UNION INTERNATIONALE DES TÉLÉCOMMUNICATIONS

UIT-T X.805

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

(10/2003)

SÉRIE X: RÉSEAUX DE DONNÉES ET
COMMUNICATION ENTRE SYSTÈMES OUVERTS

Sécurité

Architecture de sécurité pour les systèmes assurant des communications de bout en bout

Recommandation UIT-T X.805

RECOMMANDATIONS UIT-T DE LA SÉRIE X

RÉSEAUX DE DONNÉES ET COMMUNICATION ENTRE SYSTÈMES OUVERTS

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.399
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.899
TRAITEMENT RÉPARTI OUVERT	X.900–X.999

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

Recommandation UIT-T X.805

Architecture de sécurité pour les systèmes assurant des communications de bout en bout

Résumé

Dans la présente Recommandation sont définis les éléments architecturaux liés à la sécurité générale, qui, lorsqu'ils sont mis en œuvre comme il convient, assurent la sécurité du réseau de bout en bout.

Source

La Recommandation X.805 de l'UIT-T a été approuvée le 29 octobre 2003 par la Commission d'études 17 (2001-2004) 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 responsables de la mise en œuvre de consulter la base de données des brevets du TSB.

TABLE DES MATIÈRES

Introduction

Les entreprises du secteur des télécommunications et de la technologie de l'information recherchent des solutions en matière de sécurité, qui soient globales et rentables. Un réseau sûr doit être protégé contre les attaques malveillantes et contre celles qui se produisent par inadvertance. En outre, il faut qu'il soit très disponible, qu'il réponde dans les délais appropriés, qu'il soit fiable, intègre, évolutif et fournisse des informations précises concernant la facturation. Les capacités des produits en matière de sécurité sont capitales pour la sécurité globale du réseau (y compris les applications et les services). Mais comme le nombre de produits concernés ne fait qu'augmenter en vue d'apporter des solutions qui soient complètes, leur interfonctionnement ou leur non-interfonctionnement est déterminant pour la réussite de la solution. La sécurité ne doit donc pas seulement être une vague préoccupation concernant chacun des produits ou des services. Elle doit être mise en œuvre de manière à favoriser l'intégration dans la solution globale de bout en bout des capacités en matière de sécurité. Pour parvenir à une telle solution dans un environnement multivendeur, la sécurité dans le réseau doit être conçue autour d'une architecture normalisée.

Recommandation UIT-T X.805

Architecture de sécurité pour les systèmes assurant des communications de bout en bout

1 Domaine d'application

La présente Recommandation définit une architecture de sécurité de réseau permettant d'assurer la sécurité du réseau de bout en bout. Cette architecture peut s'appliquer, indépendamment de la technologie sous-jacente du réseau, à divers types de réseaux où la sécurité de bout en bout est primordiale. La présente Recommandation définit les éléments architecturaux liés à la sécurité générale, qui sont nécessaires pour assurer la sécurité de bout en bout. La présente Recommandation a pour objet d'établir les fondements devant permettre l'élaboration de Recommandations détaillées relatives à la sécurité du réseau de bout en bout.

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.

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

3 Termes et définitions

Dans la présente Recommandation sont employés les termes suivants définis dans la Rec. UIT-T X.800:

– contrôle d'accès;
– disponibilité;
– authentification;
– confidentialité;
– intégrité des données;
– non-répudiation;
– respect de la vie privée.

4 Abréviations et acronymes

La présente Recommandation utilise les abréviations suivantes:

AAA authentification, autorisation et comptabilité (*authentication, authorization and accounting*)

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

ATM mode de transfert asynchrone (*asynchronous transfer mode*)

DHCP protocole de configuration de serveur dynamique (*dynamic host configuration protocol*)

DNS service de nom de domaine (*domain name service*)

DoS déni de service (*denial of service*)

DS-3 signal numérique de niveau 3 (*digital signal level 3*)

FTP protocole de transfert de fichiers (*file transfer protocol*)

IP protocole Internet (*Internet protocol*)

IPSec protocole de sécurité IP (*IP security protocol*)

OAM&P exploitation, administration, maintenance et fourniture (*operations, administration, maintenance & provisioning*)

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

PVC circuit virtuel permanent (*permanent virtual circuit*)

QS qualité de service

RTPC réseau téléphonique public commuté

SIP protocole d'ouverture de session (*session initiation protocol*)

SMTP protocole simple de transfert de messages (*simple mail transfer protocol*)

SNMP protocole simple de gestion de réseau (*simple network management protocol*)

SONET réseau optique synchrone (*synchronous optical network*)

SS7 système de signalisation n° 7 (*signalling system no 7*)

SSL couche de connexion sécurisée (*secure socket layer*) (protocole de chiffrement et d'authentification)

VoIP téléphonie utilisant le protocole Internet (*voice over IP*)

VPN réseau privé virtuel (*virtual private network*)

5 Architecture de sécurité

L'architecture de sécurité a été développée pour relever les défis liés à la sécurité mondiale auxquels étaient confrontés les fournisseurs de service, les entreprises et les consommateurs. Elle s'applique aux réseaux analogiques, aux réseaux de données et aux réseaux convergents, qu'ils soient hertziens, optiques ou câblés. Elle traite des questions de sécurité qui concernent la gestion, la commande et l'emploi de l'infrastructure du réseau, des services et des applications. Elle donne une vue globale, de haut en bas et de bout en bout de la sécurité dans le réseau et peut s'appliquer aux éléments de réseau, aux services et aux applications, dans le but de détecter, de prévoir et de corriger les points vulnérables en matière de sécurité.

L'architecture de sécurité permet de subdiviser logiquement, en composants architecturaux distincts, un ensemble complexe de caractéristiques liées à la sécurité du réseau de bout en bout. Cette répartition permet une démarche systématique en ce qui concerne la sécurité de bout en bout, qui peut être employée pour la planification de nouvelles solutions en matière de sécurité et aussi pour l'évaluation de la sécurité des réseaux existants.

L'architecture de sécurité aborde les trois questions essentielles suivantes concernant la sécurité de bout en bout:

1) quels sont les types de protection qui font défaut et quelles sont les menaces?
2) quels sont les différents types d'équipement de réseau et de groupe d'équipements qui nécessitent une protection?
3) quels sont les différents types d'activités dans le réseau qui nécessitent une protection?

Trois composants architecturaux sont chargés de répondre à ces questions: les mesures de sécurité, les couches de sécurité et les plans de sécurité.

Les principes décrits par l'architecture de sécurité peuvent s'appliquer à une large gamme de réseaux, indépendamment de la technologie qu'ils emploient et de l'emplacement dans la pile de protocoles.

Les paragraphes suivants donnent une description détaillée des éléments architecturaux et de leurs fonctions, eu égard aux principales menaces de la sécurité.

6 Mesures de sécurité

Une mesure de sécurité est un ensemble de dispositions de sécurité conçues pour prendre en compte un aspect particulier de la sécurité du réseau. La présente Recommandation définit huit ensembles qui protègent contre toutes les principales menaces. Ces mesures ne se limitent pas au réseau, mais englobent également les applications et les informations d'utilisateur final. De plus, les mesures de sécurité s'appliquent aux fournisseurs de services et aux entreprises offrant des services de sécurité à leurs clients. Les mesures de sécurité sont les suivantes:

1) contrôle d'accès;
2) authentification;
3) non-répudiation;
4) confidentialité des données;
5) sécurité de la communication;
6) intégrité des données;
7) disponibilité;
8) respect de la vie privée.

Les mesures de sécurité conçues et appliquées comme il convient viennent à l'appui de la politique de sécurité qui est définie pour un réseau particulier et facilitent l'application des règles établies par la gestion de la sécurité.

6.1 Mesure de sécurité concernant le contrôle d'accès

La mesure de sécurité concernant le contrôle d'accès protège contre l'emploi non autorisé des ressources du réseau. Le contrôle d'accès assure que seuls les personnels ou les dispositifs autorisés peuvent accéder aux éléments de réseau, aux flux d'informations, aux services et aux applications. En outre, le contrôle d'accès en fonction des prérogatives (RBAC, *role-based access control*) institue différents niveaux d'accès, afin de garantir que les personnes et les dispositifs ne peuvent avoir accès aux éléments de réseau, aux informations emmagasinées et aux flux d'informations et ne peuvent les manipuler que s'ils y ont été autorisés.

6.2 Mesure de sécurité concernant l'authentification

La mesure de sécurité concernant l'authentification sert à confirmer les identités des entités qui communiquent. L'authentification assure la validité des identités déclarées des entités en communication (par exemple, une personne, un dispositif, un service ou une application) et donne

l'assurance qu'une entité ne tente pas d'usurper l'identité d'une autre entité ou de reprendre sans autorisation une précédente communication.

6.3 Mesure de sécurité concernant la non-répudiation

La mesure de sécurité concernant la non-répudiation donne les moyens d'empêcher une personne ou une entité de nier avoir exécuté une action particulière liée aux données, en fournissant une attestation des diverses actions dans le réseau (telle qu'une attestation d'obligation, d'intention ou d'engagement; une attestation de l'origine des données, une attestation de propriété ou une attestation de l'emploi des ressources). Elle assure la mise à disposition de la preuve qui peut être présentée à une entité tierce et être utilisée pour prouver qu'un certain type d'événement ou d'action a eu lieu.

6.4 Mesure concernant la confidentialité de données

La mesure de sécurité concernant la confidentialité des données protège les données de leur divulgation. La confidentialité des données assure que le contenu des données ne pourra être compris par des entités non autorisées. Le chiffrement, les listes de contrôle d'accès, et les permissions d'accès aux fichiers sont des méthodes souvent employées pour assurer la confidentialité des données.

6.5 Mesure de sécurité concernant la communication

La mesure de sécurité assure que les informations ne seront acheminées qu'entre les extrémités autorisées (les informations ne sont ni déviées ni interceptées au cours de leur acheminement entre ces points).

6.6 Mesure de sécurité concernant l'intégrité des données

La mesure de sécurité concernant l'intégrité des données assure l'exactitude ou la précision des données. Les données sont protégées contre toute modification, suppression, création et reproduction. La mesure signale ces activités non autorisées.

6.7 Mesure de sécurité concernant la disponibilité

La mesure de sécurité concernant la disponibilité assure qu'il n'y a pas déni de l'accès autorisé aux éléments de réseau, aux informations emmagasinées, 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 sont aussi comprises dans cette catégorie.

6.8 Mesure de sécurité concernant le respect de la vie privée

Le mesure de sécurité concernant le respect de la vie privée assure la protection des informations qui pourraient être déduites de l'examen des activités dans le réseau. Des exemples de telles informations sont notamment les sites Web que l'utilisateur a visités, le lieu géographique de l'utilisateur, ainsi que les adresses Internet (IP, *Internet protocol*) et les noms des services de noms de domaine (DNS, *domain name service*) dans un réseau de fournisseur de services.

7 Couches de sécurité

Afin de disposer d'une solution de sécurité de bout en bout, les mesures de sécurité décrites dans le paragraphe 6 doivent être appliquées à la hiérarchie de l'équipement du réseau et aux groupes d'équipements, qu'on désigne comme étant les couches de sécurité. Dans la présente Recommandation sont définies trois couches de sécurité, à savoir:

– la couche de sécurité relative à l'infrastructure;

– la couche de sécurité relative aux services;

– la couche de sécurité relative aux applications;

superposées l'une à l'autre dans le but de fournir des solutions adaptées au réseau.

Les couches de sécurité sont une suite d'activateurs dans le cadre des solutions destinées aux réseaux sécurisés: la couche infrastructure active la couche services, qui à son tour active la couche Application. L'architecture de sécurité prend en compte le fait que chacune des couches est différemment vulnérable du point de vue de la sécurité et elle fait obstacle aux menaces potentielles d'une manière souple, qui est celle qui convient le mieux à la couche de sécurité concernée.

Il faut noter que les couches de sécurité (telles qu'elles sont définies ci-dessus) représentent une catégorie distincte et que les trois couches dans leur ensemble peuvent s'appliquer à chacune des couches du modèle de référence d'interconnexion des systèmes ouverts (OSI, *open system interconnection*).

Les couches de sécurité indiquent où il convient de tenir compte de la sécurité dans les produits et dans les solutions, en offrant une vue séquentielle de la sécurité dans le réseau. La vulnérabilité en ce qui concerne la sécurité est ainsi abordée en premier lieu pour la couche infrastructure, puis, pour la couche services, et finalement pour la couche Application. La Figure 1 illustre comment les mesures de sécurité sont appliquées aux couches de sécurité afin de réduire les vulnérabilités qui existent au niveau de chacune des couches et donc d'atténuer les attaques de la sécurité.

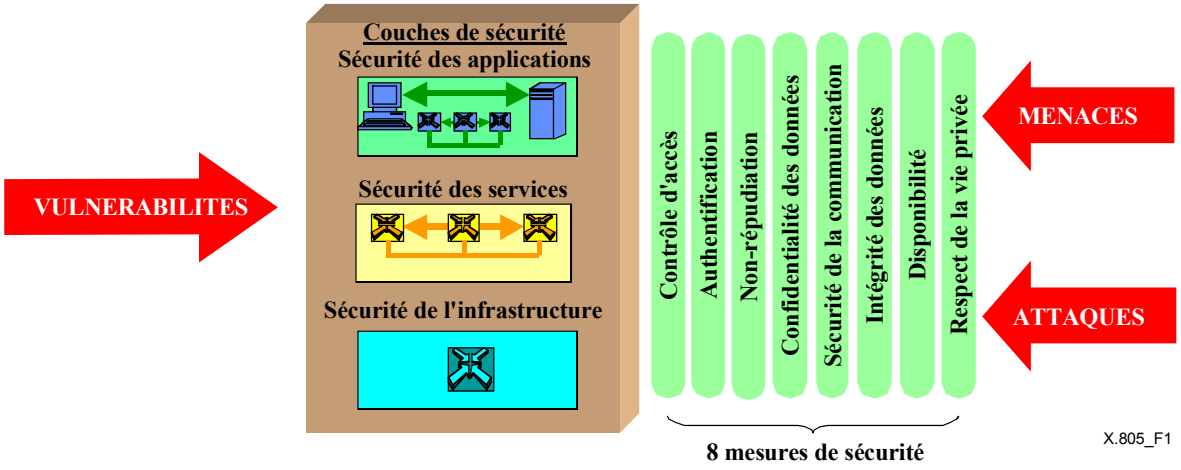

Figure 1/X.805 – Application des mesures de sécurité aux couches de sécurité

7.1 Couche de sécurité relative à l'infrastructure

La couche de sécurité relative à l'infrastructure comporte des équipements de transmission dans le réseau ainsi que des éléments de réseau individuels protégés par les mesures de sécurité. Cette couche est constituée des modules fondamentaux des réseaux, de leurs services et de leurs applications. Des exemples de composants qui appartiennent à la couche infrastructure sont les différents routeurs, les commutateurs et les serveurs ainsi que les liaisons de communication entre eux.

7.2 Couche de sécurité relative aux services

La couche de sécurité relative aux services concerne la sécurité des services que les fournisseurs de services fournissent à leurs clients (par exemple, les services d'authentification, d'autorisation et de comptabilité (AAA, *authentication, authorization and accounting*), les protocoles de configuration de serveur dynamique (DHCP, *dynamic host configuration protocol*), les services DNS, etc.), utilement complétés par des services tels que le téléphone gratuit, la qualité de service (QS), le réseau privé virtuel (VPN, *virtual private network*), les services de localisation, la messagerie instantanée, etc. La couche de sécurité relative aux services est employée pour protéger les

fournisseurs de services et leurs clients, deux cibles potentielles pour les menaces de la sécurité. Les attaquants pourraient par exemple tenter de nier que le fournisseur de services a les capacités de fournir les services, ou ils pourraient tenter d'interrompre le service destiné à un client particulier du fournisseur de services (par exemple, une entreprise).

7.3 Couche de sécurité relative aux applications

La couche de sécurité relative aux applications est consacrée à la sécurité des applications dans le réseau, auxquelles ont accès les clients des fournisseurs de services. Ces applications, activées par les services dans le réseau, sont notamment des applications d'acheminement de fichiers de base [à l'aide, par exemple, du protocole de transfert de fichiers (FTP, *file transfer protocol*)] et de navigation sur le web, des applications fondamentales telles qu'une aide en matière d'annuaire, une messagerie vocale sur le réseau et le courrier électronique, ainsi que des applications haut de gamme telles que la gestion des relations entre les clients, le commerce électronique ou mobile, la formation sur le réseau, la collaboration vidéo, etc. Les applications dans le réseau peuvent être fournies par des fournisseurs de service d'application (ASP, *application service provider*) tiers, par des fournisseurs de services faisant aussi fonction de fournisseurs ASP ou par des entreprises les hébergeant dans leurs propres centres de données (ou dans des centres en location). Au niveau de cette couche, les cibles potentielles pour les attaques de la sécurité sont au nombre de quatre: l'utilisateur des applications, le fournisseur des applications, le logiciel standard personnalisé fourni par les intégrateurs de l'entité tierce (par exemple, les services d'hébergement sur le web) et le fournisseur de services.

8 Plans de sécurité

Un plan de sécurité est un certain type d'activité dans le réseau, protégée par les mesures de sécurité. Dans la présente Recommandation sont définis trois plans de sécurité pour représenter les trois types d'activités protégées qui peuvent être exercées dans un réseau. Ces plans de sécurité sont les suivants:

1) le plan de gestion;

2) le plan de commande;

3) le plan de l'utilisateur final.

Ils assurent des besoins de sécurité particuliers, liés aux activités de gestion du réseau, de commande du réseau ou de signalisation, et aux activités qu'ont les utilisateurs finals.

Les réseaux devraient être conçus de manière que les événements qui se produisent au niveau d'un plan de sécurité soient totalement tenus isolés des autres plans de sécurité. Une consultation du service DNS trop importante au niveau du plan de l'utilisateur final, à la suite de trop nombreuses demandes, ne devrait par exemple pas interdire l'utilisation de l'interface d'exploitation, d'administration, de maintenance et de fourniture (OAM&P, *operations, administration, maintenance & provisioning*) dans le plan de gestion, qui permettrait à un administrateur de corriger le problème.

Dans la Figure 2 est représentée l'architecture de sécurité et y sont aussi indiqués les plans de sécurité. Chaque type d'activités décrites dans le réseau a ses propres besoins en matière de sécurité. Le concept des plans de sécurité permet de différencier les préoccupations liées à ces activités, qui sont spécifiques en matière de sécurité, et il permet d'y répondre indépendamment. Prenons, par exemple, un service de téléphonie utilisant le protocole Internet (VoIP, *voice over IP*) qui est traité au niveau de la couche de sécurité des services. La sécurisation de la gestion du service VoIP (par exemple, la fourniture aux utilisateurs) doit être indépendante de la sécurisation de la commande du service [par exemple, les protocoles tels que les protocoles d'ouverture de session (SIP, *session initiation protocol*)], ainsi que de la sécurisation des données des utilisateurs finals acheminées par le service (par exemple, la voix de l'utilisateur).

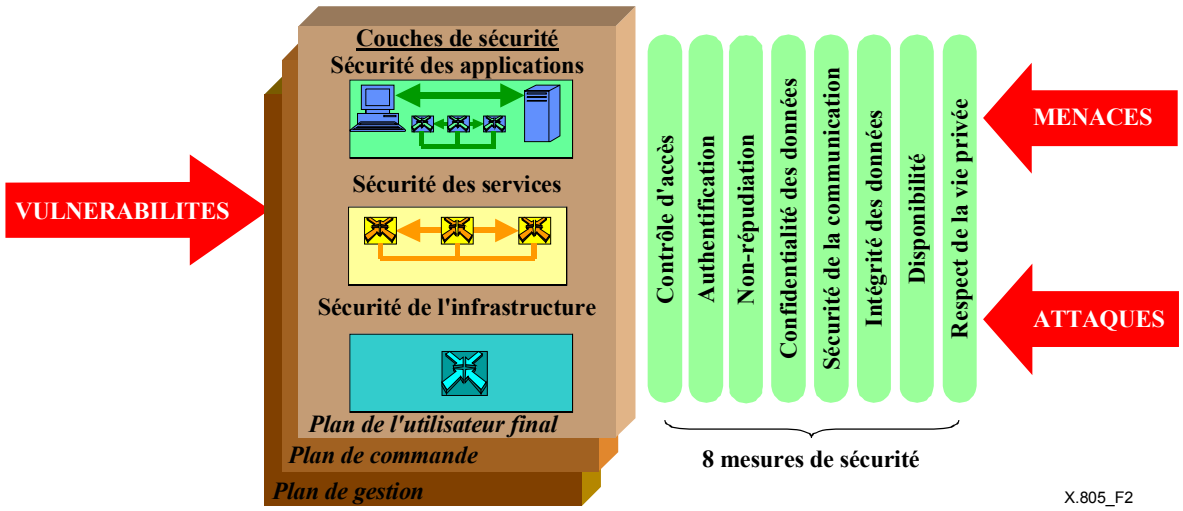

Figure 2/X.805 – Plans de sécurité rendant compte des différents types d'activités dans le réseau

8.1 Plan de sécurité relatif à la gestion

Le plan de sécurité relatif à la gestion concerne la protection des fonctions OAM&P des éléments de réseau, de l'équipement de transmission, des systèmes d'arrière-guichet (systèmes d'assistance à l'exploitation, systèmes d'assistance commerciale, systèmes d'aide aux clients, etc.) et des centres de données. Le plan de gestion prend en charge la faute, la capacité, l'administration, la configuration et la sécurité (FCAPS, *fault, capacity, administration, provisioning and security*). Il faut noter que le réseau acheminant le trafic pour ces activités peut fonctionner dans la bande ou en dehors de celle-ci par rapport au trafic de l'utilisateur du fournisseur de services.

8.2 Plan de sécurité relatif à la commande

Le plan de sécurité relatif à la commande concerne la protection des activités qui permettent une livraison efficace des informations, des services et des applications à travers le réseau. Généralement, il fait intervenir des communications d'informations de machine à machine (par exemple, des commutateurs ou des routeurs) qui leur permettent de déterminer comment acheminer ou commuter au mieux le trafic à travers le réseau de transport sous-jacent. Ce type d'informations est parfois désigné sous le nom d'informations de commande ou de signalisation. Le réseau acheminant ces types de messages peut fonctionner dans la bande ou en dehors de celle-ci par rapport au trafic de l'utilisateur du fournisseur de services. Les réseaux IP acheminent par exemple leurs informations de commande dans la bande, tandis que le réseau téléphonique public commuté (RTPC) le fait dans un réseau de signalisation hors-bande distinct [le réseau du système de signalisation n° 7 (SS7, *signalling system no 7*)]. Des exemples de trafic de ce type emploient notamment les protocoles d'acheminement, le protocole de service DNS, le protocole SIP, le protocole du système SS7, le protocole Megaco/H.248, etc.

8.3 Plan de sécurité relatif à l'utilisateur final

Le plan de sécurité relatif à l'utilisateur final assure la sécurité de l'accès et de l'emploi du réseau du fournisseur de services par l'utilisateur. Ce plan correspond aussi aux flux de données proprement dits de l'utilisateur final. Les utilisateurs finals peuvent employer un réseau qui n'assure que la connectivité, ils peuvent l'employer pour des services à valeur ajoutée tels que celui des réseaux VPN ou ils peuvent l'employer pour accéder à des applications dans le réseau.

9 Menaces de la sécurité

L'architecture de sécurité consiste en un plan et un ensemble de principes qui décrivent une structure de sécurité pour la solution de sécurité de bout en bout. Cette architecture permet de recenser les questions de sécurité à traiter afin de prévenir les menaces intentionnelles ainsi qu'accidentelles. Les menaces suivantes sont décrites dans la Rec. UIT-T X.800 (1991), *Architecture de sécurité pour l'interconnexion en systèmes ouverts d'applications du CCITT:*

- destruction des informations et/ou d'autres ressources;
- corruption ou modification d'informations;
- vol, suppression ou perte d'informations et/ou d'autres ressources;
- divulgation d'informations;
- interruption de services.

L'intersection de chacune des couches de sécurité avec chacun des plans de sécurité permet de préciser en matière de sécurité où les mesures de sécurité sont appliquées pour contrer les menaces. Le Tableau 1 donne l'application de sécurité aux menaces de la sécurité. Cette application est la même pour chaque perspective de sécurité.

La lettre "O" dans les cases situées à l'intersection des lignes et des colonnes du Tableau suivant indique qu'une menace particulière de la sécurité est contrée par une mesure de sécurité correspondante.

Tableau 1/X.805 – Mappage des mesures de sécurité aux menaces de la sécurité

Mesure de sécurité	Menace de la sécurité				
	Destruction d'informations ou d'autres ressources	Corruption ou modification d'informations	Vol, suppression ou perte d'informations et d'autres ressources	Divulgation d'informations	Interruption de services
Contrôle d'accès	O	O	O	O	
Authentification			O	O	
Non-répudiation	O	O	O	O	O
Confidentialité des données			O	O	
Sécurité de la communication			O	O	
Intégrité des données	O	O			
Disponibilité	O				O
Respect de la vie privée				O	

Dans la Figure 3 est représentée l'architecture de sécurité et y sont aussi indiqués les éléments architecturaux et les menaces de sécurité décrites ci-dessus. La figure illustre le concept de protection d'un réseau au moyen des mesures de sécurité appliquées au niveau de chaque plan de sécurité de chacune des couches de sécurité, en vue de disposer d'une solution de sécurité complète. Il faut noter qu'en fonction des exigences en matière de sécurité du réseau, il pourrait ne pas être nécessaire de mettre en œuvre tous les éléments architecturaux (c'est-à-dire l'ensemble complet des mesures de sécurité, des couches de sécurité et des plans de sécurité).

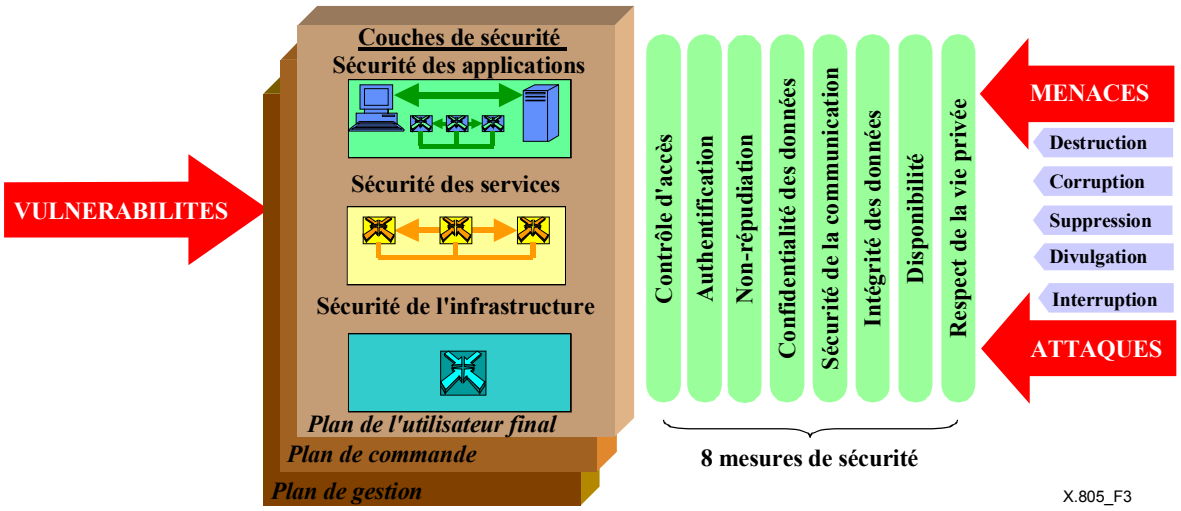

Figure 3/X.805 – Architecture de sécurité pour la sécurité du réseau de bout en bout

10 Description des objectifs atteints en appliquant des mesures de sécurité aux couches de sécurité

L'architecture de sécurité peut s'appliquer à tous les aspects et à toutes les phases d'un programme de sécurité tel que celui qui est représenté dans la Figure 4. Comme on peut l'observer dans cette figure, un programme de sécurité comporte des politiques et des procédures en plus de la technologie, et son application passe par trois phases:

1) la phase de définition et de planification;

2) la phase d'implémentation;

3) la phase de maintenance.

L'architecture de sécurité peut s'appliquer, au cours des trois phases du programme de sécurité, aux politiques et aux procédures de sécurité, ainsi qu'à la technologie.

L'architecture de sécurité peut servir de guide à l'élaboration de définitions de politiques de sécurité détaillées, de réponses aux incidents et de plans de récupération, ainsi que d'architectures en matière de technologie, en tenant compte, au cours de la phase de définition et de planification, de chaque mesure de sécurité au niveau de chacune des couches et des plans de sécurité. L'architecture de sécurité peut aussi être employée comme base d'une évaluation de la sécurité qui serait faite pour examiner comment l'implémentation du programme de sécurité assure l'application des mesures, des couches et des plans de sécurité, lorsque les politiques et les procédures sont retirées et que la technologie est déployée. Dès qu'un programme de sécurité a été mis en place, il doit être mis à jour afin de rester au fait des changements continuels de l'environnement en matière de sécurité. L'architecture de sécurité peut aider à la gestion des politiques et des procédures de sécurité, des réponses aux incidents et des plans de récupération, ainsi que des architectures en matière de technologie, en assurant que les modifications apportées au programme de sécurité concernent chacune des mesures de sécurité au niveau de chacune des couches et de chacun des plans de sécurité.

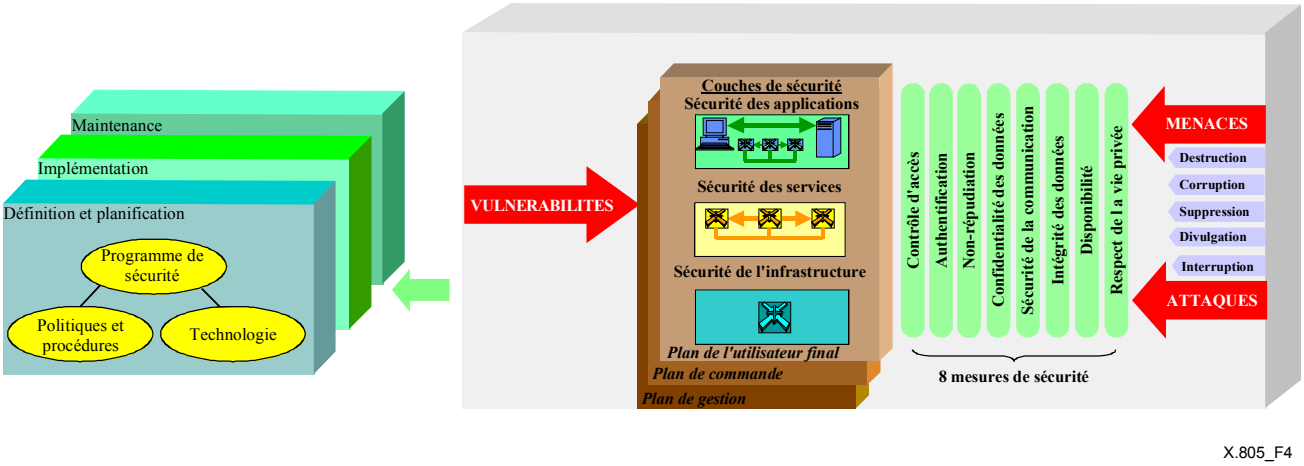

Figure 4/X.805 – Application de l'architecture de sécurité aux programmes de sécurité

En outre, l'architecture de sécurité peut s'appliquer à tout type de réseau et à tout niveau dans la pile de protocoles. Dans un réseau IP, qui est situé au niveau de la couche trois de la pile de protocoles, la couche infrastructure se réfère par exemple aux routeurs individuels, aux liaisons de communication de point à point entre les routeurs (par exemple du réseau optique synchrone (SONET, *synchronous optical network*), des circuits virtuels permanents (PVC, *permanent virtual circuit*) en mode de transfert asynchrone (ATM, *aysnchronous transfer mode*), etc.), et aux plates-formes des serveurs employées pour assurer les services d'assistance exigés par un réseau IP. La couche services se réfère aux services IP de base eux-mêmes (par exemple, la connectivité Internet), au service d'assistance IP (par exemple, les services AAA, DNS, DHCP, etc.), et aux services à valeur ajoutée proposés par le fournisseur de services (par exemple, les services VoIP, QS, VPN, etc.). Finalement la couche Application se réfère à la sécurité des applications de l'utilisateur auxquelles il accède par l'intermédiaire du réseau IP (telles que le courrier électronique, etc.).

De même, pour un réseau en mode ATM, qui est situé au niveau de la couche deux de la pile de protocoles, la couche infrastructure se réfère aux commutateurs individuels et aux liaisons de communication de point à point entre les commutateurs [aménagement de porteuse, par exemple pour le signal numérique de niveau 3 (DS-3, *digital signal level 3*)]. La couche services se réfère aux différentes classes d'acheminement assuré par un service en mode ATM qui offre (un débit binaire constant, un débit binaire variable – un débit binaire variable en temps réel – un débit binaire disponible en différé et un débit binaire non spécifié). Finalement, la couche Application se réfère aux applications qu'emploie l'utilisateur final pour accéder au réseau en mode ATM, telles que l'application de visioconférence.

Dans la Figure 5 est représentée l'architecture de sécurité sous la forme d'un tableau. Une démarche méthodique de sécurisation d'un réseau y est illustrée. Comme on peut constater, l'intersection d'une couche de sécurité avec un plan de sécurité permet de préciser de façon unique comment examiner les huit mesures de sécurité. Chacun des neuf modules regroupe les huit mesures de sécurité qui sont appliquées à une couche de sécurité particulière. Il faut noter que les mesures de sécurité des différents modules ont des objectifs différents et en conséquence comportent des ensembles différents de mesures de sécurité. La forme de tableau est un moyen convenant à la description des objectifs des mesures de sécurité pour chaque module.

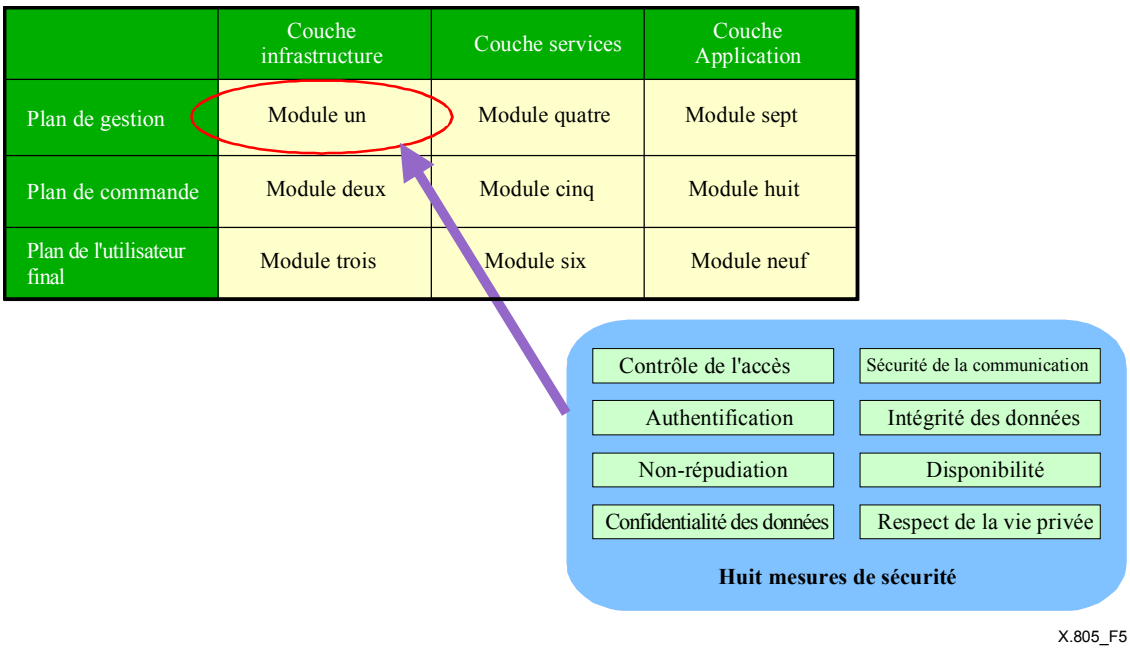

Figure 5/X.805 – Architecture de sécurité sous la forme d'un tableau

10.1 Sécurisation de la couche infrastructure

10.1.1 La sécurisation du plan de gestion de la couche infrastructure consiste en la sécurisation des fonctions OAM&P des éléments de réseau individuels, des liaisons de communication et des plates-formes du serveur qui équipent le réseau. Nous considérons que la configuration des dispositifs du réseau et des liaisons de communication est également une activité de gestion. Un exemple de gestion de l'infrastructure qui nécessite d'être sécurisée est la configuration d'un routeur ou d'un commutateur individuel par le personnel d'exploitation du réseau. Le Tableau 2 décrit les objectifs de l'application des mesures de sécurité à la couche infrastructure, au plan de gestion.

Tableau 2/X.805 – Application des mesures de sécurité à la couche infrastructure, au plan de gestion

Module 1: couche infrastructure, plan de gestion	
Mesure de sécurité	**Objectifs de sécurité**
Contrôle d'accès	Assure que seuls le personnel ou les dispositifs autorisés peuvent exercer [par exemple, dans le cas des dispositifs gérés au moyen du protocole simple de gestion de réseau (SNMP, *simple network management protocol*)] des activités administratives ou de gestion impliquant le dispositif du réseau ou la liaison de communication. Cela s'applique tant à la gestion directe du dispositif par l'intermédiaire d'un port technique qu'à la gestion à distance du dispositif.
Authentification	Vérifie l'identité de la personne ou du dispositif exerçant l'activité administrative ou de gestion impliquant le dispositif du réseau ou la liaison de communication. Les techniques d'authentification peuvent être exigées dans le cadre du contrôle d'accès.
Non-répudiation	Fournit un enregistrement identifiant la personne ou le dispositif qui a exercé chacune des activités administratives ou de gestion impliquant le dispositif du réseau ou la liaison de communication, et l'action qui a été effectuée. Cet enregistrement peut être employé comme preuve de l'exercice de l'activité administrative ou de gestion.
Confidentialité des données	Protège les informations de configuration du dispositif du réseau ou de la liaison de communication d'un accès ou d'une visualisation non autorisés. Cela s'applique aux informations de configuration qui résident dans le dispositif du réseau ou dans la liaison de communication, aux informations de configuration qui sont transmises au dispositif du réseau ou à la liaison de communication, ainsi qu'aux informations de configuration de sauvegarde qui sont entreposées en dehors de la connexion. Protège les informations d'authentification administrative (par exemple, les identifications des administrateurs et les mots de passe) d'un accès ou d'une visualisation non autorisés. Les techniques employées lors du contrôle d'accès peuvent contribuer à assurer la confidentialité des données.
Sécurité de la communication	Dans le cas de la gestion à distance d'un dispositif du réseau ou d'une liaison de communication, assure que les informations de gestion ne sont transmises qu'entre les stations de gestion à distance et les dispositifs ou les liaisons de communication qui sont gérées. Les informations de gestion ne sont ni déviées ni interceptées entre ces extrémités. Le même argument peut s'appliquer aux informations d'authentification administrative (par exemple, les identifications de l'administrateur et les mots de passe).
Intégrité des données	Protège les informations de configuration des dispositifs du réseau et des liaisons de communication contre la modification, la suppression, la création et la reproduction non autorisées. Cette protection s'applique aux informations de configuration qui résident dans le dispositif du réseau ou dans la liaison de communication, ainsi qu'aux informations de configuration qui sont en transit ou entreposées dans des systèmes non connectés. Le même argument peut s'appliquer aux informations d'authentification administrative (par exemple, les identifications de l'administrateur et les mots de passe).
Disponibilité	Assure qu'il n'y a pas déni de la capacité à gérer le dispositif du réseau ou la liaison de communication par le personnel ou les dispositifs autorisés. Cela inclut la protection contre les attaques actives telles que les attaques de déni de service (DoS, *denial of service*), ainsi que la protection contre les attaques passives telles que la modification ou la suppression des informations d'authentification administrative (par exemple, les identifications de l'administrateur et les mots de passe).
Respect de la vie privée	Assure que les informations qui peuvent être utilisées pour identifier le dispositif du réseau ou la liaison de communication ne sont pas accessibles au personnel ou aux dispositifs non autorisés. Des exemples de ce type d'informations sont notamment une adresse IP ou un nom de domaine DNS d'un dispositif du réseau. La possibilité d'identifier les dispositifs du réseau fournit par exemple des informations aux attaquants sur les cibles.

10.1.2 La sécurisation du plan de commande de la couche infrastructure consiste en la sécurisation des informations de commande ou de signalisation qui résident dans les éléments de réseau et dans les plates-formes du serveur équipant le réseau, ainsi qu'en la sécurisation de la réception ou de la transmission des informations de commande ou de signalisation par les éléments de réseau ou les

plates-formes du serveur. Il faut, par exemple, que les tables de commutation résidant dans les commutateurs du réseau soient protégées contre le trafic et la divulgation non autorisée. Il faut encore que les routeurs soient protégés de la réception et de la propagation de mises à jour de routage bâclées ou de la réponse à des demandes de routage bâclées émanant de routeurs arnaqueurs. Le Tableau 3 décrit les objectifs de l'application des mesures de sécurité à la couche infrastructure, au plan de commande.

Tableau 3/X.805 – Application des mesures de sécurité à la couche infrastructure, au plan de commande

Module 2: couche infrastructure, plan de commande	
Mesure de sécurité	**Objectifs de sécurité**
Contrôle d'accès	Assure que seuls le personnel et les dispositifs autorisés peuvent accéder aux informations de commande résidant dans le dispositif du réseau (par exemple, une table de routage) ou dans une unité de stockage non connectée. Assure que le dispositif du réseau n'acceptera que les messages d'informations de commande émanant des dispositifs autorisés du réseau (par exemple, les mises à jour de routage).
Authentification	Vérifie l'identité de la personne ou du dispositif examinant ou modifiant les informations de commande résidant dans le dispositif du réseau. Vérifie l'identité du dispositif envoyant des informations de commande aux dispositifs du réseau. Les techniques d'authentification peuvent être exigées dans le cadre du contrôle d'accès.
Non-répudiation	Fournit un enregistrement identifiant la personne ou le dispositif qui a examiné ou modifié les informations de commande dans le dispositif du réseau, et l'action qui a été effectuée. Cet enregistrement peut être employé comme preuve de l'accès ou de la modification des informations de commande. Fournit un enregistrement identifiant le dispositif émettant des messages de commande, envoyés au dispositif du réseau, et l'action qui a été effectuée. Cet enregistrement peut être employé pour prouver que le dispositif a émis le message de commande.
Confidentialité des données	Protège les informations de commande, résidant dans un dispositif du réseau ou dans une unité de stockage non connectée, d'un accès ou d'une visualisation non autorisés. Les techniques employées lors du contrôle d'accès peuvent contribuer à assurer la confidentialité des données concernant les informations de commande résidant dans le dispositif du réseau. Protège les informations de commande, destinées au dispositif du réseau, d'un accès ou d'une visualisation non autorisés, lorsqu'elles sont acheminées à travers le réseau.
Sécurité de la communication	Assure que les informations de commande acheminées à travers le réseau (par exemple, les mises à jour de routage) ne sont transmises qu'entre la source des informations de commande et la destination souhaitée. Les informations de commande ne sont ni déviées ni interceptées au cours de leur transmission entre ces extrémités.
Intégrité des données	Protège les informations de commande résidant dans les dispositifs du réseau, en transit à travers le réseau ou entreposées en dehors de la connexion, contre la modification, la suppression, la création et la reproduction non autorisées.
Disponibilité	Assure que les dispositifs du réseau sont toujours en mesure de recevoir des informations de commande émanant de sources autorisées. Cela inclut la protection contre les attaques délibérées telles que les attaques DoS et contre des accidents (par exemple, la modification du routage).
Respect de la vie privée	Assure que les informations qui peuvent être utilisées pour identifier le dispositif du réseau ou la liaison de communication ne sont pas accessibles au personnel ou aux dispositifs non autorisés. Des exemples de ce type d'informations sont notamment une adresse IP ou un nom de domaine DNS d'un dispositif du réseau. La possibilité d'identifier les dispositifs du réseau ou les liaisons de communication fournit par exemple des informations aux attaquants sur les cibles.

10.1.3 La sécurisation du plan de l'utilisateur final de la couche infrastructure consiste en la sécurisation des données et de la voix de l'utilisateur, alors qu'elles résident dans les éléments de réseau ou qu'elles sont acheminées entre eux, ainsi que lorsqu'elles sont acheminées à travers les liaisons de communication. La protection des données de l'utilisateur résidant sur les plates-formes du serveur est sujette à préoccupation ici, ainsi que leur protection contre une interception illicite au cours de leur acheminement à travers les éléments de réseau ou les liaisons de communication. Le Tableau 4 décrit les objectifs de l'application des mesures de sécurité à la couche infrastructure, au plan de l'utilisateur final.

Tableau 4/X.805 – Application des mesures de sécurité à la couche infrastructure, au plan de l'utilisateur final

Module 3: couche infrastructure, plan de l'utilisateur final	
Mesure de sécurité	**Objectifs de sécurité**
Contrôle d'accès	Assure que seuls le personnel ou les dispositifs autorisés peuvent accéder aux données de l'utilisateur final qui transitent dans un élément de réseau ou dans une liaison de communication ou qui résident dans des dispositifs de stockage non connectés.
Authentification	Vérifie l'identité de la personne ou du dispositif tentant d'accéder aux données de l'utilisateur final, qui transitent dans un élément de réseau ou dans une liaison de communication ou qui résident dans des dispositifs de stockage non connectés. Les techniques d'authentification peuvent être exigées dans le cadre du contrôle d'accès.
Non-répudiation	Fournit un enregistrement identifiant la personne ou le dispositif qui a accédé aux données de l'utilisateur final, acheminées dans un élément de réseau ou dans une liaison de communication ou résidant dans des dispositifs de stockage non connectés, et l'action qui a été effectuée. Cet enregistrement peut être employé comme preuve de l'accès aux données de l'utilisateur final.
Confidentialité des données	Protège les données qui transitent dans un élément de réseau ou dans une liaison de communication ou résident dans des dispositifs de stockage non connectés, d'un accès ou d'une visualisation non autorisés. Les techniques employées lors du contrôle d'accès peuvent contribuer à assurer la confidentialité des données de l'utilisateur final.
Sécurité de la communication	Assure que les données de l'utilisateur final qui transitent dans un élément de réseau ou dans une liaison de communication ne sont ni déviées ni interceptées entre ces extrémités sans autorisation d'accès (par exemple, les écoutes légales).
Intégrité des données	Protège les données de l'utilisateur final, qui transitent dans un élément de réseau ou dans une liaison de communication ou résident dans des dispositifs non connectés, contre la modification, la suppression, la création ou la reproduction non autorisées.
Disponibilité	Assure qu'il n'y a pas déni de l'accès aux données de l'utilisateur final résidant dans des dispositifs non connectés par le personnel autorisé (y compris les utilisateurs finals) et les dispositifs. Cela inclut la protection contre les attaques actives telles que les attaques DoS, ainsi que la protection contre les attaques passives telles que la modification ou la suppression des informations d'authentification (par exemple, les identifications de l'utilisateur et les mots de passe, les identifications de l'administrateur et les mots de passe).
Respect de la vie privée	Assure que les éléments de réseau ne fournissent pas d'informations au personnel ou aux dispositifs non autorisés, se rapportant aux activités dans le réseau de l'utilisateur final (par exemple, le lieu géographique de l'utilisateur, les sites Web visités, etc.).

10.2 Sécurisation de la couche services

La sécurisation de la couche services est compliquée par le fait que les services peuvent s'appuyer les uns sur les autres pour satisfaire aux exigences des consommateurs. Afin de fournir un service VoIP, un fournisseur de services doit d'abord assurer un service IP de base, avec ses services de mise en œuvre requis tels que les services AAA, DHCP, DNS, etc. Le fournisseur de services peut aussi avoir besoin de déployer un service de réseau VPN afin de satisfaire aux exigences du client en matière de qualité QS et de sécurité pour le service VoIP. En raison de cela, l'offre de service envisagée doit être décomposée en ses services composites pour que soit assurée sa sécurité globale.

10.2.1 La sécurisation du plan de gestion de la couche services consiste en la sécurisation des fonctions OAM&P des services dans le réseau. Nous considérons que la configuration des services dans le réseau est également une activité de gestion. Un exemple de gestion des services qui nécessite d'être sécurisée est la fourniture aux utilisateurs autorisés d'un service IP par le personnel d'exploitation du réseau. Le Tableau 5 décrit les objectifs de l'application des mesures de sécurité à la couche services, au plan de gestion.

Tableau 5/X.805 – Application des mesures de sécurité à la couche services, au plan de gestion

Module 4: couche services, plan de gestion	
Mesure de sécurité	**Objectifs de sécurité**
Contrôle d'accès	Assure que seuls le personnel et les dispositifs autorisés peuvent exercer des activités administratives ou de gestion impliquant le service dans le réseau (par exemple, la configuration des utilisateurs du service).
Authentification	Vérifie l'identité de la personne ou du dispositif tentant d'exercer des activités administratives ou de gestion impliquant le service dans le réseau. Les techniques d'authentification peuvent être exigées dans le cadre du contrôle d'accès.
Non-répudiation	Fournit un enregistrement identifiant la personne ou le dispositif qui a exercé chacune des activités administratives ou de gestion impliquant le service dans le réseau, et l'action qui a été effectuée. Cet enregistrement peut être employé pour prouver que la personne ou le dispositif indiqué a exercé l'activité administrative ou de gestion.
Confidentialité des données	Protège la configuration et les informations de gestion du service dans le réseau (par exemple, les choix du client concernant le protocole de sécurité IP (IPSec, *IP security protocol*) pour un service de réseau VPN) d'un accès ou d'une visualisation non autorisés. Cela s'applique aux informations de gestion et de configuration qui résident dans les dispositifs du réseau, sont transmises à travers le réseau ou sont entreposées en dehors de la connexion. Protège les informations administratives ou de gestion du service dans le réseau (par exemple, les identifications de l'utilisateur et les mots de passes, les identifications de l'administrateur et les mots de passe) d'un accès ou d'une visualisation non autorisés.
Sécurité de la communication	Dans le cas de la gestion à distance d'un service dans le réseau, assure que les informations administratives et de gestion ne sont transmises qu'entre les stations de gestion à distance et les dispositifs qui sont gérés dans le cadre du service dans le réseau. Les informations administratives et de gestion ne sont ni déviées ni interceptées entre ces extrémités. Le même argument peut s'appliquer aux informations d'authentification du service dans le réseau (par exemple, les identifications de l'utilisateur et les mots de passe, les identifications de l'administrateur et les mots de passe).
Intégrité des données	Protège les informations administratives et de gestion des services dans le réseau contre la modification, la suppression, la création et la reproduction non autorisées. Cette protection s'applique aux informations administratives et de gestion qui résident dans les dispositifs du réseau, sont transmises à travers le réseau ou sont entreposées dans des systèmes non connectés. Le même argument peut s'appliquer aux informations d'authentification du service dans le réseau (par exemple, les identifications de l'utilisateur et les mots de passe, les identifications de l'administrateur et les mots de passe).
Disponibilité	Assure qu'il n'y a pas déni de la capacité à gérer le service dans le réseau par le personnel ou les dispositifs autorisés. Cela inclut la protection contre les attaques actives telles que les attaques DoS, ainsi que la protection contre les attaques passives telles que la modification ou la suppression des informations d'authentification administrative du service dans le réseau (par exemple, les identifications de l'utilisateur et les mots de passe, les identifications de l'administrateur et les mots de passe).
Respect de la vie privée	Assure que les informations qui peuvent être utilisées pour identifier les systèmes administratifs ou de gestion du service dans le réseau ne sont pas accessibles au personnel ou au dispositif non autorisés. Des exemples de ce type d'informations sont notamment une adresse IP ou un nom de domaine DNS d'un système. La possibilité d'identifier les systèmes administratifs du service dans le réseau fournit par exemple des informations aux attaquants sur les cibles.

10.2.2 La sécurisation du plan de commande de la couche services consiste en la sécurisation des informations de commande ou de signalisation employées par le service dans le réseau. Les questions concernant le protocole SIP qui est utilisé pour ouvrir et maintenir les sessions VoIP sont par exemple abordées ici. Le Tableau 6 décrit les objectifs de l'application des mesures de sécurité à la couche services, au plan de commande.

Tableau 6/X.805 – Application des mesures de sécurité à la couche services, au plan de commande

Module 5: couche services, plan de commande	
Mesure de sécurité	**Objectifs de sécurité**
Contrôle d'accès	Assure que les informations de commande reçues par un dispositif du réseau concernant un service dans le réseau émanent d'une source autorisée (par exemple, un message d'ouverture de session VoIP émanant d'un utilisateur ou d'un dispositif autorisés), avant de les accepter. Protège par exemple contre la mystification d'un message d'ouverture de session VoIP par un dispositif non autorisé.
Authentification	Vérifie l'identité de l'origine des informations de commande concernant un service dans le réseau, envoyées aux dispositifs du réseau impliqués dans le service dans le réseau. Les techniques d'authentification peuvent être exigées dans le cadre du contrôle d'accès.
Non-répudiation	Fournit un enregistrement identifiant la personne ou le dispositif émettant les messages de commande concernant un service dans le réseau, reçus par un dispositif du réseau impliqué dans le service dans le réseau, et l'action qui a été effectuée. Cet enregistrement peut être employé pour prouver que la personne ou le dispositif a émis le message de commande concernant le service dans le réseau.
Confidentialité des données	Protège les informations de commande concernant un service dans le réseau, qui résident dans un dispositif du réseau (par exemple, les bases de données pour une session IPSec), sont acheminées à travers le réseau ou sont entreposées en dehors de la connexion, d'un accès ou d'une visualisation non autorisés. Les techniques employées lors du contrôle d'accès peuvent contribuer à assurer la confidentialité des données sur les informations de commande concernant un service dans le réseau, qui résident dans le dispositif du réseau.
Sécurité de la communication	Assure que les informations de commande concernant un service dans le réseau, acheminées à travers le réseau (par exemple, les messages de négociation de clé IPSec), ne sont transmises qu'entre la source des informations de commande et la destination souhaitée. Les informations de commande ne sont ni déviées ni interceptées au cours de leur transmission entre ces extrémités.
Intégrité des données	Protège les informations de commande concernant un service dans le réseau, qui résident dans les dispositifs du réseau, sont en transit à travers le réseau ou sont entreposées en dehors de la connexion, contre la modification, la suppression, la création et la reproduction non autorisées.
Disponibilité	Assure que les dispositifs du réseau impliqués dans un service dans le réseau sont toujours en mesure de recevoir des informations de commande émanant de sources autorisées. Cela inclut la protection contre les attaques actives telles que les attaques DoS.
Respect de la vie privée	Assure que les informations qui peuvent être utilisées pour identifier les dispositifs du réseau ou les liaisons de communication ne sont pas accessibles au personnel ou aux dispositifs non autorisés. Des exemples de ce type d'informations sont notamment une adresse IP ou un nom de domaine DNS d'un dispositif du réseau. La possibilité d'identifier les dispositifs du réseau ou les liaisons de communication fournit par exemple des informations aux attaquants sur les cibles.

10.2.3 La sécurisation du plan de l'utilisateur final de la couche services consiste en la sécurisation des données et de la voix de l'utilisateur, au cours de l'emploi du service dans le réseau. La confidentialité d'une conversation d'un utilisateur doit par exemple être protégée dans un service VoIP. De même, un service DNS doit assurer la confidentialité des utilisateurs de ce service. Le Tableau 7 décrit les objectifs de l'application des mesures de sécurité à la couche services, au plan de l'utilisateur final.

Tableau 7/X.805 – Application des mesures de sécurité à la couche services, au plan de l'utilisateur final

Module 6: couche services, plan de l'utilisateur final	
Mesure de sécurité	**Objectifs de sécurité**
Contrôle d'accès	Assure que seuls les utilisateurs et les dispositifs autorisés peuvent accéder au service dans le réseau.
Authentification	Vérifie l'identité de l'utilisateur ou du dispositif tentant d'accéder au service dans le réseau et d'utiliser celui-ci. Les techniques d'authentification peuvent être exigées dans le cadre du contrôle d'accès.
Non-répudiation	Fournit un enregistrement identifiant chaque utilisateur ou dispositif qui a accédé au service dans le réseau et a utilisé celui-ci, et l'action qui a été effectuée. Cet enregistrement peut être employé comme preuve de l'accès au service dans le réseau et de l'utilisation de celui-ci par l'utilisateur final ou par un dispositif.
Confidentialité des données	Protège les données de l'utilisateur final, acheminées, traitées ou emmagasinées par un service dans le réseau, d'un accès ou d'une visualisation non autorisés. Les techniques employées lors du contrôle d'accès peuvent contribuer à assurer la confidentialité des données de l'utilisateur final.
Sécurité de la communication	Assure que les données de l'utilisateur final, acheminées, traitées ou emmagasinées par un service dans le réseau ne sont ni déviées ni interceptées entre ces extrémités sans autorisation d'accès (par exemple, écoutes légales).
Intégrité des données	Protège les données de l'utilisateur final, acheminées, traitées ou emmagasinées par un service dans le réseau contre la modification, la suppression, la création ou la reproduction non autorisées.
Disponibilité	Assure qu'il n'y a pas déni de l'accès au service dans le réseau par les utilisateurs finals ou les dispositifs autorisés. Cela inclut la protection contre les attaques actives telles que les attaques DoS, ainsi que la protection contre les attaques passives telles que la modification ou la suppression des informations d'authentification de l'utilisateur final (par exemple, les identifications de l'utilisateur et les mots de passe).
Respect de la vie privée	Assure que le service dans le réseau ne fournit pas d'informations au personnel ou aux dispositifs non autorisés, se rapportant à l'utilisation du service par l'utilisateur final (par exemple, les entités appelées dans le cas d'un service VoIP).

10.3 Sécurisation de la couche Application

La sécurisation du plan de gestion de la couche Application consiste en la sécurisation des fonctions OAM&P de l'application dans le réseau. Nous considérons que la configuration des applications dans le réseau est également une activité de gestion. Pour une application concernant le courrier électronique, un exemple d'activité de gestion qui nécessite d'être sécurisée est la configuration et l'administration des boîtes aux lettres de l'utilisateur. Le Tableau 8 décrit les objectifs de l'application des mesures de sécurité à la couche Application, au plan de gestion.

Tableau 8/X.805 – Application des mesures de sécurité à la couche Application, au plan de gestion

Module 7: couche Application, plan de gestion	
Mesure de sécurité	**Objectifs de sécurité**
Contrôle d'accès	Assure que seuls le personnel et les dispositifs autorisés peuvent exercer des activités administratives ou de gestion concernant l'application dans le réseau (par exemple, l'administration des boîtes aux lettres de l'utilisateur, dans le cas du courrier électronique).
Authentification	Vérifie l'identité de la personne ou du dispositif tentant d'exercer des activités administratives ou de gestion concernant l'application dans le réseau. Les techniques d'authentification peuvent être exigées dans le cadre du contrôle d'accès.
Non-répudiation	Fournit un enregistrement identifiant la personne ou le dispositif qui a exercé chacune des activités administratives ou de gestion concernant l'application dans le réseau, et l'action qui a été effectuée. Cet enregistrement peut être employé pour prouver que l'activité administrative ou de gestion a été exercée et pour indiquer la personne ou le dispositif qui en a été chargé.
Confidentialité des données	Protège tous les fichiers employés au cours de l'élaboration et de l'exécution de l'application dans le réseau (par exemple, les fichiers source, les fichiers objet, les fichiers exécutables, les fichiers temporaires, etc.), ainsi que les fichiers de configuration de l'application, d'un accès ou d'une visualisation non autorisés. Cela s'applique aux fichiers de l'application qui résident dans les dispositifs du réseau, sont transmis à travers le réseau ou sont entreposés en dehors de la connexion. Protège les informations administratives ou de gestion concernant l'application dans le réseau (par exemple, les identifications de l'utilisateur et les mots de passes, les identifications de l'administrateur et les mots de passe) d'un accès ou d'une visualisation non autorisés.
Sécurité de la communication	Dans le cas de l'administration ou de la gestion à distance d'une application dans le réseau, assure que les informations administratives et de gestion ne sont transmises qu'entre la station de gestion à distance et les dispositifs concernés par l'application dans le réseau. Les informations administratives et de gestion ne sont ni déviées ni interceptées entre ces extrémités. Le même argument peut s'appliquer aux informations administratives ou de gestion concernant l'application dans le réseau (par exemple, les identifications de l'utilisateur et les mots de passe, les identifications de l'administrateur et les mots de passe).
Intégrité des données	Protège tous les fichiers employés au cours de l'élaboration et de l'exécution de l'application dans le réseau (par exemple, les fichiers source, les fichiers objet, les fichiers exécutables, les fichiers temporaires, etc.), ainsi que les fichiers de configuration de l'application contre la modification, la suppression, la création et la reproduction non autorisées. Cette protection s'applique aussi aux fichiers de l'application qui résident dans les dispositifs du réseau, sont transmis à travers le réseau ou sont entreposés dans des systèmes non connectés. Le même argument peut s'appliquer aux informations administratives ou de gestion concernant l'application dans le réseau (par exemple, les identifications de l'utilisateur et les mots de passe, les identifications de l'administrateur et les mots de passe).
Disponibilité	Assure qu'il n'y a pas déni de la capacité à administrer ou à gérer l'application dans le réseau par le personnel ou les dispositifs autorisés. Cela inclut la protection contre les attaques actives telles que les attaques DoS, ainsi que la protection contre les attaques passives telles que la modification ou la suppression des informations d'authentification administrative de l'application dans le réseau (par exemple, les identifications de l'administrateur et les mots de passe).
Respect de la vie privée	Assure que les informations qui peuvent être utilisées pour identifier les systèmes administratifs ou de gestion de l'application dans le réseau ne sont pas accessibles au personnel ou aux dispositifs non autorisés. Des exemples de ce type d'informations sont notamment une adresse IP ou un nom de domaine DNS d'un système. La possibilité d'identifier les systèmes administratifs de l'application dans le réseau fournit par exemple des informations aux attaquants sur les cibles.

10.3.1 La sécurisation du plan de commande de la couche Application consiste en la sécurisation des informations de commande ou de signalisation utilisées par les applications dans le réseau. Ce type d'informations implique généralement que l'application effectue une action en réponse à une information reçue. Les questions de la sécurisation du protocole de transfert de courrier (POP, *post office protocol*) et du protocole simple de transfert de messages (SMTP, *simple mail transfer protocol*) servant à commander la livraison du courrier électronique sont par exemple abordées ici. Le Tableau 9 décrit les objectifs de l'application des mesures de sécurité à la couche Application, au plan de commande.

Tableau 9/X.805 – Application des mesures de sécurité à la couche Application, au plan de commande

Module 8: couche Application, plan de commande	
Mesure de sécurité	**Objectifs de sécurité**
Contrôle d'accès	Assure, avant de les accepter, que les informations de commande, reçues par un dispositif du réseau impliqué dans une application dans le réseau, émanent d'une source autorisée (par exemple, un message dans le cadre du protocole SMTP demandant un transfert de courrier). Protège par exemple contre la mystification d'un client par un dispositif non autorisé.
Authentification	Vérifie l'identité de l'origine des informations de commande d'une application, envoyées aux dispositifs du réseau impliqués dans l'application dans le réseau. Les techniques d'authentification peuvent être exigées dans le cadre du contrôle d'accès.
Non-répudiation	Fournit un enregistrement identifiant la personne ou le dispositif qui a émis les messages de commande reçus par un dispositif du réseau impliqué dans l'application dans le réseau, et l'action qui a été effectuée. Cet enregistrement peut être employé pour prouver que la personne ou le dispositif a émis le message de commande de l'application.
Confidentialité des données	Protège les informations de commande d'une application, qui résident dans un dispositif du réseau [par exemple, les bases de données d'une session de couche de connexion sécurisée (SSL, *secure socket layer*)], sont acheminées à travers le réseau ou sont entreposées en dehors de la connexion, d'un accès ou d'une visualisation non autorisée. Les techniques employées lors du contrôle d'accès peuvent contribuer à assurer la confidentialité des données pour les informations de commande concernant une application dans le réseau, qui résident dans le dispositif du réseau.
Sécurité de la communication	Assure que les informations de commande d'une application, acheminées à travers le réseau (par exemple, les messages de négociation de session SSL), ne sont transmises qu'entre la source des informations de commande et la destination souhaitée. Les informations de commande d'une application dans le réseau ne sont ni déviées ni interceptées au cours de leur transmission entre ces extrémités.
Intégrité des données	Protège les informations de commande concernant une application dans le réseau, qui résident dans les dispositifs du réseau, sont en transit à travers le réseau ou sont entreposées en dehors de la connexion, contre la modification, la suppression, la création et la reproduction non autorisées.
Disponibilité	Assure que les dispositifs du réseau impliqués dans des applications dans le réseau sont toujours en mesure de recevoir des informations de commande émanant de sources autorisées. Cela inclut la protection contre les attaques actives telles que les attaques DoS.
Respect de la vie privée	Assure que les informations qui peuvent être utilisées pour identifier les dispositifs du réseau ou les liaisons de communication impliqués dans une application dans le réseau ne sont pas accessibles au personnel ou aux dispositifs non autorisés. Des exemples de ce type d'informations sont notamment une adresse IP ou un nom de domaine DNS d'un dispositif du réseau. La possibilité d'identifier les dispositifs du réseau ou les liaisons de communication fournit par exemple des informations aux attaquants sur les cibles.

10.3.2 La sécurisation du plan de l'utilisateur final de la couche Application consiste en la sécurisation des données de l'utilisateur fournies à l'application dans le réseau. La confidentialité d'un numéro de carte de crédit d'un utilisateur doit par exemple être protégée par une application propre au commerce électronique. Le Tableau 10 décrit les objectifs de l'application des mesures de sécurité à la couche Application, au plan de l'utilisateur final.

Tableau 10/X.805 – Application des mesures de sécurité à la couche Application, au plan de l'utilisateur final

Module 9: couche Application, plan de l'utilisateur final	
Mesure de sécurité	**Objectifs de sécurité**
Contrôle d'accès	Assure que seuls les utilisateurs et les dispositifs autorisés peuvent accéder à l'application dans le réseau et employer celle-ci.
Authentification	Vérifie l'identité de l'utilisateur ou du dispositif tentant d'accéder et d'employer l'application dans le réseau. Les techniques d'authentification peuvent être exigées dans le cadre du contrôle d'accès.
Non-répudiation	Fournit un enregistrement identifiant chaque utilisateur ou dispositif qui a accédé à l'application dans le réseau et a employé celle-ci, et l'action qui a été effectuée. Cet enregistrement peut être employé comme preuve de l'accès à l'application et de l'emploi de celle-ci par l'utilisateur final ou le dispositif.
Confidentialité des données	Protège les données de l'utilisateur final (par exemple, son numéro de carte de crédit) qui sont acheminées, traitées ou emmagasinées par une application dans le réseau, d'un accès ou d'une visualisation non autorisés. Le même argument peut s'appliquer aux données de l'utilisateur transmises de celui-ci vers l'application dans le réseau. Les techniques employées lors du contrôle d'accès peuvent contribuer à assurer la confidentialité des données de l'utilisateur final.
Sécurité de la communication	Assure que les données de l'utilisateur final, acheminées, traitées ou emmagasinées par une application dans le réseau, ne sont ni déviées ni interceptées entre ces extrémités sans autorisation d'accès (par exemple, les écoutes). Le même argument peut s'appliquer aux données de l'utilisateur transmises de celui-ci vers l'application dans le réseau.
Intégrité des données	Protège les données de l'utilisateur final, acheminées, traitées ou emmagasinées par une application dans le réseau, contre la modification, la suppression, la création ou la reproduction non autorisées. Le même argument peut s'appliquer aux données de l'utilisateur transmises de celui-ci vers l'application dans le réseau.
Disponibilité	Assure qu'il n'y a pas déni de l'accès à l'application dans le réseau par les utilisateurs finals et les dispositifs autorisés. Cela inclut la protection contre les attaques actives telles que les attaques DoS, ainsi que la protection contre les attaques passives telles que la modification ou la suppression des informations d'authentification de l'utilisateur final (par exemple, les identifications et les mots de passe).
Respect de la vie privée	Assure que l'application dans le réseau ne fournit pas d'informations au personnel ou aux dispositifs non autorisés, se rapportant à l'emploi de l'application par l'utilisateur final (par exemple, les sites Web visités). Ce type d'informations ne doit être révélé qu'aux forces de police, chargées d'un mandat de perquisition.

SÉRIES DES RECOMMANDATIONS UIT-T

Série A	Organisation du travail de l'UIT-T
Série B	Moyens d'expression: définitions, symboles, classification
Série C	Statistiques générales des télécommunications
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	RGT et maintenance des réseaux: systèmes de transmission, circuits téléphoniques, télégraphie, télécopie et circuits loués internationaux
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 et communication entre systèmes ouverts**
Série Y	Infrastructure mondiale de l'information, protocole Internet et réseaux de nouvelle génération
Série Z	Langages et aspects généraux logiciels des systèmes de télécommunication

Genève, 2004