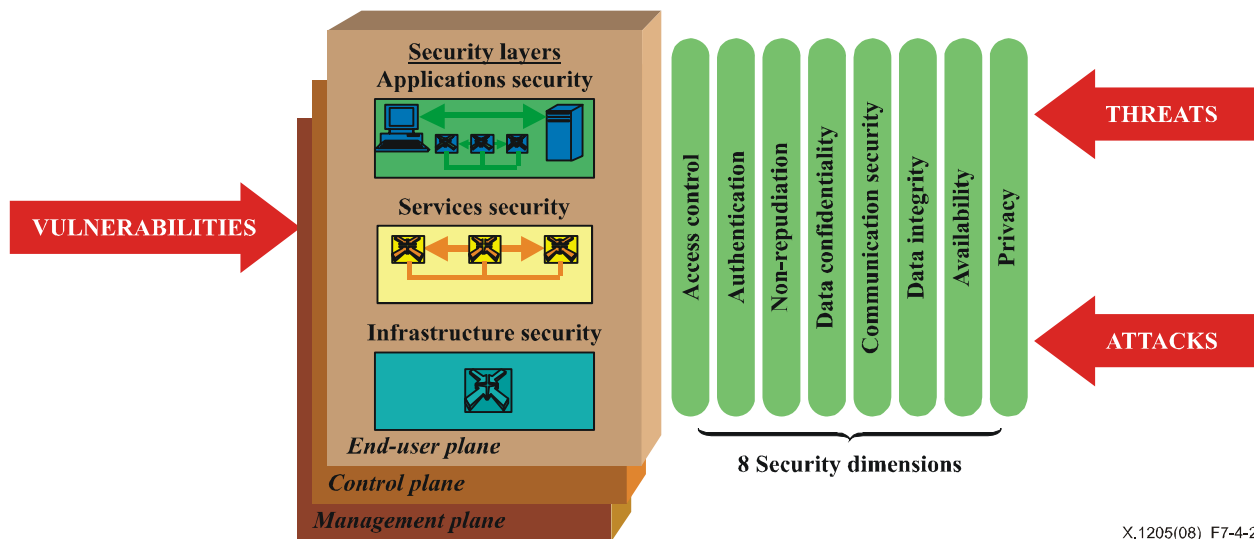
Figure 7-4.1 – Applying security dimensions to security layers

In [ITU-T X.805], a security plane is a certain type of network activity protected by security dimensions. [ITU-T X.805] defines three security planes to represent the three types of protected activities that take place on a network. The security planes are:

- 1) the management plane;
- 2) the control plane; and
- 3) the end-user plane.

These security planes address specific security needs associated with network management activities, network control or signalling activities, and end-user activities correspondingly. [ITU-T X.805] suggests that networks should be designed in such a way that events on one security plane are kept isolated from the other security planes. For example, a flood of DNS lookups on the end-user plane, initiated by end-user requests, should not lock out the OAM&P interface in the management plane that would allow an administrator to correct the problem.

Figure 7.4-2 illustrates the security architecture with the security planes included. The concept of security planes allows the differentiation of the specific security concerns associated with those activities and the ability to address them independently. For example, in a VoIP service, which is addressed by the services security layer, the task of securing the management of the service should be independent of the task of securing the control of the service. The task is independent of the task of securing the end-user data being transported by the service (e.g., the user's voice).



X.1205(08)_F7-4-2

Figure 7-4.2 – Security planes reflect the different types of network activities

8 Possible network protection strategies

Security includes all the architectural layers of a network. This approach provides a good starting point for the design of secure networks. This decomposition enables a higher layer to define their own security requirements at that specific layer, and also enables it to use the security services of the lower levels. The layered security approach allows the development of flexible, scalable security solutions across the network level, application level and management level for all organizations.

8.1 Closed loop policy management

A properly designed and implemented security policy is an absolute requirement for all types of enterprises and organizations. The security policy typically is a living document and process, which is enforced, implemented and updated to reflect the latest changes in the enterprise or organization infrastructure and service requirements.

The security policy clearly identifies the resources in the organization (also the enterprise) that are at risk and resulting threat mitigation methodologies. The security policy provides for performing vulnerability and risk assessment, and defines appropriate access control rules. Risk and vulnerability assessment are performed at all levels of the network. The policy is able to help identify and discover security violations, and states the specified violation responses.

It is recommended that IT and network administrators use tools to perform vulnerability assessment on their networks. The principle of the least privilege access is followed. IT and network administrators tasks include to ensure that audits trails are reviewed, thus closing the loop on policy management. If problems are discovered in the audits, IT and network administrators ensure that the policy is updated to reflect the revised actions.

A security policy that is not enforced is worthless. The enforcement of the security policy is dependent on people. There should be clear responsibility and accountability for policy enforcement.

8.2 Uniform access management

The term access management is used to define systems that may make use of both authentication and authorization services in order to control the use of a resource. Authentication is the process in which a user or entity requests the establishment of an identifier to a network. Authorization determines the level of privileges of that entity based on access control. The control of the level of access is based on a control policy definition and its enforcement. Figure 8-2 depicts the reference model for secure authentication and authorization.

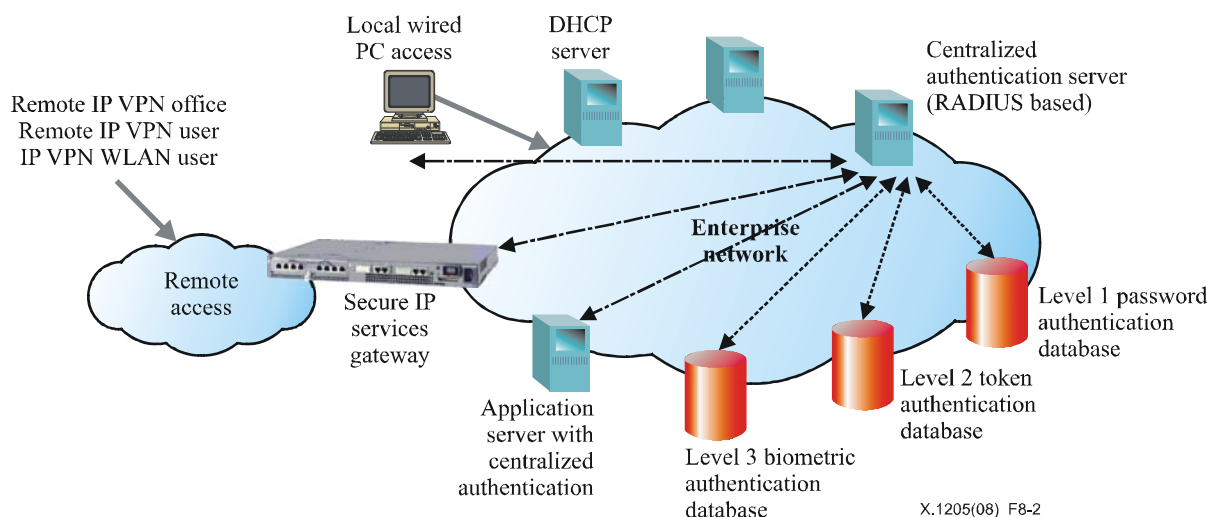


Figure 8-2 – Secure authentication and authorization reference model

From Figure 8-2, the following recommendations are given:

- 1) The use of a centralized authentication mechanism in order to facilitate administration and remove the need for locally stored passwords. (Locally stored passwords tend to be static and weak.)
- 2) The use of a centralized authorization system, tightly coupled with authentication system, with appropriate granularity for the particular enterprise.
- 3) Enforcement of strong (complex) passwords rules for all passwords.
- 4) Secure storage of all passwords in a one-way encrypted (hashed) format.
- 5) The principle of simplicity that implies ease of use and ease of administration. A simple system is a secure system since safeguards are much more likely to be followed.
- 6) Secure logging of all security related events with respect to authentication and authorization.

Approaches to access management include: IP source filtering, proxies and credential-based techniques. Each approach has its advantages and limitations. Depending on the type of the enterprise and within a given type, more than one or a combination of approaches may be used. For example, an enterprise may choose to manage access for workstations using IP source filtering, and may choose to use a credential-based scheme for other users.

Several methods can be used to authenticate a user. Techniques include: passwords, one-time pass, biometric techniques, smart cards, and certificates. Passwords-based authentication must use strong passwords (e.g., that are at least eight characters in length with at least one alphabetic, one numeric and one special character). Password authentication alone may be insufficient. Based on vulnerability assessment, it may be necessary to combine password authentication with other authentication and authorization processes, such as certificates, lightweight directory access

protocol (LDAP), remote authentication dial-in user service (RADIUS), Kerberos, and public key infrastructure (PKI).

All authentication mechanisms have advantages and drawbacks. UserID/password combinations are simple, low cost, and easy to manage; however, remembering a multitude of complex passwords is very difficult for users. Two-factor and three-factor authentication systems add additional authentication strength; however, all are costly, add additional complexity and are difficult to maintain.

A "single password" system with enforced strong passwords can be a good solution for enterprise authentication and authorization. Such system provides high authentication security, granular authorization, and is easier to administer. With this system, a user's strong single password is synchronized with many applications and systems enterprise wide for authentication and authorization. All enterprise systems and applications automatically refer authentication and authorization functions to the single password system. As users only have to remember is one strong password making the system simple to use and not likely to be bypassed. The advantages to single-password system are:

- Single consistent method for setting passwords.
- Single consistent method for authentication and authorization.
- Single method for registration and termination of user accounts.
- Enforcement of corporate password strength guidelines.
- Consistency – users know what to do.
- Standardization – easy to support and adopt.
- Fast – standard interface and APIs.
- Lower costs, lower help calls.

The open and the extended enterprise face the most challenges when designing their access management policy. It is advantageous to consider access management as an integral component of the security policy. These organizations should design of a uniform access management system with fine-grained rules that properly interfaces with:

- Directories and databases holding identity attributes
- Multiple authentication systems such as password, Kerberos, TACACS and RADIUS
- Hosts, applications and application servers.

The uniform access management system performs session management per user after the user is authenticated. The use of flexible configuration and policy enforcement with fine-grained rules that is capable of dealing with specific objects is recommended. Appropriate monitoring, accounting and secure audit trails. The use of unique accounts for each administrator with accountability for actions traceable to individuals is recommended.

8.3 Secure communications

Unified networks can carry voice, data and video packets. The objective of securing network traffic is to ensure the confidentiality, integrity and accuracy of network communications. Security should be available for call and signalling traffic in telephony networks. Encryption technology is used for data and voice and mobile networks.

Encryption can be achieved by:

- VPN techniques using IPSec, with authentication header (AH) and encapsulating security payload (ESP) or tunnelling through the use of layer 2 tunnelling protocol (L2TP).
- Key management based on Internet key exchange (IKE).
- Certificate management based on public key infrastructure [b-ITU-T X.509] (PKIX).