Unión Internacional de Telecomunicaciones

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

X.1111

(02/2007)

SERIE X: REDES DE DATOS, COMUNICACIONES DE SISTEMAS ABIERTOS Y SEGURIDAD

Seguridad de las telecomunicaciones

Marco de tecnologías de seguridad para redes domésticas

Recomendación UIT-T X.1111

Unión Internacional de Telecomunicaciones

RECOMENDACIONES UIT-T DE LA SERIE X

REDES DE DATOS, COMUNICACIONES DE SISTEMAS ABIERTOS Y SEGURIDAD

REDES PÚBLICAS DE DATOS	
Servicios y facilidades	X.1–X.19
Interfaces	X.20–X.49
Transmisión, señalización y conmutación	X.50–X.89
Aspectos de redes	X.90–X.149
Mantenimiento	X.150–X.179
Disposiciones administrativas	X.180–X.199
INTERCONEXIÓN DE SISTEMAS ABIERTOS	
Modelo y notación	X.200–X.209
Definiciones de los servicios	X.210–X.219
Especificaciones de los protocolos en modo conexión	X.220–X.229
Especificaciones de los protocolos en modo sin conexión	X.230–X.239
Formularios para declaraciones de conformidad de implementación de protocolo	X.240–X.259
Identificación de protocolos	X.260–X.269
Protocolos de seguridad	X.270–X.279
Objetos gestionados de capa	X.280–X.289
Pruebas de conformidad	X.290–X.299
INTERFUNCIONAMIENTO ENTRE REDES	
Generalidades	X.300–X.349
Sistemas de transmisión de datos por satélite	X.350–X.369
Redes basadas en el protocolo Internet	X.370–X.379
SISTEMAS DE TRATAMIENTO DE MENSAJES	X.400–X.499
DIRECTORIO	X.500–X.599
GESTIÓN DE REDES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS Y ASPECTOS DE SISTEMAS	
Gestión de redes	X.600–X.629
Eficacia	X.630–X.639
Calidad de servicio	X.640–X.649
Denominación, direccionamiento y registro	X.650–X.679
Notación de sintaxis abstracta uno	X.680–X.699
GESTIÓN DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	
Marco y arquitectura de la gestión de sistemas	X.700–X.709
Servicio y protocolo de comunicación de gestión	X.710–X.719
Estructura de la información de gestión	X.720–X.729
Funciones de gestión y funciones de arquitectura de gestión distribuida abierta	X.730–X.799
SEGURIDAD	X.800–X.849
APLICACIONES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	
Compromiso, concurrencia y recuperación	X.850–X.859
Procesamiento de transacciones	X.860–X.879
Operaciones a distancia	X.880–X.889
Aplicaciones genéricas de la notación de sintaxis abstracta uno	X.890–X.899
PROCESAMIENTO DISTRIBUIDO ABIERTO	X.900–X.999
SEGURIDAD DE LAS TELECOMUNICACIONES	**X.1000–**

Para más información, véase la Lista de Recomendaciones del UIT-T.

Recomendación UIT-T X.1111

Marco de tecnologías de seguridad para redes domésticas

Resumen

En la Recomendación UIT-T X.1111 se describen las amenazas contra la seguridad y los requisitos de seguridad en las redes domésticas desde los puntos de vista del usuario en la vivienda y del usuario distante. No se tratan los requisitos de seguridad desde el punto de vista del proveedor. Adicionalmente, esta Recomendación clasifica las tecnologías de seguridad con respecto a las funciones de seguridad que satisfacen los requisitos de seguridad ya mencionados y el sitio en que se aplican las tecnologías de seguridad en el modelo de la red doméstica. Por último, se presentan los requisitos de las funciones de seguridad de cada entidad de la red junto con las posibles capas de la puesta en práctica de la función de seguridad.

Orígenes

La Recomendación UIT-T X.1111 fue aprobada el 13 de febrero de 2007 por la Comisión de Estudio 17 (2005-2008) del UIT-T por el procedimiento de la Recomendación UIT-T A.8.

PREFACIO

La UIT (Unión Internacional de Telecomunicaciones) es el organismo especializado de las Naciones Unidas en el campo de las telecomunicaciones. El UIT-T (Sector de Normalización de las Telecomunicaciones de la UIT) es un órgano permanente de la UIT. Este órgano estudia los aspectos técnicos, de explotación y tarifarios y publica Recomendaciones sobre los mismos, con miras a la normalización de las telecomunicaciones en el plano mundial.

La Asamblea Mundial de Normalización de las Telecomunicaciones (AMNT), que se celebra cada cuatro años, establece los temas que han de estudiar las Comisiones de Estudio del UIT-T, que a su vez producen Recomendaciones sobre dichos temas.

La aprobación de Recomendaciones por los Miembros del UIT-T es el objeto del procedimiento establecido en la Resolución 1 de la AMNT.

En ciertos sectores de la tecnología de la información que corresponden a la esfera de competencia del UIT-T, se preparan las normas necesarias en colaboración con la ISO y la CEI.

NOTA

En esta Recomendación, la expresión "Administración" se utiliza para designar, en forma abreviada, tanto una administración de telecomunicaciones como una empresa de explotación reconocida de telecomunicaciones.

La observancia de esta Recomendación es voluntaria. Ahora bien, la Recomendación puede contener ciertas disposiciones obligatorias (para asegurar, por ejemplo, la aplicabilidad o la interoperabilidad), por lo que la observancia se consigue con el cumplimiento exacto y puntual de todas las disposiciones obligatorias. La obligatoriedad de un elemento preceptivo o requisito se expresa mediante las frases "tener que, haber de, hay que + infinitivo" o el verbo principal en tiempo futuro simple de mandato, en modo afirmativo o negativo. El hecho de que se utilice esta formulación no entraña que la observancia se imponga a ninguna de las partes.

PROPIEDAD INTELECTUAL

La UIT señala a la atención la posibilidad de que la utilización o aplicación de la presente Recomendación suponga el empleo de un derecho de propiedad intelectual reivindicado. La UIT no adopta ninguna posición en cuanto a la demostración, validez o aplicabilidad de los derechos de propiedad intelectual reivindicados, ya sea por los miembros de la UIT o por terceros ajenos al proceso de elaboración de Recomendaciones.

En la fecha de aprobación de la presente Recomendación, la UIT no ha recibido notificación de propiedad intelectual, protegida por patente, que puede ser necesaria para aplicar esta Recomendación. Sin embargo, debe señalarse a los usuarios que puede que esta información no se encuentre totalmente actualizada al respecto, por lo que se les insta encarecidamente a consultar la base de datos sobre patentes de la TSB en la dirección http://www.itu.int/ITU-T/ipr/.

ÍNDICE

Página

Recomendación UIT-T X.1111

Marco de tecnologías de seguridad para redes domésticas

1 Alcance

La red doméstica es una parte importante de las redes de comunicaciones de datos extremo a extremo. Debido a que utiliza diversas técnicas de transmisión cableadas e inalámbricas, las amenazas contra la red doméstica podrían ser equivalentes a las inherentes a la red cableada o a la red inalámbrica.

Para poder precisar el marco de seguridad de la red doméstica, es necesario identificar las amenazas a la red doméstica y determinar las funciones de seguridad necesarias en las entidades del modelo de red doméstica. Puesto que el modelo de amenazas de la red doméstica es similar al modelo de amenazas descrito en [UIT-T X.1121], "Marco general de tecnologías de seguridad para las comunicaciones móviles de datos de extremo a extremo", se utiliza [UIT-T X.1121] como Recomendación fundamental al elaborar el marco general de las tecnologías de seguridad para redes domésticas.

En la presente Recomendación se describen las amenazas contra la seguridad y los requisitos de seguridad en las redes domésticas desde los puntos de vista del usuario en la vivienda y del usuario distante. Adicionalmente, la Recomendación clasifica las tecnologías de seguridad con respecto a las funciones de seguridad que satisfacen los requisitos de seguridad ya mencionados y el sitio en que se aplican las tecnologías de seguridad en el modelo de la red doméstica. Por último, se presentan los requisitos de las funciones de seguridad de cada entidad de la red junto con las posibles capas de la puesta en práctica de la función de seguridad.

2 Referencias

Las siguientes Recomendaciones del UIT-T y otras referencias contienen disposiciones que, mediante su referencia en este texto, constituyen disposiciones de la presente Recomendación. Al efectuar esta publicación, estaban en vigor las ediciones indicadas. Todas las Recomendaciones y otras referencias son objeto de revisiones por lo que se preconiza que los usuarios de esta Recomendación investiguen la posibilidad de aplicar las ediciones más recientes de las Recomendaciones y otras referencias citadas a continuación. Se publica periódicamente una lista de las Recomendaciones UIT-T actualmente vigentes. En esta Recomendación, la referencia a un documento, en tanto que autónomo, no le otorga el rango de una Recomendación.

[UIT-T J.190] Recomendación UIT-T J.190 (2002), *Arquitectura de MediaHomeNet que soporta servicios basados en cable*.

[UIT-T J.192] Recomendación UIT-T J.192 (2005), *Pasarela residencial para soportar la entrega de servicios de datos por cable*.

[UIT-T Q.1701] Recomendación UIT-T Q.1701 (1999), *Marco para las redes de las telecomunicaciones móviles internacionales-2000 (IMT-2000).*

[UIT-T Q.1711] Recomendación UIT-T Q.1711 (1999), *Modelo funcional de red para las telecomunicaciones móviles internacionales-2000 (IMT-2000).*

[UIT-T Q.1761] Recomendación UIT-T Q.1761 (2004), *Principios y requisitos para la convergencia de los sistemas fijos y los sistemas IMT-2000 existentes*.

[UIT-T X.800] Recomendación UIT-T X.800 (1991), *Arquitectura de seguridad de la interconexión de sistemas abiertos para aplicaciones del CCITT*.

[UIT-T X.803] Recomendación UIT-T X.803 (1994), *Tecnología de la información – Interconexión de sistemas abiertos – Modelo de seguridad de capas superiores*.

[UIT-T X.805] Recomendación UIT-T X.805 (2003), *Arquitectura de seguridad para sistemas de comunicaciones extremo a extremo*.

[UIT-T X.810] Recomendación UIT-T X.810 (1995), *Tecnología de la información – Interconexión de sistemas abiertos – Marcos de seguridad para sistemas abiertos: Visión general*.

[UIT-T X.1121] Recomendación UIT-T X.1121 (2004*), Marco general de tecnologías de seguridad para las comunicaciones móviles de datos de extremo a extremo*.

3 Definiciones

3.1 Definiciones de la arquitectura de seguridad del modelo de referencia OSI

Los siguientes términos se definen en [UIT-T X.800]:

a) control de acceso;
b) autenticación;
c) información de autenticación;
d) intercambio de autenticación;
e) autorización;
f) disponibilidad;
g) confidencialidad;
h) criptografía;
i) integridad de los datos;
j) autenticación del origen de los datos;
k) cifrado;
l) cortafuegos;
m) integridad;
n) clave;
o) intercambio de claves;
p) gestión de claves;
q) software maligno;
r) no-repudio;
s) notarización;
t) contraseña;
u) privacidad.

3.2 Definiciones del marco general de seguridad móvil

Los siguientes términos se definen en [UIT-T X.1121]:

a) anonimato;
b) apropiación furtiva de datos;
c) terminal móvil;
d) red móvil;

e) usuario móvil;

f) servicio de aplicación;

g) servidor de aplicación;

h) proveedor de servicio de aplicación;

i) pasarela de seguridad móvil;

j) gestión de normativas de seguridad.

3.3 Definiciones relativas a la red doméstica

Los siguientes términos se definen en [UIT-T J.190]:

a) acceso a la vivienda (HA, *home access*);

b) puente en la vivienda (HB, *home bridge*);

c) cliente en la vivienda (HC, *home client*);

d) decodificador en la vivienda (HD, *home decoder*);

e) pasarela residencial;

f) planos en la red doméstica.

3.4 Definiciones adicionales

En esta Recomendación se definen los términos siguientes:

3.4.1 pasarela de vivienda segura: Un pasarela de vivienda segura es un tipo de pasarela residencial percibida desde el punto de vista de la seguridad y un punto o entidad que retransmite paquetes de datos desde una red abierta hacia una red doméstica interna, y viceversa; cambia los parámetros de seguridad o el protocolo de comunicaciones al pasar de la red doméstica a la red abierta, y viceversa, y puede llevar a cabo funciones relativas a la seguridad, como filtrado de paquetes, detección de intrusiones y la función de gestión de normativas, entre otras, de conformidad con una normativa de seguridad dada. Es decir, una pasarela de vivienda segura comprende más que un cortafuegos.

3.4.2 dispositivo doméstico: Un dispositivo doméstico es una entidad (o aparato doméstico), como un PDA, PC o TV/VCR, que controla otro dispositivo doméstico o es controlado por éste, o que proporciona un servicio a los usuarios domésticos. Desde el punto de vista de la seguridad, existen tres tipos de dispositivos domésticos: el tipo A, el tipo B y el tipo C. El dispositivo tipo A, como por ejemplo un control remoto, PC o PDA, posee la capacidad de controlar dispositivos tipo B y tipo C a través de la página de presentación y la pantalla especializada. El dispositivo doméstico tipo B es un puente que conecta los dispositivos domésticos tipo C carentes de interfaz de comunicaciones entre el equipo y la red doméstica y que, en términos generales, por un lado se comunica con los otros dispositivos de la red doméstica y, por el otro, emplea un lenguaje de marca registrada (por ejemplo, los controles de iluminación de marca registrada, etc.). Los dispositivos domésticos tipo C, como las cámaras de seguridad, dispositivos A/V, etc., sólo prestan algún tipo de servicio a los demás dispositivos domésticos. Los dispositivos domésticos tipo A y tipo C se denominan consolas de seguridad si les pertenece, desde el punto de vista de la seguridad, un dispositivo doméstico tipo B o tipo C. Todo dispositivo de la red doméstica puede clasificarse en dispositivo de tipo A, B o C, dependiendo de sus funciones.

3.4.3 proveedor de servicio de aplicaciones domésticas: El proveedor de servicio de aplicaciones domésticas (o servidor de aplicación en la vivienda) es una entidad que se conecta a la red doméstica e intercambia datos con los dispositivos domésticos o con terminales remotos, almacena contenidos multimedios o proporciona diversos servicios de aplicación a los demás dispositivos domésticos ubicados en la vivienda o en terminales remotos fuera de ésta.

3.4.4 certificado de ID: Un certificado de ID es un mensaje que, al menos, anuncia un nombre o identifica la entidad emisora, identifica al receptor, contiene la clave pública del receptor, identifica el periodo de validez del certificado, contiene un número de serie y la firma digital de una CA.

3.4.5 certificado de dispositivo: Un certificado de dispositivo es un certificado de la versión 3 de X.509 empleado para autenticar la identidad de un dispositivo doméstico. Puede ser emitido por una CA.

3.4.6 certificado de autorización: Los certificados de autorización son objetos firmados que facultan al receptor. Contienen al menos un emisor y un receptor. Pueden incluir condiciones de validez e información de autorización y delegación. En términos generales, los certificados pueden clasificarse en tres categorías: certificados de ID, que indican la correspondencia del nombre del receptor con su clave pública; certificados de atributos, que indican la correspondencia de la autorización con el nombre del receptor, y los certificados de autorización, que indican la correspondencia de la autorización con la clave pública del receptor. Los certificados de autorización y de atributos pueden delegar todos los permisos recibidos del emisor, o pueden delegar tan sólo una parte de esas facultades.

3.4.7 lista de control de acceso (ACL, *access control list*): Una ACL es un cuadro protegido que reside en la memoria del dispositivo cuyo acceso se protege. Se trata de un conjunto de registros, cada uno de los cuales contiene lo siguiente: receptor, autorización, delegación y validez. El receptor es un identificador de la entidad a la que se otorga acceso, la autorización es un indicador del permiso que se otorga a ese receptor, la delegación es una bandera que indica si el receptor puede seguir delegando estos derechos y la validez es un campo opcional con información sobre la validez del registro, como: "no después de" o "no antes de" cierta fecha y hora. La lista de control de acceso es una lista de registros desde la que se encadena una serie de certificados. La ACL, a veces denominada "lista de claves raíz", es el origen de las facultades para los certificados. Es decir, mediante los certificados se transmiten los permisos que el emisor otorga al receptor, pero es en la ACL donde se originan esos permisos (ya que, en teoría, en ella figura, como emisor implícito, el dueño del recurso que controlan). El contenido de uno de los registros de una ACL podría llegar a ser el mismo que el de un certificado, pero sin emisor (y no está firmado). Muy posiblemente habrá una ACL por cada dueño de recurso e incluso por cada recurso controlado.

3.4.8 terminal remoto: Un terminal remoto es una entidad que contiene una función de acceso a la red y una interfaz con Internet, que utiliza para conectarse a los dispositivos domésticos de la red doméstica o para controlarlos.

3.4.9 usuario distante: Un usuario distante es una entidad (persona) ubicada fuera de la red doméstica, que usa y opera un terminal remoto a fin de acceder a los dispositivos de una red doméstica.

3.4.10 usuario en la vivienda: Un usuario en la vivienda es una entidad (persona) ubicada en la red doméstica, que usa y opera un terminal remoto a fin de acceder a los dispositivos de una red doméstica.

3.4.11 consola de seguridad: Una consola de seguridad es un dispositivo que posee una interfaz de usuario para administrar el control de acceso a otros dispositivos, desde el punto de vista de la seguridad.

3.4.12 administrador de red doméstica: Un administrador de red doméstica es una entidad o un agente que efectúa actividades relacionadas con la seguridad, como generación, almacenamiento y distribución de claves, y supervisa el estado de las entidades de la red doméstica.

4 Abreviaturas, siglas o acrónimos

En esta Recomendación se utilizan las siguientes abreviaturas, siglas o acrónimos.

ACL Lista de control de acceso (*access control list*)

ASP Proveedor de servicio de aplicación (*application service provider*)

DoS Denegación de servicio (*denial of service*)

MAC Código de autenticación de mensaje (*message authentication code*)

OSI Interconexión de sistemas abiertos (*open systems interconnection*)

PC Computador personal (*personal computer*)

PDA Asistente personal de datos (*personal data assistant*)

PIN Número de identificación personal (*personal identification number*)

5 Modelo general de seguridad de las redes domésticas

Antes de describirse las tecnologías de seguridad, debe definirse el modelo general de seguridad de las redes domésticas, desde el punto de vista de la seguridad. El modelo general de seguridad de las redes domésticas identifica todas las entidades de la red doméstica, describe claramente la relación entre las entidades del modelo e indica el punto en que se deben aplicar las tecnologías de seguridad en comunicaciones móviles.

En la figura 1 se presenta el modelo general de seguridad de las redes domésticas. Hay muchos dispositivos domésticos conectados a la red doméstica como PDA, PC y TV/VCR que se controlan mutuamente o son controlados por otro dispositivo doméstico, o que prestan un servicio a los usuarios en la vivienda. Estos dispositivos se clasifican en tres tipos, desde el punto de vista de su función: El tipo A, el tipo B y el tipo C. El dispositivo tipo A, como por ejemplo un control remoto, PC o PDA, posee la capacidad de controlar dispositivos tipo B y tipo C a través de la página de presentación y la pantalla especializada. El dispositivo doméstico tipo B es un puente que conecta los dispositivos domésticos tipo C carentes de interfaz de comunicaciones entre el equipo y la red doméstica y que, en términos generales, por un lado se comunica con los otros dispositivos de la red doméstica y, por el otro, emplea un lenguaje de marca registrada (por ejemplo, los controles de iluminación de marca registrada, etc.). Los dispositivos domésticos tipo C, como las cámaras de seguridad, dispositivos de audio y vídeo, etc., sólo prestan algún tipo de servicio a los demás dispositivos domésticos. Los dispositivos domésticos tipo A y tipo C se denominan consolas de seguridad si les pertenece, desde el punto de vista de la seguridad, un dispositivo doméstico tipo B o tipo C.

El dispositivo doméstico de tecnología anterior es normalmente aquél que carece de interfaz de comunicaciones, pero posee un mecanismo propio del fabricante que le permite conectarse a un dispositivo doméstico tipo B, de forma que se puede conectar a la red doméstica a través del dispositivo tipo B. Algunos dispositivos domésticos poseen funciones que corresponden a los dispositivos tipo A y tipo C.

En la figura 1 se presenta el modelo de seguridad de las redes domésticas.

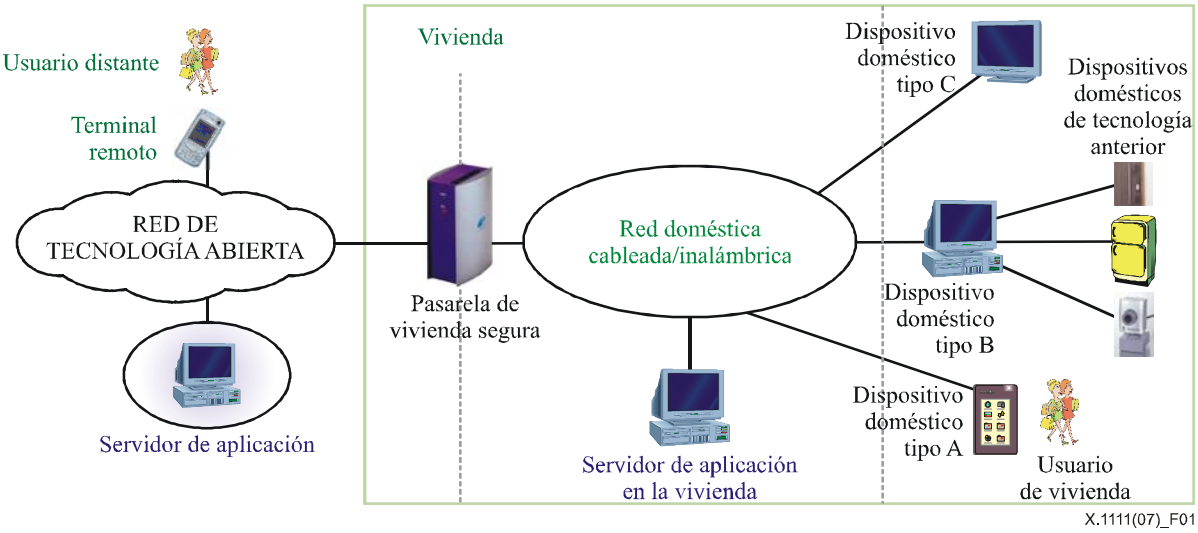

Figura 1 – Modelo de seguridad de las redes domésticas

Hay siete entidades en este modelo: el usuario distante, el terminal remoto, el servidor de aplicación, la pasarela de vivienda segura, el servidor de aplicación en la vivienda, el usuario en la vivienda y los dispositivos domésticos. Se recuerda que los dispositivos domésticos se clasifican en tres tipos de dispositivo: el dispositivo doméstico tipo A, el dispositivo doméstico tipo B y el dispositivo doméstico tipo C.

En este modelo figuran igualmente trece relaciones, a saber: entre el usuario distante y el terminal remoto, entre el terminal remoto y la pasarela de vivienda segura, entre el terminal remoto y el servidor de aplicación en la vivienda, entre el terminal remoto y el dispositivo doméstico, entre el servidor de aplicación y la pasarela de vivienda segura, entre el servidor de aplicación y el servidor de aplicación en la vivienda, entre el servidor de aplicación y el dispositivo doméstico, entre la pasarela de vivienda segura y el dispositivo doméstico, entre el servidor de aplicación en la vivienda y el dispositivo doméstico, entre el dispositivo doméstico y el usuario en la vivienda, entre un dispositivo doméstico y otro dispositivo doméstico, entre el terminal remoto y un dispositivo doméstico tipo A, y entre la pasarela de vivienda segura y el servidor de aplicación en la vivienda.

Un ejemplo de utilización de una red doméstica es aquel en que una persona utiliza una unidad portátil estéreo para escuchar música almacenada en un servidor. De hecho, varias personas podrían acceder a contenidos de audio para reproducirlos en diversas partes de la vivienda, e incluso al exterior de la vivienda, empleando para ello varios reproductores de red. Otro ejemplo de utilización es aquel en que se comparte un contenido de vídeo. En este caso los miembros de la familia podrían disfrutar del contenido desde diversas partes de la vivienda. Por ejemplo, podría ser que el hijo esté en la sala de la casa, mostrando a sus amigos algunas fotografías de las vacaciones, que se encuentran almacenadas en el PC de su padre; y al mismo tiempo la madre puede estar viendo un programa de televisión grabado en el transcurso de la semana, utilizando para ello un DVR conectado a la red y que también está ubicado en la sala de la casa; para ello selecciona el programa y configura la reproducción utilizando un segundo control remoto.

6 Características de la red doméstica

6.1 La red doméstica podría utilizar diversos medios de transmisión

En la red doméstica podrían transmitirse las señales mediante diversos medios de comunicación, como líneas de alimentación eléctrica, señales radioeléctricas y cables. Esto hace que estas redes sean susceptibles a diversos tipos de ataque como escucha clandestina, interrupción, denegación de servicio, ataque por intromisión y otros.

6.2 La red doméstica resulta de la combinación de una red inalámbrica con una red cableada

Debido a que en las redes domésticas pueden existir diversas técnicas de transmisión, éstas se componen de una red inalámbrica y de una red cableada. Las redes inalámbricas, en especial aquellas en que no se haya incorporado o no estén implementados la autorización y criptación, son más vulnerables a las amenazas contra la seguridad que las redes cableadas, debido a que hay más posibilidades de recibir tráfico indeseado o no autorizado a través del medio inalámbrico que a través del cableado. Esto hace que las amenazas que se ciernen sobre la red doméstica sean las inherentes tanto a la red cableada como a la red inalámbrica. Al instalar una red doméstica es necesario considerar las medidas para contrarrestar las amenazas y garantizar la seguridad, lo que implica que la tarea sea muy difícil ya que es necesario adoptar muchas tecnologías de seguridad.

6.3 Existen muchos entornos desde el punto de vista de la seguridad

En la vivienda existen muchos tipos de entorno, como el entorno de vivienda de una sola persona, el entorno de vivienda de una pareja con niños pequeños, el entorno de vivienda de familias con adolescentes, el entorno de adultos con compañeros de cuarto, etc. Es así como en las redes domésticas se requiere más de un tipo de dominio de seguridad. Por lo tanto, son necesarias la autenticación y autorización en las redes domésticas seguras.

6.4 Los usuarios distantes llevan consigo terminales remotos

El usuario distante que se encuentra fuera de la vivienda utiliza el terminal remoto para controlar el dispositivo doméstico que está en la vivienda y así utilizar el servicio del dispositivo doméstico a través de la red abierta. Por ejemplo, el usuario podría abrir o cerrar las cortinas de una ventana, o encender o apagar la luz antes de llegar a la vivienda, utilizando el terminal remoto.

6.5 Existen varios tipos de dispositivos de red doméstica que requieren diferentes niveles de seguridad

Existe una gran variedad de tipos de dispositivos de red doméstica, AV, PC, teléfono/facsímil y dispositivos domésticos. Cada tipo de dispositivo posee un nivel diferente de requisitos de seguridad. Aún más, es muy difícil definir un requisito general de seguridad adecuado para todos los tipos de dispositivos domésticos.

7 Amenazas contra la seguridad en el entorno de una red doméstica

La red doméstica está compuesta por una red cableada y una red inalámbrica. Las amenazas contra la red doméstica podrían ser equivalentes a las que existen en la red cableada y en la red inalámbrica. El modelo de amenazas descrito en [UIT-T X.1121] sirve de fundamento para determinar las amenazas contra la red doméstica. El modelo de amenazas contra la red doméstica puede clasificarse en dos categorías: las amenazas generales contra la seguridad y las amenazas contra la seguridad de las comunicaciones móviles, salvo por los errores de entrada ya que, según se describe en [UIT-T X.1121], éstos son causados por el usuario y no se pueden contrarrestar empleando las actuales tecnologías de seguridad.

7.1 Amenazas generales contra la seguridad, extraídas de la Rec. UIT-T X.1121

7.1.1 Escucha clandestina/divulgación/interceptación

El problema más conocido en las redes abiertas tiene que ver con la escucha clandestina proveniente de ataques anónimos. Intrusos anónimos pueden interceptar activamente los datos transmitidos y provocar divulgación de la información. Si la comunicación no está criptada, el intruso podrá leer los datos transmitidos en la comunicación y obtener información como: una dirección de origen, una dirección de destino, el tamaño de los datos transmitidos, la hora y fecha de

las transmisiones, etc. Se trata de un ataque contra la confidencialidad. Entre los ejemplos se pueden citar la intervención electrónica de cables y la copia ilegal de ficheros o programas.

7.1.2 Interrupción/perturbación de la comunicación

La perturbación de la comunicación tiene lugar cuando se presenta una señal de interferencia, intencional o no, que se impone sobre el emisor o el receptor de un enlace de comunicaciones, haciendo que éste se inutilice. Esto puede producir una DoS.

La interrupción da como resultado la destrucción de un componente de un terminal remoto o de un elemento de red. Entre los ejemplos se pueden citar la destrucción de una pieza de hardware, como un disco duro; la interrupción física de un cable de comunicaciones; o la inhabilitación de un sistema de gestión de ficheros en un terminal remoto o de una entidad en la red doméstica.

7.1.3 Inyección y modificación de datos

Esto ocurre cuando una entidad no autorizada inserta, modifica o borra la información transmitida entre un terminal remoto y un servidor de aplicación. La entidad no autorizada puede ser una persona, un programa o un computador. Estos ataques se producen cuando un intruso añade datos a una conexión existente con el objeto de apoderarse de la misma o de introducir datos con intención maliciosa. Esta amenaza puede producir una DoS o convertirse en un ataque por intromisión. Se trata de un ataque contra la integridad. Entre los ejemplos se pueden citar la modificación de un programa para que funcione de forma diferente y la modificación del contenido de un mensaje transmitido por la red doméstica.

7.1.4 Acceso no autorizado

El control de acceso es la capacidad para limitar y controlar el acceso a un servidor de aplicación a través de un enlace de comunicación. Esta amenaza ocurre cuando una entidad ilegal tiene acceso a un servidor de aplicación, a un servidor de aplicación en la vivienda o a un dispositivo doméstico, haciéndose pasar por el usuario distante real. Se debe identificar o autenticar la entidad que intenta tener acceso no autorizado. Existen, además, dos ataques importantes: exploración de puertos y software maligno. La exploración de puertos es como un ladrón que se pasea por el vecindario revisando cada puerta y ventana para ver cuáles están abiertas y cuáles cerradas con llave. El software maligno se diseña para específicamente dañar o afectar un sistema, como un virus o un caballo troyano. Estos dos ataques pueden permitir el acceso no autorizado a los elementos o dispositivos de la red doméstica.

7.1.5 Repudio

Este ataque ocurre cuando un transmisor o un receptor niega que haya transmitido o recibido un mensaje, según corresponda.

7.2 Amenazas contra la seguridad en servicios móviles, extraídas de la Rec. UIT-T X.1121

7.2.1 Escucha clandestina/divulgación/interceptación

En comunicaciones móviles, esto se logra con mayor facilidad interceptando las señales radioeléctricas y decodificando los datos transmitidos, provocando así una fuga de la información. La escucha clandestina se fundamenta en la naturaleza radioeléctrica de las transmisiones inalámbricas. En la escucha clandestina pasiva, el intruso accede a la transmisión y la supervisa pasivamente.

7.2.2 Interrupción/perturbación de la comunicación

En comunicaciones móviles, esto también se logra más fácilmente en las redes domésticas que emplean tecnología de transmisión inalámbrica. Hay dos tipos de ataque: interferencia deliberada contra un terminal móvil e interferencia deliberada contra un elemento de red. En el primero el

terminal móvil falso finge ser el terminal móvil legal. En el segundo se suplanta el elemento de red legítimo interconectándolo con el terminal móvil a través de la interfaz inalámbrica.

7.2.3 Apropiación furtiva de datos

Ocurre cuando un intruso recoge información en lugares públicos mediante la observación furtiva del teclado, lectura de la pantalla o escucha de un terminal remoto. Esto produce fuga de la información.

7.2.4 Terminal remoto perdido

Esta amenaza contra la seguridad puede ocurrir cuando el usuario distante transporta el terminal remoto. Esto puede producir la pérdida o destrucción de la información almacenada en el terminal remoto.

7.2.5 Terminal remoto robado

Esta amenaza también puede ocurrir cuando el usuario distante transporta el terminal remoto. Puede producir fuga de la información almacenada en el terminal remoto, supresión de datos como resultado del acceso no autorizado al terminal remoto robado, así como la pérdida de la información almacenada en el terminal remoto.

7.2.6 Interrupción abrupta de la comunicación

Es una amenaza contra la seguridad causada por la comunicación inestable o las limitaciones de la fuente de alimentación. Esto puede producir supresión de datos.

7.2.7 Lectura incorrecta

Esta es una amenaza que afecta la seguridad del sistema debido a una indicación visual pequeña en el terminal remoto. Puede producir supresión de datos por suplantación del ASP.

7.2.8 Error de entrada

Es una amenaza que afecta la seguridad, producida por la dificultad de ingresar datos a través del teclado o teclado numérico de un terminal remoto. Esto puede producir fallo de la autenticación del usuario.

7.3 Amenazas contra la seguridad extraídas de la Rec. UIT-T X.805

7.3.1 Reenvío anormal de paquetes

El reenvío anormal de paquetes es la amenaza que consiste en el desvío o interceptación del paquete mientras éste fluye entre los puntos extremos. Esto puede ocurrir en la pasarela doméstica segura, ocasionado por la configuración incorrecta del cuadro de encaminamiento.

7.4 Relaciones de las amenazas contra la seguridad en la red doméstica

Las amenazas contra la seguridad aparecen en entidades o ubicaciones particulares de los modelos de red doméstica. En los cuadros 1 y 2 se presentan las relaciones entre las amenazas contra la seguridad y las entidades funcionales de la red doméstica. En el cuadro 1, la letra "S" que figura en la intersección de una columna con una fila indica que esa amenaza en particular existe para la entidad o relación específica en cuestión.

Estos dos cuadros muestran que los terminales remotos, los dispositivos domésticos, los servidores de aplicación y las pasarelas de vivienda segura sufren de amenazas comunes contra la seguridad. Los cuadros muestran asimismo que en la relación se ciernen amenazas comunes contra la seguridad entre: el terminal remoto y la pasarela de vivienda segura, el terminal remoto y los dispositivos domésticos, el terminal remoto y el servidor de aplicación en la vivienda, etc.

Cuadro 1 – Relaciones entre las amenazas generales contra la seguridad y los modelos

Amenazas / Entidades o relaciones	Divulgación/ Escucha clandestina		Interrupción		Modificación/ Inyección		Acceso no autorizado		Repudio	Reenvío anormal de paquetes
	Datos almace-nados	Datos trans-mitidos	Datos almace-nados	Datos trans-mitidos	Datos almace-nados	Datos trans-mitidos	Datos almace-nados	Datos trans-mitidos		
Terminal remoto	S		S		S		S			
Dispositivo doméstico	S		S		S		S			
Pasarela de vivienda segura	S		S		S		S			S
Servidor de aplicación en la vivienda	S		S		S		S			
Relación entre el usuario distante y el terminal remoto								S*		
Relación entre el terminal remoto y la pasarela de vivienda segura		S		S		S		S		
Relación entre el terminal remoto y el servidor de aplicación en la vivienda		S		S		S		S	S	
Relación entre el terminal remoto y los dispositivos domésticos tipo B o C		S		S		S		S		
Relación entre el servidor de aplicación y la pasarela de vivienda segura		S		S		S		S		
Relación entre el servidor de aplicación y el servidor de aplicación en la vivienda		S		S		S		S	S	
Relación entre el servidor de aplicación y el dispositivo doméstico		S		S		S		S	S	
Relación entre la pasarela de vivienda segura y el dispositivo doméstico		S		S		S		S		
Relación entre el servidor de aplicación en la vivienda y el dispositivo doméstico		S		S		S		S		
Relación entre el dispositivo doméstico tipo A y los dispositivos domésticos tipo B o C		S		S		S		S		
Relación entre el dispositivo doméstico tipo A y el usuario en la vivienda								S*		
Relación entre la pasarela de vivienda segura y el servidor de aplicación en la vivienda		S		S		S		S		
Relación entre el terminal remoto y el dispositivo doméstico tipo A		S		S		S		S		

* El usuario no autorizado accede de forma no autorizada al terminal remoto, no a los datos transmitidos.

Cuadro 2 – Relación entre las amenazas contra las comunicaciones móviles estrictamente inalámbricas y los modelos

Amenazas / Entidades o relaciones	Divulgación/ Escucha clandestina		Interrupción/ Perturbación de la comunicación		Apropiación furtiva	Terminal robado/ Perdido	Interrupción abrupta	Lectura incorrecta/ Error de entrada
	Datos almace-nados	Datos trans-mitidos	Datos almace-nados	Datos trans-mitidos				
Terminal remoto						S		
Dispositivo doméstico						S		
Pasarela de vivienda segura								
Servidor de aplicación en la vivienda								
Relación entre el usuario distante y el terminal remoto					S			S
Relación entre el terminal remoto y la pasarela de vivienda segura		S		S			S	
Relación entre el terminal remoto y el servidor de aplicación en la vivienda		S		S			S	
Relación entre el terminal remoto y el dispositivo doméstico tipo B o C		S		S			S	
Relación entre el servidor de aplicación y la pasarela de vivienda segura		S		S				
Relación entre el servidor de aplicación y el servidor de aplicación en la vivienda		S		S				
Relación entre el servidor de aplicación y los dispositivos domésticos tipo B o C		S		S			S	
Relación entre la pasarela de vivienda segura y los dispositivos domésticos tipo B o C		S		S			S	
Relación entre el servidor de aplicación en la vivienda y los dispositivos domésticos tipo B o C		S		S			S	
Relación entre el dispositivo doméstico tipo A y los dispositivos domésticos tipo B o C		S		S			S	
Relación entre el dispositivo doméstico tipo A y el usuario en la vivienda					S			S
Relación entre la pasarela de vivienda segura y el servidor de aplicación en la vivienda		S		S			S	
Relación entre el terminal remoto y el dispositivo doméstico tipo A		S		S			S	

8 Requisitos de seguridad para la red doméstica

Al considerar que las redes domésticas están compuestas por una red cableada y una red inalámbrica, se infiere que los requisitos de seguridad de las redes domésticas son similares a los planteados en [UIT-T X.1121]. Pueden utilizarse los requisitos de seguridad que figuran en [UIT-T X.1121] como fundamento de los requisitos de seguridad de las redes domésticas. Algunos de los requisitos concretos de seguridad se pueden aplicar tanto a los tipos de datos almacenados en un elemento en particular como a los datos que se transmiten entre entidades, mientras que otros pueden aplicarse solo a los datos transmitidos entre las entidades. En la presente Recomendación se agrupan en un solo tipo de requisito de seguridad dos de los tipos de requisitos de seguridad de [UIT-T X.1121], ya que en el caso de la red doméstica dichos tipos se pueden considerar como uno solo. Adicionalmente, se añade a la pasarela de vivienda segura un requisito de seguridad del flujo de información, extraído de [UIT-T X.805], ya que éste garantiza que la información fluya sólo entre las entidades autorizadas de la red doméstica. (No se intercepta ni se desvía la información cuando ésta fluye entre las entidades autorizadas.)

8.1 Requisitos de seguridad extraídos de las Recs. UIT-T X.805 y X.1121

8.1.1 Confidencialidad de los datos

La confidencialidad de los datos protege los datos contra la divulgación no autorizada. La confidencialidad de los datos garantiza que los contenidos no puedan ser leídos por entidades no autorizadas. La criptación, las listas de control de acceso y los permisos sobre ficheros son métodos comúnmente utilizados para proporcionar confidencialidad de los datos.

8.1.2 Integridad de los datos

La integridad de los datos garantiza que los datos sean correctos y exactos. Protege los datos contra modificación, supresión, creación y copia no autorizadas e indica si llegan a ocurrir estas actividades no autorizadas.

8.1.3 Autenticación

Autenticación es el proceso que permite verificar si los individuos son quienes dicen ser y que los mensajes proceden de quien dicen que proceden. Hay dos tipos de autenticación: autenticación de entidades y autenticación de mensajes. La autenticación de entidades confirma la validez de la identidad que se afirma poseen las entidades, y la autenticación de mensajes confirma que el mensaje se originó en la entidad que se afirma haberlo originado. La autenticación de entidades se emplea para confirmar las identidades de las entidades que se comunican. La autenticación de mensajes garantiza la validez de las identidades reivindicadas por las entidades que participan en la comunicación (por ejemplo, una persona, un dispositivo, un servicio o una aplicación) y garantiza que no haya una entidad intentando una suplantación o la repetición no autorizada de una comunicación anterior. La autenticación se puede efectuar utilizando certificados de ID para los usuarios y certificados de dispositivo para los dispositivos domésticos.

8.1.4 Autorización o control de acceso

El control de acceso protege contra la utilización de recursos de red sin autorización. El control de acceso garantiza que sólo las personas y los dispositivos autorizados puedan acceder a los elementos de red, la información almacenada, los flujos de información, los servicios y las aplicaciones. Además, el control de acceso basado en las funciones (RBAC, *role-based access control*) establece varios niveles para restringir el acceso a los elementos de red, la información almacenada, los flujos de información, los servicios y las aplicaciones, las personas y los dispositivos autorizados. Hay tres tipos de autorización: autorización empleando ACL (listas de control de acceso), autorización empleando un servidor de autenticación y autorización utilizando el certificado de autorización o el certificado de atributos y el certificado de ID. Se puede efectuar el control de acceso o autorización utilizando certificados de autorización y listas de control de acceso.

El control de acceso o autorización se puede realizar en un cortafuegos ubicado en el punto de ingreso a la red doméstica y que actúa como pasarela de vivienda segura. El cortafuegos se diseña principalmente para impedir los accesos no autorizados desde la red pública. Con frecuencia se utilizan los cortafuegos para impedir que los usuarios de Internet accedan sin autorización a las redes privadas conectadas a Internet, en particular las intranet. Todos los mensajes que ingresen o salgan de la red intranet pasan por el cortafuegos, el cual los examina y bloquea los que no cumplan con los criterios o normas especificadas de seguridad.

8.1.5 No repudio

El no repudio proporciona medios para impedir que una persona o una entidad niegue haber realizado una cierta acción de tratamiento de datos, proporcionando pruebas de las diversas acciones efectuadas en relación con la red (como prueba de obligación, intención o compromiso; prueba de origen de los datos; prueba de propiedad; prueba de utilización de recurso). Garantiza la disponibilidad de pruebas que se pueden presentar a terceros y utilizar para demostrar que un determinado evento o acción sí ha tenido lugar.

8.1.6 Seguridad del flujo de información

La seguridad del flujo de información garantiza que la información sólo circule entre los puntos extremo autorizados (no hay desviación ni interceptación de la información que circula entre estos puntos extremo). Esta seguridad del flujo de información debería aplicarse en la pasarela de vivienda segura del entorno de una red doméstica.

8.1.7 Seguridad de la privacidad

La seguridad de la privacidad protege la información que sería posible conocer mediante análisis de las actividades o las comunicaciones realizadas en la red. Por ejemplo, los sitios web que un usuario ha visitado, la posición geográfica del usuario, y las direcciones IP de origen y de destino y los nombres de dominio (DNS) de los dispositivos en la red de un proveedor de servicio. La privacidad también contempla la privacidad de la ID en la red doméstica.

8.1.8 Disponibilidad

La disponibilidad garantiza que los sucesos que afecten la red no impidan el acceso autorizado a los elementos de red, la información almacenada, los flujos de información, los servicios y las aplicaciones. Esta categoría incluye soluciones para recuperación en caso de siniestro. Diversos ataques pueden producir la pérdida o disminución de la disponibilidad. Algunos de estos ataques pueden contrarrestarse con medidas automáticas como la autenticación y cifrado, pero para otros se requiere algún tipo de acción física que restablezca o impida la pérdida de disponibilidad de los elementos de red.

8.2 Relación entre los requisitos de seguridad y las amenazas contra la seguridad

Cada requisito de seguridad constituye una medida preventiva contra determinadas o todas las amenazas contra la seguridad. La relación entre los requisitos de seguridad y las amenazas contra la seguridad de la red doméstica figuran en los cuadros 3 y 4. En dichos cuadros, la letra "S" que aparece en la intersección de una fila con una columna indica que debe proveerse el requisito de seguridad en cuestión para anular o disminuir el efecto de la amenaza correspondiente. Se pueden evitar la lectura incorrecta y el error en la entrada mediante el diseño cuidadoso de las entidades o si el usuario presta atención, pero ese no es uno de los principales temas de la tecnología de la seguridad. Por ello no se pone ninguna marca en la columna de lectura incorrecta/error de entrada.

Cuadro 3 – Relación entre los requisitos de seguridad y las amenazas generales contra la red

Requisito de seguridad \ Amenazas		Divulgación/ Escucha clandestina		Interrupción		Modificación/ Inyección		Acceso no autorizado		Repudio	Reenvío anormal de paquetes
		Datos almacenados	Datos transmitidos	Datos almacenados	Datos transmitidos	Datos almacenados	Datos transmitidos	Datos almacenados	Datos transmitidos		
Confidencialidad	Datos transmitidos		S						S		
	Datos almacenados	S						S			
Integridad	Datos transmitios						S				
	Datos almacenados					S					S
Autenticación	Entidad	S		S		S		S		S	
	Mensaje	S		S			S	S		S	
No repudio										S	
Control de acceso	Datos transmitidos						S		S		
	Datos almacenados	S		S		S		S			
Disponibilidad	Datos transmitidos				S						
	Datos almacenados			S							
Privacidad	Datos transmitidos		S								
	Datos almacenados										
Seguridad del flujo de información											S

Cuadro 4 – Relación entre los requisitos de seguridad y las amenazas contra la seguridad exclusivas de las redes móviles

Requisito de seguridad \ Amenazas		Divulgación/ Escucha clandestina		Interrupción		Apropiación furtiva	Terminal robado/ Perdido	Interrupción abrupta	Lectura incorrecta/ Error de entrada
		Datos almacenados	Datos transmitidos	Datos almacenados	Datos transmitidos				
Confidencialidad	Datos transmitidos		S						
	Datos almacenados	S					S		
Integridad	Datos transmitidos								
	Datos almacenados								
Autenticación	Entidad	S		S			S		
	Mensaje	S		S					
No repudio									
Control de acceso	Datos transmitidos								
	Datos almacenados	S		S			S		
Disponibilidad	Datos transmitidos				S			S	
	Datos almacenados			S					
Privacidad	Entidad		S			S			
	Mensaje	S					S		
Seguridad del flujo de información					S				

9 Requisitos de seguridad de las entidades y relaciones de las redes domésticas

Estas funciones de seguridad deberían emplearse para cumplir con los requisitos de seguridad. En el cuadro 5 se indican los requisitos de seguridad exigidos para cada entidad o relación del modelo de redes domésticas. En el cuadro 5 la letra 'S' que aparece en la intersección de una fila con una columna indica que debe proveerse el requisito de seguridad en cuestión para la entidad o relación correspondiente. Por ejemplo, en la relación entre un usuario distante y un terminal remoto, el terminal remoto debería satisfacer los requisitos de autenticación de la entidad, control de acceso a los datos almacenados y privacidad de los datos almacenados.

Cuadro 5 – Requisitos de seguridad del modelo de red doméstica

Requisito de seguridad / Entidad o relación	Confidencialidad		Integridad		Autenticación		No repudio
	Datos almacenados	Datos transmitidos	Datos almacenados	Datos transmitidos	Entidad	Mensaje	
Terminal remoto	S		S		S	S	
Dispositivo doméstico	S		S		S	S	
Pasarela de vivienda segura	S		S		S	S	
Servidor de aplicación en la vivienda	S		S		S	S	
Relación entre un usuario distante y un terminal remoto					S		
Relación entre un terminal remoto y una pasarela de vivienda segura		S		S	S	S	
Relación entre un terminal remoto y un servidor de aplicación en la vivienda		S		S	S	S	S
Relación entre un terminal remoto y un dispositivo doméstico tipo B o C		S		S	S	S	
Relación entre un servidor de aplicación y una pasarela de vivienda segura		S		S		S	
Relación entre un servidor de aplicación y un servidor de aplicación en la vivienda		S		S		S	S
Relación entre un servidor de aplicación y un dispositivo doméstico		S		S	S	S	S
Relación entre un pasarela de vivienda segura y un dispositivo doméstico		S		S	S	S	
Relación entre un servidor de aplicación en la vivienda y un dispositivo doméstico tipo B o C		S		S	S	S	
Relación entre un dispositivo doméstico tipo A y un dispositivo doméstico tipo B o C		S		S	S	S	
Relación entre un dispositivo doméstico tipo A y un usuario en la vivienda					S		
Relación entre un pasarela de vivienda segura y un servidor de aplicación en la vivienda		S		S	S	S	S
Relación entre un terminal remoto y un dispositivo doméstico tipo A		S		S	S	S	

Cuadro 5 – Requisitos de seguridad del modelo de red doméstica (continuación)

Requisitos de seguridad / Entidad o relación	Control de acceso		Disponobilidad		Privacidad		Seguridad del flujo de comunicación
	Datos almacenados	Datos transmitidos	Datos almacenados	Datos transmitidos	Datos almacenados	Datos transmitidos	
Terminal remoto	S		S		S		
Dispositivo doméstico	S		S		S		
Pasarela de vivienda segura	S		S		S		S
Un servidor de aplicación en la vivienda	S		S		S		
Relación entre un usuario distante y un terminal remoto					S		
Relación entre un terminal remoto y una pasarela de vivienda segura		S		S		S	
Relación entre un terminal remoto y un servidor de aplicación en la vivienda		S		S		S	
Relación entre un terminal remoto y un dispositivo doméstico		S		S		S	
Relación entre un servidor de aplicación y una pasarela de vivienda segura		S		S		S	
Relación entre un servidor de aplicación y un servidor de aplicación en la vivienda		S		S		S	
Relación entre un servidor de aplicación y un dispositivo doméstico		S		S		S	
Relación entre una pasarela de vivienda segura y un dispositivo doméstico		S		S		S	
Relación entre un servidor de aplicación en la vivienda y un dispositivo doméstico		S		S		S	
Relación entre un dispositivo doméstico tipo A y un dispositivo doméstico tipo B o C		S		S		S	
Relación entre un dispositivo doméstico tipo A y un usuario en la vivienda					S		
Relación entre una pasarela de vivienda segura y un servidor de aplicación en la vivienda		S		S		S	
Relación entre un terminal remoto y un dispositivo doméstico tipo A		S		S		S	

10 Funciones de seguridad para satisfacer los requisitos de seguridad de la red doméstica

10.1 Funciones de seguridad extraídas de la Rec. UIT-T X.1121

10.1.1 Función cifrado (o criptación)

Con la función de cifrado se puede implementar confidencialidad a los datos transmitidos o a los datos almacenados. Los algoritmos de cifrado se pueden clasificar en dos tipos: los algoritmos simétricos y los asimétricos. En los algoritmos de clave pública se tienen dos tipos de clave: la clave pública y la clave privada. Si se conoce la clave pública no significa que se conozca la clave privada. El emisor utiliza la clave pública del receptor para cifrar el contenido. Como el receptor posee una sola clave privada, estará en capacidad de leer el mensaje, que descripta a partir del texto cifrado. En el cifrado simétrico, al conocerse la clave de cifrado se conoce también la clave de descifrado, y viceversa.

La baja capacidad de procesamiento o el tamaño limitado de la memoria de los terminales remotos dificulta la implementación de las funciones existentes de cifrado, en particular cuando se trata del algoritmo asimétrico empleado en la actual red abierta.

La función de cifrado puede implementarse en el cortafuegos ubicado en el punto de ingreso a la red doméstica.

10.1.2 Función firma digital

La función firma digital define dos procesos: uno para firmar los datos y otro para verificar los datos firmados. El primer proceso utiliza una clave privada (es decir, única y confidencial) para generar la firma. El segundo proceso utiliza una clave pública para verificar la validez de la firma.

El proceso de firma implica bien el cifrado de los datos o bien la producción de un valor de comprobación criptográfica de los datos empleando la información privada del firmante como clave privada.

El proceso de verificación entraña el uso de procedimientos e información pública para determinar si la firma se generó correctamente con la información privada del firmante.

Las características esenciales de la función firma digital es que la firma sólo se puede generar utilizando la información privada del firmante. Así, cuando se verifica la firma, se puede probar en todo momento a un tercero (por ejemplo, al juez o árbitro) que sólo el poseedor legítimo de la información privada pudo haber realizado la firma digital.

En cuanto a la función cifrado, existen algunas dificultades en aplicar las funciones de firma digital actualmente utilizadas en redes abiertas existentes debido a la baja eficacia de procesamiento o capacidad limitada de la memoria de los terminales remotos.

10.1.3 Función control de acceso

La función control de acceso puede utilizar la identidad autenticada de una entidad o información acerca de la entidad (tal como condición de miembro en un conjunto de entidades conocido) o capacidades de la entidad, a fin de determinar y poner en vigor los derechos de acceso de la entidad. Si la entidad intenta utilizar un recurso no autorizado, o un recurso autorizado con un tipo de acceso inadecuado, la función control de acceso rechazará entonces el intento y, además, puede comunicar el incidente con el propósito de generar una alarma así como grabarlo como parte de un registro de auditoria de seguridad. La función control de acceso se puede basar en la utilización de los siguientes elementos:

- bases de información de control de acceso, donde se mantiene en una base de datos el derecho de acceso de las entidades pares;
- información de autenticación tal como contraseñas, cuya posesión y subsiguiente presentación son prueba de la autorización de la entidad de acceso;
- capacidades, cuya posesión y subsiguiente presentación son prueba del derecho a acceder a la entidad o recurso definido por la capacidad;
- certificados de autorización;
- etiquetas de seguridad, las que se pueden utilizar asociadas con una entidad para acordar o denegar acceso, generalmente con arreglo a la política de seguridad en vigor;
- tiempo de tentativa de acceso;
- ruta de tentativa de acceso;
- duración del acceso; y
- ubicación física de la tentativa de acceso.

La función control de acceso se puede aplicar en cualquier entidad par de una asociación de comunicación y/o en una pasarela de vivienda segura.

El control de acceso aplicado a la entidad de origen o pasarela de seguridad móvil se utiliza para determinar si el emisor está autorizado para comunicarse con el receptor y/o utilizar los recursos de comunicación requeridos.

La función control de acceso permite al dispositivo doméstico saber lo que permite que cada dispositivo autenticado haga. Hay mecanismos de autorización predominantes como las listas de control de acceso (ACL), el servidor de autorizaciones y el certificado de autorización.

Un dispositivo puede controlar el acceso mediante una sola ACL. Esto permite suprimir fácilmente un control de acceso, ya que la ACL del dispositivo se puede modificar. Tiene la desventaja de que puede ser dispendioso modificar las listas si éstas son muchas.

Si un usuario en la vivienda posee una red doméstica con un gran número de dispositivos domésticos y por ende ACL grandes, puede ser conveniente pasar la ACL de los dispositivos domésticos a un servidor, denominado servidor de autorizaciones. Aunque cada dispositivo necesita una ACL, puede ser conveniente usar un servidor de autenticaciones.

Otra forma de administrar las autorizaciones consiste en permitir la delegación mediante certificados de autorización. Un certificado de autorización es un registro de una ACL firmado digitalmente.

La función de control de acceso puede aplicarse en el cortafuegos ubicado en el punto de ingreso a la red doméstica.

10.1.4 Función integridad de datos

Se consideran dos aspectos de integridad de los datos: la integridad de una unidad o campo de datos simple y la integridad de un tren de unidades o campos de datos. En general, se utilizan diversas tecnologías para proporcionar estos dos tipos de función de integridad, si bien el suministro del segundo tipo sin el primero no es práctico.

La determinación de la integridad de una unidad de datos simple implica dos procesos, uno en la entidad emisora y el otro en la entidad receptora. La entidad emisora añade a los datos una cantidad que es función de los datos propiamente dichos. Esta cantidad puede ser una información suplementaria tal como un código de verificación de bloque o un valor de comprobación criptográfica, y puede ser cifrada. La entidad receptora genera una cantidad correspondiente y compara su resultado con la cantidad recibida para determinar si los datos han sido modificados en el tránsito. Este proceso por sí mismo no prestará protección contra la reproducción de una unidad de datos simple.

La protección de la integridad de una secuencia de unidades de datos (es decir, protección contra desordenamiento, pérdida, repetición e inserción o modificación de los datos) requiere añadir alguna forma de orden explícito tal como numeración secuencial, indicación de tiempo, o encadenamiento criptográfico.

La integridad de los datos se fundamenta en garantizar que los datos se reciban tal y como se enviaron. La función integridad de datos utiliza el algoritmo de troceo (hash) o el algoritmo de firma digital.

La función integridad de datos puede aplicarse en el cortafuegos ubicado en el punto de ingreso a la red doméstica.

10.1.5 Función autenticación

Algunas tecnologías de seguridad que se pueden aplicar a la autenticación son:

- empleo de información de autenticación, tal como contraseñas proporcionadas por una entidad emisora y verificadas por la entidad receptora;
- tecnologías criptográficas; y
- utilización de características y/o posesiones de la entidad.

La función autenticación puede clasificarse en dos categorías: autenticación del usuario y autenticación del mensaje. La autenticación del mensaje puede ser proporcionada en la red

doméstica mediante un certificado de dispositivo o un certificado de ID. La función de autenticación del usuario puede fundamentarse en tres factores:

1) lo que se sabe;

2) lo que se tiene; y

3) lo que se es.

Se puede incorporar la función autenticación para proporcionar autenticación de entidad par. Si la función no logra autenticar la entidad, se producirá el rechazo o la terminación de la conexión y puede generar una inserción en el registro de auditoría de seguridad y/o un informe a un centro de gestión de seguridad.

Cuando se utilizan, las técnicas criptográficas se pueden combinar con protocolos de iniciación de diálogo para la protección contra repetición (es decir, asegurar el contacto activo).

La elección de la tecnología de seguridad que realiza autenticación, dependerá de las circunstancias en las cuales han de ser utilizadas con:

- indicación de tiempo y relojes sincronizados;
- tomas de contacto de dos o tres instancias (para autenticación unilateral y mutua, respectivamente); y
- funciones de no repudio obtenidas por firma digital y/o mecanismos de notarización.

La función autenticación puede aplicarse en el cortafuegos ubicado en el punto de ingreso a la red doméstica.

10.1.6 Notarización

Las propiedades de los datos comunicados entre dos o más entidades, tales como su integridad, origen, tiempo y destino, se pueden asegurar mediante una función de notarización. El mecanismo de seguridad es proporcionado por una tercera parte de confianza (notario), que se constituye en custodio de las entidades comunicantes, y que dispone de la información necesaria para prestar la seguridad requerida de manera verificable. Cada ejemplar de comunicación puede utilizar firma digital, cifrado, y funciones de integridad según sea apropiado al servicio proporcionado por el notario. Cuando se invoca la función notarización, los datos entre las entidades comunicantes se efectúan a través de las instancias de comunicación protegidas y el notario.

10.2 Funciones de seguridad adicionales

10.2.1 Función código de autenticación de mensaje (MAC, *message authentication code*)

Se define un MAC como una función pública que recibe un mensaje y una clave secreta y arroja como resultado un valor de longitud fija que actúa como autenticador, el cual permite proporcionar un mensaje autenticado y que el receptor verifique la autenticidad del mensaje. El MAC permite contrarrestar la usurpación de identidad, la modificación del contenido, la modificación de la secuencia y la modificación de la indicación de tiempo. Ejemplos comunes de la función MAC son HMAC (Código de autenticación de mensajes basado en troceado) y MAC basado en el algoritmo de cifrado simétrico.

La función código de autenticación de mensaje puede aplicarse en el cortafuegos ubicado en el punto de ingreso a la red doméstica.

10.2.2 Función gestión de claves

La función gestión de claves, esencial para todas las funciones de seguridad, se encarga de generar, distribuir, transportar, suprimir y destruir todo tipo de clave criptográfica necesaria para las otras funciones de la seguridad. La función gestión de claves abarca la función intercambio de claves de

[UIT-T X.1121]. En otras palabras, la función intercambio de claves es un subconjunto de la función gestión de claves.

La función gestión de claves puede aplicarse en el cortafuegos ubicado en el punto de ingreso a la red doméstica.

10.3 Relaciones entre los requisitos de seguridad y las funciones de seguridad

Estas funciones de seguridad se emplean para satisfacer algunos de los requisitos de seguridad. En el cuadro 6 se indican algunos conjuntos de funciones de seguridad destinados a satisfacer requisitos de seguridad específicos. En el cuadro 6, la letra 'S' que aparece en la intersección de una fila con una columna indica que puede satisfacerse el requisito de seguridad en cuestión mediante la correspondiente función de seguridad. La letra 'K' significa que el servicio de seguridad puede complementarse o reforzarse mediante el mecanismo de seguridad indicado. La letra 'X' significa que alguna de las funciones de seguridad opcionales puede proporcionar el servicio de seguridad especificado. Por ejemplo, la función de control de acceso puede agruparse en dos funciones de control de acceso: el control de acceso físico y el control de acceso técnico.

Cuadro 6 – Ilustración de las relaciones entre los requisitos de seguridad y las funciones de seguridad

Función de seguridad / Requisito de seguridad		Cifrado	Inte-gridad	MAC	Auten-ticación de la entidad	Firma digital	Notari-zación	Control de acceso		Gestión de claves	Antidisponibilidad	
								Físico	Técnico		Física	Técnico
Confidencialidad	Datos transmitidos	S						K		S		
	Datos almacenados	S						K		S		
Integridad	Datos transmitidos		X	X		X	X			S		
	Datos almacenados		X	X		X	X			S		
Autenticación	Entidad				S					S		
	Mensaje			X		X	X			S		
No repudio						S	S			S		
Control de acceso	Datos transmitidos	K						K		K		
	Datos almacenados	K		S	S	S		K	S	S		
Disponibilidad	Datos transmitidos							X			X	S
	Datos almacenados			X	X	X			K	S		S
Privacidad	Datos transmitidos	S						K		S		
	Datos almacenados	S		X	X	X		K	S	S		
Seguridad del flujo de información			X	X	X			K	S	S		

11 Tecnologías de seguridad de la red doméstica

Cuando las funciones de seguridad descritas en la cláusula 10 se llevan a la práctica en la red doméstica, se pueden aplicar varias tecnologías de seguridad. Dichas tecnologías de seguridad pueden clasificarse dependiendo de la función de seguridad y el sitio en que se aplican. Como en los modelos de redes domésticas las tecnologías de seguridad se aplican a una entidad o a una relación entre entidades, los sitios en los que se aplican las tecnologías de la seguridad son necesariamente entidades o relaciones entre entidades. En los cuadros 1 y 2 se muestran los sitios donde aparecen

las amenazas contra la seguridad en los modelos de redes domésticas; en los cuadros 3 y 4 se indican los requisitos de seguridad necesarios para contrarrestar las diversas amenazas contra la seguridad; en el cuadro 5 se muestran los requisitos de seguridad necesarios para cada entidad o relación en particular del modelo de redes domésticas; y en el cuadro 6 se ilustran las funciones de seguridad que satisfacen los requisitos de seguridad. Por lo tanto, en el cuadro 7 se pueden indicar las relaciones entre las funciones de seguridad y los sitios en que éstas se pueden aplicar dentro de los modelos. En otras palabras, en el cuadro 7 se muestra el sitio en que se pueden aplicar las tecnologías de seguridad que cumplen con ciertas funciones, dentro del modelo de red doméstica.

Cuadro 7 – Relaciones entre las tecnologías de la seguridad y los modelos

Entidad o relación \ Función de seguridad		Cifrado	Integridad	MAC	Autenticación de la entidad	Firma digital	Notarización	Control de acceso		Gestión de claves	Antidisponibilidad	
								Físico	Técnico		Física	Técnico
Datos almacenados	Terminal remoto	S	X	S	S	S	S	K	S	S		S
	Dispositivo doméstico	S	X	S	S	S	S	K	S	S		S
	Pasarela de vivienda segura	S	X	S	S	S	S	K	S	S		S
	Servidor de aplicación en la vivienda	S	X	S	S	S	S	K	S	S		S
Datos transmitidos	Relación entre el usuario distante y el terminal remoto	S		X	S	S		K	S	S		
	Relación entre el terminal remoto y la pasarela de vivienda segura	S	X	X	S	S	S	X		S	X	S
	Relación entre el terminal remoto y el servidor de aplicación en la vivienda	S	X	X	S	S	S	X		S	X	S
	Relación entre el terminal remoto y los dispositivos domésticos tipo B o C	S	X	X	S	S	S	X		S	X	S
	Relación entre el servidor de aplicación y la pasarela de vivienda segura	S	X	X		X	X	X		S	X	S
	Relación entre el servidor de aplicación y el servidor de aplicación en la vivienda	S	X	X		S	S	X		S	X	S
	Relación entre el servidor de aplicación y el dispositivo doméstico	S	X	X	S	S	S	X		S	X	S
	Relación entre la pasarela de vivienda segura y el dispositivo doméstico	S	X	X	S	S	S	X		S	X	S

Cuadro 7 – Relaciones entre las tecnologías de la seguridad y los modelos

Entidad o relación \ Función de seguridad		Cifrado	Integridad	MAC	Autenticación de la entidad	Firma digital	Notarización	Control de acceso		Gestión de claves	Antidisponibilidad	
								Físico	Técnico		Física	Técnico
Datos transmitidos	Relación entre el servidor de aplicación en la vivienda y el dispositivo doméstico	S	X	X	S	S	S	X		S	X	S
	Relación entre el dispositivo doméstico tipo A y los dispositivos domésticos tipo B o C	S	X	X	S	S	S	X		S	X	S
	Relación entre el dispositivo doméstico tipo A y el usuario en la vivienda	S		X	S	S		K	S	S		
	Relación entre la pasarela de vivienda segura y el servidor de aplicación en la vivienda	S	X	X	S	S	S	X		S	X	S
	Relación entre el terminal remoto y el dispositivo doméstico tipo A	S		X	S	S	S	X		S	X	S

Las funciones de seguridad se pueden implementar en las diversas capas. En el cuadro 8 se ilustran la o las capas en que es posible implementar la función de seguridad de cada una de las relaciones del modelo. La seguridad en el nivel de enlace de datos, la seguridad del nivel de red, la seguridad del nivel de sesión y la seguridad del nivel de aplicación pueden proveerse respectivamente en las capas de enlace de datos, de red, de transporte y de aplicación. Ejemplos de los protocolos de seguridad son IPSec, TLS y el protocolo de seguridad entre pares de aplicación, respectivamente.

Cuadro 8 – Capas en que sería posible implementar las funciones de seguridad de las relaciones del modelo

Relaciones	Capa en que se implementa la seguridad
Relación entre el terminal remoto y la pasarela de vivienda segura	Nivel de red o de sesión
Relación entre el terminal remoto y el servidor de aplicación en la vivienda	Nivel de aplicación
Relación entre el terminal remoto y el dispositivo doméstico tipo B o tipo C	Nivel de aplicación
Relación entre el servidor de aplicación y la pasarela de vivienda segura	Nivel de red o de sesión
Relación entre el servidor de aplicación y el servidor de aplicación en la vivienda	Nivel de red o de sesión, o nivel de aplicación
Relación entre el servidor de aplicación y el dispositivo doméstico tipo B o tipo C	Nivel de red, de sesión o de aplicación
Relación entre la pasarela de vivienda segura y el dispositivo doméstico tipo B o tipo C	Nivel de enlace de datos, de red o de sesión

Cuadro 8 – Capas en que sería posible implementar las funciones de seguridad de las relaciones del modelo

Relaciones	Capa en que se implementa la seguridad
Relación entre el servidor de aplicación en la vivienda y el dispositivo doméstico tipo B o tipo C	Nivel de enlace de datos, de red, de sesión o de aplicación
Relación entre el dispositivo doméstico tipo A y el dispositivo doméstico tipo B o C	Nivel de enlace de datos o de aplicación
Relación entre la pasarela de vivienda segura y el servidor de aplicación en la vivienda	Nivel de red o de sesión
Relación entre el terminal remoto y el dispositivo doméstico tipo A	Nivel de aplicación

12 Requisitos de la función de seguridad para la red doméstica

Los siguientes son los requisitos de seguridad de las entidades de red de la red doméstica:

1) Todos los elementos de red, como los terminales remotos, la pasarela de vivienda segura, el servidor de aplicación y los dispositivos domésticos deberían mantener de forma segura su información confidencial y protegerla contra acceso no autorizado, modificación no autorizada y supresión no autorizada.

2) El terminal remoto debería poseer la capacidad de autenticar al usuario distante empleando los métodos de autenticación adecuados, como los métodos de autenticación biométrica.

3) El terminal remoto debe contar con funciones de seguridad en el nivel de red o de sesión, como autenticación de entidad, gestión de claves y MAC o integridad, por si requiere comunicar datos con la pasarela de vivienda segura garantizando la confidencialidad e integridad de los datos.

4) El terminal remoto debe contar con funciones de seguridad en el nivel de aplicación o de red, como autenticación de entidad, gestión de claves, criptación y MAC o integridad, por si requiere comunicar datos con el servidor de aplicación en la vivienda garantizando la confidencialidad e integridad de los datos.

5) El terminal remoto debe contar con funciones de seguridad en el nivel de aplicación, como autenticación de entidad, gestión de claves, firma digital, criptación y MAC o integridad, por si requiere comunicar datos con los dispositivos domésticos tipo B o C, garantizando la confidencialidad e integridad de los datos.

6) Los dispositivos domésticos tipo A deberían poseer la capacidad de autenticar a los usuarios en la vivienda empleando el método apropiado de autenticación de usuarios.

7) Los dispositivos domésticos tipo A deberían contar con funciones de seguridad en el nivel de aplicación, como autenticación de entidad, gestión de claves, criptación y MAC o integridad, por si requieren comunicar datos con los dispositivos domésticos tipo B o C, garantizando la confidencialidad e integridad de los datos.

8) Los dispositivos domésticos tipo B y C deben contar con funciones de seguridad en el nivel de red, sesión o aplicación, como autenticación de entidad, gestión de claves y MAC o integridad, por si requieren comunicar datos con el servidor de aplicación en la vivienda o con el servidor de aplicación de la red, garantizando la confidencialidad e integridad de los datos.

9) Los dispositivos domésticos tipo B y C deben contar con funciones de seguridad en el nivel de red o de aplicación, como autenticación de entidad, gestión de claves y MAC o integridad, por si requieren comunicar datos con la pasarela de vivienda segura, garantizando la confidencialidad e integridad de los datos.

10) La pasarela de vivienda segura debería contar con funciones de seguridad, por lo general en el nivel de red, como autenticación de entidad, gestión de claves y MAC o integridad, por si requiere comunicar datos el servidor de aplicación en la vivienda o el proveedor de servicios de aplicación, garantizando la confidencialidad e integridad de los datos.

11) El administrador de la red doméstica debe tener la habilidad para administrar a distancia o localmente la pasarela de vivienda o el servidor de aplicación, con la anuencia del usuario.

12) La pasarela de vivienda segura debería contar con funciones relativas a la seguridad, como cortafuegos, detección de intrusos, filtrado de contenidos o una interfaz para acceso a distancia para el mantenimiento, como capacidades opcionales.

13) Debe existir una interfaz adecuada para el registro/mensajería de eventos relativos a la seguridad de la pasarela de vivienda segura, que permita que el administrador de la vivienda supervise y revise las actividades de la pasarela de vivienda segura.

Anexo A

Tipo de dispositivo de red doméstica de la Rec.UIT-T J.190

(Este anexo es parte integrante de esta Recomendación)

Los dispositivos de red doméstica deberían clasificarse desde el punto de vista de la seguridad. En [UIT-T J.190] todos los dispositivos domésticos se clasifican en las cuatro clases que se muestran en la figura A.1: Clase acceso a la vivienda (HA, *home access*), clase puente en la vivienda (HB, *home bridge*), clase cliente en la vivienda (HC, *home client*) y clase decodificador en la vivienda (HD, *home decoder*). Los HA son dispositivos en la interfaz con la red de acceso, los HB son dispositivos que sirven de puente entre las redes del dominio IPCable2Home (por ejemplo, concentradores, encaminadores, etc.), los HC son dispositivos en la interfaz entre el dominio IPCable2Home y los dispositivos del dominio privado, y los HD son dispositivos que se pueden comunicar haciendo uso de protocolos patentados (por ejemplo, DVD, D-VHS, equipos de sonido digital, impresoras, etc.). Cada dispositivo de las clases HC y HD pertenece a uno de los planos de servicio, por ejemplo, plano AV, plano PC, plano TEL/FAX y plano electrodomésticos.

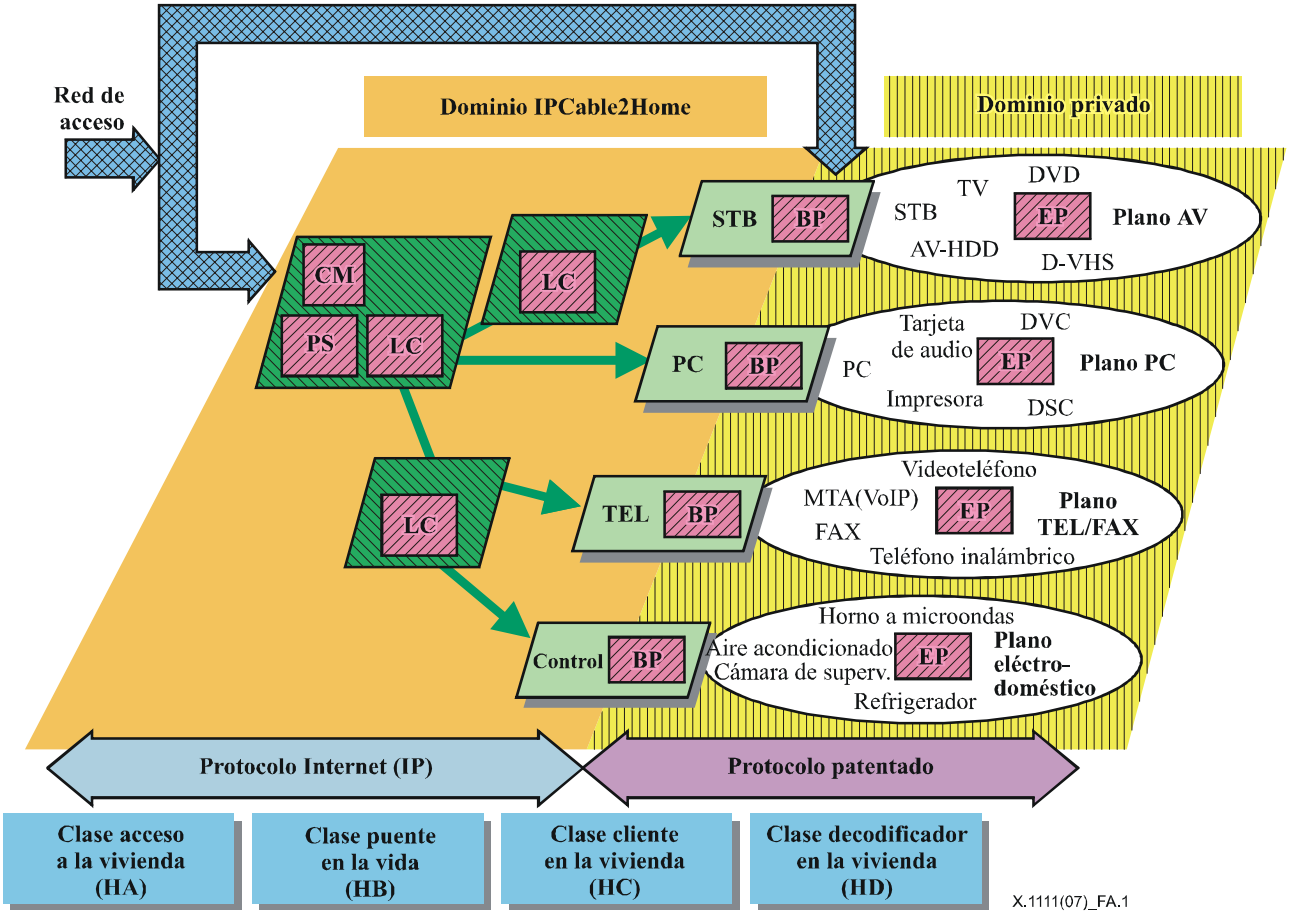

Figura A.1 – Contexto de la red doméstica UIT-T J.190

En la cláusula 5.4.3 de [UIT-T J.190] figuran más explicaciones sobre las clases y los planos de los dispositivos o aparatos.

De acuerdo con la terminología definida en la presente Recomendación, la pasarela de vivienda segura corresponde a la clase HA, ninguno de los dispositivos de la red doméstica corresponde a la clase de dispositivos HB ya que ésta normalmente no contiene funciones de seguridad, los dispositivos domésticos tipo B corresponden a la clase de dispositivos HC y por último, los dispositivos domésticos tipo C no corresponden a ninguna de las clases de dispositivos de [UIT-T J.190], pero podrían corresponder a la clase de dispositivos HD cuando no emplean protocolos patentados para comunicarse con los dispositivos tipo B. Como en la presente Recomendación las comunicaciones entre los dispositivos domésticos tipo B y los dispositivos domésticos de tecnología anterior, sin capacidades de comunicación, utilizan el mecanismo de comunicación privado, en la Recomendación no se especifican los requisitos de seguridad de dicho mecanismo de comunicación privado.

En [UIT-T J.190] se presenta el concepto "plano de usuario", que es de gran utilidad. Todos los dispositivos se agrupan en cuatro planos que dependen de sus funciones: el plano AV, el plano PC, el plano Tel/Fax y el plano electrodoméstico.

No obstante, desde el punto de vista de la seguridad, existe un dispositivo que envía instrucciones a otro a fin de controlarlo o para solicitar un servicio y también existe un dispositivo que recibe instrucciones de otro dispositivo o que suministra un servicio. En este sentido, todos los dispositivos domésticos pueden agruparse en tres tipos de dispositivo, independientemente del plano de seguridad al que pertenezcan. En la presente Recomendación se presentan los requisitos de seguridad máximos para los dispositivos domésticos, independientemente del plano al que pertenecen. Por lo tanto, deberían elegirse los requisitos de seguridad de los dispositivos de acuerdo con la normatividad del proveedor de servicios que los emplea. Como cada dispositivo requiere un nivel de requisitos de seguridad diferente, sería muy difícil definir un conjunto general de requisitos de seguridad específicos. En esta Recomendación no se tratan los requisitos de seguridad específicos.

Apéndice I

Tipos de dispositivos de red doméstica UPnP

(Este apéndice no es parte integrante de esta Recomendación)

Hay tres clases principales de dispositivos disponibles sin preparativos (UPnP, *universal plug and play*): punto de control de usuario/universal (UCP, *user/universal control point*), dispositivo controlado y puente.

- UCP – Punto de control de usuario/universal: se trata de un tipo de dispositivo, como un PC o un PDA, que permite controlar otros dispositivos UPnP mediante una página de presentación o una pantalla especializada.
- Puente: conecta dispositivos UPnP a la red doméstica. En términos generales, por un lado se comunica con los UPnP y, por el otro, emplea un lenguaje de marca registrada (entre los ejemplos se pueden citar los controles de iluminación de marca registrada, bluetooth, etc.).
- Dispositivo controlado: Todo dispositivo UPnP que permita ser controlado o que proporcione algún tipo de servicio UPnP al resto de la red doméstica (como IGD, dispositivos de audio y vídeo, cámaras de seguridad, etc.).

La clasificación de los dispositivos domésticos es, en principio, muy parecida a la de los UPnP. Según la terminología definida en la presente Recomendación, la pasarela de vivienda segura no corresponde a ninguno de los dispositivos UPnP, UCP corresponde al dispositivo tipo A, el puente corresponde al dispositivo tipo B y los dispositivos controlados corresponden al dispositivo doméstico tipo C.

Bibliografía

[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 DE RECOMENDACIONES DEL UIT-T

Serie A	Organización del trabajo del UIT-T
Serie D	Principios generales de tarificación
Serie E	Explotación general de la red, servicio telefónico, explotación del servicio y factores humanos
Serie F	Servicios de telecomunicación no telefónicos
Serie G	Sistemas y medios de transmisión, sistemas y redes digitales
Serie H	Sistemas audiovisuales y multimedia
Serie I	Red digital de servicios integrados
Serie J	Redes de cable y transmisión de programas radiofónicos y televisivos, y de otras señales multimedia
Serie K	Protección contra las interferencias
Serie L	Construcción, instalación y protección de los cables y otros elementos de planta exterior
Serie M	Gestión de las telecomunicaciones, incluida la RGT y el mantenimiento de redes
Serie N	Mantenimiento: circuitos internacionales para transmisiones radiofónicas y de televisión
Serie O	Especificaciones de los aparatos de medida
Serie P	Calidad de transmisión telefónica, instalaciones telefónicas y redes locales
Serie Q	Conmutación y señalización
Serie R	Transmisión telegráfica
Serie S	Equipos terminales para servicios de telegrafía
Serie T	Terminales para servicios de telemática
Serie U	Conmutación telegráfica
Serie V	Comunicación de datos por la red telefónica
Serie X	**Redes de datos, comunicaciones de sistemas abiertos y seguridad**
Serie Y	Infraestructura mundial de la información, aspectos del protocolo Internet y Redes de la próxima generación
Serie Z	Lenguajes y aspectos generales de soporte lógico para sistemas de telecomunicación

Impreso en Suiza
Ginebra, 2008