Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

X.1111

(02/2007)

SÉRIE X: RÉSEAUX DE DONNÉES, COMMUNICATION ENTRE SYSTÈMES OUVERTS ET SÉCURITÉ

Sécurité des télécommunications

Cadre général des technologies de sécurité pour les réseaux domestiques

Recommandation UIT-T X.1111

RECOMMANDATIONS UIT-T DE LA SÉRIE X

RÉSEAUX DE DONNÉES, COMMUNICATION ENTRE SYSTÈMES OUVERTS ET SÉCURITÉ

RÉSEAUX PUBLICS DE DONNÉES	
Services et fonctionnalités	X.1–X.19
Interfaces	X.20–X.49
Transmission, signalisation et commutation	X.50–X.89
Aspects réseau	X.90–X.149
Maintenance	X.150–X.179
Dispositions administratives	X.180–X.199
INTERCONNEXION DES SYSTÈMES OUVERTS	
Modèle et notation	X.200–X.209
Définitions des services	X.210–X.219
Spécifications des protocoles en mode connexion	X.220–X.229
Spécifications des protocoles en mode sans connexion	X.230–X.239
Formulaires PICS	X.240–X.259
Identification des protocoles	X.260–X.269
Protocoles de sécurité	X.270–X.279
Objets gérés des couches	X.280–X.289
Tests de conformité	X.290–X.299
INTERFONCTIONNEMENT DES RÉSEAUX	
Généralités	X.300–X.349
Systèmes de transmission de données par satellite	X.350–X.369
Réseaux à protocole Internet	X.370–X.379
SYSTÈMES DE MESSAGERIE	X.400–X.499
ANNUAIRE	X.500–X.599
RÉSEAUTAGE OSI ET ASPECTS SYSTÈMES	
Réseautage	X.600–X.629
Efficacité	X.630–X.639
Qualité de service	X.640–X.649
Dénomination, adressage et enregistrement	X.650–X.679
Notation de syntaxe abstraite numéro un (ASN.1)	X.680–X.699
GESTION OSI	
Cadre général et architecture de la gestion-systèmes	X.700–X.709
Service et protocole de communication de gestion	X.710–X.719
Structure de l'information de gestion	X.720–X.729
Fonctions de gestion et fonctions ODMA	X.730–X.799
SÉCURITÉ	X.800–X.849
APPLICATIONS OSI	
Engagement, concomitance et rétablissement	X.850–X.859
Traitement transactionnel	X.860–X.879
Opérations distantes	X.880–X.889
Applications génériques de l'ASN.1	X.890–X.899
TRAITEMENT RÉPARTI OUVERT	X.900–X.999
SÉCURITÉ DES TÉLÉCOMMUNICATIONS	**X.1000–**

Pour plus de détails, voir la Liste des Recommandations de l'UIT-T.

Recommandation UIT-T X.1111

Cadre général des technologies de sécurité pour les réseaux domestiques

Résumé

La Recommandation UIT-T X.1111 décrit les menaces sur la sécurité et les prescriptions de sécurité pour un réseau domestique du point de vue de l'utilisateur résidentiel ou de l'utilisateur distant. Elle ne porte pas sur les prescriptions de sécurité considérées du point de vue du fournisseur de services. De plus, elle classe les technologies de la sécurité par fonctions de sécurité satisfaisant aux prescriptions de sécurité susmentionnées et selon le lieu où ces technologies sont appliquées dans le modèle de réseau domestique. Enfin, elle présente les prescriptions de fonctions de sécurité pour chaque entité du réseau et les couches d'implémentation possibles pour les fonctions de sécurité.

Source

La Recommandation UIT-T X.1111 a été approuvée le 13 février 2007 par la Commission d'études 17 (2005-2008) de l'UIT-T selon la procédure définie dans la Recommandation UIT-T A.8.

AVANT-PROPOS

L'UIT (Union internationale des télécommunications) est une institution spécialisée des Nations Unies dans le domaine des télécommunications. L'UIT-T (Secteur de la normalisation des télécommunications) est un organe permanent de l'UIT. Il est chargé de l'étude des questions techniques, d'exploitation et de tarification, et émet à ce sujet des Recommandations en vue de la normalisation des télécommunications à l'échelle mondiale.

L'Assemblée mondiale de normalisation des télécommunications (AMNT), qui se réunit tous les quatre ans, détermine les thèmes d'étude à traiter par les Commissions d'études de l'UIT-T, lesquelles élaborent en retour des Recommandations sur ces thèmes.

L'approbation des Recommandations par les Membres de l'UIT-T s'effectue selon la procédure définie dans la Résolution 1 de l'AMNT.

Dans certains secteurs des technologies de l'information qui correspondent à la sphère de compétence de l'UIT-T, les normes nécessaires se préparent en collaboration avec l'ISO et la CEI.

NOTE

Dans la présente Recommandation, l'expression "Administration" est utilisée pour désigner de façon abrégée aussi bien une administration de télécommunications qu'une exploitation reconnue.

Le respect de cette Recommandation se fait à titre volontaire. Cependant, il se peut que la Recommandation contienne certaines dispositions obligatoires (pour assurer, par exemple, l'interopérabilité et l'applicabilité) et considère que la Recommandation est respectée lorsque toutes ces dispositions sont observées. Le futur d'obligation et les autres moyens d'expression de l'obligation comme le verbe "devoir" ainsi que leurs formes négatives servent à énoncer des prescriptions. L'utilisation de ces formes ne signifie pas qu'il est obligatoire de respecter la Recommandation.

DROITS DE PROPRIÉTÉ INTELLECTUELLE

L'UIT attire l'attention sur la possibilité que l'application ou la mise en œuvre de la présente Recommandation puisse donner lieu à l'utilisation d'un droit de propriété intellectuelle. L'UIT ne prend pas position en ce qui concerne l'existence, la validité ou l'applicabilité des droits de propriété intellectuelle, qu'ils soient revendiqués par un membre de l'UIT ou par une tierce partie étrangère à la procédure d'élaboration des Recommandations.

A la date d'approbation de la présente Recommandation, l'UIT n'avait pas été avisée de l'existence d'une propriété intellectuelle protégée par des brevets à acquérir pour mettre en œuvre la présente Recommandation. Toutefois, comme il ne s'agit peut-être pas de renseignements les plus récents, il est vivement recommandé aux développeurs de consulter la base de données des brevets du TSB sous http://www.itu.int/ITU-T/ipr/.

TABLE DES MATIÈRES

Page

Recommandation UIT-T X.1111

Cadre général des technologies de sécurité pour les réseaux domestiques

1 Domaine d'application

Le réseau domestique est un élément important du réseau de communication de données de bout en bout. Les menaces sur sa sécurité pourraient être équivalentes à celles qui pèsent sur un réseau filaire ou un réseau hertzien puisqu'il fait intervenir diverses techniques de transmission filaire ou hertzienne.

Pour établir le cadre général de sécurité d'un réseau domestique, il faut identifier les menaces potentielles et déterminer les fonctions de sécurité nécessaires dans les entités du modèle de réseau domestique. Il apparaît que le modèle de menaces applicable au réseau domestique est fondamentalement le même que celui décrit dans [UIT-T X.1121] ("Cadre général des technologies de la sécurité pour les communications mobiles de données de bout en bout"). Celle-ci sert donc de base pour établir le cadre général des technologies de sécurité pour un réseau domestique.

La présente Recommandation décrit les menaces sur la sécurité et les prescriptions de sécurité pour un réseau domestique du point de vue de l'utilisateur résidentiel ou de l'utilisateur distant. De plus, elle classe les technologies de sécurité par fonctions de sécurité satisfaisant aux prescriptions de sécurité susmentionnées et selon le lieu où ces technologies sont appliquées dans le modèle de réseau domestique. Enfin, elle présente les prescriptions de fonctions de sécurité pour chaque entité du réseau et les couches d'implémentation possibles pour les fonctions de sécurité.

2 Références normatives

La présente Recommandation se réfère à certaines dispositions des Recommandations UIT-T et textes suivants qui, de ce fait, en sont partie intégrante. Les versions indiquées étaient en vigueur au moment de la publication de la présente Recommandation. Toute Recommandation ou tout texte étant sujet à révision, les utilisateurs de la présente Recommandation sont invités à se reporter, si possible, aux versions les plus récentes des références normatives suivantes. La liste des Recommandations de l'UIT-T en vigueur est régulièrement publiée. La référence à un document figurant dans la présente Recommandation ne donne pas à ce document, en tant que tel, le statut d'une Recommandation.

[UIT-T J.190] Recommandation UIT-T J.190 (2002), *Architecture de MediaHomeNet prenant en charge les services câblés*.

[UIT-T J.192] Recommandation UIT-T J.192 (2005), *Passerelle résidentielle assurant la remise des services de données par câble*.

[UIT-T Q.1701] Recommandation UIT-T Q.1701 (1999), *Cadre général des réseaux IMT-2000*.

[UIT-T Q.1711] Recommandation UIT-T Q.1711 (1999), *Modèle fonctionnel réseau pour les IMT-2000*.

[UIT-T Q.1761] Recommandation UIT-T Q.1761 (2004), *Convergence des systèmes fixes et des systèmes IMT-2000 existants: principes et prescriptions*.

[UIT-T X.800] Recommandation UIT-T X.800 (1991), *Architecture de sécurité pour l'interconnexion en systèmes ouverts d'applications du CCITT*.

[UIT-T X.803] Recommandation UIT-T X.803 (1994), *Technologies de l'information – Interconnexion des systèmes ouverts – Modèle de sécurité pour les couches supérieures*.

[UIT-T X.805] Recommandation UIT-T X.805 (2003), *Architecture de sécurité pour les systèmes assurant des communications de bout en bout.*

[UIT-T X.810] Recommandation UIT-T X.810 (1995), *Technologies de l'information – Interconnexion des systèmes ouverts – Cadres de sécurité pour les systèmes ouverts: aperçu général.*

[UIT-T X.1121] Recommandation UIT-T X.1121 (2004), *Cadre général des technologies de la sécurité pour les communications mobiles de données de bout en bout.*

3 Définitions

3.1 Définitions relatives à l'architecture de sécurité du modèle de référence de l'OSI

Les termes suivants sont définis dans [UIT-T X.800]:

a) contrôle d'accès;
b) authentification;
c) information d'authentification;
d) échange d'authentification;
e) autorisation;
f) disponibilité;
g) confidentialité;
h) cryptographie;
i) intégrité des données;
j) authentification de l'origine des données;
k) chiffrement;
l) pare-feu;
m) intégrité;
n) clé;
o) échange de clés;
p) gestion de clés;
q) logiciel malveillant;
r) non-répudiation;
s) notarisation;
t) mot de passe;
u) respect de la vie privée.

3.2 Définitions relatives au cadre général des technologies de la sécurité pour les communications mobiles

Les termes suivants sont définis dans [UIT-T X.1121]:

a) anonymat;
b) lecture par-dessus l'épaule;
c) terminal mobile;
d) réseau mobile;
e) utilisateur mobile;
f) service d'application;

g) serveur d'application;

h) fournisseur de services d'application;

i) passerelle de sécurité mobile;

j) gestion de la politique de sécurité.

3.3 Définitions relatives au réseau domestique

Les termes suivants sont définis dans [UIT-T J.190]:

a) accès domestique (HA, *home access*);

b) passerelle domestique (HB, *home bridge*);

c) client domestique (HC, *home client*);

d) décodeur domestique (HD, *home decoder*);

e) passerelle résidentielle;

f) plans de réseau domestique.

3.4 Définitions additionnelles

La présente Recommandation définit les termes suivants:

3.4.1 passerelle domestique sécurisée: une passerelle domestique sécurisée est une sorte de passerelle domestique considérée du point de vue de la sécurité; c'est un point ou une entité qui transmet les paquets de données d'un réseau ouvert à un réseau domestique interne ou inversement, qui modifie les paramètres de sécurité ou le protocole de communication d'un réseau domestique à un réseau ouvert ou inversement et qui peut assurer des fonctions de sécurité telles que le filtrage des paquets, la détection d'intrusion ou la gestion de la politique conformément à une politique de sécurité donnée. Une passerelle domestique sécurisée ne comprend donc pas seulement un pare-feu.

3.4.2 dispositif domestique: un dispositif domestique est une entité (ou un appareil domestique) telle qu'un PDA, un PC ou un téléviseur/magnétoscope qui commande ou est commandée par un autre dispositif domestique, ou qui fournit un service aux utilisateurs résidentiels. Du point de vue de la sécurité, il existe trois types de dispositifs domestiques: le type A, le type B et le type C. Un dispositif domestique de type A (commande à distance, PC ou PDA par exemple) a une capacité de commande d'un dispositif domestique de type B ou C par le biais d'une page de présentation et d'un affichage riche. Un dispositif domestique de type B est un pont qui connecte des dispositifs domestiques de type C dépourvus d'interface de communication au réseau domestique; par essence, il permet la communication entre les autres dispositifs du réseau domestique à une extrémité et un certain langage propriétaire à l'autre extrémité (par exemple, commande d'éclairage propriétaire, etc.). Un dispositif domestique de type C (caméra de sécurité, dispositif audio/vidéo, etc.) ne fournit qu'un certain type de service aux autres dispositifs domestiques. Un dispositif domestique de type A ou C est appelé console de sécurité s'il dispose d'une fonction de sécurité de dispositif domestique de type B ou C. Tout dispositif d'un réseau domestique peut être classé comme étant de type A, de type C ou de type A/type C suivant ses fonctionnalités.

3.4.3 fournisseur de services d'application domestique: un fournisseur de services d'application domestique (ou un serveur d'application domestique) est une entité qui connecte pour la communication de données le réseau domestique à un dispositif domestique ou à un terminal distant qui stocke le contenu multimédia ou qui fournit divers services d'application aux autres dispositifs domestiques du domicile ou à un terminal distant hors du domicile.

3.4.4 certificat d'identification: un certificat d'identification est un message qui, au minimum, mentionne un nom ou identifie l'autorité d'émission, identifie le sujet, contient la clé publique du sujet, identifie la période de validité du certificat, contient un numéro de série et contient la signature électronique d'une autorité de certification.

3.4.5 certificat de dispositif: un certificat de dispositif est un certificat X.509 de version 3 utilisé pour authentifier l'identité d'un dispositif de réseau résidentiel. Il peut être émis par une autorité de certification.

3.4.6 certificat d'autorisation: un certificat d'autorisation est un objet signé qui habilite le sujet. Il mentionne au moins un émetteur et un sujet. Il peut contenir des conditions de validité ainsi que des informations d'autorisation et de délégation. En général, les certificats peuvent être groupés en trois catégories: les certificats d'identification qui mappent le nom et une clé publique d'un sujet, les certificats d'attribut qui mappent une autorisation et le nom d'un sujet et les certificats d'autorisation qui mappent une autorisation et une clé publique d'un sujet. Un certificat d'autorisation ou d'attribut peut déléguer dans son intégrité la permission qu'il a reçue de l'émetteur ou peut ne déléguer qu'une partie de cette habilitation.

3.4.7 liste de contrôle d'accès (ACL, *access control list*): une liste de contrôle d'accès est une table protégée placée en mémoire du dispositif contenant les ressources dont l'accès est protégé. Elle comprend un ensemble d'entrées formées des éléments suivants: sujet, autorisation, délégation et validité. Le sujet est l'identificateur de l'entité à laquelle l'accès est accordé, l'autorisation est un indicateur de la permission accordée à ce sujet, la délégation est un drapeau indiquant si le sujet peut lui-même déléguer ce droit, tandis que la validité est un champ facultatif indiquant la validité de l'entrée sous la forme d'une date et d'une heure de début ou de fin de validité. Une liste de contrôle d'accès est une liste d'entrées qui spécifie une chaîne de certificats. Parfois appelée "liste de clés racines", elle est la source d'habilitation des certificats. En d'autres termes, un certificat transmet la permission de son émetteur à son sujet tandis que la liste de contrôle d'accès est la source de cette permission (puisque théoriquement elle est propriétaire de la ressource qu'elle contrôle en tant qu'émetteur implicite). Une entrée de la liste a potentiellement le même contenu que le corps du certificat mais n'a pas d'émetteur (et n'est pas signée). Il y a très probablement une liste de contrôle d'accès pour chaque propriétaire de ressources, si ce n'est pour chaque ressource contrôlée.

3.4.8 terminal distant: un terminal distant est une entité disposant d'une fonction d'accès au réseau et d'une interface Internet pour connecter ou commander les dispositifs domestiques du réseau domestique.

3.4.9 utilisateur distant: un utilisateur distant est une entité (une personne) située hors du réseau domestique qui utilise et exploite le terminal distant pour accéder aux dispositifs du réseau domestique.

3.4.10 utilisateur domestique: un utilisateur domestique est une entité (une personne) du réseau domestique qui utilise et exploite le terminal distant pour accéder aux dispositifs du réseau domestique.

3.4.11 console de sécurité: une console de sécurité est un dispositif qui fournit une interface d'utilisateur pour administrer le contrôle d'accès à d'autres dispositifs du point de vue de la sécurité.

3.4.12 administrateur de réseau domestique: un administrateur de réseau domestique est une entité ou un agent qui assure des activités liées à la sécurité (génération, stockage ou distribution de clés, par exemple) et surveille le statut des entités du réseau domestique.

4 Abréviations et acronymes

La présente Recommandation utilise les abréviations et acronymes suivants:

ACL liste de contrôle d'accès (*access control list*)

ASP fournisseur de services d'application (*application service provider*)

DoS déni de service (*denial of service*)

MAC code d'authentification de message (*message authentication code*)

OSI interconnexion des systèmes ouverts (*open systems interconnection*)

PC ordinateur personnel (*personal computer*)

PDA assistant personnel électronique (*personal data assistant*)

PIN numéro d'identification personnel (*personal identification number*)

5 Modèle général de réseau domestique du point de vue de la sécurité

Avant de décrire les technologies de sécurité, il convient de définir un modèle général de réseau domestique du point de vue de la sécurité. Il s'agit d'identifier toutes les entités du réseau domestique, de clarifier les relations entre ces entités et de préciser où les technologies mobiles sûres devraient être appliquées.

Le modèle proposé est représenté sur la Figure 1. Le réseau domestique comprend de nombreux dispositifs domestiques (PDA, PC et téléviseur/magnétoscope par exemple) qui commandent ou sont commandés par un autre dispositif domestique ou qui fournissent un service aux utilisateurs domestiques. Ils sont classés en trois types suivant leur rôle (types A, B et C). Un dispositif domestique de type A (commande à distance, PC ou PDA par exemple) a une capacité de commande d'un dispositif domestique de type B ou C par le biais d'une page de présentation et d'un affichage riche. Un dispositif domestique de type B est un pont qui connecte des dispositifs domestiques de type C dépourvus d'interface de communication au réseau domestique; par essence, il permet la communication entre les autres dispositifs du réseau domestique à une extrémité et un certain langage propriétaire à l'autre extrémité (par exemple commande d'éclairage propriétaire, etc.). Un dispositif domestique de type C (caméra de sécurité, dispositif audio/vidéo, etc.) ne fournit qu'un certain type de service aux autres dispositifs domestiques. Un dispositif domestique de type A ou C est appelé console de sécurité s'il dispose d'une fonction de sécurité de dispositif domestique de type B ou C.

Le dispositif domestique d'origine est généralement dépourvu d'interface de communication mais comme il dispose d'un chemin propriétaire pour être connecté à un dispositif domestique de type B, il peut être rattaché au réseau domestique via ce dernier. Certains dispositifs domestiques associent des fonctions de dispositifs résidentiels de type A et des fonctions de dispositifs domestiques de type C.

La Figure 1 décrit le modèle général de réseau domestique du point de vue de la sécurité.

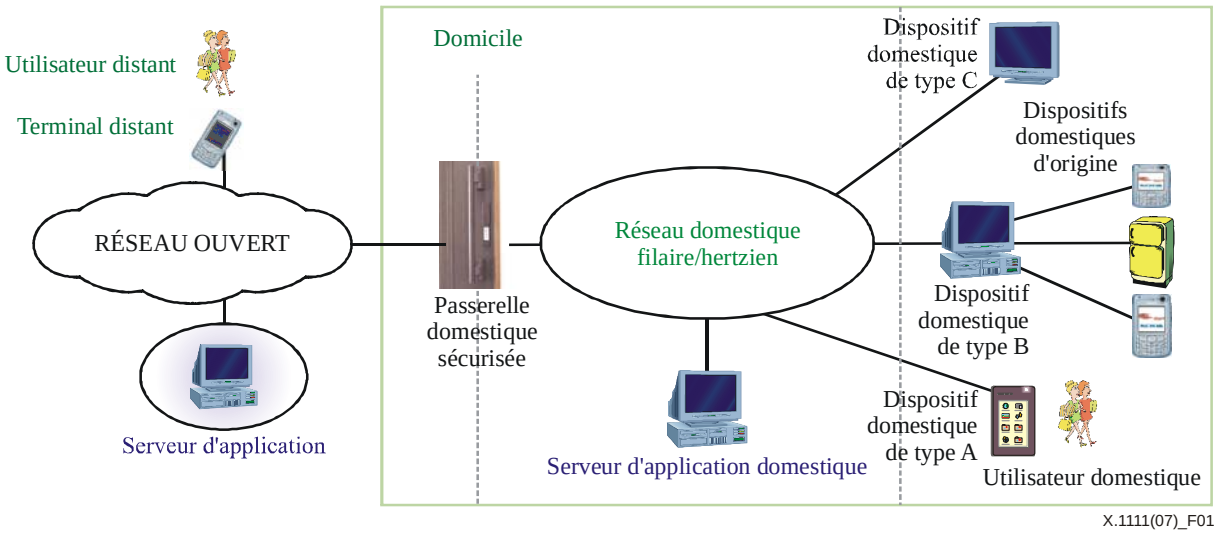

Figure 1 – Modèle général de réseau domestique du point de vue de la sécurité

Ce modèle comprend sept entités: utilisateur distant, terminal distant, serveur d'application, passerelle domestique sécurisée, serveur d'application domestique, utilisateur domestique et dispositifs domestiques. Comme on l'a déjà indiqué, les dispositifs domestiques peuvent être groupés suivant leur type en trois catégories: type A, type B et type C.

On dénombre dans ce modèle treize relations: utilisateur distant/terminal distant, terminal distant/passerelle domestique sécurisée, terminal distant/serveur d'application domestique, terminal distant/dispositif domestique, serveur d'application/passerelle domestique sécurisée, serveur d'application/serveur d'application domestique, serveur d'application/dispositif domestique, passerelle domestique sécurisée/dispositif domestique, serveur d'application domestique/dispositif domestique, dispositif domestique/utilisateur domestique, dispositif domestique/autre dispositif domestique, terminal distant/dispositif domestique de type A et passerelle domestique sécurisée/serveur d'application domestique.

Un cas courant d'utilisation du réseau domestique est celui d'une personne pouvant écouter grâce à une unité stéréo portable de la musique stockée sur un serveur. En fait, plusieurs personnes situées en divers endroits du domicile ou même hors du domicile peuvent avoir accès à un contenu audio et l'écouter en utilisant des lecteurs de réseau différents. On peut également citer le cas du partage de vidéo, où des membres d'une famille situés dans des pièces différentes peuvent visionner un contenu média. Le fils peut par exemple partager des photos de camping avec des amis depuis la pièce familiale où ces photos sont stockées sur le PC du père tandis que la mère regarde une émission télévisée enregistrée plus tôt dans la semaine sur le magnétoscope en réseau, qui est dans la pièce familiale, en sélectionnant le programme et en réglant tous les paramètres de visualisation à partir d'une seconde commande à distance.

6 Caractéristiques du réseau domestique

6.1 Divers supports de transmission peuvent être utilisés pour un réseau domestique

Divers supports de transmission (lignes électriques, communications radio, câbles) peuvent être utilisés pour transmettre un signal dans le réseau domestique. Celui-ci est donc très sensible à divers types d'attaque (écoute illicite, interruption, déni de service, attaque par intercepteur, etc.).

6.2 Un réseau domestique associe un réseau hertzien à un réseau filaire

Diverses techniques de transmission pouvant lui être appliquées, un réseau domestique comprend un réseau hertzien et un réseau filaire. Un réseau hertzien, notamment lorsque les mécanismes d'autorisation et de chiffrement ne sont pas implémentés ou autorisés, est plus sensible qu'un réseau filaire aux menaces sur la sécurité. Cela est dû au fait que le risque de recevoir un trafic brouilleur ou non autorisé est plus grand via un support hertzien que via un support filaire. Les menaces sur un réseau domestique sont donc à la fois celles qui pèsent sur un réseau filaire et celles qui pèsent sur un réseau hertzien. Toutes les contre-mesures à ces menaces devraient être prises en compte pour établir un réseau domestique sûr, ce qui est très difficile compte tenu du grand nombre de technologies de sécurité qu'il faudrait alors adopter.

6.3 Il existe un grand nombre d'environnements du point de vue de la sécurité

Il existe divers environnements domestiques, tels que celui d'une personne seule, celui d'un couple avec de jeunes enfants, celui d'une famille avec des adolescents, celui d'adultes colocataires, etc. Il faut donc plusieurs domaines de sécurité pour un réseau domestique donné ainsi que des procédures d'authentification et d'autorisation pour en assurer la sécurité.

6.4 Les terminaux distants sont transportés par des utilisateurs distants

Un utilisateur distant peut utiliser hors domicile un terminal distant pour commander un dispositif domestique ou mettre en œuvre un service d'application à partir d'un dispositif domestique au

travers du réseau ouvert. Par exemple, il peut, avant d'arriver chez lui, fermer ou ouvrir les rideaux d'une fenêtre ou allumer ou éteindre les lumières en utilisant hors domicile un terminal distant.

6.5 Il existe différents types de dispositifs de réseau domestique qui exigent différents niveaux de sécurité

Il existe de très nombreux types de dispositifs de réseau domestique (dispositif audio/vidéo, PC, téléphone/fax et appareil domestique). Chaque type de dispositif domestique requiert un niveau de sécurité différent. En outre, il est très difficile de définir une prescription de sécurité générale applicable à tous les types de dispositifs domestiques.

7 Menaces sur la sécurité dans un environnement de réseau domestique

Un réseau domestique comprend un réseau filaire et un réseau hertzien. Les menaces auxquelles il est confronté sont équivalentes à celles qui pèsent sur ces deux types de réseau. Le modèle de menaces décrit dans [UIT-T X.1121] peut servir de base pour définir celles qui pèsent sur un réseau domestique. On peut classer les menaces sur la sécurité en deux catégories: celles qui sont d'ordre général et celles qui concernent les communications mobiles, sauf, comme on le décrit dans [UIT-T X.1121], pour ce qui est des erreurs de saisie puisque celles-ci sont dues à l'utilisateur et ne peuvent être évitées grâce aux technologies de sécurité actuelles.

7.1 Menaces d'ordre général sur la sécurité d'après la Rec. UIT-T X.1121

7.1.1 Ecoute illicite/divulgation/interception

Le problème le plus largement identifié dans les réseaux ouverts est celui de l'écoute illicite par attaques anonymes. L'attaquant anonyme peut intercepter volontairement des données transmises et donc entraîner leur divulgation. Il peut, si la communication n'est pas chiffrée, lire les données transmises et en tirer des informations telles que l'adresse source, l'adresse de destination, la taille des données transmises, l'heure et la date de la communication, etc. Il s'agit d'une attaque visant la confidentialité, par exemple via un branchement clandestin pour accéder aux données transmises ou via la copie illégale de fichiers ou de programmes.

7.1.2 Interruption/brouillage des communications

Le brouillage des communications se produit lorsqu'un brouillage volontaire ou involontaire perturbe l'émetteur ou le récepteur d'une liaison de communication et la rend inexploitable. Il peut en résulter un déni de service.

L'interruption résulte de la destruction d'un composant de terminal distant ou d'élément de réseau. On peut citer à titre d'exemple la destruction d'un élément matériel tel que le disque, la coupure d'une ligne de communication ou l'inactivation du système de gestion des fichiers dans un terminal distant ou une entité du réseau domestique.

7.1.3 Adjonction et modification de données

Ces phénomènes se produisent lorsqu'une entité non autorisée (une personne, un programme ou un ordinateur par exemple) insère, modifie ou supprime des informations transmises entre un terminal distant et un serveur d'application. Ces attaques surviennent lorsqu'une personne ajoute des données à une connexion existante dans le but de la détourner ou de transmettre des données à des fins malveillantes. Il peut en résulter une attaque par déni de service ou par intercepteur, c'est-à-dire une attaque de l'intégrité. Ces attaques consistent par exemple à modifier les valeurs d'un fichier de données, à transformer un programme pour qu'il donne des résultats différents ou à changer le contenu du message transmis dans le réseau domestique.

7.1.4 Accès non autorisé

Le contrôle d'accès est la capacité de limiter et de contrôler par le biais d'une liaison de communication l'accès à un serveur d'application. Il y a menace lorsqu'une entité non autorisée obtient l'accès à un serveur d'application, à un serveur d'application domestique ou à un dispositif domestique en se faisant passer pour un utilisateur distant réel. L'entité qui cherche à obtenir un accès non autorisé doit être identifiée ou authentifiée. Il existe en outre deux principaux types d'attaque: par balayage de ports ou par logiciel malveillant. En ce qui concerne le balayage de ports, on peut penser à l'image d'un voleur dans un quartier vérifiant si chaque porte et chaque fenêtre de chaque maison est ouverte ou fermée. Le balayage peut être effectué par un dispositif de balayage dans le réseau domestique ou par un attaquant pour déterminer quels sont les ports ouverts et les ports fermés d'un élément ou d'un système du réseau domestique. Un logiciel malveillant peut aussi être appelé maliciel (*malware*). Un logiciel malveillant (virus ou cheval de Troie par exemple) est spécifiquement conçu pour endommager ou détruire un système. Ces deux types d'attaque peuvent conduire à un accès non autorisé à un élément ou à des dispositifs du réseau domestique.

7.1.5 Répudiation

Le type attaque se produit lorsqu'un émetteur ou un récepteur nie avoir émis ou reçu un message.

7.2 Menaces sur la sécurité des communications mobiles (d'après la Rec. UIT-T X.1121)

7.2.1 Ecoute illicite/divulgation/interception

Dans le cas de communications mobiles, ce type d'attaque est plus facile car il suffit d'intercepter volontairement le signal radioélectrique et de décoder les données transmises (fuite de données). L'écoute illicite est facilitée par la nature radioélectrique des émissions hertziennes. En cas d'écoute passive, l'attaquant effectue une surveillance passive et a accès aux données transmises.

7.2.2 Interruption/brouillage des communications

Ici aussi, lorsqu'il s'agit de communications mobiles, ce type d'attaque est plus facile dans un réseau utilisant une technologie de transmission hertzienne. Il existe deux types d'attaque: le brouillage d'un terminal distant et le brouillage d'un élément de réseau. Dans le premier cas, on fait passer le terminal distant agresseur pour le terminal distant agréé et, dans le second cas, on usurpe l'identité de l'élément de réseau homologué qui assure la connexion avec le terminal distant par le biais de l'interface hertzienne.

7.2.3 Lecture par-dessus l'épaule

Ce type d'attaque correspond au vol d'informations par observation du clavier, lecture de l'écran ou écoute des sons d'un terminal distant dans un lieu fréquenté.

7.2.4 Perte de terminal distant

La sécurité peut être menacée si le terminal distant est perdu par l'utilisateur distant en déplacement. Il peut y avoir perte ou destruction des informations stockées dans le terminal distant.

7.2.5 Vol de terminal distant

Ce type de menace apparaît également lorsque l'utilisateur distant se déplace avec son terminal distant. Il peut y avoir fuite des données stockées dans le terminal distant, suppression des données à la suite d'un accès non autorisé au terminal distant volé s'ajoutant à la perte d'informations stockées dans le terminal distant.

7.2.6 Interruption imprévue de la communication

La communication risque d'être interrompue lorsqu'elle n'est pas stable ou lorsque l'alimentation électrique cesse d'être assurée (risque de suppression des données).

7.2.7 Erreur de lecture

Ce type de menace est dû à la dimension réduite des terminaux mobiles. Il peut y avoir suppression de données due à l'usurpation de l'identité du fournisseur de services d'application.

7.2.8 Erreur de saisie

Ce type de menace est dû aux dimensions réduites du clavier ou du pavé numérique d'un terminal distant (ce qui rend la saisie des données difficile). L'authentification de l'utilisateur risque d'échouer.

7.3 Menaces sur la sécurité (d'après la Rec. UIT-T X.805)

7.3.1 Transmission anormale de paquets

Il s'agit du risque qu'un paquet ne soit pas correctement routé ou qu'il soit intercepté lors de son acheminement entre les deux points d'extrémité du flux. Ce risque existe dans une passerelle domestique sécurisée lorsque la table de routage est mal configurée.

7.4 Relations entre les menaces sur la sécurité et les entités du réseau domestique

Les menaces sur la sécurité apparaissent dans certaines entités ou en certains endroits du réseau domestique modélisé. Les relations entre ces menaces et les entités fonctionnelles du réseau domestique sont décrites dans les Tableaux 1 et 2. La mention de la lettre "O" dans une case à l'intersection d'une ligne et d'une colonne signifie que la menace considérée existe pour l'entité ou la liaison considérée.

Ces deux tableaux montrent que les mêmes menaces pèsent sur un terminal distant, un dispositif domestique, un serveur d'application domestique et une passerelle domestique sécurisée. On constate également de nombreuses similitudes entre les menaces pesant sur les liaisons entre: terminal distant et passerelle domestique sécurisée, terminal distant et dispositifs domestiques, terminal distant et serveur d'application domestique, etc.

Tableau 1 – Relations entre les menaces d'ordre général sur la sécurité et les entités ou liaisons modélisées

Menaces / Entités ou liaisons	Divulgation/ écoute illicite		Interruption		Modification/ adjonction		Accès non autorisé		Répu-dia-tion	Trans-mission anornale de paquets
	Données stockées	Données transmises	Données stockées	Données transmises	Données stockées	Données transmises	Données stockées	Données transmises		
Terminal distant	O		O		O		O			
Dispositif domestique	O		O		O		O			
Passerelle domestique sécurisée	O		O		O		O			O
Serveur d'application domestique	O		O		O		O			
Liaison entre un utilisateur distant et un terminal distant								O*		
Liaison entre un terminal distant et une passerelle domestique sécurisée		O		O		O		O		
Liaison entre un terminal distant et un serveur d'application domestique		O		O		O		O	O	
Liaison entre un terminal distant et un dispositif domestique de type B ou C		O		O		O		O		
Liaison entre un serveur d'application et une passerelle domestique sécurisée		O		O		O		O		
Liaison entre un serveur d'application et un serveur d'application domestique		O		O		O		O	O	
Liaison entre un serveur d'application et un dispositif domestique		O		O		O		O	O	
Liaison entre une passerelle domestique sécurisée et un dispositif domestique		O		O		O		O		
Liaison entre un serveur d'application domestique et un dispositif domestique		O		O		O		O		

Tableau 1 – Relations entre les menaces d'ordre général sur la sécurité et les entités ou liaisons modélisées

Menaces / Entités ou liaisons	Divulgation/ écoute illicite		Interruption		Modification/ adjonction		Accès non autorisé		Répu-dia-tion	Trans-mission anornale de paquets
	Données stockées	Données transmises	Données stockées	Données transmises	Données stockées	Données transmises	Données stockées	Données transmises		
Liaison entre un dispositif domestique de type A et un dispositif domestique de type B ou C		O		O		O		O		
Liaison entre un dispositif domestique de type A et un utilisateur domestique								O*		
Liaison entre une passerelle domestique sécurisée et un serveur d'application domestique		O		O		O		O		
Liaison entre un terminal distant et un dispositif domestique de type A		O		O		O		O		
* Il s'agit ici de l'accès non autorisé d'un utilisateur non autorisé à un terminal distant, et non à des données transmises.										

Tableau 2 – Relations entre des menaces sur la sécurité pour les communications mobiles dans un réseau hertzien uniquement et les entités ou liaisons modélisées

Menaces / Entités ou liaisons	Divulgation/ écoute illicite		Interruption/brouillage des communications		Lecture par dessus l'épaule	Terminal perdu/ volé	Inter-ruption imprévue	Erreur de lecture/ erreur de saisie
	Données stockées	Données transmises	Données stockées	Données transmises				
Terminal distant						O		
Dispositif domestique						O		
Passerelle domestique sécurisée								
Serveur d'application domestique								
Liaison entre un utilisateur distant et un terminal distant					O			O
Liaison entre un terminal distant et une passerelle domestique sécurisée		O		O			O	
Liaison entre un terminal distant et un serveur d'application domestique		O		O			O	

Tableau 2 – Relations entre des menaces sur la sécurité pour les communications mobiles dans un réseau hertzien uniquement et les entités ou liaisons modélisées

Menaces / Entités ou liaisons	Divulgation/ écoute illicite		Interruption/brouillage des communications		Lecture par dessus l'épaule	Terminal perdu/ volé	Inter-ruption imprévue	Erreur de lecture/ erreur de saisie
	Données stockées	Données transmises	Données stockées	Données transmises				
Liaison entre un terminal distant et un dispositif domestique de type B ou C		O		O			O	
Liaison entre un serveur d'application et une passerelle domestique sécurisée		O		O				
Liaison entre un serveur d'application et un serveur d'application domestique		O		O				
Liaison entre un serveur d'application et un dispositif domestique de type B ou C		O		O			O	
Liaison entre une passerelle domestique sécurisée et un dispositif domestique de type B ou C		O		O			O	
Liaison entre un serveur d'application domestique et un dispositif domestique de type B ou C		O		O			O	
Liaison entre un dispositif domestique de type A et un dispositif domestique de type B ou C		O		O			O	
Liaison entre un dispositif domestique de type A et un utilisateur domestique					O			O
Liaison entre une passerelle domestique sécurisée et un serveur d'application domestique		O		O			O	
Liaison entre un terminal distant et un dispositif domestique de type A		O		O			O	

8 Prescriptions de sécurité applicables à un réseau domestique

Un réseau domestique étant un réseau filaire ou un réseau hertzien, les prescriptions de sécurité qui lui sont applicables sont similaires à celles qui figurent dans [UIT-T X.1121]. Les prescriptions de sécurité de [UIT-T X.1121] peuvent servir de base pour établir celles qui sont applicables au réseau domestique. Si certaines prescriptions de sécurité peuvent être appliquées aux deux types de données (données stockées dans un élément spécifique ou données transmises entre deux entités), d'autres ne peuvent s'appliquer qu'aux données transmises. Dans la présente Recommandation, les deux types de prescriptions de sécurité de [UIT-T X.1121] sont regroupés en un seul type parce qu'un tel regroupement est possible en particulier dans le cas d'un réseau domestique. On observe en outre, pour ce qui est des passerelles domestique sécurisées, les prescriptions de [UIT-T X.805] sur la sécurité des flux de communication pour s'assurer que les flux d'informations circulent uniquement entre les entités autorisées du réseau domestique (pas de détournement ou d'interception des informations transmises entre des entités autorisées).

8.1 Prescriptions de sécurité tirées des Recommandations UIT-T X.805 et UIT-T X.1121

8.1.1 Confidentialité des données

La confidentialité des données permet de protéger les données contre une divulgation non autorisée. Elle garantit que le contenu des données ne peut être lu par des entités non autorisées. Elle passe souvent par l'utilisation d'un chiffrement, de listes de contrôle d'accès ou de permissions de fichiers.

8.1.2 Intégrité des données

L'intégrité des données permet de garantir l'exactitude ou la précision des données. Les données sont protégées contre toute modification, suppression, création ou duplication non autorisées et indiquent si des activités non autorisées de cette nature ont été effectuées.

8.1.3 Authentification

L'authentification est le processus qui permet de vérifier si un individu possède bien l'identité déclarée ou de s'assurer de l'identité de l'expéditeur d'un message. Il existe deux types d'authentification: l'authentification d'entité et l'authentification de message. Si l'authentification d'entité garantit la validité de l'identité déclarée pour une entité, l'authentification de message garantit qu'un message provient bien de l'entité déclarée. L'authentification d'entité sert à confirmer les identités des entités communicantes. L'authentification de message garantit la validité des identités déclarées des entités participant à la communication (une personne, un dispositif, un service ou une application par exemple) et permet de s'assurer qu'une entité ne tente pas d'usurper une identité ou de reprendre sans autorisation une communication précédente. L'authentification pourrait être réalisée par l'utilisation d'un certificat d'identification pour un utilisateur ou d'un certificat de dispositif pour un dispositif domestique.

8.1.4 Contrôle d'accès ou autorisation

Le contrôle d'accès offre une protection contre l'utilisation non autorisée des ressources de réseau. Il garantit que seuls les personnes ou les dispositifs autorisés sont habilités à accéder aux éléments de réseau, aux informations stockées, aux flux d'informations, aux services et aux applications. En outre, le contrôle d'accès en fonction des prérogatives (RBAC, *role-based access control*) définit différents niveaux d'accès pour garantir que les personnes et les dispositifs ne peuvent avoir accès aux éléments de réseau, aux informations stockées et aux flux d'informations et ne peuvent les exploiter que s'ils y ont été autorisés. Il existe trois types d'autorisation: autorisation à l'aide d'une liste de contrôle d'accès, autorisation à l'aide d'un serveur d'authentification et autorisation à l'aide d'un certificat d'autorisation ou d'un certificat d'attribut et d'un certificat d'identification. Le contrôle d'accès ou l'autorisation pourrait être réalisé à l'aide d'un certificat d'autorisation ou d'une liste de contrôle d'accès. Le contrôle d'accès ou l'autorisation au point d'entrée du réseau domestique peut être réalisé par un pare-feu faisant office de passerelle domestique sécurisée. Un pare-feu sert

surtout à empêcher l'accès non autorisé depuis un réseau public. On l'utilise souvent pour empêcher des utilisateurs d'Internet non autorisés d'accéder à des réseaux privés connectés à l'Internet, en particulier les réseaux intranet. Tous les messages entrant ou sortant d'un réseau intranet passent par le pare-feu, qui examine chaque message et bloque ceux qui ne sont pas conformes aux critères ou à la politique de sécurité spécifiés.

8.1.5 Non-répudiation

Le processus de non-répudiation permet d'empêcher un individu ou une entité de nier avoir effectué une action donnée relative à des données en présentant la preuve de diverses actions liées au réseau (par exemple une preuve d'obligation, d'intention ou d'engagement, une preuve de l'origine des données, une preuve de propriété ou une preuve d'utilisation des ressources). Il garantit qu'une preuve peut être présentée à une tierce partie pour prouver qu'un certain type d'événement ou d'action a eu lieu.

8.1.6 Sécurité du flux de communication

Le processus de sécurité du flux de communication garantit que les informations circulent uniquement entre les points d'extrémité autorisés (les informations ne sont pas détournées ou interceptées lorsqu'elles circulent entre ces points d'extrémité). Il devrait être appliqué à la passerelle domestique sécurisée dans un environnement de réseau domestique.

8.1.7 Respect de la vie privée

Le mécanisme de sécurité assurant le respect de la vie privée permet de protéger les informations qui pourraient être déduites de l'examen des activités ou des communications de réseau. On peut citer comme exemple d'informations les sites web auxquels l'utilisateur a accédé, l'emplacement géographique de l'utilisateur ou encore les adresses IP source et destination et les noms des services de noms de domaine (DNS, *domain name service*) dans un réseau de fournisseur de services. Il faut en outre respecter le caractère privé des identificateurs dans un réseau domestique.

8.1.8 Disponibilité

Le mécanisme de disponibilité garantit qu'il n'y a pas de déni d'accès autorisé aux éléments de réseau, aux informations stockées, aux flux d'informations, aux services et aux applications en raison d'événements ayant une incidence sur le réseau. Des solutions de récupération en cas de catastrophe appartiennent également à cette catégorie. Diverses attaques peuvent se traduire par la perte ou une diminution de la disponibilité. Certaines peuvent faire l'objet de contre-mesures automatisées, telles que l'authentification et le chiffrement, tandis que d'autres exigent un certain type d'action physique pour empêcher la perte de disponibilité d'éléments de réseau ou rétablir leur fonctionnement.

8.2 Relations entre les prescriptions de sécurité et les menaces sur la sécurité

Chaque prescription de sécurité correspond à une contre-mesure répondant à certaines ou à toutes les menaces qui pèsent sur la sécurité d'un réseau domestique. Les Tableaux 3 et 4 décrivent les relations entre les prescriptions de sécurité et les menaces sur la sécurité dans un réseau domestique. La mention de la lettre "O" dans une case à l'intersection d'une ligne et d'une colonne signifie qu'une prescription de sécurité donnée devrait être respectée pour supprimer ou réduire une menace spécifique. Les erreurs de lecture ou de saisie peuvent être évitées grâce à une conception soignée des entités ou à la vigilance de l'utilisateur, ce qui fondamentalement ne relève pas des technologies de la sécurité. La lettre "O" n'est par conséquent inscrite dans aucune case de la colonne erreur de lecture/erreur de saisie.

Tableau 3 – Relation entre les prescriptions de sécurité et les menaces d'ordre général sur la sécurité

Prescriptions de sécurité \ Menaces		Divulgation/ écoute illicite		Interruption		Modification/adjonction		Accès non autorisé		Répu-diation	Trans-mission anormale de paquets
		Données stockées	Données transmises	Données stockées	Données transmises	Données stockées	Données transmises	Données stockées	Données transmises		
Confidentialité	Données transmises		O						O		
	Données stockées	O						O			
Intégrité	Données transmises						O				
	Données stockées					O					O
Authentification	Entité	O		O		O		O		O	
	Message	O		O			O	O		O	
Non-répudiation										O	
Contrôle d'accès	Données transmises						O		O		
	Données stockées	O		O		O		O			
Disponibilité	Données transmises				O						
	Données stockées			O							
Respect de la vie privée	Données transmises		O								
	Données stockées										
Sécurité du flux de communication											O

Tableau 4 – Relations entre les prescriptions de sécurité et les menaces sur la sécurité pour les communications mobiles dans un réseau hertzien uniquement

Prescriptions de sécurité \ Menaces		Divulgation/écoute illicite		Interruption		Lecture par dessus l'épaule	Terminal perdu/volé	Inter-ruption imprévue	Erreur de lecture/ erreur de saisie
		Données stockées	Données transmises	Données stockées	Données transmises				
Confidentialité	Données transmises		O						
	Données stockées	O					O		
Intégrité	Données transmises								
	Données stockées								
Authentification	Entité	O		O			O		
	Message	O		O					
Non-répudiation									
Contrôle d'accès	Données transmises								
	Données stockées	O		O			O		
Disponibilité	Données transmises				O			O	
	Données stockées			O					
Respect de la vie privée	Données transmises		O			O			
	Données stockées	O					O		
Sécurité du flux de communication					O				

9 Prescriptions de sécurité applicables aux entités et aux liaisons d'un réseau domestique

Les fonctions de sécurité devraient être utilisées pour respecter certaines ou toutes les prescriptions de sécurité. Le Tableau 5 indique les prescriptions de sécurité requise pour une entité ou une liaison spécifique du modèle de réseau domestique. La mention de la lettre "O" dans une case à l'intersection d'une ligne et d'une colonne signifie qu'une prescription de sécurité donnée devrait être respectée pour l'entité ou la liaison considérée. Par exemple, dans le cas d'une liaison entre un utilisateur distant et un terminal distant, le terminal distant devrait satisfaire aux prescriptions d'authentification, de contrôle d'accès pour les données stockées et de respect de la vie privée pour les données stockées.

Tableau 5 – Prescriptions de sécurité applicables au modèle de réseau domestique

Prescription de sécurité / Entité ou relation	Confidentialité		Intégrité		Authentification		Non-répudiation
	Données stockées	Données transmises	Données stockées	Données transmises	Entité	Message	
Terminal distant	O		O		O	O	
Dispositif domestique	O		O		O	O	
Passerelle domestique sécurisée	O		O		O	O	
Serveur d'application domestique	O		O		O	O	
Liaison entre un utilisateur distant et un terminal distant					O		
Liaison entre un terminal distant et une passerelle domestique sécurisée		O		O	O	O	
Liaison entre un terminal distant et un serveur d'application domestique		O		O	O	O	O
Liaison entre un terminal distant et un dispositif domestique de type B ou C		O		O	O	O	
Liaison entre un serveur d'application et une passerelle domestique sécurisée		O		O		O	
Liaison entre un serveur d'application et un serveur d'application domestique		O		O		O	O
Liaison entre un serveur d'application et un dispositif domestique		O		O	O	O	O
Liaison entre une passerelle domestique sécurisée et un dispositif domestique		O		O	O	O	
Liaison entre un serveur d'application domestique et un dispositif domestique de type B ou C		O		O	O	O	
Liaison entre un dispositif domestique de type A et un dispositif domestique de type B ou C		O		O	O	O	
Liaison entre un dispositif domestique de type A et un utilisateur domestique					O		
Liaison entre une passerelle domestique sécurisée et un serveur d'application domestique		O		O	O	O	O
Liaison entre un terminal distant et un dispositif domestique de type A		O		O	O	O	

Tableau 5 – Prescriptions de sécurité applicables au modèle de réseau domestique (fin)

Prescriptions de sécurité / Entité ou relation	Contrôle d'accès		Disponibilité		Respect de la vie privée		Sécurité du flux de communication
	Données stockées	Données transmises	Données stockées	Données transmises	Données stockées	Données transmises	
Terminal distant	O		O		O		
Dispositif domestique	O		O		O		
Passerelle domestique sécurisée	O		O		O		O
Serveur d'application domestique	O		O		O		
Liaison entre un utilisateur distant et un terminal distant					O		
Liaison entre un terminal distant et une passerelle domestique sécurisée		O		O		O	
Liaison entre un terminal distant et un serveur d'application domestique		O		O		O	
Liaison entre un terminal distant et un dispositif domestique		O		O		O	
Liaison entre un serveur d'application et une passerelle domestique sécurisée		O		O		O	
Liaison entre un serveur d'application et un serveur d'application domestique		O		O		O	
Liaison entre un serveur d'application et un dispositif domestique		O		O		O	
Liaison entre une passerelle domestique sécurisée et un dispositif domestique		O		O		O	
Liaison entre un serveur d'application domestique et un dispositif domestique		O		O		O	
Liaison entre un dispositif domestique de type A et un dispositif domestique de type B ou C		O		O		O	
Liaison entre un dispositif domestique de type A et un utilisateur domestique					O		
Liaison entre une passerelle domestique sécurisée et un serveur d'application domestique		O		O		O	
Liaison entre un terminal distant et un dispositif domestique de type A		O		O		O	

10 Fonctions de sécurité répondant aux prescriptions de sécurité dans un réseau domestique

10.1 Fonctions de sécurité tirées de la Rec. UIT-T X.1121

10.1.1 Fonction de chiffrement

La fonction de chiffrement peut assurer la confidentialité des données transmises ou des données stockées. Il existe deux types d'algorithmes de chiffrement, les algorithmes symétriques et les algorithmes asymétriques. Dans les algorithmes à clé publique, on distingue deux types de clés: les clés publiques et les clés privées. La connaissance de la clé publique n'implique pas celle de la clé privée. Un émetteur utilise la clé publique d'un récepteur pour chiffrer un contenu. Comme un récepteur n'a qu'une clé privée, il doit être capable de lire un message déchiffré à partir d'un cryptogramme. Si le chiffrement est symétrique, la connaissance de la clé de chiffrement implique celle de la clé de déchiffrement et inversement.

La capacité de traitement ou la mémoire des terminaux distants étant limitée, il est assez difficile d'appliquer les fonctions de chiffrement existantes, en particulier les algorithmes asymétriques, que l'on utilise dans les réseaux ouverts actuels.

La fonction de chiffrement peut être implémentée par le pare-feu situé au point d'entrée du réseau résidentiel.

10.1.2 Fonction de signature numérique

La fonction de signature numérique définit deux processus: l'un pour la signature des données et l'autre pour la vérification des données signées. Le premier utilise une clé privée (c'est-à-dire unique et confidentielle) pour générer la signature. Le second utilise une clé publique pour vérifier la validité de la signature.

Le processus de signature conduit à chiffrer les données ou à générer une valeur de vérification cryptographique de données, les informations privées du signataire étant alors utilisées comme clé privée.

Le processus de vérification nécessite l'utilisation de procédures et d'informations publiques pour déterminer si la signature a été générée correctement à partir des informations privées du signataire.

La caractéristique essentielle de la fonction de signature est que la signature ne peut être générée qu'à l'aide des informations privées du signataire. Ainsi, lorsque la signature est vérifiée, on peut ultérieurement et à tout moment prouver à une tierce partie (un juge ou un arbitre, par exemple) que seul le détenteur des informations privées était en mesure d'établir la signature.

En ce qui concerne la fonction de chiffrement, il est difficile, en raison des limites de traitement ou de mémoire des terminaux distants, d'implémenter les fonctions de signature numérique utilisées dans les réseaux ouverts actuels.

10.1.3 Fonction de contrôle d'accès

La fonction de contrôle d'accès peut utiliser l'identité authentifiée d'une entité, des informations sur l'entité (par exemple l'appartenance à un ensemble d'entités connu) ou encore les capacités de l'entité pour déterminer et faire appliquer les droits d'accès de l'entité. Si l'entité cherche à utiliser une ressource non autorisée ou tenter d'accéder à une ressource autorisée à l'aide d'un type d'accès impropre, la fonction de contrôle d'accès rejette la tentative et peut en outre signaler l'incident aux fins de déclenchement d'une alarme et/ou d'enregistrement dans le cadre d'un audit de sécurité. La fonction de contrôle d'accès peut reposer sur l'utilisation des éléments suivants:

- bases d'informations de contrôle d'accès, les droits d'accès des entités homologues étant mémorisés dans une base de données;

- informations d'authentification (mot de passe, par exemple), dont la possession et la présentation prouvent que l'entité qui demande l'accès est habilitée à le faire;
- capacités, dont la détention et la présentation établissent le droit d'accéder à l'entité ou à la ressource définie par la capacité;
- certificat d'autorisation;
- étiquettes de sécurité qui, associées à une entité, peuvent servir à accorder ou à refuser l'accès, en général en fonction d'une politique de sécurité;
- heure de la tentative d'accès;
- trajet de la tentative d'accès;
- durée de l'accès;
- localisation physique de la tentative d'accès.

La fonction de contrôle d'accès peut être appliquée à l'une des entités homologues d'une association de communication et/ou au niveau d'une passerelle domestique sécurisée.

Le mécanisme de contrôle d'accès appliqué au niveau de l'entité d'origine ou de la passerelle de sécurité mobile sert à déterminer si l'expéditeur est autorisé à communiquer avec le destinataire et/ou à utiliser les ressources de communication requises.

La fonction de contrôle d'accès permet à un dispositif résidentiel de savoir ce que chaque dispositif authentifié est autorisé à faire. Il existe des mécanismes d'autorisation prédominants tels que la liste de contrôle d'accès, le serveur d'autorisation et le certificat d'autorisation.

Un dispositif peut contrôler l'accès via seulement une liste de contrôle d'accès. Cela permet de supprimer facilement un contrôle d'accès étant donné que l'on peut éditer la liste de contrôle d'accès d'un dispositif. Cela a le désavantage, suivant le cas, de nécessiter beaucoup de travail d'édition.

Si un utilisateur domestique utilise un réseau domestique comprenant un grand nombre de dispositifs domestiques avec une longue liste de contrôle d'accès, il pourrait être utile de transférer la liste de contrôle d'accès de chaque dispositif domestique vers un serveur, qui est appelé un serveur d'autorisation. Même si chaque dispositif nécessite une liste de contrôle d'accès, il pourrait être avantageux d'utiliser un serveur d'autorisation.

Une autre façon d'administrer l'autorisation est d'autoriser la délégation au moyen de certificats d'autorisation. Un certificat d'autorisation est une entrée de la liste de contrôle d'accès numériquement signée.

La fonction de contrôle d'accès peut être implémentée par le pare-feu situé au point d'entrée du réseau résidentiel.

10.1.4 Fonction d'intégrité des données

On considère ici deux aspects de l'intégrité des données: intégrité d'une unité ou d'un champ de données unique et intégrité d'un flux d'unités ou de champs de données. En général, on utilise des technologies différentes pour ces deux types de fonction d'intégrité, bien qu'il ne soit pas pratique d'assurer la seconde en l'absence de la première.

La détermination de l'intégrité d'une unité de données fait intervenir deux processus, l'un au niveau de l'entité expéditrice et l'autre au niveau de l'entité réceptrice. L'entité expéditrice associe aux données une quantité qui est fonction des données elles-mêmes. Cette quantité peut être une information supplémentaire, par exemple un code de vérification de bloc ou une valeur de vérification cryptographique, et elle peut être chiffrée. L'entité réceptrice génère une quantité correspondante et la compare à la quantité reçue pour déterminer si les données ont été modifiées pendant le transit. Ce processus n'offre pas à lui seul de protection contre la répétition d'une unité de données unique.

Pour protéger l'intégrité d'une séquence d'unités de données (c'est-à-dire assurer la protection contre les risques de mauvais ordonnancement, de perte, de répétition, d'insertion ou de modification), il faut ajouter une forme d'ordonnancement explicite telle que la numérotation des séquences, l'horodatage ou le chaînage cryptographique.

La fonction d'intégrité des données vise essentiellement à s'assurer que les données reçues sont identiques aux données envoyées. Elle utilise l'algorithme de hachage ou l'algorithme de signature numérique.

La fonction d'intégrité des données peut être mise en œuvre par le pare-feu situé au point d'entrée du réseau domestique.

10.1.5 Fonction d'authentification

Diverses techniques de sécurité peuvent être appliquées pour l'authentification, par exemple:

- l'utilisation d'informations d'authentification (le mot de passe, par exemple) fournies par l'entité expéditrice et vérifiées par l'entité réceptrice;
- les technologies cryptographiques;
- l'utilisation des caractéristiques et/ou des détentions de l'entité.

Il existe deux catégories de fonctions d'authentification: l'authentification d'utilisateur ou l'authentification de message. L'authentification de message peut se faire par le biais d'un certificat de dispositif ou d'un certificat d'identité dans le réseau domestique. La fonction d'authentification d'utilisateur peut être fondée sur trois facteurs:

1) ce que l'on sait;
2) ce que l'on a;
3) ce que l'on est.

La fonction d'authentification peut être incorporée pour assurer l'authentification d'entités homologues. Si la fonction ne parvient pas à authentifier l'entité, il y a rejet ou terminaison de la connexion et éventuellement inscription d'une entrée dans l'audit de sécurité et/ou envoi d'un rapport au centre de gestion de la sécurité.

Lorsqu'elles sont utilisées, les techniques cryptographiques peuvent être associées à des protocoles de "prise de contact" pour assurer une protection contre la répétition (c'est-à-dire pour garantir l'émission directe).

La technologie de sécurité relative à l'authentification sera choisie en fonction des circonstances entre les moyens suivants:

- horodatage et utilisation d'horloges synchronisés;
- prises de contact bi ou tridirectionnelles (pour une authentification respectivement unilatérale ou mutuelle);
- fonctions de non-répudiation (signature numérique et/ou notarisation).

La fonction d'authentification peut être implémentée par le pare-feu situé au point d'entrée du réseau résidentiel.

10.1.6 Notarisation

Les propriétés des données communiquées entre plusieurs entités (intégrité, origine, heure et destination, par exemple) peuvent être garanties par une fonction de notarisation. L'assurance requise est alors fournie par une tierce partie, un agent assermenté qui représente les entités en communication et qui détient les informations nécessaires pour donner l'assurance requise de manière vérifiable. Chaque instance de communication peut utiliser des fonctions de signature numérique, de chiffrement et d'intégrité selon les besoins du service fourni par l'agent assermenté. Lorsqu'une telle fonction de notarisation est demandée, les données sont communiquées entre les

entités de communication par l'intermédiaire des instances de communication protégées et de l'agent assermenté.

10.2 Fonctions de sécurité additionnelles

10.2.1 Fonction de code d'authentification de message

Une fonction de code d'authentification est définie comme une fonction publique comprenant un message d'entrée et une clé secrète générant une valeur de longueur constante utilisée pour authentifier un message et permettre au récepteur de vérifier l'authenticité du message. Elle fournit des contre-mesures contre l'usurpation d'identité, la modification de contenu, la modification de séquence et la modification de date. Un exemple type de fonction MAC est la fonction HMAC (code d'identification de message avec hachage, *hashed message authentication code*), qui est une fonction MAC fondée sur un algorithme de chiffrement symétrique.

La fonction de code d'authentification de message peut être implémentée par le pare-feu situé au point d'entrée du réseau domestique.

10.2.2 Fonction de gestion de clés

Une fonction de gestion de clés est une structure regroupant toutes les fonctions de sécurité afin de générer, distribuer, transmettre, supprimer ou détruire tous les types de clés cryptographiques requises pour d'autres fonctions de sécurité. Elle englobe la fonction d'échange de clés décrite dans [UIT-T X.1121].

La fonction de gestion de clés peut être implémentée par le pare-feu situé au point d'entrée du réseau domestique.

10.3 Relations entre les prescriptions de sécurité et les fonctions de sécurité

Les fonctions de sécurité sont utilisées pour satisfaire certaines des prescriptions de sécurité. Le Tableau 6 indique les fonctions de sécurité nécessaires pour respecter des prescriptions de sécurité. La mention de la lettre "O" dans une case à l'intersection d'une ligne et d'une colonne signifie qu'un service de sécurité peut être assuré par la fonction de sécurité correspondante; celle de la lettre "K" signifie que le service de sécurité pourrait être complété ou renforcé par le mécanisme de sécurité indiqué; celle de la lettre "X" signifie qu'un service de sécurité spécifié peut être assuré par l'une des fonctions de sécurité facultatives. Par exemple, la fonction de contrôle d'accès peut être divisée en deux: le contrôle d'accès physique et le contrôle d'accès technique.

Tableau 6 – Illustration des relations entre les prescriptions de sécurité et les fonctions de sécurité

Fonction de sécurité / Prescription de sécurité		Chiffrement	Intégrité	MAC	Authentification d'entité	Signature numérique	Notarisation	Contrôle d'accès		Gestion de clés	Non-disponibilité	
								Physique	Technique		Physique	Technique
Confidentialité	Données transmises	O						K		O		
	Données stockées	O						K		O		
Intégrité	Données transmises		X	X		X	X			O		
	Données stockées		X	X		X	X			O		
Authentification	Entité				O					O		
	Message			X		X	X			O		
Non-répudiation						O	O			O		
Contrôle d'accès	Données transmises	K						K		K		
	Données stockées	K		O	O	O		K	O	O		

Tableau 6 – Illustration des relations entre les prescriptions de sécurité et les fonctions de sécurité

Fonction de sécurité / Prescription de sécurité		Chiffrement	Inté-grité	MAC	Authenti-fication d'entité	Signature numé-rique	Notari-sation	Contrôle d'accès		Gestion de clés	Non-disponibilité	
								Physique	Technique		Physique	Technique
Disponibilité	Données transmises							X			X	O
	Données stockées			X	X	X			K	O		O
Respect de la vie privée	Données transmises	O						K		O		
	Données stockées	O		X	X	X		K	O	O		
Sécurité du flux de communication			X	X	X			K	O	O		

11 Technologies de sécurité applicables au réseau domestique

Pour assurer les fonctions de sécurité décrites au § 10, on peut appliquer au réseau domestique diverses technologies de sécurité. Celles-ci sont classées selon les fonctions de sécurité qu'elles assurent et le lieu où elles sont appliquées. Le lieu où une technologie de sécurité est appliquée est une entité ou une liaison entre entités parce qu'une technologie de sécurité s'applique à une entité ou à une liaison entre entités. Les Tableaux 1 et 2 montrent où apparaissent les menaces de sécurité dans le réseau domestique modélisé. Les Tableaux 3 et 4 montrent les prescriptions de sécurité nécessaires pour faire face à certaines menaces sur la sécurité. Le Tableau 5 indique les prescriptions de sécurité applicables à une entité ou à une liaison dans le modèle de réseau domestique. Le Tableau 6 décrit les fonctions de sécurité qui permettent de répondre aux prescriptions de sécurité. On peut donc indiquer dans le Tableau 7 les relations entre les fonctions de sécurité et leur lieu d'application dans le modèle. En d'autres termes, le Tableau 7 montre où les technologies de sécurité, qui réalisent certaines fonctions de sécurité, sont appliquées dans le modèle de réseau domestique.

Tableau 7 – Relations entre les technologies et sécurité et les entités ou liaisons modélisées

Fonctions de sécurité / Entité ou liaison		Chiffrement	Intégrité	MAC	Authen-tification d'entité	Signature numérique	Notari-sation	Contrôle d'accès		Gestion des clés	Non-disponibilité	
								Physique	Technique		Physique	Technique
Données stockées	Terminal distant	O	X	O	O	O	O	K	O	O		O
	Dispositif domestique	O	X	O	O	O	O	K	O	O		O
	Passerelle domestique sécurisée	O	X	O	O	O	O	K	O	O		O
	Serveur d'application domestique	O	X	O	O	O	O	K	O	O		O
Données transmises	Liaison entre un utilisateur distant et un terminal distant	O		X	O	O		K	O	O		
	Liaison entre un terminal distant et une passerelle domestique sécurisée	O	X	X	O	O	O	X		O	X	O

Tableau 7 – Relations entre les technologies et sécurité et les entités ou liaisons modélisées

Entité ou liaison \ Fonctions de sécurité		Chiffrement	Intégrité	MAC	Authen-tification d'entité	Signature numérique	Notari-sation	Contrôle d'accès		Gestion des clés	Non-disponibilité	
								Physique	Technique		Physique	Technique
Données transmises	Liaison entre un terminal distant et un serveur d'application domestique	O	X	X	O	O	O	X		O	X	O
	Liaison entre un terminal distant et un dispositif domestique de type B ou C	O	X	X	O	O	O	X		O	X	O
	Liaison entre un serveur d'application et une passerelle domestique sécurisée	O	X	X		X	X	X		O	X	O
	Liaison entre un serveur d'application et un serveur d'application domesstique	O	X	X		O	O	X		O	X	O
	Liaison entre un serveur d'application et un dispositif domestique	O	X	X	O	O	O	X		O	X	O
	Liaison entre une passerelle domestique sécurisée et un dispositif domestique	O	X	X	O	O	O	X		O	X	O
	Liaison entre un serveur d'application domestique et un dispositif domestique	O	X	X	O	O	O	X		O	X	O
	Liaison entre un dispositif domestique de type A et un dispositif domestique de type B ou C	O	X	X	O	O	O	X		O	X	O
	Liaison entre un dispositif domestique de type A et un utilisateur domestique	O		X	O	O		K	O	O		
	Liaison entre une passerelle domestique sécurisée et un serveur d'application domestique	O	X	X	O	O	O	X		O	X	O
	Liaison entre un terminal distant et un dispositif domestique de type A	O		X	O	O	O	X		O	X	O

Les fonctions de sécurité peuvent être implémentées dans les différentes couches. Le Tableau 8 illustre la ou les couches possibles pour l'implémentation de la fonction de sécurité de chaque relation du modèle. La sécurité de niveau liaison de données, la sécurité de niveau réseau, la sécurité de niveau session et la sécurité de niveau application peuvent être assurées respectivement dans la couche Liaison de données, dans la couche Réseau, dans la couche Transport et dans la couche Application. Les exemples de protocoles de sécurité associés sont respectivement IPSec, TLS sécurité de la couche Transport, TLS (*transport level security*) et le protocole de sécurité homologue à homologue d'application.

Tableau 8 – Couche possible pour l'implémentation des fonctions de sécurité pour chaque liaison du modèle

Relations	Couche d'implémentation de la sécurité
Liaison entre un terminal distant et une passerelle domestique sécurisée	Niveau réseau ou session
Liaison entre un terminal distant et un serveur d'application domestique	Niveau application
Liaison entre un terminal distant et un dispositif domestique de type B ou C	Niveau application
Liaison entre un serveur d'application et une passerelle domestique sécurisée	Niveau réseau ou session
Liaison entre un serveur d'application et un serveur d'application domestique	Niveau réseau ou session ou niveau application
Liaison entre un serveur d'application et un dispositif domestique de type B ou C	Niveau réseau, session ou niveau application
Liaison entre une passerelle domestique sécurisée et un dispositif domestique de type B ou C	Niveau liaison de données, réseau ou session
Liaison entre un serveur d'application domestique et un dispositif domestique de type B ou C	Niveau liaison de données, réseau, session ou niveau application
Liaison entre des dispositifs domestiques de type A et un dispositif domestique de type B ou C	Niveau liaison de données ou niveau application
Liaison entre une passerelle domestique sécurisée et un serveur d'application domestique	Niveau réseau ou session
Liaison entre un terminal distant et un dispositif domestique de type A	Niveau application

12 Prescriptions relatives aux fonctions de sécurité dans un réseau domestique

Les prescriptions de sécurité applicables aux entités de réseau d'un réseau domestique sont les suivantes:

1) tous les éléments de réseau (terminal distant, passerelle domestique sécurisée, serveur d'application domestique et dispositifs domestiques, par exemple) devraient conserver leurs informations sensibles de façon sûre et devraient les protéger contre les risques d'accès non autorisé, de modification non autorisée ou de suppression non autorisée;

2) un terminal distant devrait avoir la capacité d'authentifier un utilisateur distant en utilisant une méthode d'authentification d'utilisateur appropriée (par exemple une méthode d'authentification biométrique);

3) un terminal distant doit disposer de fonctions de sécurité (authentification d'entité, gestion de clés, code d'authentification de message ou intégrité, par exemple) par rapport à une passerelle domestique sécurisée au niveau application ou réseau si la confidentialité et l'intégrité de données transmises sont requises;

4) un terminal distant doit disposer de fonctions de sécurité (authentification d'entité, gestion de clés, chiffrement, code d'authentification de message ou intégrité, par exemple) par rapport au serveur d'application domestique au niveau application ou réseau si la confidentialité et l'intégrité de données transmises sont requises;

5) un terminal distant doit disposer de fonctions de sécurité (authentification de l'entité, gestion de clés, signature numérique, chiffrement, code d'authentification de données ou intégrité, par exemple) par rapport à un dispositif domestique de type B ou C au niveau application si la confidentialité et l'intégrité de données transmises sont requises;

6) un dispositif domestique de type A devrait avoir la capacité d'authentifier un utilisateur domestique en utilisant la méthode d'authentification d'utilisateur appropriée;

7) un dispositif domestique de type A devrait disposer de fonctions de sécurité (authentification d'entité, gestion de clés, chiffrement, code d'authentification de données ou intégrité, par exemple) par rapport à un dispositif domestique de type B ou C au niveau application si la confidentialité et l'intégrité des données transmises sont requises;

8) un dispositif domestique de type B ou C doit disposer de fonctions de sécurité (authentification d'entité, gestion de clés, code d'authentification de message ou intégrité, par exemple) par rapport à un serveur d'application domestique ou à un serveur domestique au niveau réseau, session ou application si la confidentialité et l'intégrité des données transmises sont requises;

9) un dispositif domestique de type B ou C doit disposer de fonctions de sécurité (authentification d'entité, gestion de clés, code d'authentification de message ou intégrité, par exemple) par rapport à une passerelle domestique sécurisée au niveau réseau ou session si la confidentialité et l'intégrité des données transmises sont requises;

10) une passerelle domestique sécurisée devrait disposer de fonctions de sécurité (authentification de l'entité, gestion de clés, code d'authentification de message ou intégrité, par exemple) par rapport à un serveur d'application domestique sécurisé ou à un fournisseur de services d'application généralement au niveau réseau si la confidentialité et l'intégrité des données transmises sont requises;

11) un administrateur de réseau domestique doit avoir la capacité de gérer à distance ou localement une passerelle domestique ou un serveur d'application domestique en cas d'approbation de l'utilisateur;

12) une passerelle domestique sécurisée devrait présenter des fonctions de sécurité (pare-feu, détection d'intrusion, filtrage de contenu ou interface d'accès distant pour la maintenance) servant de capacités facultatives;

13) la passerelle domestique sécurisée doit disposer d'une interface de messagerie/de journalisation des événements pour permettre à l'administrateur de réseau de surveiller et d'examiner les activités de cette passerelle.

Annexe A

Type de dispositifs de réseau domestique de la Rec. UIT-T J.190

(Cette annexe fait partie intégrante de la présente Recommandation)

Les dispositifs de réseau domestique devraient être classés du point de vue de la sécurité. Dans [UIT-T J.190], les dispositifs sont répartis en quatre classes (voir la Figure A.1): accès domestique (HA), pont domestique (HB), client domestique (HC) et décodeur domestique (HD). On trouve dans la classe HA les dispositifs d'interface avec le réseau d'accès, dans la classe HB les dispositifs faisant office de ponts entre des réseaux de domaine IPCable2Home (par exemple, concentrateur, routeur, etc.), dans la classe HC les dispositifs d'interface entre dispositifs de domaine IPCable2Home et dispositifs de domaine propriétaire et dans la classe HD les dispositifs capables de communiquer via des protocoles propriétaires (DVD, D-VHS, IC-audio, imprimante, par exemple). Chaque dispositif des classes HC et HD appartient à l'un des plans de service (plan AV, plan PC, plan TEL/FAX ou plan appareils domestiques, par exemple).

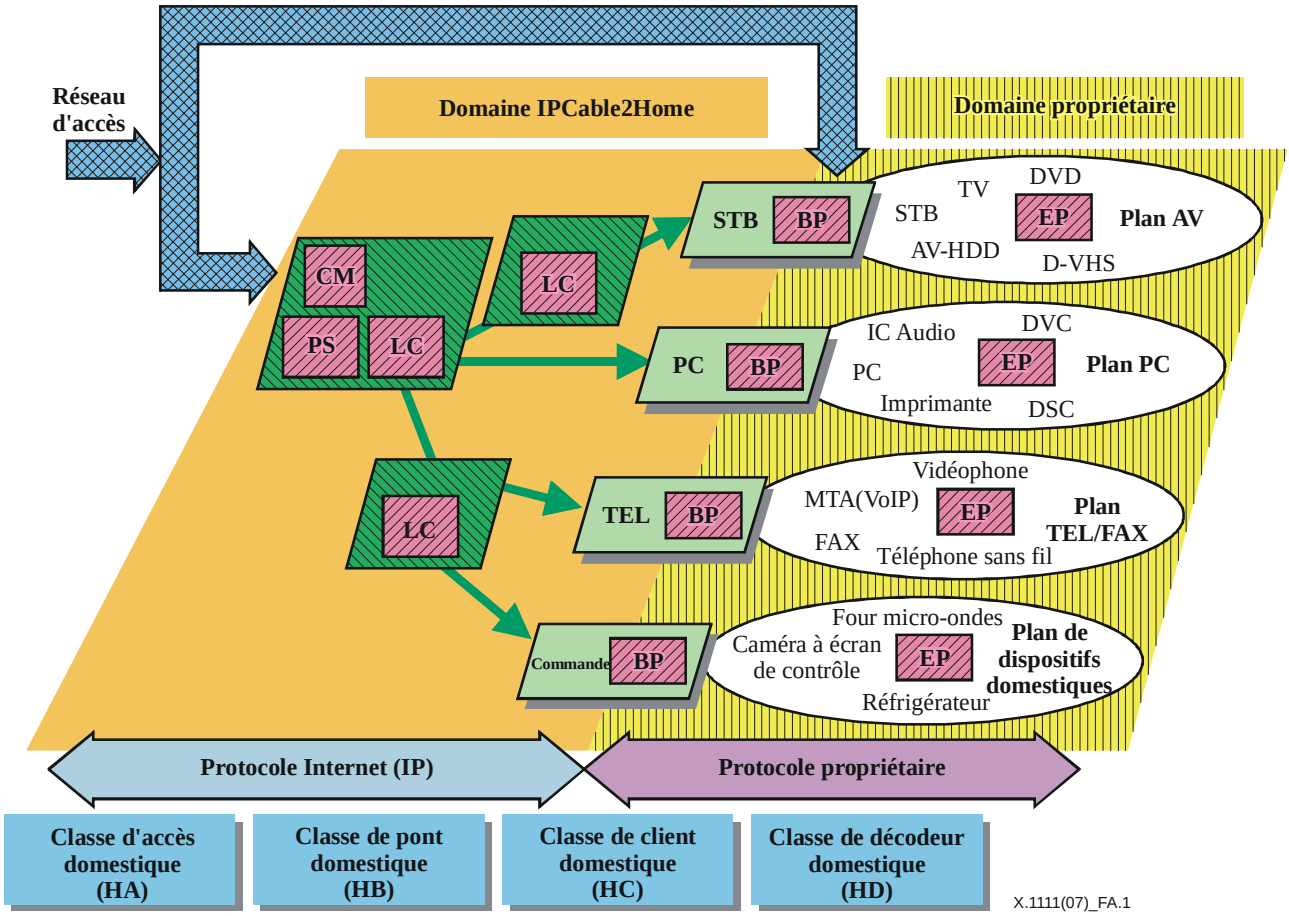

Figure A.1 – Contexte de réseau domestique UIT-T J.190

On trouvera plus de détails sur les classes et les plans de dispositifs au § 5.4.3 de [UIT-T J.190].

D'après les terminologies définies par la présente Recommandation, les passerelles de réseau sécurisées appartiennent à la classe HA, aucun dispositif n'appartient à la classe HB (car celle-ci ne contient généralement pas de fonction de sécurité), les dispositifs domestiques de type B appartiennent à la classe HC et enfin les dispositifs domestiques de type C n'appartiennent à aucune

classe de dispositifs de [UIT-T J.190] mais correspondent à la classe HD sauf en cas d'utilisation d'un protocole propriétaire pour communiquer avec un dispositif de type B. Etant donné que, dans la présente Recommandation, les communications entre un dispositif domestique de type B et un dispositif domestique d'origine sans capacité de communication sont fondées sur le chemin de communication propriétaire, on ne spécifie ici aucune prescription de sécurité concernant ce chemin propriétaire.

Dans [UIT-T J.190], le concept utile de "plan d'utilisateur" a été introduit et tous les dispositifs sont répartis en quatre plans suivant leurs fonctions: plan AV, plan PC, plan TEL/FAX et plan appareils domestiques.

Toutefois, du point de vue de la sécurité, on a un dispositif qui envoie une commande à un autre dispositif pour le contrôler ou demander un service et un dispositif qui reçoit une commande d'un autre dispositif ou qui fournit un service. Ainsi, tous les dispositifs domestiques peuvent être groupés selon trois types, quel que soit leur plan de sécurité. La présente Recommandation contient le nombre maximal de prescriptions de sécurité nécessaires pour l'ensemble des dispositifs domestiques, quel que soit le plan de service du dispositif considéré. Les prescriptions de sécurité applicables à un dispositif donné devraient être sélectionnées conformément à la politique du fournisseur de services utilisant le dispositif. Chaque dispositif ayant son propre niveau de prescriptions de sécurité, il est très difficile de définir un ensemble général de prescriptions de sécurité spécifiques. La définition de prescriptions de sécurité spécifiques ne relève pas de la présente Recommandation.

Appendice I

Type de dispositifs de réseau domestique UPnP

(Cet appendice ne fait pas partie intégrante de la présente Recommandation)

Il existe trois classes principales de dispositifs UPnP (dispositifs universels prêts à fonctionner, *universal plug and play*): les dispositifs UCP, les dispositifs commandés et les ponts.

- Dispositif UCP (point de commande universel/d'utilisateur, *user/universal control point*) – Il s'agit d'un dispositif (PC ou PDA par exemple) qui permet de commander d'autres dispositifs UPnP par le biais d'une page de présentation et d'un affichage riche.
- Pont – Ce dispositif connecte des dispositifs non UPnP au réseau domestique; par essence, il communique en mode UPnP à une extrémité et en un langage propriétaire à l'autre extrémité (commande d'éclairage propriétaire, technologie bluetooth, etc.)
- Dispositif commandé – Tout dispositif UPnP permettant de commander d'autres dispositifs du réseau domestique (dispositifs IGD, dispositifs audio/vidéo, caméras de sécurité, etc.) ou de leur fournir un service UPnP.

La classification applicable aux dispositifs domestiques est pour l'essentiel très semblable à celle qui s'applique aux dispositifs UPnP. Selon les terminologies de la présente Recommandation, les passerelles domestiques sécurisées ne correspondent à aucun dispositif UPnP, les dispositifs UCP correspondent aux dispositifs domestiques de type A, les ponts correspondent aux dispositifs domestiques de type B et les dispositifs commandés correspondent aux dispositifs domestiques de type C.

Bibliographie

[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*.

SÉRIES DES RECOMMANDATIONS UIT-T

Série A	Organisation du travail de l'UIT-T
Série D	Principes généraux de tarification
Série E	Exploitation générale du réseau, service téléphonique, exploitation des services et facteurs humains
Série F	Services de télécommunication non téléphoniques
Série G	Systèmes et supports de transmission, systèmes et réseaux numériques
Série H	Systèmes audiovisuels et multimédias
Série I	Réseau numérique à intégration de services
Série J	Réseaux câblés et transmission des signaux radiophoniques, télévisuels et autres signaux multimédias
Série K	Protection contre les perturbations
Série L	Construction, installation et protection des câbles et autres éléments des installations extérieures
Série M	Gestion des télécommunications y compris le RGT et maintenance des réseaux
Série N	Maintenance: circuits internationaux de transmission radiophonique et télévisuelle
Série O	Spécifications des appareils de mesure
Série P	Qualité de transmission téléphonique, installations téléphoniques et réseaux locaux
Série Q	Commutation et signalisation
Série R	Transmission télégraphique
Série S	Equipements terminaux de télégraphie
Série T	Terminaux des services télématiques
Série U	Commutation télégraphique
Série V	Communications de données sur le réseau téléphonique
Série X	**Réseaux de données, communication entre systèmes ouverts et sécurité**
Série Y	Infrastructure mondiale de l'information, protocole Internet et réseaux de prochaine génération
Série Z	Langages et aspects généraux logiciels des systèmes de télécommunication

Imprimé en Suisse
Genève, 2008