

International Telecommunication Union

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



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.

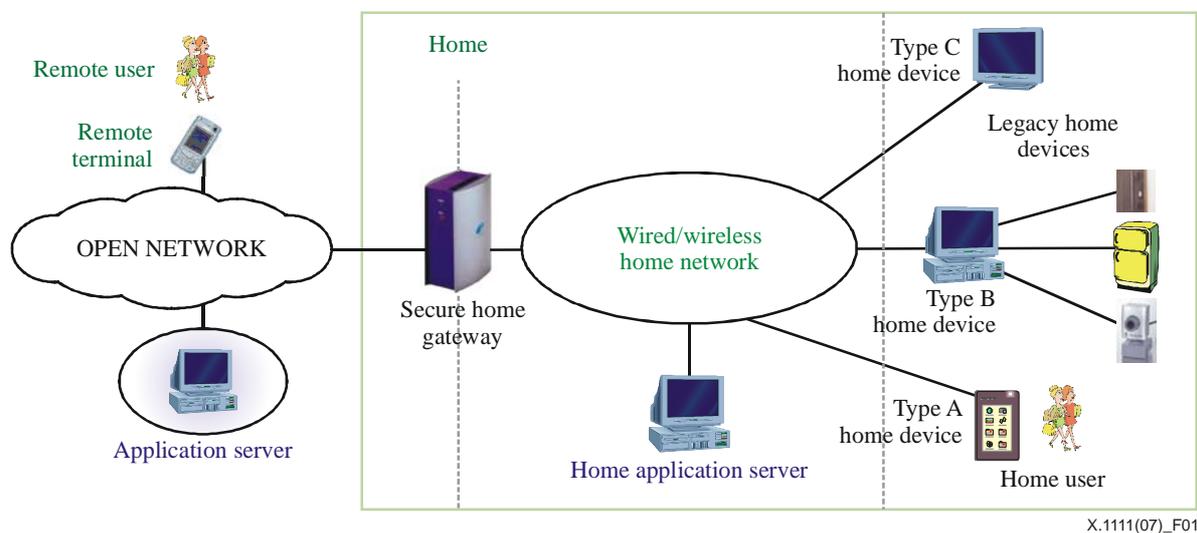


Figure 1 – General home network model for security

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

where the pictures are stored on the father's PC and the mother watches a TV show recorded earlier in the week on the networked DVR, which is in the family room and she selects the program and adjusts play settings all from a second remote.

6 Characteristics of the home network

6.1 Various transmission mediums can be used for the home network

Various transmission mediums, such as power lines, radio communication, and wired cable, can be used to transmit a signal in the home network. So, it is very susceptible to a variety of attacks, such as eavesdropping, interruption, denial of service, man-in-the middle attack, and so on.

6.2 Home network is a combination of a wireless network and a wired network

As various transmission techniques can be applied to home network, the home network consists of a wireless network and wired network. A wireless network, especially a wireless network in which authorization and encryption is not implemented or not enabled, is more vulnerable to security threats than is a wired network. This is due to the greater opportunity for receipt of unwanted or unauthorized traffic via the wireless medium than via the wired medium. So, threats in the home network consist of those from both a wired network and a wireless network. All the countermeasures to threats should be taken into consideration for secure home network and it is very difficult to establish the secure home network as a lot of security technologies should be adopted.

6.3 There are many environments from the security point of view

The home has a variety of environments, such as environment with single-person home, environment with a couple with small children, environment with families with teenagers, environment with adults and roommates, and so on. So, there needs to be more than one security domain in the home network. Therefore, authentication and authorization are needed for secure home network.

6.4 Remote terminals are carried around by remote users

The remote user outside home would use the remote terminal to control the home device in the home, to have an application service from the home device over the open network. For instance, a user can close or open the curtains of a window or turn the light on or off before he or she arrives home using the remote terminal outside home.

6.5 There are various types of home network devices requiring different levels of security

There are so many types of home network devices: AV, PC, Tel/fax and home appliance. A different type of home device needs a different level of security requirement. Moreover, it is very difficult to define a general security requirement satisfying all the types of home devices.

7 Security threats in the home network environment

Home network consists of wired network and wireless network. The threats in the home network are equivalent to those existing in both the wired network and wireless network. The threats model in [ITU-T X.1121] can be used as a base for establishing the threats in the home network. The threats model to home network can be grouped into two categories: general security threats and mobile-oriented security threat, except for input error, as described in [ITU-T X.1121], because the input error is made by the user and cannot be protected by using current security technologies.

7.1 General security threats from ITU-T Rec. X.1121

7.1.1 Eavesdropping/Disclosure/Interception

The most widely identified problem in open networks is eavesdropping by anonymous attacks. Anonymous attackers can actively intercept transmitted data, causing a disclosure of data. Assuming the communication is not encrypted, an attacker can read data transmitted in the communication and gain some information, such as source address, destination address, size of transmitted data, time and date of transmissions, and so on. This is an attack on confidentiality. Examples include wiretapping to obtain data in the transmission, and illegal copying of files or programs.

7.1.2 Interruption/Communication jamming

Communication jamming takes place when an intentional or unintentional interference overpowers the sender or receiver of a communication link, thereby effectively rendering the communication link useless. This can result in a DoS attack.

Interruption results in the destruction of a component of a remote terminal or a network element, examples include destruction of a piece of hardware, such as a hard disk; the cutting of a communication line; or the disabling of the file management system in a remote terminal or an entity in the home network.

7.1.3 Injection and modification of data

This occurs when an unauthorized entity inserts, changes, or deletes information transmitted between a remote terminal and an application server. The unauthorized entity could be a person, a program, or a computer. These attacks occur when an attacker adds data to an existing connection with the intent of hijacking the connection or maliciously sending data. This can result in a DoS attack or man-in-the-middle attack. This is an attack on integrity. Examples include changing values in the data file, altering a program so that it performs differently, and modifying the content of the message being transmitted in the home network.

7.1.4 Unauthorized access

Access control is the ability to limit and control the access to an application server via a communication link. This threat occurs when an illegal entity gains access to an application server, a home application server, or home device by masquerading as a real remote user. The entity trying to gain an unauthorized access must be identified, or authenticated. In addition, there are two major attacks: port scanning and the malware. The port scanning is similar to a thief going through your neighbourhood and checking every door and window on each house to see which ones are open and which ones are locked. The type of port scanning can be performed by the scanner in the home network or attacker to check which ports of the home network element or system are open or closed. The malware is a short term for malicious software. It is designed specifically to damage or disrupt a system, such as a virus or a Trojan horse. These two attacks may result in an unauthorized access to the home network element or devices.

7.1.5 Repudiation

This attack occurs when a sender or receiver denies the fact of having transmitted or received a message, respectively.

7.2 Mobile-oriented security threats from ITU-T Rec. X.1121

7.2.1 Eavesdropping/Disclosure/Interception

In mobile communications, this can be carried out more easily by actively intercepting radio signals and decoding the data being transmitted, causing a leakage of data. The eavesdropping is due to the

radio-based nature of the wireless transmission. In passive eavesdropping, the attacker passively monitors and has access to the transmission.

7.2.2 Interruption/Communication jamming

In mobile communications, this can also be carried out more easily in a home network using a wireless transmission technology. There are two types of attacks: jamming against a remote terminal and jamming against a network element. The former allows the rogue remote terminal to impersonate the legal remote terminal. The latter impersonates the legitimate network element interfacing with the remote terminal through the wireless interface.

7.2.3 Shoulder surfing

This occurs when an attacker collects information in busy places by watching keystroke, reading a remote terminal's screen, or listening to sound from a remote terminal. This results in leakage of information.

7.2.4 Lost remote terminal

This security threat may occur as the remote terminal is carried around by the remote user. This can result in the loss or destruction of information stored in the remote terminal.

7.2.5 Stolen remote terminal

This threat may also occur as the remote terminal is carried around by the remote user. This can cause leakage of information stored in the remote terminal, data deletion resulting from unauthorized access of the stolen remote terminal in addition to the loss of information stored in the remote terminal.

7.2.6 Unprepared communication shutdown

This is a security threat caused by unstable communication or the limitation of power supply. This can result in data deletion.

7.2.7 Misreading

This is a security threat caused by a small display of remote terminals. This can result in data deletion by masquerading of ASP.

7.2.8 Input error

This is a security threat caused by the difficulty of inputting data via a small keyboard or the keypad of a remote terminal. This can cause the failure of user authentication.

7.3 Security threats from ITU-T Rec. X.805

7.3.1 Packet abnormal-forwarding

Packet abnormal-forwarding is the threat that the packet is not diverted or intercepted as it flows between these end points. It may happen in the secure home gateway due to misconfiguration of the routing table.

7.4 Relationship of security threats in the home network

These security threats appear in a particular entity or location in the home network models. The relationship of security threats and functional entities in the home network is shown in Tables 1 and 2. In Tables 1 and 2, the letter 'Y' in a cell formed by the intersection of the table's columns and rows designates that a particular threat exists for a specific entity or relationship.

These two tables show that there are the same security threats in a remote terminal, a home device, a home application server, and a secure home gateway. Moreover, these tables also show that there

are many similarities of threats in the relation between: remote terminal and secure home gateway; remote terminal and home devices; remote terminal and home application server, and so on.

Table 1 – Relationship of general security threats to models

Threats Entities or relations	Disclosure/ Eavesdropping		Interruption		Modification/ Injection		Unauthorized access		Repudiation	Packet abnormal- forwarding
	Stored data	Communi- cation data	Stored data	Communi- cation data	Stored data	Communi- cation data	Stored data	Communi- cation data		
Remote terminal	Y		Y		Y		Y			
Home device	Y		Y		Y		Y			
Secure home gateway	Y		Y		Y		Y			Y
Home application server	Y		Y		Y		Y			
Relation between remote user and remote terminal								Y*		
Relation between remote terminal and secure home gateway		Y		Y		Y		Y		
Relation between remote terminal and home application server		Y		Y		Y		Y	Y	
Relation between remote terminal and type B or C home device		Y		Y		Y		Y		
Relation between application server and secure home gateway		Y		Y		Y		Y		
Relation between application server and home application server		Y		Y		Y		Y	Y	
Relation between application server and home device		Y		Y		Y		Y	Y	
Relation between secure home gateway and home device		Y		Y		Y		Y		
Relation between home application server and home device		Y		Y		Y		Y		
Relation between type A home device and type B or C home device		Y		Y		Y		Y		
Relation between type A home device and home user								Y*		
Relation between secure home gateway and home application server		Y		Y		Y		Y		
Relation between remote terminal and type A home device		Y		Y		Y		Y		

* This means the unauthorized access to remote terminal by unauthorized user, not to communication data.

Table 2 – Relationship of mobile-oriented security threats for a wireless network only and models

Threats Entities or relations	Disclosure/Eavesdropping		Interruption/Communication jamming		Shoulder surfing	Lost/Stolen terminal	Unprepared shutdown	Misreading /input error
	Stored data	Communi- cation data	Stored data	Communi- cation data				
Remote terminal						Y		
Home device						Y		
Secure home gateway								
Home application server								
Relation between remote user and remote terminal					Y			Y
Relation between remote terminal and secure home gateway		Y		Y			Y	
Relation between remote terminal and home application server		Y		Y			Y	
Relation between remote terminal and type B or C home device		Y		Y			Y	
Relation between application server and secure home gateway		Y		Y				
Relation between application server and home application server		Y		Y				
Relation between application server and type B or C home device		Y		Y			Y	
Relation between secure home gateway and type B or C home device		Y		Y			Y	
Relation between home application server and type B or C home device		Y		Y			Y	
Relation between type A home device and type B or C home device		Y		Y			Y	
Relation between type A home device and home user					Y			Y
Relation between secure home gateway and home application server		Y		Y			Y	
Relation between remote terminal and type A home device		Y		Y			Y	

8 Security requirements for home network

Considering that a home network consists of wired network or wireless network, security requirements for home network threats are similar to those of [ITU-T X.1121]. The security requirements in [ITU-T X.1121] can be used as a base for establishing the security requirements in the home network. While some specific security requirements can be applied to two types of data, which consist of the stored data on a specific element and communication data between the entities, others can be applied to only communication data between the entities. In this Recommendation, two types of security requirements in [ITU-T X.1121] are grouped into one type of security requirement, because two types of security requirements can be considered as one security requirement especially for the home network. In addition, communication flow security requirement from [ITU-T X.805] is added for secure home gateway, because it ensures that information flows only between the authorized entities in the home network. (The information is not diverted or intercepted as it flows between these authorized entities.)

8.1 Security requirements from ITU-T Recs X.805 and X.1121

8.1.1 Data confidentiality

Data confidentiality protects data from unauthorized disclosure. Data confidentiality ensures that the data content cannot be read by unauthorized entities. Encryption, access control lists, and file permissions are methods often used to provide data confidentiality.

8.1.2 Data integrity

Data integrity ensures the correctness or accuracy of data. The data is protected against unauthorized modification, deletion, creation, and replication and provides an indication of these unauthorized activities.

8.1.3 Authentication

Authentication is the process of identifying that individuals are who they claim to be or of ensuring the identity of the sender whom the message claims to be from. There are two types of authentication: entity authentication and message authentication. While entity authentication ensures the validity of the claimed identities of the entities, message authentication ensures that a message is originated from the claimed entity. Entity authentication serves to confirm the identities of communicating entities. Message authentication ensures the validity of the claimed identities of the entities participating in communication (e.g., person, device, service or application) and provides assurance that an entity is not attempting a masquerade or unauthorized replay of a previous communication. Authentication could be achieved by using ID certificate for a user and device certificate for a home device.

8.1.4 Access control or authorization

Access control protects against unauthorized use of network resources. Access control ensures that only authorized personnel or devices are allowed access to network elements, stored information, information flows, services and applications. In addition, role-based access control (RBAC) provides different access levels to guarantee that individuals and devices can only gain access to and perform operations on network elements, stored information, and information flows that they are authorized for. There are three types of authorization: authorization using ACL (access control list), authorization using authentication server, authorization using the authorization certificate or the attribute certificate and ID certificate. Access control or authorization could be achieved by using authorization certificate and access control list. Access control or authorization at the entry point of the home network can be performed by a firewall as a secure home gateway. The firewall is designed mainly to prevent unauthorized access from a public network. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially intranets. All messages entering or leaving the intranet pass through the firewall,

which examines each message and blocks those that do not meet the specified security criteria or policy.

8.1.5 Non-repudiation

Non-repudiation provides the means for preventing an individual or entity from denying having performed a particular action related to data by making available proof of various network-related actions (such as proof of obligation, intent, or commitment; proof of data origin, proof of ownership, proof of resource use). It ensures the availability of evidence that can be presented to a third party and used to prove that some kind of event or action has taken place.

8.1.6 Communication flow security

Communication flow security ensures that information flows only between the authorized end points (the information is not diverted or intercepted as it flows between these end points). This communication flow security should be applied to the secure home gateway in a home network environment.

8.1.7 Privacy security

Privacy security provides for the protection of information that might be derived from the observation of network activities or communication. Examples of this information include web sites that a user has accessed to, a user's geographic location, and the source and destination IP addresses and DNS names of devices in a service provider network. In addition, the privacy includes the ID privacy in the home network.

8.1.8 Availability

Availability ensures that there is no denial of authorized access to network elements, stored information, information flows, services and applications due to events impacting the network. Disaster recovery solutions are included in this category. A variety of attacks can result in the loss of or reduction in availability. Some of these attacks are amenable to automated countermeasures, such as authentication and encryption, while others require some sort of physical action to prevent or recover from loss of availability of network elements.

8.2 Relationship between security requirements and security threats

Each security requirement is a countermeasure against some or all certain security threats in home network. The relationship between security requirements and security threats is shown in Tables 3 and 4 for the home network. In Tables 3 and 4, the letter 'Y' in a cell formed by the intersection of the table's columns and rows designates that a particular security requirement should be provided in order to remove or mitigate a specific threat. Misreading and input error can be prevented by careful design of entities or attention of a user, which is not basically the issue of security technology. So, there is no mark related to misreading/input error.

Table 3 – Relationship between security requirements and general security threats

Security requirement \ Threats		Disclosure/Eavesdropping		Interruption		Modification/Injection		Unauthorized access		Repudiation	Packet abnormal-forwarding
		Stored data	Communication data	Stored data	Communication data	Stored data	Communication data	Stored data	Communication data		
Confidentiality	Communication data		Y						Y		
	Stored data	Y						Y			
Integrity	Communication data						Y				
	Stored data					Y					Y
Authentication	Entity	Y		Y		Y		Y		Y	
	Message	Y		Y			Y	Y		Y	
Non-repudiation										Y	
Access control	Communication data						Y		Y		
	Stored data	Y		Y		Y		Y			
Availability	Communication data				Y						
	Stored data			Y							
Privacy	Communication data		Y								
	Stored data										
Communication flow security											Y

Table 4 – Relationship between security requirements and mobile-oriented security threats for a wireless only

Security requirement \ Threats		Disclosure/Eavesdropping		Interruption		Shoulder surfing	Lost/Stolen terminal	Unprepared shutdown	Misreading/Input error
		Stored data	Communication data	Stored data	Communication data				
Confidentiality	Communication data		Y						
	Stored data	Y					Y		
Integrity	Communication data								
	Stored data								
Authentication	Entity	Y		Y			Y		
	Message	Y		Y					
Non-repudiation									
Access control	Communication data								
	Stored data	Y		Y			Y		
Availability	Communication data				Y			Y	
	Stored data			Y					
Privacy	Communication data		Y			Y			
	Stored data	Y					Y		
Communication flow security					Y				

9 Security requirements in the entities and relationships of the home network

These security functions should be used to meet all or some security requirements. Table 5 shows which security requirements are required for a specific entity or a relationship in the model of the home network. In Table 5, the letter 'Y' in a cell formed by the intersection of the table's columns and rows designates that a particular security requirement should exist for a specific entity or relationship. For example, in a case of a relation between remote user and remote terminal, a remote terminal should meet entity authentication, access control for stored data, and privacy for stored data.

Table 5 – Security requirements for home network model

Security requirement Entity or relation	Confidentiality		Integrity		Authentication		Non- repudiation
	Stored data	Communication data	Stored data	Communication data	Entity	Message	
Remote terminal	Y		Y		Y	Y	
Home device	Y		Y		Y	Y	
Secure home gateway	Y		Y		Y	Y	
Home application server	Y		Y		Y	Y	
Relation between remote user and remote terminal					Y		
Relation between remote terminal and secure home gateway		Y		Y	Y	Y	
Relation between remote terminal and home application server		Y		Y	Y	Y	Y
Relation between remote terminal and type B or C home device		Y		Y	Y	Y	
Relation between application server and secure home gateway		Y		Y		Y	
Relation between application server and home application server		Y		Y		Y	Y
Relation between application server and home device		Y		Y	Y	Y	Y
Relation between secure home gateway and home device		Y		Y	Y	Y	
Relation between home application server and type B or C home device		Y		Y	Y	Y	
Relation between type A home device and type B or C home device		Y		Y	Y	Y	
Relation between type A home device and home user					Y		
Relation between secure home gateway and home application server		Y		Y	Y	Y	Y
Relation between remote terminal and type A home device		Y		Y	Y	Y	

Table 5 – Security requirements for home network model (continued)

Security requirement Entity or relation	Access control		Availability		Privacy		Comm. Flow security
	Stored data	Communication data	Stored data	Communication data	Stored data	Communication data	
Remote terminal	Y		Y		Y		
Home device	Y		Y		Y		
Secure home gateway	Y		Y		Y		Y
Home application server	Y		Y		Y		
Relation between remote user and remote terminal					Y		
Relation between remote terminal and secure home gateway		Y		Y		Y	
Relation between remote terminal and home application server		Y		Y		Y	
Relation between remote terminal and home device		Y		Y		Y	
Relation between application server and secure home gateway		Y		Y		Y	
Relation between application server and home application server		Y		Y		Y	
Relation between application server and home device		Y		Y		Y	
Relation between secure home gateway and home device		Y		Y		Y	
Relation between home application server and home device		Y		Y		Y	
Relation between type A home device and type B or C home device		Y		Y		Y	
Relation between type A home device and home user					Y		
Relation between secure home gateway and home application server		Y		Y		Y	
Relation between remote terminal and type A home device		Y		Y		Y	

10 Security functions for satisfying security requirements in the home network

10.1 Security functions from ITU-T Rec. X.1121

10.1.1 Encipherment function (or encryption)

The encipherment function can implement confidentiality of either communication data or stored data. Encipherment algorithms may be classified into two types of encipherment algorithm: symmetrical or asymmetrical algorithm. In public-key algorithm, there are two kinds of keys: the public key and the private key. The knowledge of the public key does not imply knowledge of the private key. A sender uses a public key of a receiver to encrypt the content. As a receiver only has a private key, he or she is capable of reading a message which is decrypted from a ciphertext. In symmetric encipherment, knowledge of the encipherment key implies knowledge of the decipherment key and vice versa.

Because of the low processing capability or small memory size of remote terminals, there are some difficulties in implementing existing encipherment functions, especially asymmetric algorithm, used in an existing open network.

The encipherment function may be implemented by the firewall residing at the entry point of the home network.

10.1.2 Digital signature function

The digital signature function defines two processes: a process for signing a data, and a process for verifying a signed data. The first process uses private key (i.e., unique and confidential) to produce the signature. The second process uses public key to verify the validity of signature.

The signing process involves either an encipherment of the data or the production of a cryptographic check value of the data, using the signatory's private information as a private key.

The verification process involves the use of public procedures and information to determine whether the signature was produced correctly with the signatory's private information.

The essential characteristic of the signature function is that the signature can only be produced using the signatory's private information. Thus when the signature is verified, it can subsequently be proven to a third party (e.g., a judge or arbitrator) at any time that only the unique holder of the private information could have produced the signature.

As for encipherment function, due to the low processing performance or small memory size of remote terminals, there are some difficulties in implementing the existing digital signature functions used in an existing open network.

10.1.3 Access control function

The access control function may use the authenticated identity of an entity or information about the entity (such as membership in a known set of entities) or capabilities of the entity, in order to determine and enforce the access rights of the entity. If the entity attempts to use unauthorized resource, or an authorized resource with an improper type of access, then the access control function will reject the attempt and may additionally report the incident for the purposes of generating an alarm and/or recording it as part of a security audit trail. The access control function may be based on the use of the following items:

- access control information bases, where the access rights of peer entities are maintained in a database;
- authentication information such as passwords, possession and subsequent presentation of which is evidence of the accessing entity's authorization;
- capabilities, possession and subsequent presentation of which is evidence of the right to access the entity or resource defined by the capability;
- an authorization certificate;
- security labels, which when associated with an entity may be used to grant or deny access, usually according to a security policy;
- time of attempted access;
- route of attempted access;
- duration of access; and
- a physical location of attempted access.

The access control function may be applied at either peer entities of a communication association and/or at a secure home gateway.

Access control involved at the origin entity or mobile security gateway is used to determine whether the sender is authorized to communicate with the recipient and/or to use the required communication resources.

Access control function allows a home device to know what each authenticated device is allowed to do. There are predominant authorization mechanisms, such as access control list (ACL), authorization server and authorization certificate.

A device can control access by an ACL alone. This allows an access control to be deleted with ease, given that one can edit the ACL of the device. It has the disadvantage of requiring a lot of ACL editing if there is a large number of ACL editing.

If a home user has a home network containing a number of home devices, each containing a large size ACL, then it might make sense to move the ACL from each home device to a server, which is called authorization server. Even though each device needs an ACL, there might be advantages to using an authorization server.

Another way to administer authorization is to allow delegation by means of authorization certificates. An authorization certificate is a digitally signed ACL entry.

The access control function may be implemented by the firewall residing at the entry point of the home network.

10.1.4 Data integrity function

Two aspects of data integrity are considered: the integrity of a single data unit or field and the integrity of a stream of data units or fields. In general, different technologies are used to provide these two types of integrity function, although provision of the second without the first is not practical.

Determining the integrity of a single data unit involves two processes, one at the sending entity and one at the receiving entity. The sending entity appends to data a quantity that is a function of the data itself. This quantity may be supplementary information such as a block check code or a cryptographic check value and it may be enciphered. The receiving entity generates a corresponding quantity and compares its result with the received quantity to determine whether the data has been modified in transit. This process alone will not protect against the replay of a single data unit.

Protecting the integrity of a sequence of data units (i.e., protecting against disordering, losing, replaying and inserting or modifying data) requires the addition of some form of explicit ordering such as sequence numbering, time stamping, or cryptographic chaining.

Data integrity focuses on ensuring that the received data is received as sent. Data integrity function uses the hash algorithm or digital signature algorithm.

The data integrity function may be implemented by the firewall residing at the entry point of the home network.

10.1.5 Authentication function

Some security technologies that may be applied to authentication are:

- use of authentication information, such as passwords supplied by a sending entity and checked by the receiving entity;
- cryptographic technologies; and
- use of characteristics and/or possessions of the entity.

The authentication function can be grouped into two categories: user authentication, message authentication. Message authentication can be provided by a device certificate or an ID certificate in the home network. User authentication function can be based on three factors:

- 1) what you know;
- 2) what you have; and
- 3) what you are.

The authentication function may be incorporated in order to provide peer entity authentication. If the function does not succeed in authenticating the entity, this will result in rejection or termination of the connection and may cause an entry in the security audit trail and/or a report to a security management centre.

When cryptographic techniques are used, they may be combined with "handshaking" protocols to protect against replay (i.e., to ensure liveness).

The choices of security technologies, which realize authentication, will depend upon the circumstances in which they need to be used with:

- time stamping and synchronized clocks;
- two- and three-way handshakes (for unilateral and mutual authentication, respectively); and
- non-repudiation functions achieved by digital signature and/or notarization mechanisms.

The authentication function may be implemented by the firewall residing at the entry point of the home network.

10.1.6 Notarization

Properties of the data communicated between two or more entities, such as its integrity, origin, time and destination, can be assured by the provision of a notarization function. The assurance is provided by a third-party notary, which is the communicating entities trust, and which holds the necessary information to provide the required assurance in a verifiable manner. Each instance of communication may use digital signature, encipherment, and integrity functions as appropriate to the service being provided by the notary. When such a notarization function is invoked, the data is communicated between the communicating entities via the protected instances of communication and the notary.

10.2 Additional security functions

10.2.1 Message authentication code (MAC) function

A MAC is defined as a public function with an input message and a secret key that produces a fixed-length value that serves as the authenticator in order to authenticate a message and enable the receiver to verify the authenticity of message. A MAC is to provide countermeasures against masquerade, content modification, sequence modification, and timing modification. A typical example of MAC functions are HMAC (Hash-based MAC) and MAC based on the symmetrical encryption algorithm.

The message authentication code function may be implemented by the firewall residing at the entry point of the home network.

10.2.2 Key management function

A key management function is an infrastructure of all the security functions, which is to generate, distribute, transport, delete, or destruct all kinds of cryptographical keys required for other security functions. The key management function covers the key exchange function in [ITU-T X.1121], that is the key exchange function is a subset of the key management function.

The key management function may be implemented by the firewall residing at the entry point of the home network.

10.3 Relationship between a security requirement and a security function

These security functions are used to satisfy some of the security requirements. Table 6 shows some set of security functions to satisfy specific security requirements. In Table 6, the letter 'Y' in a cell formed by the intersection of the table's columns and rows designates that a particular security service can be opposed by a corresponding security function, the letter 'K' means that the security

service could be supplemented or reinforced by a marked security mechanism, and the letter 'X' means that a specified security service can be provided by one of the optional security functions. For example, access control function can be grouped into two access control functions: physical access control and technical access control.

Table 6 – Illustration of relationship between security requirements and security functions

Security function		Encipherment	Integrity	MAC	Entity authentication	Digital signature	Notarization	Access control		Key management	Anti-availability	
								Physical	Technical		Physical	Technical
Confidentiality	Communication data	Y						K		Y		
	Stored data	Y						K		Y		
Integrity	Communication data		X	X		X	X			Y		
	Stored data		X	X		X	X			Y		
Authentication	Entity				Y					Y		
	Message			X		X	X			Y		
Non-repudiation						Y	Y			Y		
Access control	Communication data	K						K		K		
	Stored data	K		Y	Y	Y		K	Y	Y		
Availability	Communication data							X			X	Y
	Stored data			X	X	X			K	Y		Y
Privacy	Communication data	Y						K		Y		
	Stored data	Y		X	X	X		K	Y	Y		
Communication flow security			X	X	X			K	Y	Y		

11 Security technologies for home network

To realize the security functions as described in clause 10, a variety of security technologies for the home network can be applied. These security technologies are categorized by security functions realized by the security technology and where the security technology applies. Because a security technology applies to an entity or a relation between entities in models of the home network, the places at which the security technology is applied denote entities or relations between entities. Tables 1 and 2 show where security threats appear in models of the home network. Tables 3 and 4 show the necessary security requirements for countermeasures to particular security threats. Table 5 shows the necessary security requirements for a specific entity or a relationship in the model of home network. Table 6 shows the security functions which meet the security requirements. Therefore, the relationship between security functions and places to apply these security functions in models can be shown in Table 7. In other words, Table 7 shows where security technologies, which realize certain security functions, are applied to in the home network model.

Table 7 – Relationship between security technologies and models

Entity or relationship		Security functions					Access control		Key management	Anti-availability		
		Encipherment	Integrity	MAC	Entity authentication	Digital signature	Notarization	Physical		Technical	Physical	Technical
Stored data	Remote terminal	Y	X	Y	Y	Y	Y	K	Y	Y		Y
	Home device	Y	X	Y	Y	Y	Y	K	Y	Y		Y
	Secure home gateway	Y	X	Y	Y	Y	Y	K	Y	Y		Y
	Home application server	Y	X	Y	Y	Y	Y	K	Y	Y		Y
Communication data	Relation between remote user and remote terminal	Y		X	Y	Y		K	Y	Y		
	Relation between remote terminal and secure home gateway	Y	X	X	Y	Y	Y	X		Y	X	Y
	Relation between remote terminal and home application server	Y	X	X	Y	Y	Y	X		Y	X	Y
	Relation between remote terminal and type B or type C home device	Y	X	X	Y	Y	Y	X		Y	X	Y
	Relation between application server and secure home gateway	Y	X	X		X	X	X		Y	X	Y
	Relation between application server and home application server	Y	X	X		Y	Y	X		Y	X	Y
	Relation between application server and home device	Y	X	X	Y	Y	Y	X		Y	X	Y
	Relation between secure home gateway and home device	Y	X	X	Y	Y	Y	X		Y	X	Y
	Relation between home application server and home device	Y	X	X	Y	Y	Y	X		Y	X	Y
	Relation between type A home device and type B or C home device	Y	X	X	Y	Y	Y	X		Y	X	Y
	Relation between type A home device and home user	Y		X	Y	Y		K	Y	Y		

Table 7 – Relationship between security technologies and models

Security functions Entity or relationship		Encipherment	Integrity	MAC	Entity authentication	Digital signature	Notarization	Access control		Key management	Anti-availability	
								Physical	Technical		Physical	Technical
	Relation between secure home gateway and home application server	Y	X	X	Y	Y	Y	X		Y	X	Y
	Relation between remote terminal and type A home device	Y		X	Y	Y	Y	X		Y	X	Y

The security functions can be implemented on the various layers. Table 8 illustrates the possible layer or layers for implementing the security functions of each relation in the model. The data link-level, network-level security, session-level security, and application-level security can be provided in the data link layer, network layer, the transport layer, and application layer, respectively. The examples of each security protocol are IPSec, TLS, and application peer-to-peer security protocol, respectively.

Table 8 – Possible layers for implementing security functions of each relationship in the model

Relations	Security-implemented layer
Relation between remote terminal and secure home gateway	Network, or session level
Relation between remote terminal and home application server	Application level
Relation between remote terminal and type B or type C home device	Application level
Relation between application server and secure home gateway	Network, or session level
Relation between application server and home application server	Network or session level, or application level
Relation between application server and type B or type C home device	Network, session level, or application level
Relation between secure home gateway and type B or type C home device	Data link, network, or session level
Relation between home application server and type B or type C home device	Data link, network, session level, or application level
Relation between type A home devices and type B or C home device	Data link, or application level
Relation between secure home gateway and home application server	Network or session level
Relationship between the remote terminal and type A home device	Application level

12 Security function requirements for home network

The security requirements for network entity in the home network are as follows:

- 1) All the network elements such as a remote terminal, a secure home gateway, a home application server, and home devices should keep their sensitive information securely, and should protect their information against unauthorized access, unauthorized modification, or unauthorized deletion.
- 2) The remote terminal should have a capability to authenticate a remote user by using the appropriate user authentication method, such as biometric authentication method.
- 3) The remote terminal must have security functions, such as entity authentication, key management, and MAC or integrity, with the secure home gateway in the network or session level in case that it requires the communication data confidentiality and integrity with the home gateway.
- 4) The remote terminal must have security functions, such as entity authentication, key management, encryption, and MAC or integrity, with the home application server in the application level or network level in case that it requires the communication data confidentiality and integrity with the home application server.
- 5) The remote terminal must have security functions such as entity authentication, key management, digital signature, encryption, and MAC or integrity, with the type B or type C home device in the application level in case that it requires the communication data confidentiality and integrity with the type B or type C device.
- 6) The type A home device should have a capability to authenticate a home user by using the appropriate user authentication method.
- 7) The type A home device should have security functions such as entity authentication, key management, encryption, and MAC or integrity, with the type B or type C home device in the application level in case that it requires the communication data confidentiality and integrity with the type B or type C device.
- 8) The type B or type C home device must have security functions such as entity authentication, key management, and MAC or integrity with the home application server or application server in the network, session, or application level in the case that it requires the communication data confidentiality and integrity with the home application server or application server in the network.
- 9) The type B or type C home device must have security functions such as entity authentication, key management, and MAC or integrity with the secure home gateway in the network or session level in the case that it requires the communication data confidentiality and integrity with the secure home gateway.
- 10) The secure home gateway should have security functions, such as entity authentication, key management, and MAC or integrity, with the secure home application server or application service provider usually in the network level in the case that it requires the communication data confidentiality and integrity with the secure home application server or application service provider.
- 11) The home network administrator must have the ability to remotely or locally manage the home gateway, or home application server with user approval.
- 12) The secure home gateway should have security-related functions, such as a firewall, intrusion detection, a content filtering, or an interface for remote access for maintenance, as optional capabilities.
- 13) A related event logging/messaging interface of secure home gateway security must exist that allows the home administrator to monitor and review activities of secure home gateway.

Annex A

Type of home network device in ITU-T Rec. J.190

(This annex forms an integral part of this Recommendation)

The home network device should be classified from the security viewpoint. In [ITU-T J.190], all home devices are categorized into four classes as shown in Figure A.1: home access (HA) class, home bridge (HB) class, home client (HC) class and home decoder (HD) class. HAs are interface devices with Access Network, HBs are bridging devices between IP-Cable2Home domain networks, (e.g., HUB, router, etc.), HCs are interface devices between IP-Cable2Home and proprietary domain devices. HDs are devices that can communicate by proprietary protocols (e.g., DVD, D-VHS, IC Audio, Printer, etc.). Each device of HC and HD classes belongs to one of the service planes, for example, AV plane, PC plane, TEL/FAX plane, and home appliance plane.

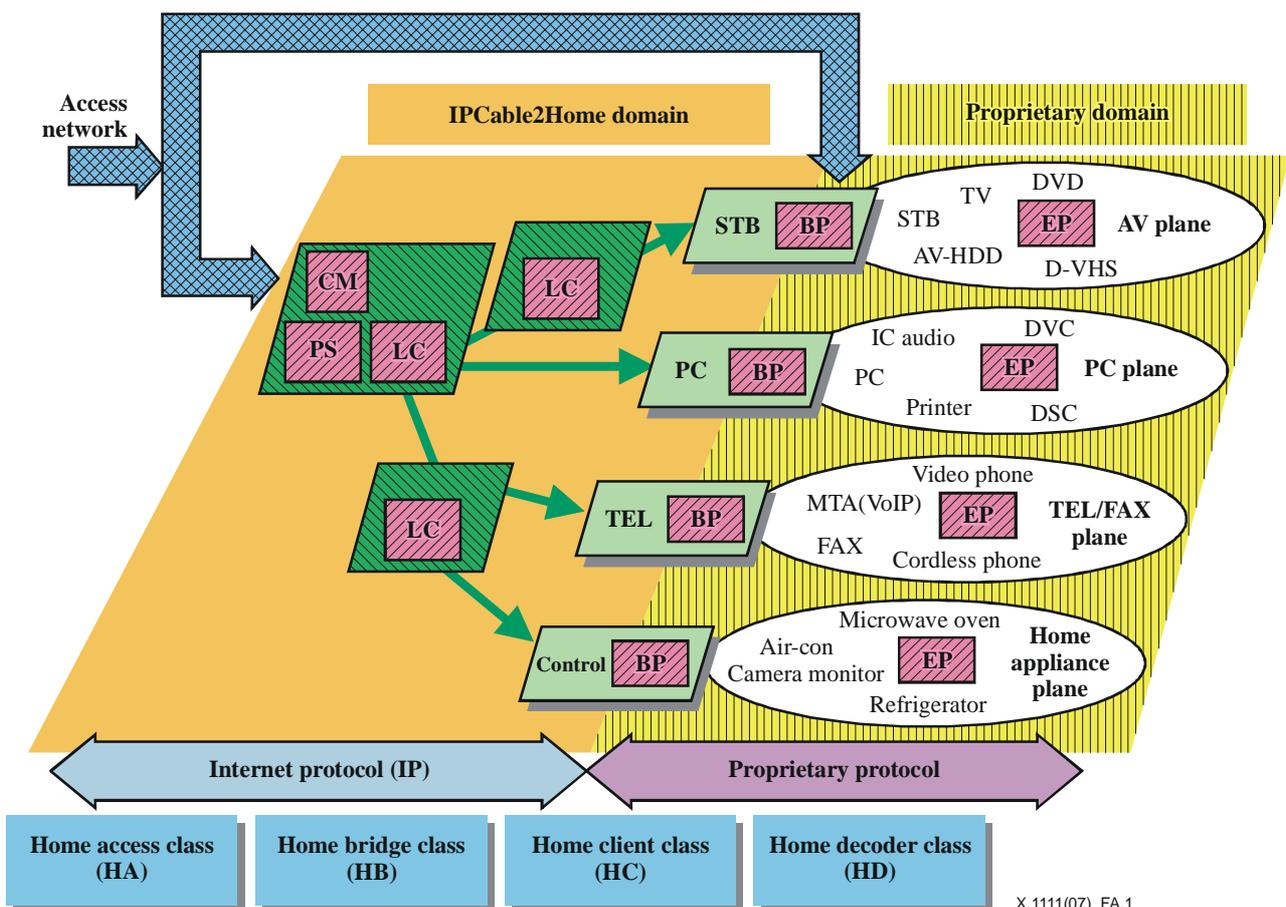


Figure A.1 – ITU-T J.190 home network context

Further details concerning device classes and planes are contained in clause 5.4.3 of [ITU-T J.190]. According to the terminology defined by this Recommendation, a secure home gateway corresponds to HA device class, no device corresponds to HB device class because it normally contains no security function, type B home device corresponds to all HC device classes, and finally type C home device does not correspond to any device class in [ITU-T J.190] but it corresponds to HD device class except those using proprietary protocol to communicate with type B device. In this Recommendation, as communications between type B home device and legacy home device

without communication capability are based on the proprietary communication path, this Recommendation does not specify any security requirements in that proprietary path.

In [ITU-T J.190], a useful concept, "user plane", has been introduced, all devices are grouped into four planes according to their functions: AV plane, PC plane, Tel/Fax plane, and home appliance plane.

However, from the point of view of security, there is a device which sends a command to another device to control it or request a service from it, and a device which receives such a command or a service request from another device. In this case, all home devices can be grouped into three device types, regardless of the security plane of the home devices. In this Recommendation, maximum security requirements which are needed for any home device are developed, regardless of the service plane of the device. Therefore, security requirements in any device should be selected according to a policy of the service provider using the devices; since different devices have different levels of security requirements, it is very difficult to define a generalized set of specific security requirements. The specific security requirements are outside the scope of this Recommendation.

Appendix I

Type of home network devices in UPnP

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

In UPnP, there are three major classes of UPnP devices: UCP, controlled device and bridge.

- UCP – User/Universal Control Point: This is a device, such as a PC or PDA, which allows for control of other UPnP devices through the presentation page and rich display.
- Bridge: Connects non-UPnP devices to the home network; basically, it speaks UPnP on one end and some proprietary language on the other end (some examples include proprietary lighting control, bluetooth, etc.).
- Controlled device: Any UPnP device that allows control or provides some sort of UPnP service to the rest of the home network (such as IGDs, A/V devices, security cameras, etc.).

The home device classification is basically very similar to that of UPnP. According to the terminology defined by this Recommendation, secure home gateway corresponds to no device in UPnP, UCP corresponds to type A device, bridge corresponds to type B home device, and controlled device corresponds to type C home device.

Bibliography

- [b-UPnP Arch] UPnP (2003), *UPnP Device Architecture 1.0*.
- [b-UPnP] UPnP, *Introduction to Universal Plug and Play*.
- [b-IETF RFC 3767] IETF RFC 3767 (2004), *Securely Available Credentials Protocol*.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	Global information infrastructure, Internet protocol aspects and next-generation networks
Series Z	Languages and general software aspects for telecommunication systems