

Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

X.1032

(12/2010)

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

Sécurité de l'information et des réseaux – Sécurité des
réseaux

**Architecture de corrélations externes dans un
système de sécurité d'un réseau de
télécommunication IP**

Recommandation UIT-T X.1032



RECOMMANDATIONS UIT-T DE LA SÉRIE X
RÉSEAUX DE DONNÉES, COMMUNICATION ENTRE SYSTÈMES OUVERTS ET SÉCURITÉ

RÉSEAUX PUBLICS DE DONNÉES	X.1–X.199
INTERCONNEXION DES SYSTÈMES OUVERTS	X.200–X.299
INTERFONCTIONNEMENT DES RÉSEAUX	X.300–X.399
SYSTÈMES DE MESSAGERIE	X.400–X.499
ANNUAIRE	X.500–X.599
RÉSEAUTAGE OSI ET ASPECTS SYSTÈMES	X.600–X.699
GESTION OSI	X.700–X.799
SÉCURITÉ	X.800–X.849
APPLICATIONS OSI	X.850–X.899
TRAITEMENT RÉPARTI OUVERT	X.900–X.999
SÉCURITÉ DE L'INFORMATION ET DES RÉSEAUX	
Aspects généraux de la sécurité	X.1000–X.1029
Sécurité des réseaux	X.1030–X.1049
Gestion de la sécurité	X.1050–X.1069
Télébiométrie	X.1080–X.1099
APPLICATIONS ET SERVICES SÉCURISÉS	
Sécurité en multidiffusion	X.1100–X.1109
Sécurité des réseaux domestiques	X.1110–X.1119
Sécurité des télécommunications mobiles	X.1120–X.1139
Sécurité de la toile	X.1140–X.1149
Protocoles de sécurité	X.1150–X.1159
Sécurité d'homologue à homologue	X.1160–X.1169
Sécurité des identificateurs en réseau	X.1170–X.1179
Sécurité de la télévision par réseau IP	X.1180–X.1199
SÉCURITÉ DU CYBERESPACE	
Cybersécurité	X.1200–X.1229
Lutte contre le pollupostage	X.1230–X.1249
Gestion des identités	X.1250–X.1279
APPLICATIONS ET SERVICES SÉCURISÉS	
Communications d'urgence	X.1300–X.1309
Sécurité des réseaux de capteurs ubiquitaires	X.1310–X.1339
ECHANGE D'INFORMATIONS SUR LA CYBERSÉCURITÉ	
Aperçu général de la cybersécurité	X.1500–X.1519
Echange concernant les vulnérabilités/les états	X.1520–X.1539
Echange concernant les événements/les incidents/l'heuristique	X.1540–X.1549
Echange de politiques	X.1550–X.1559
Heuristique et demande d'informations	X.1560–X.1569
Identification et découverte	X.1570–X.1579
Echange garanti	X.1580–X.1589

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

Recommandation UIT-T X.1032

Architecture de corrélations externes dans un système de sécurité d'un réseau de télécommunication IP

Résumé

La Recommandation UIT-T X.1032 propose quatre modèles permettant de passer en revue les corrélations entre un système de sécurité d'un réseau de télécommunication (TNSS, *telecommunication network security system*) IP et divers groupes d'objets externes. Chaque objet est considéré selon ses fonctionnalités principales et son effet probable sur la construction d'un TNSS et ses principes de fonctionnement. La présente Recommandation sert de base au développement de Recommandations détaillées sur la sécurité du réseau quant à l'effet d'objets externes.

Historique

Edition	Recommandation	Approbation	Commission d'études
1.0	ITU-T X.1032	2010-12-17	17

AVANT-PROPOS

L'Union internationale des télécommunications (UIT) est une institution spécialisée des Nations Unies dans le domaine des télécommunications et des technologies de l'information et de la communication (ICT). Le Secteur de la normalisation des télécommunications (UIT-T) 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/>.

© UIT 2011

Tous droits réservés. Aucune partie de cette publication ne peut être reproduite, par quelque procédé que ce soit, sans l'accord écrit préalable de l'UIT.

TABLE DES MATIÈRES

	Page
1	Domaine d'application 1
2	Références..... 2
3	Définitions 2
3.1	Termes définis ailleurs 2
3.2	Termes définis dans la présente Recommandation 3
4	Abréviations et acronymes 3
5	Conventions 3
6	Généralités 3
7	Corrélations d'un TNSS avec les systèmes de sécurité de systèmes d'information et structure d'information..... 4
7.1	Modèle de corrélations 4
7.2	Fonctions des objets externes et leur effet sur un TNSS 4
8	Corrélations d'un TNSS avec les objets d'un système de télécommunication..... 5
8.1	Modèle de corrélations d'un TNSS..... 5
8.2	Fonctions d'objets externes et leur effet sur un TNSS..... 5
9	Corrélations d'un TNSS avec des organisations externes..... 7
9.1	Modèle de corrélations 7
9.2	Fonctions d'organisations externes et leur effet sur un TNSS..... 7
10	Corrélations d'un TNSS avec les sources de menace pour la sécurité..... 8
10.1	Modèle de corrélations 8
10.2	Fonctions des objets externes et leur effet sur un TNSS 8
	Appendice I – Composition possible des moyens techniques du réseau de télécommunication IP 10
	Bibliographie..... 11

Recommandation UIT-T X.1032

Architecture de corrélations externes dans un système de sécurité d'un réseau de télécommunication IP

1 Domaine d'application

1.1 Une étude de chacun des objets doit être considérée, non seulement les interconnexions entre les différents éléments à l'intérieur de l'objet, mais également les corrélations externes de l'objet. Grâce à ses corrélations externes l'objet exécute ses fonctions dans le contexte du système global. De plus, ces corrélations peuvent agir comme des menaces diverses, qui peuvent perturber le fonctionnement de l'objet.

Une étude de ces objets est particulièrement importante pour le système de sécurité d'un réseau de télécommunication IP (TNSS), qui doit protéger le réseau de télécommunication IP principalement contre les menaces externes (voir Figure 1).

Une composition possible de ressources techniques dans un réseau de télécommunication IP est présentée dans l'Appendice I.

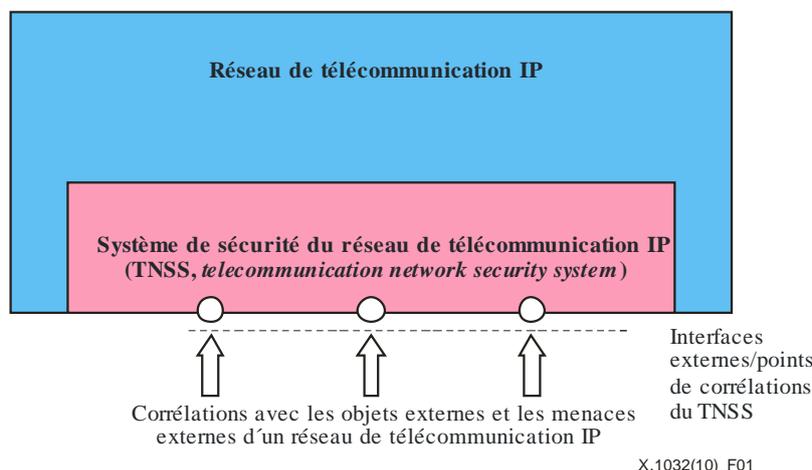


Figure 1 – Corrélations entre un système de sécurité d'un réseau de télécommunication IP et des objets externes

1.2 Le TNSS ne fonctionne pas en tant que système indépendant; il travaille en étroite relation avec un certain nombre de systèmes externes.

Premièrement, ces systèmes comprennent le réseau de télécommunication IP lui-même qui protège le TNSS. Les principes de construction du support de transport et des plates-formes de service déterminent directement les prescriptions du TNSS et des principes de construction du TNSS.

Deuxièmement, ces systèmes externes incluent les utilisateurs du réseau de télécommunication IP dont les prescriptions doivent être satisfaites par le biais du réseau de télécommunication incluant son TNSS.

Certaines autres organisations externes peuvent également affecter les principes de construction d'un TNSS. Ces organisations comprennent:

- les autorités nationales de réglementation;
- les tiers de confiance fournissant des services pour le système de sécurité (sur le principe de "l'externalisation");

- les organisations utilisant des services de réseau de télécommunication IP pour la création de réseaux d'information.

Finalement, les principales tâches d'un TNSS consistent en la protection d'un réseau de télécommunication IP et des informations transmises via ce réseau contre les menaces externes pour la sécurité dans l'environnement dans lequel fonctionne le TNSS.

La liste ci-dessus indique qu'un TNSS a des corrélations avec de nombreux objets externes qui peuvent être subdivisés en plusieurs groupes.

1.3 Les corrélations d'un TNSS avec des objets externes peuvent soit directement, soit indirectement affecter les prescriptions d'un TNSS et les constructions et principes de fonctionnement d'un TNSS. C'est la raison pour laquelle ces interconnexions doivent être prises en compte au cours du développement d'un TNSS. Il existe des Recommandations de l'UIT-T qui donnent la considération qui se doit à certains aspects de ce problème (par exemple, les Recommandations [UIT-T X.842] et [UIT-T X.843] portent sur les corrélations avec un tiers de confiance). Toutefois, de nombreux aspects des corrélations d'un TNSS avec des objets externes n'ont pas encore été examinés.

1.4 La présente Recommandation couvre une architecture générale des corrélations d'un TNSS avec des objets externes. Cette architecture peut s'appliquer à différents types de réseaux de télécommunication et à différents systèmes de sécurité de télécommunication. L'objectif de la présente Recommandation est de fournir une vue d'ensemble de toutes les corrélations externes d'un TNSS. La Recommandation peut servir de base à l'élaboration de recommandations détaillées sur la sécurité de réseau quant à l'effet d'objets externes.

2 Références

Les Recommandations UIT-T et autres références suivantes contiennent des dispositions qui, par suite de la référence qui y est faite, constituent des dispositions de la présente Recommandation. Au moment de la publication, les éditions indiquées étaient en vigueur. Les Recommandations et autres références étant sujettes à révision, les utilisateurs de la présente Recommandation sont invités à rechercher la possibilité d'appliquer les éditions les plus récentes des Recommandations et autres références énumérées ci-dessous. La liste des Recommandations 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.

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

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

[ITU-T X.842] Recommandation UIT-T X.842 (2000) | ISO/CEI TR14516:2002, *Technologies de l'information – Techniques de sécurité – Lignes directrices pour l'utilisation et la gestion des services de tiers de confiance*.

[ITU-T X.843] Recommandation UIT-T X.843 (2000) | ISO/CEI 15945:2002, *Technologies de l'information – Techniques de sécurité – Spécification de services TTP pour la prise en charge des applications de signature numérique*.

3 Définitions

3.1 Termes définis ailleurs

Sans objet.

3.2 Termes définis dans la présente Recommandation

Les termes ci-après sont définis dans la présente Recommandation:

3.2.1 système de sécurité: divers éléments corrélés (certains principes, organisations et mesures techniques pour mettre à disposition une certaine sécurité) qui minimisent la vulnérabilité des biens et des ressources.

3.2.2 système de sécurité d'un réseau de télécommunication IP (TNSS): système de sécurité utilisé dans un réseau de télécommunication IP.

4 Abréviations et acronymes

La présente Recommandation utilise les abréviations suivantes:

TIC technologies de l'information et de la communication

TNSS système de sécurité d'un réseau de télécommunication IP (*telecommunication network security system*)

5 Conventions

Sans objet.

6 Généralités

6.1 L'examen des corrélations d'un TNSS avec des objets externes est rendu complexe en raison du grand nombre de ces objets et des différents types de relations et d'interfaces. C'est pourquoi l'un des problèmes majeurs est la possibilité de décomposition (division) des ensembles de corrélations. La présente Recommandation propose quatre types de corrélations externes:

- les corrélations d'un TNSS avec les systèmes de sécurité qui se superposent à l'infrastructure des systèmes d'information et aux structures d'information;
- les corrélations d'un TNSS avec des objets d'un système de télécommunication;
- les corrélations d'un TNSS avec d'autres objets, par exemple des organisations externes;
- les corrélations d'un TNSS avec des menaces pour la sécurité, qui peuvent provenir soit des objets susnommés, soit de nouveaux objets.

Ces types de corrélations sont considérés ci-dessous dans les paragraphes 7, 8, 9 et 10, respectivement.

6.2 De plus, chaque paragraphe 7, 8, 9 et 10 utilise le principe de décomposition. Tout d'abord, un modèle de corrélation est défini sous forme graphique. Ce modèle contient les objets externes et leurs corrélations avec le TNSS. Les fonctions de chaque objet externe sont ensuite décrites. Enfin, à partir de ces fonctions, de brèves évaluations sont faites concernant:

- les effets possibles des objets externes sur un TNSS (par exemple, les effets des prescriptions sur un TNSS, les effets des principes de construction d'un TNSS et de son fonctionnement);
- les types possibles de corrélations (par exemple, une interface électrique, des prescriptions organisationnelles, les influences de l'environnement externe).

7 Corrélations d'un TNSS avec les systèmes de sécurité de systèmes d'information et structure d'information

7.1 Modèle de corrélations

La Figure 2 montre les corrélations d'un TNSS avec les systèmes de sécurité qui se superposent à l'infrastructure des systèmes d'information, qui à leur tour ont des interfaces avec les systèmes de sécurité d'une structure d'information.

7.2 Fonctions des objets externes et leur effet sur un TNSS

7.2.1 Les systèmes d'information emploient différentes sortes de technologies de l'information utilisant des télécommunications. Les fonctions des systèmes d'information incluent par exemple la collecte, l'enregistrement et la restitution d'information, l'organisation de bases de données et de sites des utilisateurs, le support technique de l'édition, de la conversion et d'autres sortes de traitement de l'information. Les systèmes d'information peuvent réaliser les fonctions de transfert et de distribution d'information à distance à l'aide de services de télécommunication (c'est-à-dire former des réseaux d'information-télécommunication). "Internet" est un exemple de réseau d'information-télécommunication public.

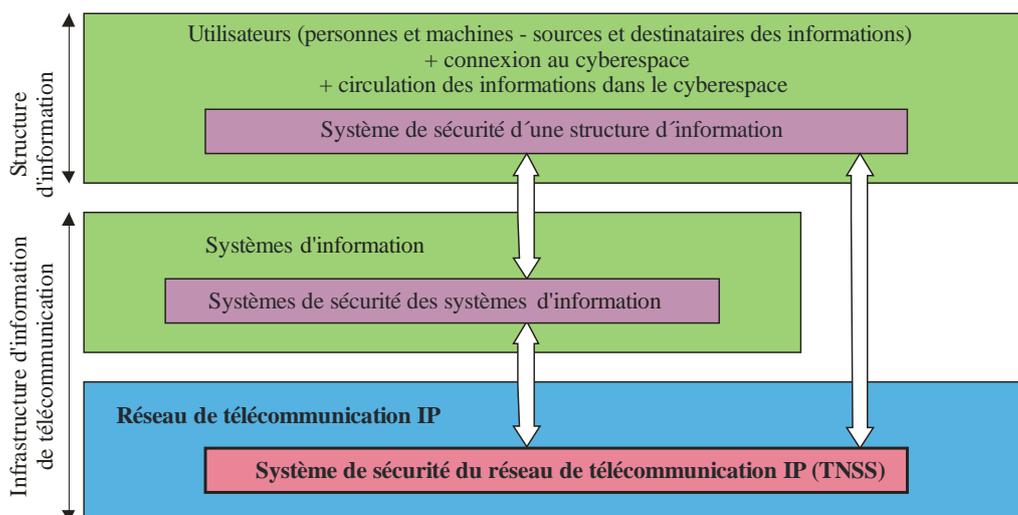
Les types de communication traditionnels (par exemple, la communication téléphonique et la communication par télécopie) peuvent être affectés à la fois avec et sans l'utilisation du réseau d'information-télécommunication.

Les systèmes de sécurité d'un système d'information servent à protéger les moyens techniques de ce système et les informations enregistrées et transférées au sein de ces systèmes. Les systèmes de sécurité d'un système d'information peuvent affecter un TNSS de la manière suivante, par exemple:

- se compléter mutuellement lors de la protection contre certaines menaces, par exemple, contre la divulgation d'informations;
- introduire des limitations pour les protocoles de sécurité utilisés dans un TNSS.

Les corrélations externes d'un TNSS avec les systèmes de sécurité d'un système d'information peuvent se présenter ainsi:

- des interfaces matérielles ou logicielles; ou
- des accords contractuels.



X.1032(10)_F02

Figure 2 – Modèle de corrélations d'un TNSS avec les systèmes de sécurité de systèmes d'information et de structure d'information

7.2.2 Une structure d'information assure l'utilisation des informations dans toutes les sphères des activités humaines. Le système de sécurité de la structure d'information sert à protéger les utilisateurs du cyberspace (auteurs, propriétaires, sources, destinataires et acheteurs d'informations) contre toute intrusion indésirable dans le cyberspace, qui interrompt le travail de l'utilisateur. Les utilisateurs du cyberspace comprennent à la fois les personnes et les machines (éléments détecteurs, actionneurs, automatiques, etc.). Les exemples d'intrusion indésirable sont les virus, les "vers", le spam, divers logiciels malveillants qui existent dans le cyberspace. Une intrusion indésirable peut également inclure un déni de service dans l'infrastructure d'information et de communication.

Le système de sécurité d'une structure d'information peut affecter un TNSS directement ou via les systèmes de sécurité du réseau d'information. Il peut, par exemple, imposer des prescriptions au TNSS quant à la protection du cyberspace à l'aide d'outils techniques pouvant prendre en charge l'application de mesures légales, administratives et d'organisation utilisées au sein du système de sécurité de la structure d'information. De tels outils techniques incluent les moyens de riposte aux virus et spams.

Les corrélations externes d'un TNSS avec un système de sécurité d'une structure d'information peuvent se présenter sous forme d'un accord contractuel.

8 Corrélation d'un TNSS avec les objets d'un système de télécommunication

8.1 Modèle de corrélations d'un TNSS

La Figure 3 montre les corrélations d'un TNSS avec ses propres objets de réseau de télécommunication et avec les systèmes de sécurité d'autres objets de système de télécommunication, c'est-à-dire avec les systèmes de sécurité de l'équipement terminal des utilisateurs et mes réseaux de télécommunication voisins.

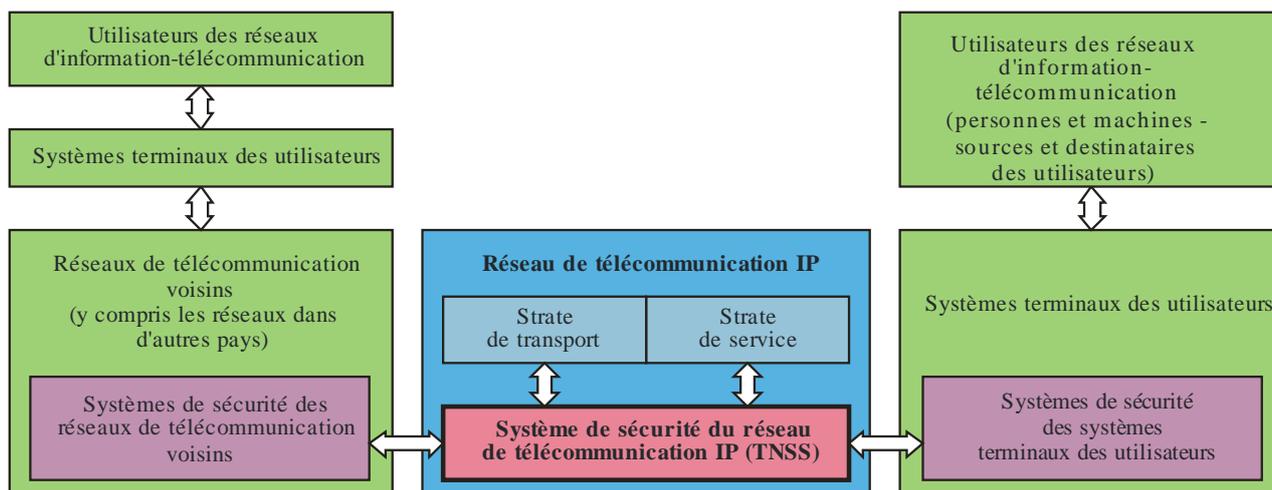
8.2 Fonctions d'objets externes et leur effet sur un TNSS

8.2.1 Les objets internes d'un réseau de télécommunication (strate de transport et strate de service) déterminent la nomenclature des services de télécommunication fournis, ainsi que les caractéristiques aussi bien quantitatives que qualitatives de ces services. Ces objets affectent directement un TNSS. En particulier, ils déterminent:

- la liste des services à protéger;
- les possibilités du réseau concernant la réalisation des mécanismes de sécurité.

Les corrélations externes d'un TNSS avec la strate de transport et la strate de service peuvent se présenter ainsi:

- des interfaces matérielles ou logicielles;
- des accords contractuels.



X.1032(10)_F03

Figure 3 – Modèle de corrélations d'un TNSS avec les objets d'un système de télécommunication

8.2.2 Les systèmes terminaux des utilisateurs peuvent contenir des équipements terminaux (appareils téléphoniques, télévisions, ordinateurs et toute autre sorte de terminal) et les connexions de réseau domestique/professionnel correspondantes (pour plus de détails, voir l'Appendice A). Les systèmes de sécurité des systèmes terminaux des utilisateurs réalisent les fonctions de protection pour les équipements terminaux et les réseaux domestique/professionnel contre les menaces pour la sécurité. Ces menaces peuvent provenir soit du réseau de télécommunication proprement dit ou de sources internes (par exemple les systèmes terminaux des utilisateurs). De plus, les systèmes de sécurité des systèmes terminaux des utilisateurs utilisent des mécanismes pour protéger les informations transmises au réseau de télécommunication.

Les systèmes de sécurité des systèmes terminaux des utilisateurs peuvent agir sur un TNSS. En particulier, ils peuvent:

- se soutenir l'un l'autre durant la protection des informations de l'utilisateur contre certaines menaces, par exemple, en cryptant les données transmises;
- déterminer les prescriptions requises pour un/des niveau(x) de sécurité souhaité(s) que le TNSS doit assurer.

Les corrélations externes d'un TNSS avec les systèmes de sécurité des systèmes terminaux des utilisateurs peuvent se présenter ainsi:

- une interface électrique; ou
- des prescriptions et limitations organisationnelles.

8.2.3 Les réseaux de télécommunication voisins (y compris les réseaux d'autres pays) réalisent un échange de trafic avec les systèmes de télécommunication considérés. Les systèmes de sécurité des réseaux de télécommunication voisins réalisent des fonctions pour protéger ces réseaux et les informations transmises via ces réseaux contre les menaces pour la sécurité. Ces systèmes peuvent agir sur un TNSS, en particulier, ils peuvent:

- se soutenir l'un l'autre durant la protection des informations de l'utilisateur contre certaines menaces, par exemple, contre l'altération ou la modification des informations; et
- introduire des limitations d'utilisation de certains mécanismes de sécurité d'un TNSS ou de certains modes de fonctionnement de ces mécanismes.

Les corrélations externes d'un TNSS avec les systèmes de sécurité des réseaux de télécommunication voisins peuvent être:

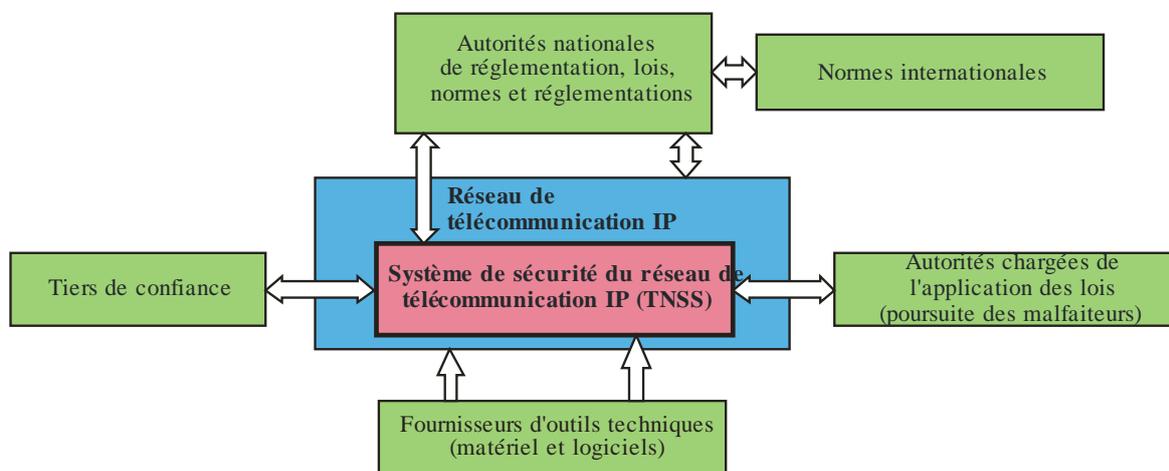
- une interface électrique;
- des dispositions organisationnelles convenues de manière bilatérale.

9 Corrélations d'un TNSS avec des organisations externes

9.1 Modèle de corrélations

La Figure 4 montre les corrélations d'un TNSS avec différentes organisations externes (pour un réseau de télécommunication) comprenant:

- les autorités de réglementation;
- les tiers de confiance;
- les autorités chargées de faire appliquer la loi; et
- les fournisseurs d'outils techniques (matériel et logiciels).



X.1032(10)_F04

Figure 4 – Modèle de corrélations d'un TNSS avec des organisations externes

9.2 Fonctions d'organisations externes et leur effet sur un TNSS

9.2.1 Les autorités de réglementation définissent des politiques générales dans le domaine des télécommunications. En particulier, elles contribuent à l'élaboration et à l'application de normes, lois et règlements internationaux tout en participant à l'élaboration des normes nationales.

9.2.2 Conformément aux accords bilatéraux conclus avec un opérateur de réseau de télécommunication, les tiers peuvent réaliser certaines fonctions pour assurer l'exploitation d'un TNSS.

La liste de ces fonctions et principes d'interaction entre les tiers et un TNSS sont déterminées par l'opérateur de l'infrastructure qui incorpore le TNSS donné.

Les corrélations externes d'un TNSS avec des tiers peuvent se présenter ainsi:

- des interfaces matérielles ou logicielles;
- des accords contractuels.

9.2.3 Les autorités chargées de faire appliquer la loi (poursuite des malfaiteurs) doivent réagir face aux violations des lois nationales concernant les réseaux d'information et de télécommunication. Plus précisément, elles devraient arrêter les personnes coupables de ces violations. Le travail des autorités chargées de faire appliquer la loi et le fonctionnement d'un TNSS se complètent, ce qui renforce la sécurité des télécommunications.

Compte tenu de l'importance des technologies de l'information et de la communication dans toutes les sphères de l'activité humaine, l'élaboration de lois est et restera déterminante, à l'ère de la société de l'information. A terme, cette tendance renforcera le rôle des autorités chargées de faire appliquer la loi.

Dans cette optique, les autorités chargées de faire appliquer la loi devraient recevoir les données fiables des opérateurs de réseaux de télécommunication concernant les incidents de sécurité qui constituent des violations de la loi. Un TNSS devrait effectuer l'acquisition, le stockage et l'analyse des informations, ce qui permettrait de compiler les messages correspondants et de les envoyer aux autorités chargées de faire appliquer la loi. La possibilité de transférer des informations sur des incidents de sécurité émanant d'organisations de télécommunication aux autorités chargées de faire appliquer la loi est illustrée dans les documents [b-ITU-T E.409], [b-ITU-T X.1051] et [b-ITU-T X.1056].

Les corrélations externes d'un TNSS avec les autorités chargées de faire appliquer la loi peuvent se présenter ainsi:

- interface électrique ou autres services de télécommunication ou services postaux;
- dispositions organisationnelles convenues de manière bilatérale.

10 Corrélations d'un TNSS avec les sources de menace pour la sécurité

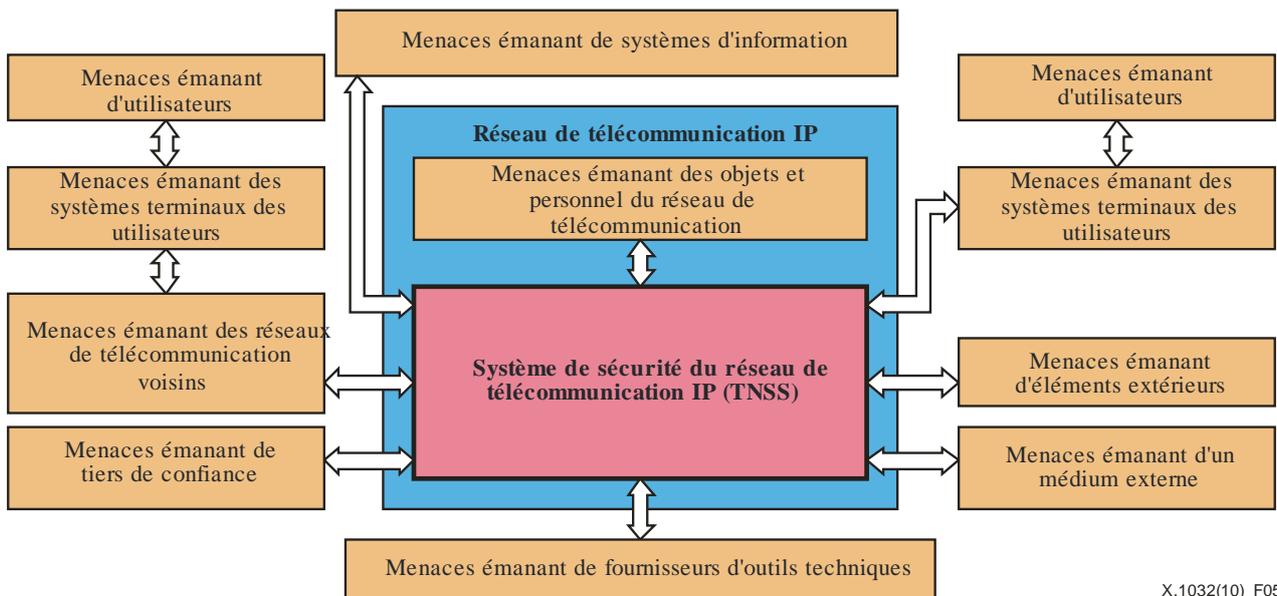
10.1 Modèle de corrélations

La Figure 5 montre un modèle de corrélations d'un TNSS avec différentes sources de menace pour la sécurité qui comprennent:

- les utilisateurs et leurs systèmes terminaux connectés au réseau de télécommunication considéré;
- les médias extérieurs (non-utilisateurs) et externes;
- les objets et personnel du propre réseau de télécommunication;
- les réseaux de télécommunication voisins incluant les utilisateurs et systèmes terminaux des utilisateurs pertinents;
- les systèmes d'information connectés;
- les tiers de confiance; et
- les fournisseurs d'outils techniques.

10.2 Fonctions des objets externes et leur effet sur un TNSS

Les sources de menaces pour la sécurité peuvent attaquer les réseaux de télécommunication. Un système de sécurité d'un réseau de télécommunication (TNSS) est habitué à avertir, détecter et neutraliser de telles attaques. C'est la raison pour laquelle il est prudent de dire que les menaces pour la sécurité sont en relation directe avec un TNSS comme le montre la Figure 5.



X.1032(10)_F05

Figure 5 – Modèle de corrélations d'un TNSS avec sources des menaces pour la sécurité

Les menaces sont classées en cinq types comme l'indiquent les documents [UIT-T X.800] et [UIT-T X.805]:

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

La politique de sécurité dans un réseau de télécommunication peut être utilisée pour riposter à toutes les menaces, ou à certaines de ces menaces. En conséquence, les dimensions de sécurité requises sont sélectionnées au cours de l'élaboration du TNSS. Le mappage des menaces pour la sécurité aux dimensions de sécurité est donné dans le Tableau 1 de [UIT-T X.805].

Les corrélations externes d'un TNSS avec les sources de menaces pour la sécurité peuvent se présenter ainsi:

- interfaces électriques;
- actions de personnes;
- attaques utilisant des moyens techniques via le réseau de télécommunication et des moyens techniques externes;
- influences de l'environnement externe;
- mesures techniques de riposte aux attaques;
- mesures organisationnelles de riposte aux attaques.

Appendice I

Composition possible des moyens techniques du réseau de télécommunication IP

(Le présent Appendice ne fait pas partie intégrante de la présente Recommandation.)

I.1 la présente Recommandation utilise le terme de "réseau de télécommunication" pour couvrir les moyens suivants des opérateurs de télécommunication:

- les moyens des fournisseurs d'infrastructure (c'est-à-dire nœuds de réseau, leurs circuits de connexion, les réseaux d'accès, etc.);
- les moyens des fournisseurs de service (c'est-à-dire les serveurs de service, etc.); le rôle de fournisseur de service peut être joué par le fournisseur d'infrastructure; autrement, le fournisseur de service peut agir au sein du réseau indépendamment;
- les moyens des fournisseurs d'application (c'est-à-dire les serveurs d'application, etc.); le rôle de fournisseur d'application peut être joué par le fournisseur de service; autrement, le fournisseur d'application peut fonctionner au sein du réseau indépendamment;
- la connexion, connecter l'utilisateur avec l'opérateur de télécommunication (c'est-à-dire avec le fournisseur d'infrastructure/service/applications); et
- les informations en cours de transfert et enregistrées par les moyens dont les fournisseurs d'infrastructure/service/applications disposent).

I.2 Le réseau de télécommunication n'inclut pas les "systèmes terminaux des utilisateurs". De tels systèmes contiennent:

- un ou plusieurs terminaux d'abonné de télécommunication (ainsi que les logiciels nécessaires à l'exécution des fonctions d'un utilisateur d'infrastructure, un utilisateur de service et un utilisateur d'applications, y compris l'exécution de certaines fonctions locales – par exemple, la préparation et l'édition de messages);
- un ou plusieurs serveurs d'applications, si l'utilisateur exécute les fonctions d'un fournisseur de services d'applications externes à la structure de réseau;
- un réseau professionnel/local/domestique (si présent);
- pare-feu/passarelle (si présent); et
- les informations de l'utilisateur – transmises, reçues et enregistrées.

Bibliographie

- [b-UIT-T E.409] Recommandation ITU-T E.409 (2004), *Organisation en cas d'incident et prise en charge des incidents relatifs à la sécurité: lignes directrices destinées aux organisations de télécommunication.*
- [b-UIT-T X.1051] Recommandation ITU-T X.1051 (2008) | ISO/IEC 27011:2008, *Technologies de l'information – Techniques de sécurité – Lignes directrices de la gestion de la sécurité de l'information pour les organisations de télécommunications sur la base de l'ISO/IEC 27002.*
- [b-UIT-T X.1056] Recommandation ITU-T X.1056 (2009), *Lignes directrices de la gestion des incidents relatifs à la sécurité destinées aux organisations de télécommunication.*

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	Terminaux et méthodes d'évaluation subjectives et objectives
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