Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

X.1582

(01/2014)

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

Echange d'informations sur la cybersécurité – Echange garanti

Protocoles de transport prenant en charge l'échange d'informations sur la cybersécurité

Recommandation UIT-T X.1582

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.1582

Protocoles de transport prenant en charge l'échange d'informations sur la cybersécurité

Résumé

La Recommandation UIT-T X.1582 vise à donner un aperçu des protocoles de transport ayant été choisis et adaptés afin d'être utilisés dans le cadre du modèle d'échange d'informations de cybersécurité (CYBEX). Elle traite des applications de transport et des caractéristiques des protocoles de transport, ainsi que des questions de sécurité.

Historique

Edition	Recommandation	Approbation	Commission d'études	ID unique*
1.0	ITU-T X.1582	2014-01-24	17	11.1002/1000/12037

Mots clés

Informations de cybersécurité, protocoles d'échange d'informations, transfert d'informations.

* 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

Introduction

Il existe déjà un certain nombre de mécanismes et de protocoles d'échange d'informations servant à l'échange d'informations de cybersécurité. Cependant, bon nombre d'entre eux, sinon la majeure partie, sont difficiles à utiliser dans le cadre de l'échange mondial d'informations de cybersécurité, soit parce qu'ils sont réservés à un usage privé et que l'on manque de renseignements à leur sujet, soit parce qu'ils sont mal connus. En outre, la plupart des applications d'échange existantes ne sont utilisables que par un nombre limité de partenaires d'échange, en raison de restrictions portant sur la quantité d'opérations de cybersécurité, ou sur la zone où ces opérations ont lieu.

Etabli en vue d'améliorer l'interopérabilité de l'échange d'informations de cybersécurité dans une perspective mondiale et d'élargir la gamme des espaces d'applications entre lesquels cet échange peut avoir lieu, le modèle *d'échange d'informations de cybersécurité* (CYBEX) décrit de manière générale une famille de spécifications propres aux protocoles, visant à favoriser la mondialisation de l'échange d'informations de cybersécurité entre des espaces d'applications aussi nombreux que possible.

Recommandation UIT-T X.1582

Protocoles de transport prenant en charge l'échange d'informations sur la cybersécurité

1 Domaine d'application

La présente Recommandation vise à donner un aperçu des protocoles de transfert et d'échange actuellement utilisés dans l'espace des applications de transfert et d'échange d'informations de cybersécurité, ayant ou non été normalisés en vue de cette utilisation, et qui ont été choisis et adaptés afin d'être utilisés dans les Recommandations UIT-T de la série X.1500.

La présente Recommandation intéresse en premier lieu les personnes qui conçoivent et mettent en œuvre des applications, et dont le rôle consiste à faciliter le transfert et l'échange d'informations de cybersécurité aux niveaux local, régional et mondial.

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. Une liste des Recommandations UIT-T en vigueur est publiée périodiquement. La référence à un document figurant dans la présente Recommandation ne donne pas à ce document en tant que tel le statut de Recommandation.

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

3 Définitions

3.1 Termes définis ailleurs

La présente Recommandation utilise les termes suivants définis ailleurs:

3.1.1 cybersécurité [b-UIT-T X.1205]: ensemble des outils, politiques, concepts de sécurité, mécanismes de sécurité, lignes directrices, méthodes de gestion des risques, actions, formations, bonnes pratiques, garanties et technologies qui peuvent être utilisés pour protéger le cyberenvironnement et les actifs des organisations et des utilisateurs. Les actifs des organisations et des utilisateurs comprennent les dispositifs informatiques connectés, le personnel, l'infrastructure, les applications, les services, les systèmes de télécommunication et la totalité des informations transmises et/ou stockées dans le cyberenvironnement. La cybersécurité cherche à garantir que les propriétés de sécurité des actifs des organisations et des utilisateurs sont assurées et maintenues par rapport aux risques affectant la sécurité dans le cyberenvironnement. Les objectifs généraux en matière de sécurité sont la disponibilité, l'intégrité (qui peut englober l'authenticité, la non-répudiation et la confidentialité).

NOTE – (ne fait pas partie de [b-UIT-T X.1205]) Certaines réglementations et lois nationales spécifiques peuvent exiger la mise en œuvre de mécanismes de protection d'informations d'identification personnelles.

3.1.2 protocole d'échange [UIT-T X.1500]: ensemble de règles techniques et de formats régissant l'échange d'informations entre deux ou plusieurs entités.

3.2 Termes définis dans la présente Recommandation

Le terme suivant est défini dans la présente Recommandation:

3.2.1 entité de cybersécurité: entité quelconque possédant ou cherchant des informations sur la cybersécurité.

4 Abréviations et acronymes

Les abréviations et acronymes suivants sont utilisés dans la présente Recommandation:

BEEP protocole d'échange extensible de blocs (*blocks extensible exchange protocol*)

CAPEC liste et classification des schémas d'attaque courants (*common attack pattern enumeration and classification*)

CYBEX échange d'informations sur la cybersécurité (*cybersecurity information exchange*)

DDoS déni de service réparti (*distributed denial of service*)

EVCERT certificat de validation étendu (*extended validation certificate*)

HTTP protocole de transfert hypertexte (*hypertext transfer protocol*)

HSTS mécanisme de transport sécurisé pour le protocole de transfert hypertexte (*hypertext transfer protocol strict transport security*)

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

MIME extensions de messagerie Internet à fonctions multiples (*multipurpose Internet mail extensions*)

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

RSS syndication vraiment simple (*really simple syndication*)

SCTP protocole de transmission des commandes de flux (s*tream control transmission protocol*)

SOAP protocole simple d'accès aux objets (*simple object access protocol*)

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

TLS sécurité de la couche transport (*transport layer security*)

UDP protocole datagramme d'utilisateur (*user datagram protocol*)

URI identificateur uniforme de ressource (*uniform resource identifier*)

XML langage de balisage extensible (*extensible markup language*)

5 Conventions

Néant.

6 Protocoles de transport prenant en charge l'échange d'informations de cybersécurité

6.1 Applications de transport

L'échange d'informations de cybersécurité s'utilise dans des scénarios très divers, pouvant être mis en œuvre au moyen de différents protocoles de transport, dont chacun possède des caractéristiques uniques. Afin de faire ressortir les caractéristiques respectives de ces protocoles, quatre applications de transport représentatives sont décrites ci-après.

6.1.1 Diffusion d'informations

Les entités de cybersécurité peuvent diffuser des informations de façon non discriminatoire. Elles disposent à cet effet de protocoles d'alimentation de données très courants, tels que les flux RSS. Dans le cadre de cette diffusion, le même flux d'informations peut être transmis à tout utilisateur, sans qu'il soit nécessaire de filtrer les données ou de les adapter à une partie donnée.

6.1.2 Publication/abonnement

Une entité de cybersécurité peut souscrire un abonnement auprès d'un fournisseur d'informations sur une base bilatérale, et ce fournisseur d'informations peut émettre un flux de données adapté aux spécificités de la partie à l'origine de la demande. Dans ce scénario, le fournisseur d'informations peut jouer le rôle d'intermédiaire entre le publicateur d'informations (par exemple un vendeur de logiciel) et l'abonné. La fourniture de ces services "publication/abonnement" nécessite un filtrage au niveau de l'intermédiaire, filtrage qui lui-même exige une énumération et une requête (par exemple énumération des actifs et requête visant à obtenir des informations pertinentes).

6.1.3 Echange confirmé d'informations

Des entités de cybersécurité disposant de capacités similaires peuvent échanger des informations entre elles, afin d'étendre leur couverture ou de raccourcir les délais d'intervention en cas d'incident. Les protocoles de format d'échange de description d'objet incident (IODEF) [b-UIT-T X.1541] et de défense en temps réel interréseaux (RID) [b-UIT-T X.1580] sont deux exemples de protocole utilisés pour ce type d'échange d'informations. Les entités de cybersécurité identifient les points d'extrémité de communication et s'envoient mutuellement des demandes d'authentification et de confirmation. Dans le cadre de ces échanges confirmés d'informations, chaque entité de cybersécurité peut avoir besoin d'établir des communications avec d'autres entités, ce qui s'effectue au moyen de protocoles de transport bidirectionnels.

6.1.4 Preuve de possession d'informations

Des entités de cybersécurité peuvent souhaiter communiquer avec des parties concernées par un événement ou un incident particulier, sans que des renseignements ne soient divulgués à d'autres voisins non concernés. Ce type de communication utilise des protocoles cryptographiques, tels que l'intersection d'ensembles préservant la confidentialité [b-Kissner]. Les échanges utilisant ce type de protocole consistent essentiellement à fournir la preuve de la possession des informations, sans échanger les informations elles-mêmes, ce qui permet de garantir la confidentialité des informations sensibles. Ces protocoles cryptographiques peuvent être mis en œuvre au-dessus de protocoles de transport bidirectionnels.

6.2 Considérations relatives aux protocoles de transport

En fonction du rôle joué par les entités de cybersécurité, les points d'extrémité de communication peuvent fonctionner de manière asymétrique ou en tant qu'homologues.

Dans une configuration typique où les rôles des deux points d'extrémité sont fixés de manière asymétrique, les protocoles de demande-réponse sont considérés appropriés, car la communication est toujours établie par l'un des deux points d'extrémité. Lorsque les deux points d'extrémité sont en position d'homologues, la communication peut être établie par chacun d'entre eux, d'où il résulte que les protocoles bidirectionnels sont considérés appropriés.

6.2.1 Protocoles de demande-réponse

Dans les protocoles de demande-réponse, la connexion est établie par le client, et le serveur joue le rôle de répondeur. Ce n'est pas la distinction client-serveur qui détermine le flux d'informations: les clients peuvent fournir ou recevoir des informations selon la répartition des rôles.

Dans ce type de protocole, il est possible que les serveurs ne soient pas en mesure de diffuser les informations aux clients dans des délais appropriés, à moins que les clients interrogent les serveurs

sans discontinuer. En d'autres termes, les clients sont à l'origine de l'échange d'informations, tandis que les serveurs jouent dans cet échange le rôle des répondeurs.

Le Tableau 1 donne un aperçu des protocoles de demande-réponse disponibles.

Tableau 1 – Protocoles de demande-réponse disponibles pour le transfert et l'échange

Nom du protocole	Caractéristiques	Références
Protocole de transfert hypertexte (HTTP)	Le protocole HTTP utilise des mécanismes de base servant à soumettre des informations au répondeur ou à récupérer des informations transmises par ce dernier. Le protocole HTTP permet d'échanger tout type d'informations identifiable par un identificateur uniforme de ressource (URI) et pouvant être spécifié au moyen des types d'extensions de messagerie Internet à fonctions multiples (MIME).	[b-IETF RFC 2616]
Protocole simple d'accès aux objets (SOAP)	Le protocole SAOP est mis en œuvre au-dessus du protocole HTTP pour faciliter les communications des paires attribut-valeur. Un schéma en langage de balisage extensible (XML) est utilisé afin de spécifier le type des attributs et des valeurs.	[b-SOAP]

6.2.2 Protocoles bidirectionnels

Dans les protocoles bidirectionnels, les deux extrémités peuvent être à l'origine de l'échange d'informations. Ces protocoles peuvent être asymétriques, c'est-à-dire que l'une des extrémités a le statut de client et doit établir la connexion. Ce type de protocole peut également être symétrique, c'est-à-dire que les deux extrémités peuvent établir la connexion si elles le souhaitent.

Les protocoles bidirectionnels permettent d'échanger des informations à une vitesse appropriée sans qu'il soit nécessaire de répéter les interrogations trop fréquemment. Les avantages des protocoles bidirectionnels ne se limitent pas aux cas d'utilisation symétrique, dans lesquels plusieurs entités de cybersécurité échangent des informations entre elles; ces protocoles présentent également des avantages en termes d'extensibilité lorsqu'il est nécessaire de diffuser des informations auprès d'un grand nombre de nœuds clients.

Il est également possible de mettre en place une connexion bidirectionnelle à partir d'une paire de connexions demande-réponse indépendantes. Dans ce type de combinaison, il est nécessaire que les deux points d'extrémité agissent à la fois comme client et comme serveur, ce qui peut créer des problèmes liés à l'utilisation de logiciels supplémentaires.

Le Tableau 2 donne un aperçu des protocoles bidirectionnels disponibles.

Tableau 2 – Protocoles bidirectionnels disponibles pour le transfert et l'échange

Nom du protocole	Caractéristiques	Références
Protocole d'échange extensible de blocs (BEEP)	Le protocole BEEP peut fonctionner avec des points d'extrémité symétriques ou asymétriques. Les deux extrémités peuvent être à l'origine de la connexion ou jouer le rôle de répondeur.	[b-IETF RFC 3080]
WebSocket	Le protocole WebSocket se situe au-dessus du protocole HTTP, de sorte que les clients sont toujours à l'origine de la connexion. Bien qu'il y ait une distinction entre le client et le serveur, ce dernier peut être à l'origine de l'interaction de protocole dans le cadre d'une connexion établie par le client.	[b-IETF RFC 6455]

6.3 Considérations relatives à la sécurité

Parmi les protocoles de transport CYBEX, ceux pris en charge par les navigateurs web nécessitent une analyse de sécurité approfondie avant d'être utilisés, car certains navigateurs web opèrent une distinction sommaire entre les scripts exécutés sur les sites web, avec un niveau de fiabilité souvent variable. Si une entité de cybersécurité fiable peut très bien utiliser un navigateur web pour échanger des informations, ce même navigateur peut servir à se rendre sur des sites web non fiables, qui peuvent héberger un code potentiellement nuisible pour un certain point d'extrémité CYBEX. Parmi ces menaces, la falsification de requête intersites (CSRF – *cross-site request forgery*) (CAPEC ID 62) et l'exécution de script intersites (XSS – *cross site scripting*) (CAPEC ID 63) sont deux exemples connus d'atteinte à la sécurité liés à la violation du principe de séparation entre les sites web n'ayant pas le même niveau de fiabilité.

Des parades à ces menaces sont disponibles sous forme d'extensions du protocole HTTP (voir Tableau 3). Les extensions prises en charge peuvent varier en fonction de la marque et de la version du navigateur web utilisé.

Tableau 3 – Extensions du protocole HTTP disponibles pour améliorer la sécurité

Nom	Caractéristiques	Références
Politique de sécurité des contenus (CSP – *content security policy*)	La politique CSP permet de restreindre les sources d'objets intégrés, y compris les scripts dynamiques, à un ensemble de sites web prédéfini.	[b-CSP]
Mécanisme de transport sécurisé pour le protocole de transfert hypertexte (HSTS)	Le mécanisme HSTS permet de restreindre les interactions de protocole ultérieures à des canaux sécurisés, tels que le protocole de sécurité de la couche transport (TLS), pendant une certaine durée.	[b-IETF RFC 6797]
HttpOnly	HttpOnly empêche les programmes exécutés par des navigateurs web d'avoir accès aux données d'authentification, par exemple les cookies.	[b-IETF RFC 6265]
Origin Cookies	Origin Cookies empêche les sites web d'altérer les cookies générés par le serveur web d'origine; les cookies d'origine sont modifiables uniquement à partir d'une origine exacte.	[b-Bortz]

D'autres protocoles de couche application sont exposés à des menaces similaires. Etant donné que les navigateurs web modernes peuvent exécuter des programmes arbitraires dans les modules d'extension de navigation, tels que les scripts Java et Flash, ils peuvent être utilisés afin de créer des interactions de protocole. Par conséquent, les points d'extrémité CYBEX devraient éviter d'héberger et d'exécuter des logiciels provenant de sources peu fiables, y compris les sites web. Si l'application de ces restrictions à l'autre point d'extrémité paraît impraticable en raison de la nature non discriminatoire d'une application particulière, il convient de mesurer et de contrôler le niveau d'exposition au risque.

6.4 Considérations relatives au transport et à la couche de session

Dans la mesure où les points d'extrémité CYBEX doivent préserver l'intégrité du canal de communication, il est recommandé d'utiliser les protocoles TCP et SCTP [b-IETF RFC 4960]. En outre, les opérateurs des points d'extrémité CYBEX devraient considérer différents moyens de se protéger contre le déni de service, par exemple les SYN cookies [b-IETF RFC 4987] et autres mesures de protection contre le déni de service réparti (DDoS) [b-Mirkovic]. Ils peuvent encore renforcer la protection du canal de communication en utilisant des codes d'authentification de message, conformément à l'option d'authentification du protocole de commande de transmission (TCP) [b-IETF RFC 5925] et aux fragments authentifiés du protocole de transmission des commandes de flux (SCTP) [b-IETF RFC 4895].

Les menaces connues contre le protocole SCTP, ainsi que leurs contre-mesures, sont répertoriées dans la norme [b-IETF RFC 5062]. L'utilisation du protocole UDP est à éviter, afin de réduire les risques d'attaque par réflexion [b-Paxson].

Afin de garantir la confidentialité des communications, il est recommandé d'utiliser le protocole TLS [b-IETF RFC 5246] [b-IETF RFC 3436]. Dans les cas où il paraît nécessaire de connaître avec certitude l'identité du point d'extrémité, il est recommandé d'utiliser un certificat de validation étendue (ECVERT) [b-EVCERT].

Bibliographie

[b-UIT-T X.1205] Recommandation UIT-T X.1205 (2008), *Présentation générale de la cybersécurité.*

[b-UIT-T X.1541] Recommandation UIT-T X.1541 (2012), *Format d'échange de descriptions d'objet concernant les incidents.*

[b-UIT-T X.1544] Recommandation UIT-T X.1544 (2013), *Liste et classification des schémas d'attaque courants.*

[b-UIT-T X.1580] Recommandation UIT-T X.1580 (2012), *Défense interréseaux en temps réel*.

[b-Bortz] Andrew Bortz, Adam Barth et Alexei Czeskis, Origin Cookies: Session Integrity for Web Applications, W2SP 2011.

[b-CSP] W3C, Content Security Policy 1.0. http://www.w3.org/TR/CSP/

[b-EVCERT] CA/Browser Forum, *Guidelines for the Issuance and Management of Extended Validation Certificates*, Ver. 1.3.

[b-IETF RFC 2616] IETF RFC 2616 (1999), *Hypertext Transfer Protocol* – HTTP/1.1.

[b-IETF RFC 3080] IETF RFC 3080 (2001), *The Blocks Extensible Exchange Protocol Core*.

[b-IETF RFC 3436] IETF RFC 3436 (2002), *Transport Layer Security over Stream Control Transmission Protocol*.

[b-IETF RFC 4895] IETF RFC 4895 (2007), *Authenticated Chunks for the Stream Control Transmission Protocol*.

[b-IETF RFC 4960] IETF RFC 4960 (2007), *Stream Control Transmission Protocol*.

[b-IETF RFC 4987] IETF RFC 4987 (2007), *TCP SYN Flooding Attacks and Common Mitigations*.

[b-IETF RFC 5062] IETF RFC 5062 (2007), *Security Attacks Found Against the Stream Control Transmission Protocol (SCTP) and Current Countermeasures*.

[b-IETF RFC 5246] IETF RFC 5246 (2008), *The Transport Layer Security (TLS) Protocol Version 1.2*.

[b-IETF RFC 5925] IETF RFC 5925 (2010), *The TCP Authentication Option*.

[b-IETF RFC 6265] IETF RFC 6265 (2011), *HTTP State Management Mechanism*.

[b-IETF RFC 6455] IETF RFC 6455 (2011), *The WebSocket Protocol*.

[b-IETF RFC 6797] IETF RFC 6797 (2012), *HTTP Strict Transport Security*.

[b-Kissner] Lea Kissner and Dawn Song, *Privacy-Preserving Set Operations*, CRYPTO 2005.

[b-Mirkovic] Jelena Mirkovic et Peter Reiher, *A Taxonomy of DDoS Attack and DDoS Defense Mechanisms*, ACM SIGCOMM Computer Communication Review, 34(2), avril 2004.

[b-Paxson] Vern Paxson, *An Analysis of Using Reflectors for Distributed Denial-of-Service Attacks*, ACM SIGCOMM Computer Communication Review, 31(3), juillet 2001.

[b-SOAP] W3C, *Simple Object Access Protocol*.
SOAP Version 1.2 Part 1: Messaging Framework, (2007).
SOAP Version 1.2 Part 2: Adjuncts, (2007).

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