Union internationale des télécommunications

# UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

# X.1210

(01/2014)

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

Sécurité du cyberespace – Cybersécurité

# Description générale des mécanismes de résolution des problèmes de sécurité à la source dans les réseaux fondés sur le protocole Internet

Recommandation UIT-T X.1210

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 |
| SÉCURITÉ DE L'INFORMATIQUE EN NUAGE | |
| Aperçu de la sécurité de l'informatique en nuage | X.1600–X.1601 |
| Conception de la sécurité de l'informatique en nuage | X.1602–X.1639 |
| Bonnes pratiques et lignes directrices concernant la sécurité de l'informatique en nuage | X.1640–X.1659 |
| Mise en oeuvre de la sécurité de l'informatique en nuage | X.1660–X.1679 |
| Sécurité de l'informatique en nuage (autres) | X.1680–X.1699 |

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

# Recommandation UIT-T X.1210

## Description générale des mécanismes de résolution des problèmes de sécurité à la source dans les réseaux fondés sur le protocole Internet


### Résumé

La Recommandation UIT-T X.1210 décrit les mécanismes de résolution des problèmes de sécurité à la source ainsi que les critères de sélection et les lignes directrices de base en matière de sécurité concernant ces mécanismes.

La résolution des problèmes de sécurité à la source dans les réseaux fondés sur le protocole Internet fait intervenir des techniques permettant de découvrir des informations techniques concernant les points d'entrée, les trajets, les trajets partiels ou la source d'un ou de plusieurs paquets à l'origine d'un problème dans un réseau, généralement aux fins de l'application de mesures d'atténuation.



### Historique

| Edition | Recommandation | Approbation | Commission d'études | ID unique* |
|---|---|---|---|---|
| 1.0 | ITU-T X.1210 | 2014-01-24 | 17 | 11.1002/1000/12043 |


* Pour accéder à la Recommandation, reporter cet URL http://handle.itu.int/ dans votre navigateur Web, suivi de l'identifiant unique, par exemple http://handle.itu.int/11.1002/1000/11830-en.

## 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/.

## TABLE DES MATIÈRES

# Recommandation UIT-T X.1210

## Description générale des mécanismes de résolution des problèmes de sécurité à la source dans les réseaux fondés sur le protocole Internet

### 1 Domaine d'application

La présente Recommandation donne une vue d'ensemble des mécanismes de résolution des problèmes de sécurité à la source, des critères d'évaluation et des lignes directrices de base en matière de sécurité concernant ces mécanismes.

Les responsables chargés de la mise en œuvre et les utilisateurs de la présente Recommandation de l'UIT-T doivent respecter toutes les lois, réglementations et politiques applicables aux niveaux national et régional.

### 2 Références

Sans objet.

### 3 Définitions

#### 3.1 Termes définis ailleurs

La présente Recommandation utilise les termes suivants définis ailleurs:

**3.1.1 déni de service** [b-UIT X.800]: Impossibilité d'accéder à des ressources pour des utilisateurs autorisés ou introduction d'un retard pour le traitement d'opérations critiques.

**3.1.2 domaine de sécurité** [b-UIT-T T.411]: Ensemble de ressources soumis à une politique de sécurité unique

**3.1.3 menace** [b-UIT-T X.800]: Violation potentielle de la sécurité.

#### 3.2 Termes définis dans la présente Recommandation

Sans objet.

### 4 Abréviations et acronymes

La présente Recommandation utilise les abréviations et les acronymes suivants:

AS système autononme (*autonomous system*)

BGP protocole de passerelle frontière (*border gateway protocol*)

DoS déni de service (*denial of service*)

FAI fournisseur d'accès à l'Internet ou fournisseur de services Internet (*Internet service provider*)

ICMP protocole de message de commande Internet (*Internet control message protocol*)

IP protocole Internet (*Internet Protocol*)

IPFIX exportation d'informations sur les flux IP (*IP flow information export*)

IPv4/v6 version 4/version 6 du protocole Internet (*Internet protocol version 4/version 6*)

RID défense interréseaux en temps réel (*real-time inter-network defense*)

TCP protocole de commande de transmission (*transmission control protocol*)

## 5 Conventions

Sans objet.

## 6 Aperçu général des mécanismes de résolution des problèmes de sécurité à la source

La résolution des problèmes de sécurité à la source dans les réseaux utilisant le protocole Internet (IP) fait généralement intervenir un processus technique ou administratif qui permet d'identifier en toute fiabillité l'origine d'un ou de plusieurs paquets IP susceptibles ou non d'acheminer l'adresse IP correcte de l'expéditeur, ou les trajets – ou parties de trajet – à l'origine de problèmes de sécurité.

Les mécanismes de résolution des problèmes de sécurité à la source peuvent servir à identifier en temps réel l'emplacement physique ou logique de ces événements relatifs à un problème de sécurité, avec l'aide d'éléments de réseaux tels que les routeurs ou les serveurs du réseau.

Les mécanismes de résolution des problèmes de sécurité à la source dans les réseaux IP sont examinés ci-après.

### 6.1 Mécanismes de résolution des problèmes de sécurité à la source avec mise à l'essai de la liaison

La résolution des problèmes peut commencer depuis le routeur le plus proche de la victime et tester de manière interactive ses liaisons amont jusqu'à ce que les fournisseurs de services Internet puissent déterminer celle qui est alors utilisée pour acheminer le trafic préjudiciable. Dans l'idéal, on répète cette procédure de manière récurrente sur le routeur amont, jusqu'à ce que l'on identifie la source du problème de sécurité.

Cette technique suppose qu'un problème de sécurité reste actif jusqu'à ce que la procédure de résolution des problèmes ait été achevée. A cet égard, elle ne convient pas lorsque les attaques sont décelées après coup ou se produisent de manière intermittente ou encore lorsque les attaques modulent leur comportement suite à la résolution d'un problème de sécurité.

La correction des erreurs à l'entrée est une mise en œuvre du mécanisme de mise à l'essai de la liaison. Il s'agit d'une fonctionnalité qui existe déjà sur de nombreux routeurs et qui permet à l'administrateur de déterminer les liaisons d'arrivée du réseau pour des paquets spécifiques. Si l'opérateur du routeur connaît les caractéristiques particulières du trafic de l'attaque (appelées "*signature de l'attaque*"), il est alors possible de déterminer la liaison d'arrivée du réseau sur le routeur.

### 6.2 Mécanisme de résolution des problèmes de sécurité à la source avec un réseau de recouvrement

Un mécanisme d'attaque par trou noir [b-IETF RFC 3882] est une technique opérationnelle utilisant un tunnel en forme de puits ("sinkhole"), qui est mis en œuvre à tous les points d'entrée possible depuis lesquels les attaques peuvent pénétrer dans le système autonome (AS) de destination/attaqué. A l'aide du protocole de passerelle frontière (BGP) [b-IETF RFC 4271], le trafic à destination du serveur attaqué/visé peut être supprimé du réseau (constituant ainsi un trou noir) ou être redirigé vers un trajet spécial (tunnel) dans lequel un dispositif peut détecter le trafic afin de l'analyser, puis supprimer ce trafic.

### 6.3 Résolution des problèmes de sécurité à la source par sondage

Le protocole de message de commande Internet (ICMP) pour la version 4 du protocole Internet (IPv4) [b-IETF RFC 792] et la version 6 du protocole Internet (IPv6) [b-IETF RFC 4443] constitue – et demeurera – le mécanisme de résolution des problèmes le plus utile pour les réseaux IP. Un certain nombre d'outils, y compris le sondage par écho et le suivi de cheminement, sont utilisés conjointement avec des systèmes d'exploitation courants qui emploient le protocole ICMP pour résoudre des problèmes de bout en bout ou au niveau de la liaison.

### 6.4 Résolution des problèmes de sécurité à la source par journalisation et échantillonnage

L'échantillonnage des flux peut constituer un mécanisme utile pour résoudre les problèmes de sécurité dans les réseaux IP. Les opérateurs peuvent utiliser les fonctions sFlow [b-IETF RFC 3176], NetFlow [b-IETF RFC 3954] ou IPFIX (exportation d'informations sur les flux IP) [b-IETF RFC 5655], en tenant compte des normes d'échantillonnage de flux prises en charge dans les routeurs déployés.

### 6.5 Résolution des problèmes de sécurité à la source dans les systèmes autonomes

En cas de problèmes de sécurité de grande ampleur touchant plusieurs systèmes autonomes, les opérateurs peuvent avoir recours à des outils de résolution des problèmes reposant sur le sondage (voir le § 6.3) et sur les dispositifs de sondage en ligne qui existent sur l'Internet, par exemple le dispositif Looking Glass [b-LG]. A terme, les opérateurs pourront peut-être faciliter l'échange d'informations, afin de disposer d'outils de résolution des problèmes plus perfectionnés dans les systèmes autonomes, par exemple en utilisant la défense interréseaux en temps réel (RID) [b-IETF RFC 6045].

## 7 Principes directeurs de base en matière de sécurité pour les mécanismes de résolution des problèmes de sécurité à la source

Les principes directeurs de base en matière de sécurité pour les mécanismes de résolution des problèmes de sécurité à la source sont définis comme suit:

- Les mécanismes de résolution des problèmes de sécurité à la source devraient être conçus pour être modulables, robustes et résistants.
- Les mécanismes de résolution des problèmes de sécurité à la source devraient être déployés et exploités à travers de multiples domaines, dont chacun sera géré par un administrateur de sécurité responsable (résolution des problèmes entre systèmes autonomes (AS)).
- Les mécanismes de résolution des problèmes de sécurité à la source devraient être mis en œuvre selon l'un des deux types de modèles de déploiement suivants: modèle de déploiement centralisé ou modèle de déploiement réparti.
- Les mécanismes de résolution des problèmes de sécurité à la source devraient permettre de découvrir des informations techniques concernant les points d'entrée, les trajets, les trajets partiels ou la source d'un ou de plusieurs paquets à l'origine d'un problème dans le réseau, généralement aux fins de l'application de mesures d'atténuation.
- Pour le choix d'un mécanisme de résolution des problèmes de sécurité à la source approprié, les mécanismes devraient être évalués en fonction des critères décrits au § 8.
- L'interface des mécanismes de résolution des problèmes de sécurité à la source dans l'ensemble des systèmes autonomes devrait assurer la confidentialité, l'authentification de l'origine des données et l'intégrité des informations échangées entre les différents domaines de sécurité et peut prévoir la mise à disposition du mécanisme de résolution des problèmes.

## 8 Critères régissant l'évaluation des mécanismes de résolution des problèmes à la source

Les critères pouvant être utilisés pour évaluer les mécanismes de résolution des problèmes sont spécifiés comme suit:

- Degré de participation du fournisseur de services Internet (FAI): Degré de participation du FAI lorsque la résolution des problèmes est spécifiée par un administrateur du FAI. La plupart des mécanismes de résolution des problèmes supposent que les FAI mettent à disposition des moyens limités pour permettre la résolution des problèmes. Dans l'idéal, un système de résolution des problèmes nécessiterait un niveau de participation peu important du FAI.

- Nombre de paquets nécessaires à la résolution des problèmes: Nombre de paquets utilisés par un administrateur pour identifier la source du problème de sécurité une fois que celui-ci a été décelé.
- Efficacité du déploiement partiel: Degré d'efficacité de la résolution des problèmes, lorsque les systèmes de résolution des problèmes sont déployés partiellement dans un seul FAI. L'efficacité varie de l'incapacité à produire une identification significative.
- Opérations de traitement pour la résolution des problèmes. Quantité d'opérations de traitement au niveau de l'élément de réseau intermédiaire ou du serveur victime potentiel. Dans l'idéal, on privilégiera un système de résolution des problèmes comportant le moins possible d'opérations de traitement au niveau de l'élément de réseau intermédiaire ou du serveur victime.
- Degré d'accroissement de la largeur de bande: Quantité de trafic additionnelle nécessaire à la résolution des problèmes. Un mécanisme de résolution des problèmes souhaitable devrait faire l'objet d'un accroissement minime de la largeur de bande additionnelle, voire d'aucun accroissement du tout.
- Mémoire requise: Quantité de mémoire additionnelle requise sur les éléments de réseau ou sur un serveur spécial réservé à la résolution des problèmes. Il n'y a pas lieu de prévoir une mémoire additionnelle sur l'élément de réseau, tandis qu'une mémoire additionnelle sur des serveurs spéciaux est acceptable. Dans l'idéal, le mécanisme de résolution des problèmes aura besoin d'une quantité de mémoire additionnelle limitée, mais n'aura besoin d'aucune mémoire additionnelle au niveau de l'élément de réseau.
- Robustesse de la résolution des problèmes: Capacité du mécanisme de résolution des problèmes de produire des résultats significatifs en matière de qualité de fonctionnement, même si certains éléments de réseau ont été détournés. Il y a détournement en raison d'erreurs dues à la mauvaise configuration de l'élément de réseau ou à un correctif logiciel inapproprié.
- Modularité: Configuration additionnelle effectuée sur les autres éléments de réseau qui est nécessaire pour ajouter un élément de réseau unique. La modularité indique si le système de résolution des problèmes peut facilement être étendu. Elle est considérée comme satisfaisante si seul l'élément de réseau qui vient d'être ajouté nécessite une configuration et comme médiocre si l'adjonction d'un élément de réseau unique exige la configuration complète du reste des éléments de réseau. Dans l'idéal, un mécanisme de résolution des problèmes devra être modulable.
- Nombre de fonctions nécessaires à la mise en oeuvre de la résolution des problèmes: Quantité de fonctions additionnelles requises pour mettre en oeuvre le système de résolution des problèmes donné.
- Capacité de traiter des problèmes de sécurité massifs à l'échelle du réseau: Capacité du système de résolution des problèmes d'indiquer l'efficacité avec laquelle le système de résolution des problèmes permet d'identifier des problèmes de sécurité à l'échelle du réseau. Dans l'idéal, un système de résolution de problèmes devra identifier tout problème de sécurité, y compris les attaques par déni de service réparti (DDoS).
- Capacité de résoudre des problèmes en cas de transformation des paquets: Capacité du système de résolution des problèmes d'identifier l'origine des problèmes, même en cas de transformation des paquets. Par transformation des paquets, on entend la modification des paquets lorsque l'acheminement des paquets est effectué. Une transformation courante est la conversion d'adresse de réseau, dans laquelle l'adresse d'origine et/ou l'adresse de destination du ou des paquets est/sont modifiée(s).

# Bibliographie


[b-UIT-T T.411] Recommandation UIT-T T.411 (1993), *Technologies de l'information - Architecture ouverte des documents et format d'échange: introduction et principes généraux*.

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

[b-IETF RFC 792] IETF RFC 792 (1981), *Internet Control Message Protocol*.

[b-IETF RFC 3176] IETF RFC 3176 (2001), *InMon Corporation's sFlow: A Method for Monitoring Traffic in Switched and Routed Networks*.

[b-IETF RFC 3882] IETF RFC 3882 (2004), *Configuring BGP to Block Denial-of-Service Attacks*.

[b-IETF RFC 3954] IETF RFC 3954 (2004), *Cisco Systems NetFlow Services Export Version 9*.

[b-IETF RFC 4271] IETF RFC 4271 (2006), *A Border Gateway Protocol 4 (BGP-4)*.

[b-IETF RFC 4443] IETF RFC 4443 (2006), *Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification*.

[b-IETF RFC 5655] IETF RFC 5655 (2009), *Specification of the IP Flow Information Export (IPFIX) File Format*.

[b-IETF RFC 6045] IETF RFC 6045 (2010), *Real-time Inter-network Defense (RID)*.

[b-LG] BGP Looking Glass, http://www.lookinglass.org/

## 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 |

Imprimé en Suisse
Genève, 2014