Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

X.1580

(09/2012)

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

Echange d'informations sur la cybersécurité – Echange garanti

Défense interréseaux en temps réel

Recommandation UIT-T X.1580

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.1580

Défense interréseaux en temps réel

Résumé

La Recommandation UIT-T X.1580 sur la défense interréseaux en temps réel (RID, *real-time inter-network defence*) présente une méthode de communication interréseaux proactive visant à faciliter l'automatisation du partage d'informations relatives à la prise en charge des incidents. Les implémentations peuvent être intégrées aux systèmes existants de gestion des incidents ainsi qu'aux mécanismes de détection, d'identification de la source et d'atténuation, afin de disposer d'une solution de prise en charge des incidents plus complète. Cette Recommandation définit une méthode permettant de communiquer en toute sécurité des informations sur les incidents, avec l'échange de documents XML au format d'échange de description d'objet incident (IODEF, *incident object description exchange format*). Elle décrit un moyen technique de procéder à des contrôles liés à la sécurité, aux politiques et au respect de la vie privée pour permettre l'échange d'informations potentiellement sensibles. Il est possible de faire correspondre les capacités techniques avec les politiques pertinentes, afin de donner aux fournisseurs de services ou aux organisations la possibilité de prendre des décisions adaptées en fonction de leurs politiques.

La présente Recommandation spécifie la défense interréseaux en temps réel en énumérant les dispositions pertinentes de la norme RFC 6545 de l'IETF et en indiquant si elles ont un caractère normatif ou informatif.

Historique

Edition	Recommandation	Approbation	Commission d'études
1.0	ITU-T X.1580	2012-09-07	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/.

TABLE DES MATIÈRES

			Page
1	Domaine d'application		1
2	Références		1
3	Définitions		1
	3.1	Termes définis ailleurs	1
	3.2	Termes définis dans la présente Recommandation	1
4	Abréviations et acronymes		1
5	Conventions		2
6	Défense interréseaux en temps réel		2
	6.1	Introduction	2
	6.2	Caractéristiques des incidents	2
	6.3	Communications entre équipes CSIRT et fournisseurs de services	2
	6.4	Formats des messages	3
	6.5	Schéma IODEF-RID	3
	6.6	Messages RID	3
	6.7	Flux de communication RID	4
	6.8	Définition de schéma RID	4
	6.9	Impératifs de sécurité	4
	6.10	Considérations relatives à la sécurité	5
	6.11	Internationalisation	5
	6.12	Considérations de l'IANA	5
	6.13	Résumé	5
	6.14	Références	5
Bibliographie			6

Introduction

La Recommandation UIT-T X.1500, Techniques d'échange d'informations sur la cybersécurité, fournit des lignes directrices relatives à l'échange d'informations sur la cybersécurité, y compris des informations sur les incidents et les indicateurs, telles que celles qui sont données dans la présente Recommandation de l'UIT-T. Les organisations peuvent améliorer leur connaissance de la situation et bénéficier de l'assistance d'autres organisations via l'échange d'informations sur les incidents. Cet échange permet aux organisations de mettre en commun des ressources pour identifier les incidents, réduire les activités malveillantes visant leurs ressources informatiques et prendre connaissance des menaces potentielles.

La prise en charge des incidents consiste à détecter, notifier et atténuer les incidents, quels qu'ils soient: problème anodin de configuration, incident informatique, infraction à un accord de niveau de service (SLA, *service level agreement*), compromission de système par ingénierie sociale, attaque par déni de service (DoS, *denial-of-service*), etc. Après la détection d'un incident, il existe plusieurs réponses possibles: soumettre un rapport, envoyer ce rapport à la source de l'incident, demander de l'assistance en vue d'une éventuelle résolution/atténuation, ou faire une demande de traçage de la source.

La défense interréseaux en temps réel (RID, *real-time inter-network defence*) offre une méthode de communication interréseaux proactive visant à faciliter le partage d'informations relatives à la prise en charge des incidents. La RID peut être intégrée aux mécanismes existants de gestion, de détection, d'identification de la source et d'atténuation des incidents, afin de disposer d'une solution complète de prise en charge des incidents. La RID offre un moyen technique de procéder à des contrôles liés à la sécurité, aux politiques et au respect de la vie privée pour permettre l'échange d'informations potentiellement sensibles. La RID permet d'échanger automatiquement et en toute sécurité des documents XML au format d'échange de description d'objet incident (IODEF). Les fournisseurs de services ou les organisations peuvent ainsi prendre des décisions adaptées en fonction de leurs politiques en mettant en correspondance les politiques et accords avec les contrôles techniques mis en oeuvre. La RID comporte des dispositions relatives au secret, à la confidentialité, à l'intégrité et à l'authentification pour l'échange d'informations sur les incidents.

Les données contenues dans les messages RID sont représentées dans un document XML au format IODEF avec une enveloppe RID. L'application de ce modèle permet de constituer une interface de programmation d'application basée sur IODEF et RID en vue d'une intégration avec d'autres outils de prise en charge des incidents. Des marqueurs de données et des valeurs d'énumération XML sont définis afin d'indiquer les actions recommandées pour faire cesser l'incident ou l'attaque ou en atténuer les effets. La RID a pour objet d'offrir une méthode de communication d'informations pertinentes. Etant donné que la RID et le protocole de transport associé offrent simplement une interface d'automatisation des communications entre des outils, l'interopérabilité est assurée avec diverses solutions de détection et de réponse existantes ou futures éventuelles. Les incidents peuvent toucher à la sécurité informatique ou être d'autres types.

Les considérations relatives à la sécurité et au respect de la vie privée sont très importantes car des informations potentiellement sensibles peuvent être échangées par le biais de messages RID. L'échange de messages RID s'appuie sur des techniques existantes incluant des fonctions de sécurité XML en plus de marqueurs de données XML pour indiquer les impératifs en matière de respect de la vie privée et de politiques via le schéma RID. Le schéma RID est une enveloppe XML utilisée pour la communication des documents IODEF. La RID est définie dans la norme RFC 6545 de l'IETF. Les messages RID peuvent être encapsulés en vue d'un transport sécurisé. Le transport RID est défini dans une Recommandation distincte, UIT-T X.1581. On peut combiner les fonctionnalités d'authentification, d'intégrité et d'autorisation de la RID et du transport RID pour parvenir au niveau de sécurité nécessaire.

De nombreuses considérations d'ordre juridique ou ayant trait aux procédures, à la confiance ou aux politiques peuvent restreindre ou empêcher l'échange d'informations.

Recommandation UIT-T X.1580

Défense interréseaux en temps réel

1 Domaine d'application

La présente Recommandation spécifie la défense interréseaux en temps réel (RID, *real-time inter-network defence*) et présente une méthode permettant d'échanger en toute sécurité des informations sur les incidents. Elle définit l'ensemble des messages de coordination en cas d'incident nécessaires à la communication sécurisée de documents IODEF entre entités. La RID permet essentiellement d'envelopper les documents XML au format IODEF, éventuellement étendu. Les messages normalisés et les formats d'échange tiennent compte des considérations relatives aux politiques, au respect de la vie privée et à la sécurité qui sont nécessaires dans un schéma global de coordination en cas d'incident. La RID est une couche de sécurité entre les documents IODEF et le protocole de transport, assurée sur la base des options du schéma XML IODEF-RID et des impératifs de sécurité concernant les flux de communication RID.

Les implémentations assurant l'échange d'informations sur les incidents doivent pouvoir être conformes à toutes les législations, réglementations et politiques nationales et régionales applicables.

Les responsables de l'implémentation et les utilisateurs de toutes les Recommandations UIT-T, y compris la présente Recommandation et les techniques sous-jacentes, doivent respecter toutes les législations, réglementations et politiques nationales et régionales applicables.

2 Références

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.

[IETF RFC 6545] Norme RFC 6545 (2012) de l'IETF, *Real-time Inter-network Defense (RID)*, https://datatracker.ietf.org/doc/rfc6545/

3 Définitions

3.1 Termes définis ailleurs

Aucun.

3.2 Termes définis dans la présente Recommandation

Aucun.

4 Abréviations et acronymes

La présente Recommandation utilise les abréviations et acronymes suivants:

CSIRT équipe d'intervention en cas d'incident relatif à la sécurité informatique (*computer security incident response team*)

DoS déni de service (*denial of service*)

IODEF format d'échange de description d'objet incident (*incident object description exchange format*)

IT technologies de l'information (*information technology*)

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

SLA accord de niveau de service (*service level agreement*)

5 Conventions

Les termes suivants sont considérés comme équivalents:

- A l'UIT, l'emploi du futur d'obligation ("shall" en anglais) est équivalent à celui d'autres moyens d'expression de l'obligation (comme "must" en anglais), la même chose valant pour leurs formes négatives.
- A l'UIT, l'emploi du futur d'obligation ("shall" en anglais) est équivalent à l'emploi à l'IETF du mot "MUST" en anglais.
- A l'UIT, l'emploi de la forme négative du futur d'obligation ("shall not" en anglais) est équivalent à l'emploi à l'IETF des mots "MUST NOT" en anglais.

NOTE – A l'IETF, les mots en anglais "shall" et "must" (en caractères minuscules) sont employés dans les textes informatifs.

6 Défense interréseaux en temps réel

Le présent paragraphe définit l'échange de messages de défense interréseaux en temps réel (RID), tel qu'il est spécifié dans la norme RFC 6545 de l'IETF. Ce paragraphe fait directement référence à la norme RFC 6545 de l'IETF. Y sont mis en correspondance les numéros des paragraphes avec ceux des sections de manière que le paragraphe 6.x corresponde à la section x de la norme RFC 6545 de l'IETF, leurs intitulés concordant aussi.

6.1 Introduction

La section 1 de la norme [IETF RFC 6545] est informative.

6.1.1 Modifications par rapport à la norme RFC 6045

La section 1.1 de la norme [IETF RFC 6545] est informative.

6.1.2 Sections normatives et sections informatives

La section 1.2 de la norme [IETF RFC 6545] est informative.

6.1.3 Terminologie

La section 1.3 de la norme [IETF RFC 6545] est normative.

6.2 Caractéristiques des incidents

La section 2 de la norme [IETF RFC 6545] est informative.

6.3 Communications entre équipes CSIRT et fournisseurs de services

La section 3 de la norme [IETF RFC 6545] est informative.

6.3.1 Echange de messages RID de fournisseur interréseaux

La section 3.1 de la norme [IETF RFC 6545] est informative.

6.3.2 Topologie de communication RID

La section 3.2 de la norme [IETF RFC 6545] est informative.

6.4 Formats des messages

La section 4 de la norme [IETF RFC 6545] est normative.

6.4.1 Types de données RID

La section 4.1 de la norme [IETF RFC 6545] est normative.

6.4.1.1 Booléen

La section 4.1.1 de la norme [IETF RFC 6545] est normative.

6.4.2 Types de messages RID

La section 4.2 de la norme [IETF RFC 6545] est normative.

6.5 Schéma IODEF-RID

La section 5 de la norme [IETF RFC 6545] est normative.

6.5.1 Classe RIDPolicy

La section 5.1 de la norme [IETF RFC 6545] est normative.

6.5.1.1 Classe ReportSchema

La section 5.1.1 de la norme [IETF RFC 6545] est normative.

6.5.2 Classe RequestStatus

La section 5.2 de la norme [IETF RFC 6545] est normative.

6.5.3 Classe IncidentSource

La section 5.3 de la norme [IETF RFC 6545] est normative.

6.5.4 Espaces de noms RID

La section 5.4 de la norme [IETF RFC 6545] est normative.

6.5.5 Codage

La section 5.5 de la norme [IETF RFC 6545] est normative.

6.5.6 Inclusion de documents XML IODEF ou autres

La section 5.6 de la norme [IETF RFC 6545] est normative.

6.5.6.1 Inclusion de documents XML dans un message RID

La section 5.6.1 de la norme [IETF RFC 6545] est normative.

6.6 Messages RID

La section 6 de la norme [IETF RFC 6545] est normative.

6.6.1 Demande

La section 6.1 de la norme [IETF RFC 6545] est normative.

6.6.2 Accusé de réception

La section 6.2 de la norme [IETF RFC 6545] est normative.

6.6.3 Résultat

La section 6.3 de la norme [IETF RFC 6545] est normative.

6.6.4 Rapport

La section 6.4 de la norme [IETF RFC 6545] est normative.

6.6.5 Interrogation

La section 6.5 de la norme [IETF RFC 6545] est normative.

6.7 Flux de communication RID

La section 7 de la norme [IETF RFC 6545] est normative.

6.7.1 Flux de communication de traçage amont

La section 7.1 de la norme [IETF RFC 6545] est normative.

6.7.1.1 Exemple de demande de traçage RID

La section 7.1.1 de la norme [IETF RFC 6545] est normative.

6.7.1.2 Exemple de message d'accusé de réception

La section 7.1.2 de la norme [IETF RFC 6545] est informative.

6.7.1.3 Exemple de message de résultat

La section 7.1.3 de la norme [IETF RFC 6545] est informative.

6.7.2 Flux de communication de demande d'investigation

La section 7.2 de la norme [IETF RFC 6545] est normative.

6.7.2.1 Exemple de demande d'investigation

La section 7.2.1 de la norme [IETF RFC 6545] est informative.

6.7.2.2 Exemple de message d'accusé de réception

La section 7.2.2 de la norme [IETF RFC 6545] est informative.

6.7.3 Flux de communication de rapport

La section 7.3 de la norme [IETF RFC 6545] est normative.

6.7.3.1 Exemple de rapport

La section 7.3.1 de la norme [IETF RFC 6545] est informative.

6.7.4 Flux de communication d'interrogation

La section 7.4 de la norme [IETF RFC 6545] est normative.

6.7.4.1 Exemple d'interrogation

La section 7.4.1 de la norme [IETF RFC 6545] est informative.

6.8 Définition de schéma RID

La section 8 de la norme [IETF RFC 6545] est normative.

6.9 Impératifs de sécurité

La section 9 de la norme [IETF RFC 6545] est normative.

6.9.1 Signatures numériques XML et chiffrement

La section 9.1 de la norme [IETF RFC 6545] est normative.

6.9.2 Transport des messages

La section 9.2 de la norme [IETF RFC 6545] est normative.

6.9.3 Infrastructure de clé publique

La section 9.3 de la norme [IETF RFC 6545] est normative.

6.9.3.1 Authentification

La section 9.3.1 de la norme [IETF RFC 6545] est normative.

6.9.3.2 Authentification de demande à plusieurs bonds

La section 9.3.2 de la norme [IETF RFC 6545] est normative.

6.9.4 Consortiums et infrastructure de clé publique

La section 9.4 de la norme [IETF RFC 6545] est normative.

6.9.5 Considérations relatives au respect de la vie privée et lignes directrices pour l'utilisation du système

La section 9.5 de la norme [IETF RFC 6545] est normative.

6.9.6 Profils de partage et politiques

La section 9.6 de la norme [IETF RFC 6545] est normative.

6.10 Considérations relatives à la sécurité

La section 10 de la norme [IETF RFC 6545] est normative.

6.11 Internationalisation

La section 11 de la norme [IETF RFC 6545] est normative.

6.12 Considérations de l'IANA

La section 12 de la norme [IETF RFC 6545] est normative.

6.13 Résumé

La section 13 de la norme [IETF RFC 6545] est informative.

6.14 Références

6.14.1 Références normatives

La section 14.1 de la norme [IETF RFC 6545] est informative.

Dans la présente Recommandation, la section 14.1 de la norme RFC 6545 de l'IETF est identifiée comme étant informative, car l'UIT-T n'a pas adopté de position sur ces références par rapport à la présente Recommandation. Toutefois, il est reconnu que l'IETF a identifié un ensemble de références normatives pour la norme RFC 6545 de l'IETF.

6.14.2 Références informatives

La section 14.2 de la norme [IETF RFC 6545] est informative.

Bibliographie

[b-UIT-T X.1500] Recommandation UIT-T X.1500 (2011), *Techniques d'échange d'informations sur la cybersécurité*.

[b-UIT-T X.1541] Recommandation UIT-T X.1541 (2012), *Format d'échange de description d'objet incident*.

[b-UIT-T X.1581] Recommandation UIT-T X.1581 (2012), *Transport de messages de défense interréseaux en temps réel*.

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, 2012