

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

X.1111

(02/2007)

SERIES X: DATA NETWORKS, OPEN SYSTEM
COMMUNICATIONS AND SECURITY

Telecommunication security

Framework of security technologies for home network

ITU-T Recommendation X.1111



International
Telecommunication
Union

Documents
Document Sharing Hub

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.

ITU-T Recommendation X.1111

Framework of security technologies for home network

Summary

ITU-T Recommendation X.1111 describes security threats and security requirements to the home network from the point of view of home user and remote user. It excludes the security requirements from the service provider's viewpoint. In addition, this Recommendation categorizes security technologies by security functions that satisfy the above security requirements and by the place to which the security technologies are applied to in the model of the home network. Finally, the security function requirements for each entity in the network and possible implementation layers for security function are also presented.

Source

ITU-T Recommendation X.1111 was approved on 13 February 2007 by ITU-T Study Group 17 (2005-2008) under the ITU-T Recommendation A.8 procedure.

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, 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 2007

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	OSI reference model security architecture definitions	2
3.2	Mobile security framework definitions	2
3.3	Home network-related definitions	3
3.4	Terms defined in this Recommendation.....	3
4	Abbreviations and acronyms	4
5	General home network model for security	4
6	Characteristics of the home network	6
6.1	Various transmission mediums can be used for the home network	6
6.2	Home network is a combination of a wireless network and a wired network	6
6.3	There are many environments from the security point of view.....	6
6.4	Remote terminals are carried around by remote users	6
6.5	There are various types of home network devices requiring different levels of security	6
7	Security threats in the home network environment	6
7.1	General security threats from ITU-T Rec. X.1121.....	7
7.2	Mobile-oriented security threats from ITU-T Rec. X.1121	7
7.3	Security threats from ITU-T Rec. X.805.....	8
7.4	Relationship of security threats in the home network	8
8	Security requirements for home network	11
8.1	Security requirements from ITU-T Recs X.805 and X.1121	11
8.2	Relationship between security requirements and security threats.....	12
9	Security requirements in the entities and relationships of the home network	14
10	Security functions for satisfying security requirements in the home network	15
10.1	Security functions from ITU-T Rec. X.1121.....	15
10.2	Additional security functions	18
10.3	Relationship between a security requirement and a security function	18
11	Security technologies for home network	19
12	Security function requirements for home network	22
	Annex A – Type of home network device in ITU-T Rec. J.190.....	23
	Appendix I – Type of home network devices in UPnP.....	25
	Bibliography.....	26

ITU-T Recommendation X.1111

Framework of security technologies for home network

1 Scope

The home network is an important part of an end-to-end data communication network. Because it uses various wired or wireless transmission techniques, the threats to the home network could be equivalent to those resulting from either wired network or wireless network.

In order to establish the security framework for home network, it is required to identify threats to the home network and find out the necessary security functions in the entities of home network model. It is found that the threat model to the home network is basically the same as the threat model described in [ITU-T X.1121] "Framework of security technologies for mobile end-to-end data communications". Therefore, [ITU-T X.1121] is used as a base Recommendation for setting up the framework for security technologies in the home network.

This Recommendation describes security threats and security requirements to the home network from the point of view of home user and remote user. In addition, this Recommendation categorizes security technologies by security functions that satisfy the above security requirements and by the place to which the security technologies are applied to in the model of the home network. Finally, the security function requirements for each entity in the network and possible implementation layers for security function are also presented.

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 J.190] ITU-T Recommendation J.190 (2002), *Architecture of MediaHomeNet that supports cable-based services*.
- [ITU-T J.192] ITU-T Recommendation J.192 (2005), *A residential gateway to support the delivery of cable data services*.
- [ITU-T Q.1701] ITU-T Recommendation Q.1701 (1999), *Framework for IMT-2000 networks*.
- [ITU-T Q.1711] ITU-T Recommendation Q.1711 (1999), *Network functional model for IMT-2000*.
- [ITU-T Q.1761] ITU-T Recommendation Q.1761 (2004), *Principles and requirements for convergence of fixed and existing IMT-2000 systems*.
- [ITU-T X.800] ITU-T Recommendation X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT applications*.
- [ITU-T X.803] ITU-T Recommendation X.803 (1994), *Information technology – Open Systems Interconnection – Upper layers security model*.
- [ITU-T X.805] ITU-T Recommendation X.805 (2003), *Security architecture for systems providing end-to-end communications*.

- [ITU-T X.810] ITU-T Recommendation X.810 (1995), *Information technology – Open Systems Interconnection – Security frameworks for open systems: Overview*.
- [ITU-T X.1121] ITU-T Recommendation X.1121 (2004), *Framework of security technologies for mobile end-to-end data communications*.

3 Definitions

3.1 OSI reference model security architecture definitions

The following terms are defined in [ITU-T X.800]:

- a) access control;
- b) authentication;
- c) authentication information;
- d) authentication exchange;
- e) authorization;
- f) availability;
- g) confidentiality;
- h) cryptography;
- i) data integrity;
- j) data origin authentication;
- k) encipherment;
- l) firewall;
- m) integrity;
- n) key;
- o) key exchange;
- p) key management;
- q) malware;
- r) non-repudiation;
- s) notarization;
- t) password;
- u) privacy.

3.2 Mobile security framework definitions

The following terms are defined in [ITU-T X.1121]:

- a) anonymity;
- b) shoulder surfing;
- c) mobile terminal;
- d) mobile network;
- e) mobile user;
- f) application service;
- g) application server;
- h) application service provider;
- i) mobile security gateway;

- j) security policy management.

3.3 Home network-related definitions

The following terms are defined in [ITU-T J.190]:

- a) home access (HA);
- b) home bridge (HB);
- c) home client (HC);
- d) home decoder (HD);
- e) residential gateway;
- f) home network planes.

3.4 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.4.1 secure home gateway: A secure home gateway is a kind of residential gateway seen from the point of view of security, and a point or an entity which forwards data packets from open network to internal home network or vice versa, changes security parameter or communication protocol from home network to open network or vice versa, and can perform security-related functions, such as packet filtering, intrusion detection, and policy management function and so on, according to a given security policy. That is, a secure home gateway comprises more than only firewall.

3.4.2 home device: A home device is an entity (or a home appliance), such as PDA, PC, and TV/VCR, which controls or is controlled by another home device, or provides a service to home users. There are three types of home devices from the security point of view: type A, type B and type C. Type A home device, such as remote controller, PC or PDA, has a controlling capability of the type B home device or type C home device through the presentation page and rich display. Type B home device is a bridge that connects type C home devices with no communication interface to the home network; basically it communicates with the other devices in the home network on one end and uses some proprietary language on the other end (some examples include proprietary lighting control, etc.). Type C home device, such as security cameras, A/V devices, etc., only provides some sort of service to the rest of the home devices. Type A or type C home device is called a security console, if it has a security ownership of type B home device or type C home device. Any device in the home network can be classified into type A, type C or type A/type C according to the functionalities of a device.

3.4.3 home application service provider: A home application service provider (or a home application server) is an entity that connects to the home network for data communication with home device or remote terminal, stores the multimedia content, or provides a variety of the application services to the rest of home devices within home or a remote terminal outside home.

3.4.4 ID certificate: An ID certificate is a message that, at least, states a name or identifies the issuing authority, identifies the subject, contains the subject's public key, identifies the validity period of certificate, contains serial number, and is digitally signed by a CA.

3.4.5 device certificate: A device certificate is an X.509 version 3 certificate used for identity authentication of home network device. It may be issued by CA.

3.4.6 authorization certificate: An authorization certificate is a signed object that empowers the subject. It contains at least an issuer and a subject. It can contain validity conditions, authorization and delegation information. In general, certificates can be grouped into three categories: ID certificate which maps the name and a public key of a subject, attribute certificate that maps an authorization and a name of the subject, and authorization certificate that maps an authorization and

a public key of subject. An authorization or attribute certificate can delegate all the permissions it has received from the issuer or it can delegate along only a portion of that empowerment.

3.4.7 access control list (ACL): An ACL is a protected table residing in memory in the same device as a resource whose access is protected. It is a set of entries, and each entry contains the following: subject, authorization, delegation and validity. The subject is an identifier of the entity being granted access, the authorization is an indicator of the permission being granted that subject, the delegation is a flag, indicating whether the subject may further delegate these rights, the validity is an optional field on the validity of the entry such as "not-after" and "not-before" date and time. Access control list is a list of entries that anchors a certificate chain. Sometimes called a "list of root keys", the ACL is the source of empowerment for certificates. That is, a certificate passes permission from its issuer to its subject, but the ACL is the source of that permission (since it theoretically has the owner of the resource it controls as its implicit issuer). An ACL entry has potentially the same content as a certificate body, but has no issuer (and is not signed). There is most likely one ACL for each resource owner, if not for each controlled resource.

3.4.8 remote terminal: Remote terminal is an entity that has network access function and an Internet interface to connect or control the home devices in the home network.

3.4.9 remote user: Remote user is an entity (person) outside the home network that uses and operates the remote terminal for accessing the devices in the home network.

3.4.10 home user: home user is an entity (person) within the home network that uses and operates the remote terminal for accessing the devices in the home network.

3.4.11 security console: Security console is a device which offers a user interface for administration of access control on other devices from the security point of view.

3.4.12 administrator of home network: A home network administrator is an entity or an agent that performs security-related activities, such as a key generation, a key store, and a key distribution, and monitors the status of entities in the home network.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

ACL	Access Control List
ASP	Application Service Provider
DoS	Denial of Service
MAC	Message Authentication Code
OSI	Open Systems Interconnection
PC	Personal Computer
PDA	Personal Data Assistant
PIN	Personal Identification Number

5 General home network model for security

Before describing the security technologies, a general home network model for security should be defined from the security viewpoint. The general home network model for security is to identify all entities in the home network, to clarify the relationship between entities in the model and the location to which the secure mobile technologies should be applied.

General home network model for security is shown in Figure 1. In the home network, there are many home devices, such as PDA, PC, and TV/VCR, which control the other one or are controlled

by other home devices, or provide a service to home users. However, these home devices are classified into three types from the viewpoint of its role: type A, type B and type C. Type A home device, such as remote controller, PC or PDA, has a controlling capability of the type B home device or type C home device through the presentation page and rich display. Type B home device is a bridge that connects type C home devices with no communication interface to the home network; basically it communicates with the other devices in the home network on one end and uses some proprietary language on the other end (some examples include proprietary lighting control, etc.). Type C home device, such as security cameras, A/V devices, etc., only provides some sort of service to the rest of the home devices. Type A or type C home device is called a security console, if it has a security ownership of type B home device or type C home device.

The legacy home device is normally one with no communication interface, but proprietary path to be connected to type B home device, so it can be attached to the home network via type B home device. Some home devices have combined functions with type A home device and type C home device.

Figure 1 shows the general home network model for security.

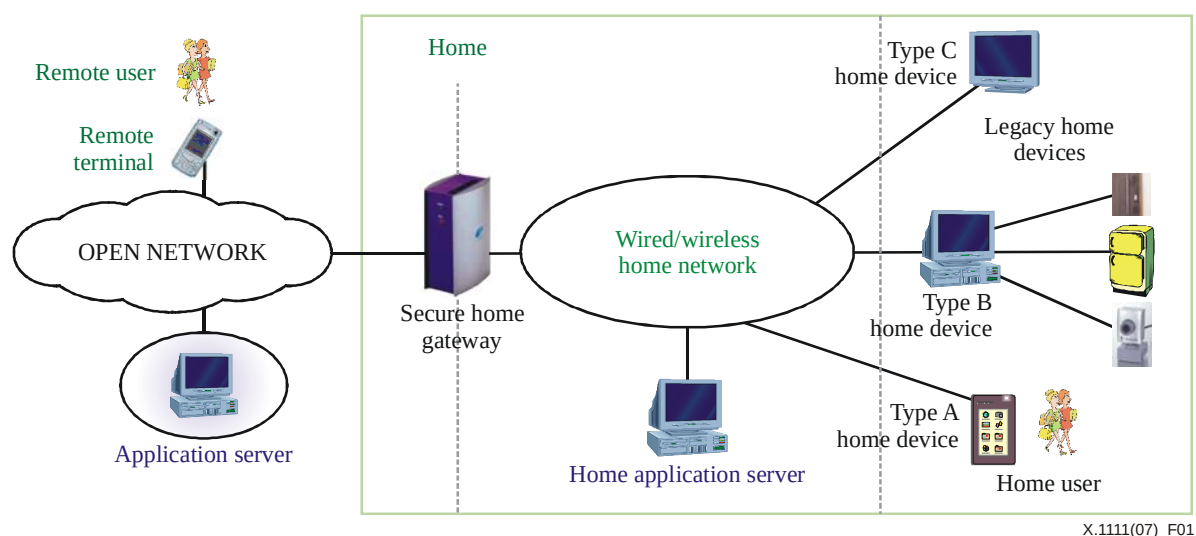


Figure 1 – General home network model for security

There are seven entities in this model: remote user, remote terminal, application server, secure home gateway, home application server, home user and home devices. Again, the home devices can be grouped into three categories of home devices: type A home device, type B home device, type C home device.

And there are thirteen relationships in this model, between: remote user and remote terminal, remote terminal and secure home gateway, remote terminal and home application server, remote terminal and home device, application server and secure home gateway, application server and home application server, application server and home device, secure home gateway and home device, home application server and home device, home device and home user, home device and other home device, remote terminal and type A home device, and secure home gateway and home application server.

The use case to home network is one, in which a person is able to listen to music stored on a server using a portable stereo unit. In fact, several people may be accessing and playing audio content from different locations in the home or even outside the home using different network players. The other one is a video sharing case, in which the family members are able to enjoy media content in different rooms. For example, the son is sharing some camp pictures with friends in the family room