Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

X.1606

(09/2020)

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

Sécurité de l'informatique en nuage – Conception de la sécurité de l'informatique en nuage

Exigences de sécurité pour l'environnement des applications de communication en tant que service

Recommandation UIT-T X.1606

Union internationale des télécommunications

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 (1)	
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 (1)	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 spam	X.1230–X.1249
Gestion des identités	X.1250–X.1279
APPLICATIONS ET SERVICES SÉCURISÉS (2)	
Communications d'urgence	X.1300–X.1309
Sécurité des réseaux de capteurs ubiquitaires	X.1310–X.1319
Sécurité des réseaux électriques intelligents	X.1330–X.1339
Courrier certifié	X.1340–X.1349
Sécurité de l'Internet des objets (IoT)	X.1360–X.1369
Sécurité des systèmes de transport intelligents	X.1370–X.1389
Sécurité de la technologie des registres distribués	X.1400–X.1449
Protocoles de sécurité (2)	X.1450–X.1459
ECHANGE D'INFORMATIONS SUR LA CYBERSÉCURITÉ	
Aperçu général de la cybersécurité	X.1500–X.1519
Échange concernant les vulnérabilités/les états	X.1520–X.1539
Échange concernant les événements/les incidents/l'heuristique	X.1540–X.1549
Échange de politiques	X.1550–X.1559
Heuristique et demande d'informations	X.1560–X.1569
Identification et découverte	X.1570–X.1579
Échange 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 œuvre de la sécurité de l'informatique en nuage	X.1660–X.1679
Sécurité de l'informatique en nuage (autres)	X.1680–X.1699
COMMUNICATIONS QUANTIQUES	
Terminologie	X.1700–X.1701
Générateur quantique de nombres aléatoires	X.1702–X.1709
Cadre de sécurité pour les réseaux QKDN	X.1710–X.1711
Conception de la sécurité pour les réseaux QKDN	X.1712–X.1719
Techniques de sécurité pour les réseaux QKDN	X.1720–X.1729
SÉCURITÉ DES DONNÉES	
Sécurité des mégadonnées	X.1750–X.1759
SÉCURITÉ DE LA 5G	X.1800–X.1819

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

Recommandation UIT-T X.1606

Exigences de sécurité pour l'environnement des applications de communication en tant que service

Résumé

La Recommandation UIT-T X.1606 recense les menaces de sécurité et contient des recommandations concernant les exigences de sécurité pour l'environnement des applications de communication en tant que service (CaaS). Elle décrit les scénarios et les caractéristiques des applications CaaS dotées de capacités de multicommunication. Elle recense en outre les menaces qui découlent des caractéristiques uniques des applications CaaS et contient des recommandations relatives aux exigences de sécurité appropriées pour les applications CaaS.

Historique

Edition	Recommandation	Approbation	Commission d'études	Identifiant unique*
1.0	UIT-T X.1606	03-09-2020	17	11.1002/1000/14265

Mots clés

CaaS, informatique en nuage, risque, exigence de sécurité.

* 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 on 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.1606

Exigences de sécurité pour l'environnement des applications de communication en tant que service

1 Domaine d'application

La présente Recommandation porte essentiellement sur les exigences de sécurité pour l'environnement des applications de communication en tant que service (CaaS), qui diffèrent de celles applicables à l'environnement des applications de logiciel en tant que service (SaaS) telles qu'identifiées dans [UIT-T X.1602]. Les applications CaaS des organisations de télécommunication associent les capacités de communication des télécommunications et de l'Internet. La convergence débouche sur certaines caractéristiques uniques des applications CaaS, qui sont soumises à des risques spécifiques. La présente Recommandation recense ces risques et fournit des recommandations relatives aux exigences appropriées en matière de sécurité.

La mesure de ces exigences tient compte des obligations légales et réglementaires nationales auxquelles les applications CaaS sont soumises au sein des différents États Membres dont elles relèvent. Le texte est établi selon la méthode décrite au paragraphe 10 de [UIT-T X.1601].

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.

[UIT-T X.1601] Recommandation UIT-T X.1601 (2015), *Cadre de sécurité applicable à l'informatique en nuage.*

[UIT-T X.1602] Recommandation UIT-T X.1602 (2016), *Exigences de sécurité pour l'environnement des applications de logiciel en tant que service.*

[UIT-T Y.3501] Recommandation UIT-T Y.3501 (2016), *Cadre et exigences de haut niveau applicables à l'informatique en nuage.*

3 Définitions

3.1 Termes définis ailleurs

La présente Recommandation utilise les termes suivants définis ailleurs:

3.1.1 authentification [UIT-T X.1601]: vérification de l'identité d'un utilisateur, d'un processus ou d'un dispositif souvent indispensable pour pouvoir accéder aux ressources d'un système d'information.

3.1.2 capacité [b-ISO 15531-1]: qualité permettant d'accomplir une activité donnée.

3.1.3 informatique en nuage [b-UIT-T Y.3500]: modèle permettant d'offrir un accès via le réseau à un ensemble modulable et élastique de ressources physiques ou virtuelles mutualisables, fournies et administrées à la demande et en libre-service.

NOTE – Comme exemples de ressources, on peut citer les serveurs, les systèmes d'exploitation, les réseaux, les logiciels, les applications et les équipements de stockage.

3.1.4 service en nuage [b-UIT-T Y.3500]: une ou plusieurs capacités offertes par l'intermédiaire de l'informatique en nuage demandées à l'aide d'une interface définie.

3.1.5 client d'un service en nuage [b-UIT-T Y.3500]: partie à une relation commerciale aux fins de l'utilisation de services en nuage.

NOTE – Une relation commerciale n'implique pas nécessairement des accords financiers.

3.1.6 partenaire de services en nuage [b-UIT-T Y.3500]: partie fournissant un appui ou une aide aux activités d'un fournisseur de services en nuage, d'un client de services en nuage, ou des deux.

3.1.7 fournisseur de services en nuage [b-UIT-T Y.3500]: partie qui met à disposition des services en nuage.

3.1.8 utilisateur de services en nuage [b-UIT-T Y.3500]: personne physique, ou entité agissant en son nom, associée à un client de services en nuage qui utilise des services en nuage.

NOTE – Comme exemples de ces entités, on peut citer les dispositifs et applications.

3.1.9 communications en tant que service (CaaS) [b-UIT-T Y.3500]: catégorie de services en nuage pour laquelle la capacité fournie au client du service en nuage est une interaction et une collaboration en temps réel.

NOTE – La communication CaaS peut correspondre à la fourniture de capacités de plate-forme et de capacités d'application.

3.1.10 multilocataires [b-UIT-T Y.3500]: attribution de ressources physiques ou virtuelles selon laquelle plusieurs locataires ainsi que leurs calculs et leurs données sont isolés les uns des autres et inaccessibles entre eux.

3.1.11 orchestration [b-UIT-T Y.3100]: dans le cadre des systèmes IMT-2000, processus visant l'agencement, la coordination, l'instanciation et l'utilisation automatisés des fonctions et des ressources du réseau pour les infrastructures physiques et virtuelles sur la base de critères d'optimisation.

3.1.12 logiciel en tant que service (SaaS) [b-UIT-T Y.3500]: catégorie de services en nuage pour laquelle le type de capacité en nuage fourni au client de services en nuage correspond à des capacités d'application.

3.2 Termes définis dans la présente Recommandation

Aucun.

4 Abréviations et acronymes

La présente Recommandation utilise les abréviations et acronymes suivants:

CaaS communications en tant que service (*communications as a service*)

CSC client de services en nuage (*cloud service customer)*

CSN partenaire de services en nuage (*cloud service partner*)

CSP fournisseur de services en nuage (*cloud service provider*)

CSU utilisateur de services en nuage (*cloud service user*)

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

GSM système mondial de communications mobiles (*global system for mobile communications*)

IAM gestion des identités et de l'accès (*identity and access management*)

IaaS infrastructure en tant que service (*infrastructure as a service*)

ID identificateur

MMS service de messagerie multimédia (*multimedia messaging service*)

NaaS réseau en tant que service (*network as a service*)

OS système d'exploitation (*operating system*)

PaaS plate-forme en tant que service (*platform as a service*)

PC ordinateur personnel (*personal computer*)

QR réponse rapide (*quick response*)

SaaS logiciel en tant que service (*software as a service*)

SDK kit de développement logiciel (*software development kit*)

SIM module d'identification de l'abonné (*subscriber identity module*)

SMS service de messages courts (*short message service*)

URL localisateur uniforme de ressources (*uniform resource locator*)

(U)SIM Module d'identité d'abonné (universel) (*universal) subscriber identity module*)

VoLTE téléphonie utilisant la technologie LTE (évolution à long terme) (*voice over long term evolution*)

VPN réseau privé virtuel (*virtual private network*)

5 Conventions

Dans la présente Recommandation, il n'est fait aucune différence entre les expressions "serveur" et "serveur virtuel".

6 Présentation générale des applications de communication en tant que service

La définition des applications de communication en tant que service (CaaS) est donnée au paragraphe 3.1.9. Les exigences générales recommandées concernant les applications CaaS sont l'ouverture des capacités de communication, le support logiciel de communication et des communications unifiées (voir paragraphe 11 de [UIT-T Y.3501]).

Conformément à la pratique professionnelle, les applications CaaS sous-tendent ou soutiennent généralement les capacités suivantes:

– combinaison de services de télécommunication et de services Internet;
– communication en temps réel;
– synchronisation multi-dispositifs;
– isolation des ressources de communication;
– mise à jour de la présence des utilisateurs;
– conversation ou réunion de groupe;
– intégration avec d'autres logiciels en tant que service (SaaS);
– opt-in ou opt-out de l'utilisateur;
– personnalisation du processus de service;
– partage des données ou des fichiers;

– gestion des identités et de l'accès (IAM).

La Figure 6-1 présente un modèle de service général CaaS, qui se décline en quatre couches: "utilisateur"; "accès"; "service"; et "ressource".

– La couche "utilisateur" comprend les terminaux d'utilisateur de services en nuage (CSU) qui peuvent gérer certains clients CaaS et accéder à l'Internet de même qu'aux réseaux de télécommunications.

– La couche "accès" présente divers types de tunnels, permettant généralement aux terminaux d'accéder au service CaaS ciblé.

– La couche "service", qui est aussi la couche CaaS, est détenue par un fournisseur de services en nuage (CSP), qui s'appuie sur les ressources internes et externes nécessaires à l'exploitation des services. Cette couche personnalise les processus de service et attribue les ressources aux clients de services en nuage (CSC), entretient un réseau de service (virtuellement) dynamique pour un client CSC et ses utilisateurs et isole les ressources informatiques et les réseaux de communication pour tous les clients CSC.

– La couche "ressource" fournit les ressources de base en termes d'infrastructure pour le traitement et la communication des données, dont une partie pourrait être l'infrastructure en tant que service (IaaS), la plate-forme en tant que service (PaaS) et le réseau en tant que service (NaaS).

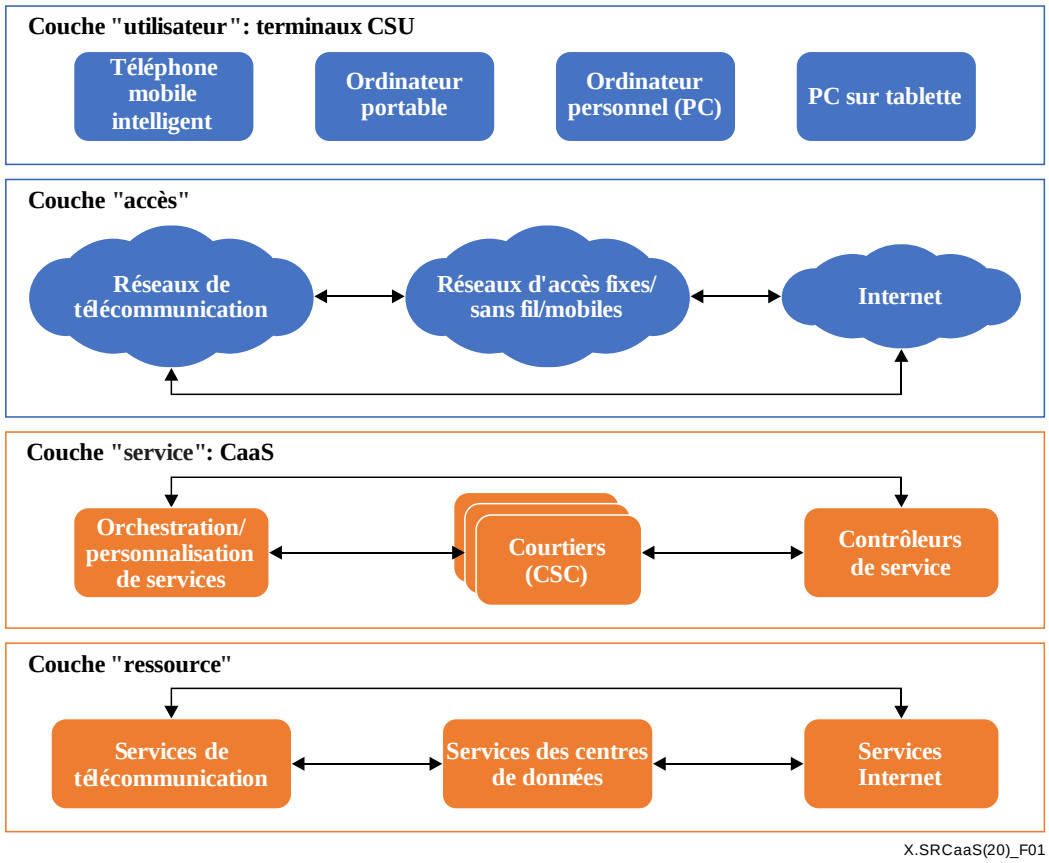

Figure 1 – Modèle de service général CaaS

Dans la suite de la présente Recommandation:

– Le paragraphe 7 analyse les menaces de sécurité pour les applications CaaS, qui ciblent une ou plusieurs couches.

– Le paragraphe 8 contient des recommandations concernant les exigences de sécurité pour les applications CaaS, qui s'appliquent aux menaces sur trois couches:

- couche du terminal de l'utilisateur des services en nuage (CSU);
- couche des applications de communication en tant que service (CaaS);
- couche des ressources de service.

La couche d'accès n'est pas concernée ici, car ses capacités de sécurité ne sont pas contrôlées par les applications CaaS, bien que son niveau de sécurité puisse être évalué ou surveillé par les applications CaaS et l'utilisateur de services en nuage.

7 Menaces de sécurité pour les applications de communication en tant que service (CaaS)

Les menaces et problèmes de sécurité concernant l'informatique en nuage, tels qu'identifiés dans [UIT-T X.1601] (également listés à l'Appendice I), peuvent s'appliquer à divers scénarios CaaS. De plus, certaines menaces spécifiques aux applications CaaS sont décrites aux paragraphes 7.1 à 7.8.

7.1 Menaces liées à l'identité

Les applications de communication en tant que service (CaaS) reposent avant tout sur des capacités de communication unifiée et se démarquent ainsi légèrement des applications de logiciel en tant que service (SaaS). Les applications CaaS prennent en charge la plupart des types de terminaux ou de systèmes d'exploitation (OS) courants, tels que les téléphones intelligents ou ordinateurs personnels (PC).

Aussi, les applications CaaS peuvent-elles, dans le cadre du modèle de communication multipoint à multipoint, être exposées à des menaces spécifiques en cas d'utilisation abusive de l'identité.

7.1.1 Vol de justificatifs d'identité

Par souci de commodité pour les utilisateurs de services en nuage, de nombreuses applications de communication en tant que service (CaaS) adoptent une solution d'authentification par numéro de mobile (identificateur mobile) ou par nom d'utilisateur et mot de passe, ou les deux à la fois. Dans ce cas, le nom d'utilisateur par défaut dans la solution peut être configuré comme l'identificateur mobile. De plus, certaines applications CaaS prennent en charge un utilisateur de services en nuage avec un identificateur pour accéder au service avec plusieurs terminaux simultanément, ou gèrent la synchronisation de l'historique des communications entre plusieurs terminaux.

La sécurité de l'authentification par numéro de mobile repose largement sur la confiance dans l'authentification, le chiffrement de l'opérateur de réseau mobile et la carte de module d'identité d'abonné (universel) détenant les justificatifs d'information. Les réseaux mobiles présentent certaines vulnérabilités (prouvées sur le terrain), en particulier le réseau GSMA (*Global System for Mobile Communications Alliance*), qui pourraient affaiblir la confiance et conduire (temporairement) au vol de justificatifs d'identité. Par exemple, certains types de cartes de module d'identité d'abonné (SIM) peuvent être dupliqués physiquement et certains codes d'authentification dynamique transférés par service de messages courts (SMS) dans les réseaux de communication GSM (*global system for mobile communications*) peuvent être interceptés. Les clés de chiffrement temporaires interceptées peuvent également être utilisées abusivement pour détourner l'identificateur temporairement et silencieusement.

L'authentification par nom d'utilisateur et mot de passe peut, quant à elle, donner à l'auteur de l'abus la possibilité d'utiliser ce type d'authentification avec d'autres terminaux qualifiés pour surveiller un utilisateur de services en nuage (simultanément). Par exemple, s'il peut utiliser un terminal mobile CSU avec une carte (U) SIM ou des justificatifs de cartes SIM logicielles, l'auteur de l'abus peut obtenir le nom d'utilisateur dans le cache et utiliser le mécanisme de réinitialisation pour définir un nouveau mot de passe qui sera gardé en cache dans le terminal. L'utilisateur de services en nuage peut très bien ne pas réaliser que le mot de passe a été réinitialisé et le contenu de la communication en cours de même que son historique pourraient tous deux être surveillés en silence par l'auteur de l'abus.

7.1.2 Contrefaçon d'identité

Si un justificatif d'identité est volé auprès d'un utilisateur de services en nuage ou intercepté de manière abusive, celui-ci peut être utilisé frauduleusement pour accéder au service appartenant à un client CSC auquel l'utilisateur est associé. Parallèlement, l'auteur de l'abus peut aussi obtenir une entité sociale dotée du justificatif d'identité CSU voire contrefaire une autre entité sociale ou en créer une nouvelle. Cela peut être observé notamment au travers de la fonction "présence".

La fonction "présence" est l'une des principales fonctions CaaS, qui implémente généralement l'autoportrait d'un utilisateur de services en nuage avec une image de petite taille et un texte court. Elle permet aux utilisateurs qui sont associés au même client CSC d'obtenir un accusé de réception rapide auprès d'un utilisateur de services en nuage. Cependant, la présence d'une identité utilisée abusivement peut être falsifiée et livrée à des activités frauduleuses. L'auteur d'un abus peut ainsi se saisir de données financières confidentielles d'une entreprise auprès d'un comptable en falsifiant sa présence en tant que membre du conseil d'administration.

Les conversations vidéo en temps réel peuvent être une configuration standard des applications CaaS. La scène montrée par l'identité abusée à travers le flux vidéo peut également être falsifiée pour renforcer l'authenticité de l'entité sociale et l'activité frauduleuse.

7.2 Menaces liées à la gestion du cycle de vie des comptes

L'utilisateur de services en nuage, au même titre que le client de services en nuage ou le fournisseur de services en nuage, a normalement le droit d'exiger la suppression d'un compte sur lequel il a autorité. Dans le cycle de vie global des comptes, lorsqu'un compte doit être retiré, il convient de définir en amont ce que le fournisseur de services en nuage est censé faire en ce qui concerne la communication du contenu et des informations sur les comptes via l'ensemble de son service CaaS, à savoir si le client peut conserver ces données dans son espace logique ou si l'utilisateur peut conserver ces données dans son terminal.

L'élimination ou le vol d'un terminal peut également signifier que toutes les informations de compte mises en cache doivent être effacées que toutes les données associées supprimées.

7.3 Menaces liées à l'orchestration

Grâce à la fonction d'orchestration (voir [b-UIT-T Y.3100]), un client de services en nuage (CSC) peut personnaliser lui-même ses processus et capacités de service ou mandater son fournisseur pour le faire. Par exemple, un client peut ajuster le processus et le privilège de gérer l'appartenance à un groupe de discussion et également abaisser ou augmenter les limites de la plage de recherche de contacts pour l'utilisateur.

En termes d'exigences client, un fournisseur de services en nuage peut permettre à plus de deux clients de partager leurs contacts et même de communiquer directement entre eux, ainsi que de pouvoir fusionner plusieurs clients en un client de plus grande taille.

Enfin, pour implémenter une nouvelle fonction de service, un fournisseur de services en nuage peut améliorer ou déclasser les préconditions de sécurité sur un réseau auquel un utilisateur de services en nuage a accès.

Toute orchestration, si l'on ne prend pas pleinement en compte la sécurité, peut impacter négativement l'isolation des informations et des services. Ainsi, si l'application CaaS d'un client de services en nuage est orchestrée de manière à intégrer les services voix et message d'un réseau GSM, il est presque impossible de mettre en œuvre la fonction d'isolation de bout en bout, car les entités du réseau GSM ont adopté des technologies précoces ne pouvant prendre en charge les fonctions d'isolation. Si un type de réseau non sécurisé est autorisé par orchestration à prendre en charge une fonctionnalité de service plus flexible, cela peut augmenter le niveau de risque pour les applications CaaS de clients CSC. Par exemple, le fait de reconfigurer l'exigence d'accès au réseau privé virtuel (VPN) en tant que

méthode d'isolation – de l'obligation à l'option – pour garantir la qualité de la conversation vidéo dans une application CaaS, augmente le risque d'interception.

7.4 Menaces liées au contexte des terminaux

Le contexte de sécurité des terminaux dans une application CaaS peut être incertain, en particulier si les terminaux en question sont des téléphones intelligents ou des dispositifs portables. Le fait que ces terminaux soient des biens personnels augmente encore la complexité. Ces terminaux pourraient être utilisés par des proches ou des visiteurs de l'utilisateur. L'écran d'un terminal pourrait être projeté ou partagé avec un autre écran rendant ainsi possible un enregistrement sur un écran inconnu. Les vulnérabilités d'un terminal pourraient être exposées plus directement à un attaquant dans un réseau non sécurisé. Le contenu de communication via une application CaaS pourrait être déchiffré et stocké dans un terminal. Ces différents cas de figure peuvent entraîner une fuite de données.

Si un attaquant peut contrôler un terminal (à distance ou en local), il peut l'utiliser abusivement pour exploiter les vulnérabilités d'une application CaaS et de son utilisateur. Si plusieurs terminaux sont contrôlés simultanément dans le cadre d'un botnet, l'attaquant pourrait également déclencher une attaque par déni de service réparti (DDoS).

7.5 Menaces liées aux spams et distribution de logiciels malveillants

Un utilisateur de services en nuage peut être harcelé voire hameçonné via une attaque de spam provenant d'autres utilisateurs au travers d'une application CaaS. Dans la majorité des cas, il est effectivement difficile pour un utilisateur de services en nuage de déterminer rationnellement s'il peut faire confiance aux informations d'un localisateur uniforme de ressource (URL) court ou d'un code de réponse rapide (QR). Il peut rapidement accéder à un site web de hameçonnage ou télécharger un logiciel malveillant.

7.6 Menaces liées aux modules complémentaires

Il est courant qu'une application CaaS fournisse des modules complémentaires dans le cadre de son service de base, tels que le partage de fichiers, un navigateur web intégré, un système de gestion de contenu et même des services de commerce électronique. Dans la plupart des cas, ces modules complémentaires sont plutôt légers.

Les vulnérabilités de ces modules complémentaires peuvent représenter des menaces importantes pour les applications CaaS. Par exemple, un clic sur une URL courte non sécurisée peut appeler les extensions du navigateur web, lesquelles n'ont pas la capacité de contrer une adresse web dangereuse, ce qui augmente considérablement le risque de voir la sécurité de l'utilisateur et même de l'application mise en danger.

Certains modules complémentaires peuvent inciter l'utilisateur à quitter l'application en cours pour basculer vers un autre service non sollicité. Dans la mesure où il n'est pas au courant de la bascule, l'utilisateur n'est pas en capacité d'ajuster sa confiance de manière appropriée et en temps opportun, ce qui provoque de sérieux dommages (plus de vulnérabilités exploitées, extorsion, rançongiciel, etc.).

7.7 Menaces liées au kit de développement logiciel

Une application CaaS peut fournir un kit de développement logiciel (SDK) pour encourager l'intégration par d'autres applications ou services de logiciels en tant que service (SaaS). Qui dit intégration dit, dans une certaine mesure, confiance entre l'application de communication en tant que service (CaaS) et l'utilisateur du kit de développement logiciel qui lui est rattaché. Par conséquent, les vulnérabilités de l'utilisateur du kit peuvent accroître les menaces d'attaques ou d'abus pour l'application CaaS.

Sachant qu'un terminal peut avoir plusieurs justificatifs d'identité pour des clients de services en nuage (CSC) différents, l'utilisateur du kit SDK d'une application CaaS peut utiliser ces justificatifs abusivement et illégalement sans avoir obtenu la permission d'accéder à d'autres clients.

7.8 Menaces liées aux vulnérabilités du réseau de télécommunications

Si, en plus de l'accès à l'Internet, une application de communication en tant que service (CaaS) intègre d'autres capacités de l'opérateur de réseau de télécommunications, telles que les SMS, la téléphonie utilisant la technologie LTE (VoLTE), les appels avec commutation par circuits, les services de messagerie multimédia (MMS) et localisation, la sécurité du réseau de télécommunications peut avoir des conséquences directes sur l'application CaaS.

Toute exploitation abusive des vulnérabilités du réseau de télécommunications peut entraîner une fuite de données de l'application CaaS. De même, toute attaque lancée contre le réseau de télécommunications, en particulier sur les nœuds connectés aux serveurs CaaS, peut augmenter la surface d'exposition de l'application CaaS.

De plus, considérant que les terminaux modernes disponibles sur le marché peuvent changer activement de réseau d'accès et de réseau privé virtuel (VPN) entre différents fournisseurs selon des politiques définies au préalable, et ce sans tenir réellement compte de la confiance et de l'authenticité du réseau d'accès, l'utilisateur des services en nuage peut ne pas avoir connaissance de l'utilisation d'un environnement réseau non sécurisé, ce qui peut entraîner une fuite d'informations confidentielles.

8 Exigences de sécurité pour les applications de communication en tant que service (CaaS)

Les exigences de sécurité pour les applications de logiciel en tant que service (SaaS), telles qu'identifiées dans [UIT-T X.1602], s'appliquent aux scénarios CaaS. De plus, le présent paragraphe formule des exigences de sécurité supplémentaires pour faire face aux menaces identifiées au paragraphe 7.

8.1 Gestion des identités et de l'accès

8.1.1 Gestion des identités

Les applications de communication en tant que service (CaaS) devraient fixer une limite supérieure concernant le nombre de terminaux simultanés partageant les mêmes justificatifs d'information. Les applications CaaS peuvent vérifier un terminal avec le matériel et l'identification de service nécessaires en tant que contrôleur principal, ce qui peut autoriser l'accès par d'autres terminaux à la demande.

Les applications de communication en tant que service (CaaS) peuvent surveiller les terminaux simultanés avec le même justificatif d'identité et garder tous les terminaux (ou au moins le contrôleur principal) informés du dernier état des autres terminaux simultanés. Un utilisateur de services en nuage peut utiliser le contrôleur principal ou adopter une authentification plus sûre (telle qu'une authentification de contournement) pour obliger un terminal donné à se déconnecter, interdire tout accès ultérieur par son biais voire supprimer les informations résiduelles qu'il contient.

Les applications de communication en tant que service (CaaS) peuvent envisager d'orienter un utilisateur de services en nuage vers l'utilisation de plusieurs justificatifs (et au moins différents mots de passe) pour différents clients CSC, ce qui peut diminuer le risque d'utilisation d'un justificatif volé pour accéder à plusieurs clients CSC.

8.1.2 Contrôle d'accès

À supposer que la simultanéité de terminaux pour un seul justificatif d'identité soit une capacité courante des applications de communication en tant que service (CaaS), il serait judicieux de permettre aux applications CaaS d'acquérir et de mettre à jour la localisation géographique des

terminaux de façon à ce qu'elles puissent repérer toute anomalie d'accès aux terminaux. Sachant qu'un terminal peut accéder à plusieurs réseaux en même temps, les applications CaaS peuvent envisager la possibilité d'utiliser des informations multidimensionnelles pour vérifier l'authenticité de la localisation.

Dans l'éventualité où la sécurité du réseau ne peut être garantie, un réseau privé virtuel (VPN) peut constituer un bon choix pour améliorer la sécurité de l'infrastructure. Les applications de communication en tant que service (CaaS) devraient envisager d'exiger qu'un utilisateur ou client de services en nuage utilise un service VPN obligatoire et d'interdire à l'un comme à l'autre d'adopter tout autre service VPN comme bond ou relais pour accéder au service VPN obligatoire. Un réseau privé virtuel optionnel ou non fiable pourrait masquer la localisation d'un terminal et augmenter par là même le risque d'attaque par un intermédiaire.

Par ailleurs, si le risque d'interception d'un SMS du GSM ne peut pas être accepté par le client CSC, les applications de communication en tant que service (CaaS) devraient envisager de surveiller le type de réseau auquel les utilisateurs accèdent et refuser l'utilisation d'un SMS comme méthode d'authentification si l'utilisateur se trouve sur un réseau GSM. À défaut, les applications CaaS peuvent simplement exclure la ressource SMS du GSM pour le client CSC.

8.1.3 Vérification d'identité

Sachant qu'un utilisateur de services en nuage peut utiliser des données masquées, inexactes et même falsifiées dans le cadre d'un auto-portrait, les applications de communication en tant que service (CaaS) devraient alerter tous les utilisateurs sur le fait qu'une identité sociale dans leurs contacts peut être vérifiée par un tiers de confiance. Ce tiers de confiance peut être un client de services en nuage (CSC), une application de communication en tant que service (CaaS) ou toute autre autorité indépendante. La vérification peut être obligatoire ou optionnelle. Dans le cas où elle est optionnelle, il peut être nécessaire d'avertir l'utilisateur que le fournisseur CSP ou le client CSC ne peut être tenu pour responsable de l'authenticité des identités sociales dans le client CSC.

Sachant que l'identité sociale ou commerciale d'un client CSC utilisée pour devenir client d'une application CaaS pourrait être totalement différente de celle utilisée en public, il est suggéré que l'application CaaS envisage de comparer l'identité déclarée d'un client CSC en public avec les informations disponibles pour empêcher une éventuelle fraude visant les particuliers ou les entreprises. Par exemple, un client CSC malveillant pourrait prétendre être une organisation caritative et falsifier des objets de don pour tromper l'utilisateur.

8.1.4 Gestion des comptes

Sachant qu'un utilisateur de services en nuage peut posséder au moins un compte sous un client de services en nuage (CSC) et qu'un client CSC peut lui aussi posséder au moins un compte sous une application de communication en tant que service (CaaS), les applications CaaS devraient fournir à l'utilisateur ou au client de services en nuage le privilège d'un accès complet aux données, en fonction de la propriété des données. Par ailleurs, si un compte doit être annulé ou supprimé, les applications CaaS devraient fournir une capacité fiable pour détruire physiquement les données du compte du côté du terminal, du côté du service et du côté du réseau, conformément aux conditions de l'autorisation légale du propriétaire des données.

8.2 Sécurité des terminaux

8.2.1 Sécurité interne

Les applications de communication en tant que service (CaaS) devraient définir des mesures techniques, telles qu'un outil de sécurité ou un module de sécurité intégré aux terminaux CSU, pour procéder à un contrôle de sécurité périodique ou à la demande. Ce contrôle de sécurité pourrait déterminer si le contexte d'un terminal CSU remplit ou non les exigences de sécurité obligatoires avant d'accéder à une application de communication en tant que service (CaaS). Dans l'éventualité où

un terminal CSU échoue à ce contrôle, l'application CaaS pourrait refuser de fournir (partiellement) les services. Dans le même temps, l'application CaaS devrait orienter l'utilisateur de services en nuage vers l'élimination des risques de sécurité découverts et pourrait corriger les vulnérabilités directement avec l'autorisation de l'utilisateur de services en nuage.

8.2.2 Sécurité externe

Les logiciels utilisés sur les terminaux CSU devraient être fournis par les applications de communication en tant que service (CaaS). Les applications CaaS devraient également mettre à disposition une plate-forme ou des sources (officielles ou autorisées) de distribution de logiciels sécurisés. Elles devraient aussi permettre aux terminaux CSU de lancer le mécanisme de vérification pour contrôler l'authenticité et l'intégrité avant la mise à jour. Le système d'exploitation ou même le logiciel installé sur les terminaux CSU devrait avoir la capacité de remonter les informations en cas d'échec de la mise à jour.

Dans la majorité des cas, la mise à jour de sécurité des logiciels sur les terminaux est facultative. Cependant, dans le cas où une vulnérabilité est susceptible d'entraîner de sérieux dommages pour les applications CaaS, un client CSC ou même un autre utilisateur CSU, et où une mise à jour de sécurité du logiciel sur le terminal pourrait corriger cette vulnérabilité, les applications CaaS peuvent envisager de refuser temporairement l'accès au service par un terminal CSU avant exécution de la mise à jour, conformément aux conditions d'utilisation.

La distribution de logiciels de terminal par les applications CaaS est généralement publique. Toutefois, un client CSC peut dans certains cas exiger des logiciels personnalisés et demander à ce que la distribution soit limitée, par exemple aux seuls clients CSC. La distribution devrait alors être privée. Une authentification bidirectionnelle entre un terminal CSU et une application CaaS serait nécessaire avant de télécharger ou de mettre à jour un logiciel.

8.3 Sécurité des services

8.3.1 Sécurité en matière d'orchestration

Avant qu'un changement d'orchestration ne soit déployé ou configuré, il y a lieu d'évaluer si ce changement peut affecter la limite de sécurité, diminuer le niveau de sécurité ou nuire à la relation de confiance. Dans l'hypothèse de la survenue de certains effets négatifs, les exigences de sécurité ou accords y relatifs passés pour les applications de communication en tant que service (CaaS) devraient être renégociés et réagréés par le fournisseur, le client et même l'utilisateur de services en nuage.

8.3.2 Lutte contre le spam

Les applications de communication en tant que service (CaaS) devraient envisager d'intégrer une fonction antispam comme capacité facultative pour le client de services en nuage (CSC). Un fournisseur de services en nuage (CSP) pourrait également envisager d'autoriser le client CSC à intégrer dans sa propre application Caas une fonction tierce de lutte contre le spam. Selon les accords de service et accords d'utilisateur conclus entre les fournisseurs, les clients et les utilisateurs de services en nuage, des contraintes différentes peuvent être imposées sur l'opportunité et la manière d'utiliser une fonction de lutte contre le spam.

Par exemple, si tous les utilisateurs de services en nuage sont employés chez le même client CSC et si l'application CaaS correspondante est utilisée au profit exclusif d'un client CSC, alors l'accord passé entre le fournisseur CSP et le client CSC peut suffire pour utiliser une fonction de lutte contre le spam.

A l'inverse, si certains utilisateurs de services en nuage sont clients d'un client CSC, ces utilisateurs devront autoriser le client de services en nuage (et le fournisseur de services en nuage) à les aider dans la lutte contre le spam.

De façon générale, la fonction de lutte contre le spam doit se situer du côté du terminal, du côté du nuage ou les deux à la fois. Pour les technologies alternatives utilisées dans la fonction, voir [b-UIT-T X.1244] et [b-UIT-T X.1246].

8.4 Coordination en matière de sécurité

8.4.1 Sécurité des modules complémentaires et du kit de développement logiciel

Les applications de communication en tant que service (CaaS) ne devraient autoriser que des modules complémentaires ayant passé avec succès le contrôle de sécurité disponible sur leur service. Le logiciel du terminal devrait fournir à l'application CaaS les moyens de contrôler et d'analyser toute anomalie portant sur les modules complémentaires. L'application CaaS peut, sur la base d'une liste blanche, limiter la capacité d'un module complémentaire à accéder à un lien externe ou à un nom de domaine.

Si un module complémentaire nécessite d'accéder aux données client pour fournir le service, l'obtention d'une autorisation claire de l'utilisateur de services en nuage est une précondition. Les accès aux données client enregistrés par un module complémentaire devront être clairement consignés pour faciliter les audits ultérieurs.

Un kit de développement logiciel (SDK) pour les applications CaaS devrait pouvoir contrôler et analyser les anomalies d'application ou les logiciels en tant que service (SaaS) qui intègrent le kit SDK. Le kit SDK devrait chiffrer et isoler les justificatifs d'identité afin d'éviter tout abus éventuel. Par exemple, l'application A et l'application B intègrent toutes les deux le même kit de développement logiciel et sont présentes dans le même terminal, mais aucune des deux ne peut accéder aux justificatifs d'identité de son homologue.

8.4.2 Sécurité de l'infrastructure

Les applications de communication en tant que service (CaaS) devraient être conscientes des menaces venant de l'infrastructure, par exemple lorsqu'elles intègrent les capacités de service des réseaux de télécommunication telles que les SMS et appels vocaux. Les applications CaaS devraient envisager la mise en place d'une passerelle entre elles et les réseaux de télécommunication pour contrôler, prévenir ou filtrer les possibles spams et usurpations d'identité des services de télécommunication. Il serait bon que les applications CaaS puissent informer les utilisateurs de services en nuage au sujet des types de canaux ou de services de communication utilisés.

Appendice I

Guide rapide des menaces et problèmes de sécurité listés dans la Recommandation UIT-T X.1601

(Cet appendice ne fait pas partie intégrante de la présente Recommandation.)

Comme mentionné au paragraphe 7, les menaces et problèmes de sécurité concernant l'informatique en nuage, tels qu'identifiés dans [UIT-T X.1601], peuvent s'appliquer à divers scénarios CaaS. Cet Appendice présente l'ensemble des menaces et problèmes de sécurité listés dans [UIT-T X.1601] pour un contrôle rapide. Pour plus de détails, voir [UIT-T X.1601].

– Menaces de sécurité visant l'informatique en nuage
  a) Menaces de sécurité visant les clients de services en nuage (CSC)
    1) Perte et fuite de données
    2) Accès non sécurisé aux services
    3) Menaces internes
  b) Menaces de sécurité visant les fournisseurs de services en nuage (CSP)
    1) Accès non autorisé aux fonctions d'administration
    2) Menaces internes
– Problèmes de sécurité posés par l'informatique en nuage
  a) Problèmes de sécurité pour les clients de services en nuage (CSC)
    1) Répartition ambiguë des responsabilités
    2) Perte de confiance
    3) Perte de gouvernance
    4) Perte de confidentialité
    5) Indisponibilité des services
    6) Enfermement vis-à-vis du fournisseur de services en nuage
    7) Détournement de la propriété intellectuelle
    8) Perte d'intégrité d'un logiciel
  b) Problèmes de sécurité pour les fournisseurs de services en nuage (CSP)
    1) Répartition ambiguë des responsabilités
    2) Environnement partagé
    3) Incohérence ou conflit entre les mécanismes de protection
    4) Conflit juridictionnel
    5) Risques liés à l'évolution
    6) Migration et intégration médiocres
    7) Discontinuité de l'activité
    8) Enfermement vis-à-vis d'un partenaire de services en nuage
    9) Vulnérabilité de la chaîne d'approvisionnement
    10) Dépendance entre les logiciels
  c) Problèmes de sécurité pour les partenaires de services en nuage (CSN)
    1) Répartition ambiguë des responsabilités
    2) Détournement de la propriété intellectuelle
    3) Perte d'intégrité d'un logiciel

Appendice II

Mise en correspondance des menaces de sécurité et des exigences de sécurité

(Cet appendice ne fait pas partie intégrante de la présente Recommandation.)

Le Tableau I.1 met en correspondance les menaces et les exigences de sécurité, présentées respectivement aux paragraphes 7 et 8 de la présente Recommandation.

Tableau I.1 – Correspondance entre les menaces et les exigences de sécurité listées dans la présente Recommandation

Menaces présentées au paragraphe 7	Exigences correspondantes présentées au paragraphe 8
7.1 Menaces liées à l'identité	8.1 Gestion des identités et de l'accès
7.1.1 Vol de justificatifs d'identité	8.1.1 Gestion des identités 8.1.2 Contrôle d'accès 8.1.4 Gestion des comptes
7.1.2 Contrefaçon d'identité	8.1.3 Vérification d'identité 8.1.4 Gestion des comptes
7.2 Menaces liées à la gestion du cycle de vie des comptes	8.1.4 Gestion des comptes
7.3 Menaces liées à l'orchestration	8.3.1 Sécurité en matière d'orchestration
7.4 Menaces liées au contexte des terminaux	8.2 Sécurité des terminaux
7.5 Menaces liées aux spams et distribution de logiciels malveillants	8.2 Sécurité des terminaux 8.3.2 Lutte contre le spam
7.6 Menaces liées aux modules complémentaires	8.4.1 Sécurité des modules complémentaires et du kit de développement logiciel
7.7 Menaces liées au kit de développement logiciel	8.4.1 Sécurité des modules complémentaires et du kit de développement logiciel
7.8 Menaces liées aux vulnérabilités du réseau de télécommunication	8.4.2 Sécurité de l'infrastructure

Bibliography

[b-ITU-T X.1244] Recommendation ITU-T X.1244 (2008), *Aspects généraux de la lutte contre le spam dans les applications multimédias IP*.

[b-ITU-T X.1246] Recommendation ITU-T X.1246 (2015), *Technologies intervenant dans la lutte contre le spam vocal dans les organisations de télécommunication*.

[b-ITU-T Y.3100] Recommendation ITU-T Y.3100 (2017), *Réseaux IMT-2020: termes et définitions*.

[b-ITU-T Y.3500] Recommendation ITU-T Y.3500 (2014) | ISO/IEC 17788:2014, *Technologies de l'information – Informatique en nuage – Présentation générale et vocabulaire*.

[b-ISO 15531-1] ISO 15531-1:2004, *Systèmes d'automatisation industrielle et intégration — Données de gestion de fabrication industrielle — Partie 1: Aperçu général*.

SÉRIES DES RECOMMANDATIONS UIT-T

Série A	Organisation du travail de l'UIT-T
Série D	Principes de tarification et de comptabilité et questions de politique générale et d'économie relatives aux télécommunications internationales/TIC
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	Environnement et TIC, changement climatique, déchets d'équipements électriques et électroniques, efficacité énergétique; 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	Qualité de transmission téléphonique, installations téléphoniques et réseaux locaux
Série Q	Commutation et signalisation et mesures et tests associés
Série R	Transmission télégraphique
Série S	Équipements 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, réseaux de prochaine génération, Internet des objets et villes intelligentes
Série Z	Langages et aspects généraux logiciels des systèmes de télécommunication

Imprimé en Suisse
Genève, 2021