Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

X.1814

(09/2022)

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

Sécurité des IMT-2020

Lignes directrices relatives à la sécurité des systèmes de communication IMT-2020

Recommandation UIT-T X.1814

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 (1)	X.1140–X.1149
Sécurité des applications (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.1350–X.1369
Sécurité des systèmes de transport intelligents	X.1370–X.1399
Sécurité de la technologie des registres distribués	X.1400–X.1429
Sécurité des applications (2)	X.1450–X.1459
Sécurité de la toile (2)	X.1470–X.1489
ÉCHANGE 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
Cyberdéfense	X.1590–X.1599
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
Protection des données	X.1770–X.1789
SÉCURITÉ DES IMT-2020	**X.1800–X.1819**

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

Recommandation UIT-T X.1814

Lignes directrices relatives à la sécurité des systèmes de communication IMT-2020

Résumé

Les dispositifs de l'Internet des objets (IoT) connectés et les applications mobiles nécessitent un accès au réseau hertzien résilient, sûr et à même de protéger la vie privée des utilisateurs. Les systèmes de communication IMT-2020 devraient être conçus de manière à répondre à ces exigences de haut niveau. Il est nécessaire de définir un cadre de sécurité pour les systèmes de communication IMT-2020, qui pourrait servir de base à l'élaboration de nouvelles Recommandations techniques détaillées sur les thèmes liés à la sécurité des IMT-2020.

La Recommandation UIT-T X.1814 identifie tous les éléments relatifs à la sécurité des systèmes de communication IMT-2020 et définit des lignes directrices sur la sécurité des systèmes de communication IMT-2020. Elle décrit une architecture générique des IMT-2020 et les domaines correspondants. En outre, elle recense les menaces qui pèsent sur chacun des éléments et indique les exigences de sécurité pour chacun d'eux, en tenant compte de la spécificité des fonctions du réseau. Cette Recommandation est fondée sur l'architecture de sécurité de la 5G élaborée par le 3GPP.

Historique

Édition	Recommandation	Approbation	Commission d'études	Identifiant unique*
1.0	UIT-T X.1814	02-09-2022	17	11.1002/1000/14992

Mots clés

Capacité, système de communication IMT-2020, informatique en périphérie à accès multiples, découpage de réseau, virtualisation des réseaux, lignes directrices relatives à la sécurité, menaces.

* 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 (TIC). 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.

À 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 ou par des droits d'auteur afférents à des logiciels, et dont l'acquisition pourrait être requise 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 responsables de la mise en œuvre de consulter les bases de données appropriées de l'UIT-T disponibles sur le site web de l'UIT-T à l'adresse http://www.itu.int/ITU-T/ipr/.

TABLE DES MATIÈRES

Page

Recommandation UIT-T X.1814

Lignes directrices relatives à la sécurité des systèmes de communication IMT-2020

1 Champ d'application

La présente Recommandation définit les lignes directrices relatives à la sécurité des systèmes de communication IMT-2020. Elle identifie tous les éléments relatifs à la sécurité de ces systèmes, par exemple l'équipement d'utilisateur, le réseau d'accès et le réseau central. Elle décrit une architecture générique des IMT-2020 et les domaines correspondants. En outre, elle recense les menaces qui pèsent sur chacun des éléments et indique les exigences en matière de capacités de sécurité pour chacun d'eux, en tenant compte de la spécificité des fonctions propres au réseau, comme l'informatique en périphérie à accès multiples, les réseaux pilotés par logiciel, la virtualisation dynamique des fonctions de réseau et le découpage de réseau. Cette Recommandation est fondée sur l'architecture de sécurité de la 5G élaborée par le 3GPP.

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. Toute recommandation ou autre référence étant sujette à révision, les utilisateurs de la présente Recommandation sont invités à rechercher la possibilité d'appliquer les éditions les plus récentes des recommandations et autres références énumérées ci-dessous. La liste des Recommandations 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.

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

[UIT-T X.1038] Recommandation UIT-T X.1038 (2016), *Exigences de sécurité et architecture de référence pour les réseaux pilotés par logiciel.*

3 Définitions

3.1 Termes définis ailleurs

3.1.1 La présente Recommandation utilise les termes de la Recommandation UIT-T X.800 suivants:

– contrôle d'accès;
– authentification;
– disponibilité;
– confidentialité;
– intégrité des données;
– respect de la vie privée;
– répudiation;
– service de sécurité.

De plus, la présente Recommandation emploie les termes additionnels suivants définis ailleurs:

3.1.2 mesure de sécurité [b-UIT-T X.1408]: mesure qui modifie un risque.

NOTE 1 – Les mesures de sécurité comprennent tous les processus, politiques, dispositifs, pratiques ou autres actions qui modifient un risque.

NOTE 2 – Il est possible que les mesures de sécurité ne puissent pas toujours aboutir à la modification voulue ou supposée.

3.1.3 attaque par déni de service réparti (DDoS) [b-UIT-T Y.4807]: accès non autorisé à une ressource de système ou introduction d'un retard dans les opérations ou les fonctions du système en vue de compromettre plusieurs systèmes, afin de submerger la largeur de bande ou les ressources du système visé, entraînant une perte de disponibilité pour les utilisateurs autorisés.

3.1.4 ligne directrice [b-UIT-T X.1401]: description précisant ce qu'il convient de faire et comment atteindre les objectifs fixés dans les politiques.

3.1.5 fonction de réseau [UIT-T Y.3100]: dans le contexte des IMT-2020, fonction de traitement au sein d'un réseau.

NOTE 1 – Les fonctions de réseau incluent, sans s'y limiter, les fonctionnalités des nœuds de réseau, par exemple la gestion des sessions, la gestion de la mobilité et les fonctions de transport, dont on définit le comportement fonctionnel et les interfaces.

NOTE 2 – Les fonctions de réseau peuvent être mises en œuvre dans un équipement matériel dédié ou dans un logiciel, de manière virtuelle.

NOTE 3 – Les fonctions de réseau ne sont pas considérées comme des ressources, mais toute fonction de réseau peut être instanciée en utilisant les ressources.

3.1.6 virtualisation des fonctions de réseau [b-UIT-T X.1811]: technologie qui permet de créer des subdivisions de réseau isolées de manière logique sur des réseaux physiques partagés de telle sorte que des collections hétérogènes de plusieurs réseaux virtuels peuvent coexister simultanément sur les réseaux partagés.

3.1.7 tranche de réseau [b-UIT-T Y.3100]: réseau logique qui offre des capacités de réseau et des caractéristiques de réseau spécifiques.

NOTE 1 – Les tranches de réseau permettent de créer des réseaux personnalisés qui offrent des solutions souples à différents scénarios de marché ayant des exigences diverses en ce qui concerne les fonctionnalités, la qualité de fonctionnement et l'attribution des ressources.

NOTE 2 – Une tranche de réseau peut être doté de la capacité d'exposer ses capacités.

NOTE 3 – Le comportement d'une tranche de réseau est réalisé via une ou plusieurs instances de tranche de réseau.

3.1.8 orchestration [b-UIT-T Y.3100]: dans le contexte d'IMT-2020, 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.

3.1.9 capacité de sécurité [b-ISO 81001-1]: catégorie générale de contrôles techniques, administratifs ou organisationnels visant à gérer les risques en matière de confidentialité, d'intégrité, de disponibilité et de responsabilité des données et systèmes.

3.1.10 fournisseur [b-ISO 10393]: organisation ou personne fournissant un produit ou un service.

3.1.11 système [b-ISO/CEI 27000]: applications, services, actifs informatiques ou autres composants du traitement de l'information.

3.1.12 menace [b-UIT-T X.1406]: cause potentielle d'un incident indésirable pouvant nuire à un système ou à une organisation.

3.1.13 fonction de réseau virtualisée [b-UIT-T Y.3150]: fonction de réseau dont le logiciel fonctionnel est découplé à partir de l'équipement et exécuté sur une ou plusieurs machines virtuelles.

3.2 Termes définis dans la présente Recommandation

La présente Recommandation définit les termes suivants:

3.2.1 domaine: groupement d'entités de réseau suivant des aspects physiques ou logiques qui se rapportent à un réseau IMT-2020.

3.2.2 système de communication IMT-2020: système de gestion des processus de communication IMT-2020 pour les services IMT-2020.

NOTE 1 – Par "5G", on entend les systèmes IMT-2020 dans le contexte de l'UIT-T.

NOTE 2 – Dans la présente Recommandation, les termes "systèmes de communication IMT-2020" et "système IMT-2020" sont équivalents.

3.2.3 écosystème IMT-2020: ensemble de parties prenantes qui interagissent pour former un système IMT-2020 fonctionnant de manière stable.

NOTE – Ce concept repose principalement sur les technologies de communication IMT-2020, dans lesquelles une communauté d'organismes évolutifs comprend des producteurs, des consommateurs et des fournisseurs qui contribuent à la réalisation d'un système IMT-2020 à différents niveaux (infrastructure, réseau, plate-forme, service et application).

3.2.4 service IMT-2020: prestation fournie par l'écosystème IMT-2020.

3.2.5 attaque par débordement des tables de flux: attaque utilisant des tables de flux qui réexpédient et traitent des paquets de flux, ce qui ne laisse aucun espace pour que d'autres flux puissent installer des règles de flux et provoque un déni de service (DoS) dans le réseau.

4 Abréviations et acronymes

La présente Recommandation utilise les abréviations et acronymes suivants:

4G	technologies de communication mobile de quatrième génération (*fourth generation of mobile communication technology*)
AMF	fonctions de gestion des accès et de la mobilité (*access and mobility management function*)
API	interface de programmation d'application (*application programming interface*)
AUSF	fonction de serveur d'authentification (*authentication server function*)
C-PDU	unités de données de protocole de commande (*control protocol data unit*)
CU/DU	unité centrale/unité répartie (*central unit/distributed unit*)
DCI	interconnexion des centres de données (*data centres interconnect*)
DDoS	déni de service réparti (*distributed denial-of-service*)
DoS	déni de service (*denial-of-service*)
eMBB	large bande mobile évolué (*enhanced mobile broadband*)
FAT	table d'allocation de fichiers (*file allocation table*)
IMSI	identité internationale d'abonné mobile (*international mobile subscriber identity*)
IMT-2020	Télécommunications mobiles internationales-2020 (*international mobile telecommunications-2020*)
IoT	Internet des objets (*internet of things*)

LTE	évolution à long terme (*long term evolution*)
MAC	code d'authentification de message (*message authentication code*)
MEC	informatique en périphérie à accès multiples (*multi-access edge computing*)
MEHW	matériel d'équipement mobile (*mobile equipment hardware*)
mIoT	Internet des objets massif (*massive internet of things*)
mMTC	communications massives de type machine (*massive machine-type communication*)
MNO	opérateur de réseau mobile (*mobile network operator*)
NAS	strate hors accès (*non-access stratum*)
NF	fonction de réseau (*network function*)
NFV	virtualisation des fonctions de réseau (*network function virtualization*)
NFVI	infrastructure de virtualisation des fonctions de réseau (*network functions virtualization infrastructure*)
NRF	fonction de référentiel de fonction de réseau (*network function repository function*)
OAM	exploitation, administration et gestion (*operation, administration, and management*)
O&M	exploitation et gestion (*operations and management*)
PII	informations d'identification personnelle (*personally identifiable information*)
PSK	clé pré-partagée (*pre-shared key*)
RA/CA	autorité d'enregistrement et autorité de certification (*registration authority and certification authority*)
RRC	contrôle des ressources radioélectriques (*radio resource control*)
SBA	architecture fondée sur les services (*service-based architecture*)
SBI	interface fondée sur les services (*service-based interface*)
SDN	réseau piloté par logiciel (*software-defined network*)
SMF	fonction de gestion de session (*session management function*)
SQL	langage de requête structuré (*structured query language*)
SSL	couche de connexion sécurisée (*secure sockets layer*)
TA	ancre de confiance (*trust anchor*)
TLS	sécurité dans la couche transport (*transport layer security*)
TMSI	identité temporaire d'abonné mobile (*temporary mobile subscriber's identity*)
TPM	module de plate-forme fiable (*trusted platform module*)
UDM	gestion de données unifiée (*unified data management*)
UE	équipement d'utilisateur (*user equipment*)
UICC	carte à circuit intégré universelle (*universal integrated circuit card*)
URLLC	communications ultra fiables à faible temps de latence (*ultra-reliable and low-latency communications*)
USIM	module d'identité universelle d'abonné (*universal subscriber identity module*)
VM	machines virtuelles (*virtual machines*)

VNF fonction de réseau virtuelle (*virtual network function*)

VoIP téléphonie utilisant le protocole Internet (*voice over internet protocol*)

5 Conventions

Dans la présente Recommandation, l'expression "il est recommandé" indique une spécification qui est recommandée mais qui n'est pas absolument nécessaire. Cette spécification n'est donc pas indispensable pour déclarer la conformité.

6 Vue d'ensemble de la sécurité des systèmes de communication IMT-2020

6.1 Architecture simplifiée des IMT-2020

Le présent paragraphe donne une vue d'ensemble des systèmes de communication IMT-2020. Les dispositifs mobiles connectés et les applications mobiles nécessitent un accès au réseau hertzien résilient, sûr et fiable. Les systèmes de communication IMT-2020 devraient être conçus de manière à répondre à ces exigences de haut niveau.

Un système de communication IMT-2020 comprend des dispositifs connectés à un réseau d'accès IMT-2020, qui à son tour est connecté au reste du système, appelé réseau central IMT-2020.

La Figure 1 illustre une architecture simplifiée du système 3GPP 5G. Le réseau d'accès IMT-2020 comprend des stations de base radioélectriques 3GPP ou un réseau d'accès non 3GPP. L'architecture du réseau central IMT-2020 est nettement meilleure que la 4G en ce qui concerne sa capacité à prendre en charge la mise en œuvre du nuage et de l'Internet des objets, et présente des améliorations majeures concernant le découpage de réseau et l'architecture fondée sur les services (SBA).

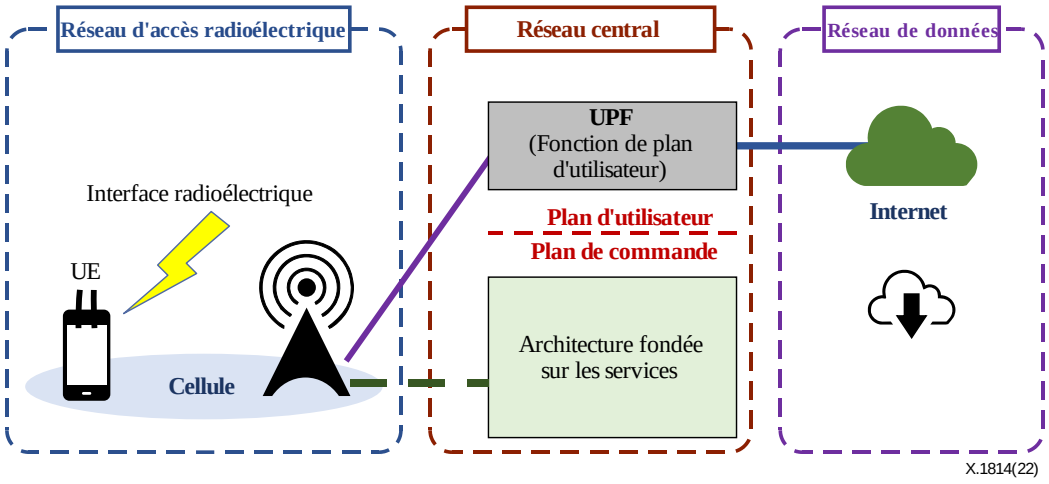

Figure 1 – Architecture simplifiée des IMT-2020

6.2 Architecture générale des systèmes IMT-2020

Les systèmes IMT-2020 visent à fournir une gamme variée de services ayant des exigences de fonctionnement différentes. Selon les spécifications 3GPP, les services fournis dans les réseaux IMT-2020 peuvent être classés en trois catégories: 1) le large bande mobile évolué (eMBB), qui prend en charge des débits de données plus élevés et une plus grande mobilité de l'utilisateur que les technologies mobiles de quatrième génération/évolution à long terme (4G/LTE); 2) l'Internet des objets massif (mIoT), qui prend en charge des communications massives de type machine; 3) les communications ultra fiables à faible temps de latence (URLLC), qui prennent en charge des services essentiels pour la mission nécessitant une grande fiabilité et un faible temps de latence. Les systèmes IMT-2020 ont vocation à constituer une plate-forme souple permettant de mettre en place de nouveaux scénarios commerciaux et d'intégrer des secteurs verticaux, comme l'industrie automobile,

l'industrie manufacturière, le secteur de l'énergie, la cybersanté et le divertissement. En outre, le déploiement et la maintenance seront plus faciles pour les systèmes IMT-2020 que pour les réseaux mobiles des générations précédentes. Pour répondre à ces exigences ambitieuses, des technologies innovantes ont été introduites dans les systèmes IMT-2020, par exemple le découpage du réseau, la virtualisation des fonctions de réseau (NFV), la technologie de réseau piloté par logiciel (SDN), l'architecture SBA et la séparation unité centrale/unité répartie (CU/DU).

Une architecture générale des systèmes IMT-2020 [b-UIT-T X.1811] est illustrée dans la Figure 2, y compris la couche transport, la couche réseau, la couche serveur et le plan de gestion, en fonction des fonctionnalités requises.

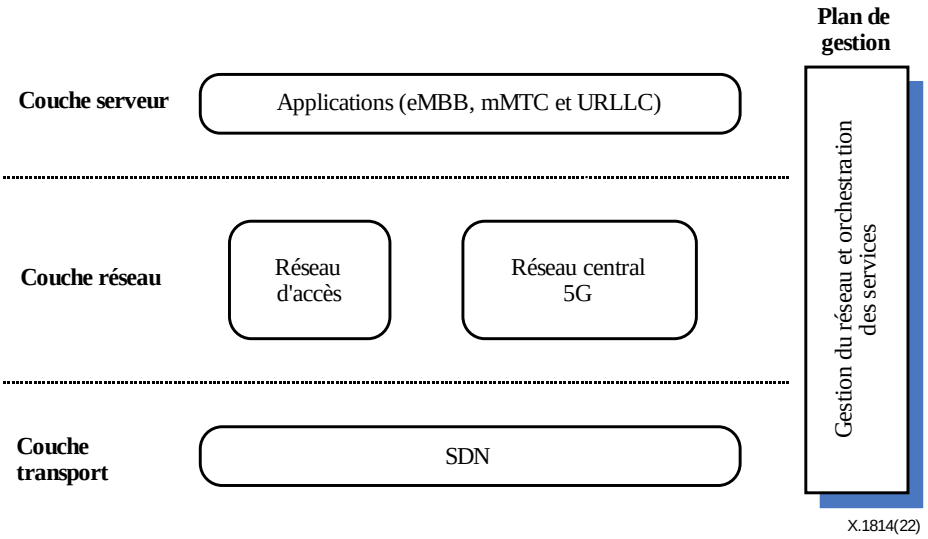

Figure 2 – Architecture générale des systèmes IMT-2020 [b-UIT-T X.1811], [b-TS 33.501]

- Couche transport: sert à transporter des paquets entre la source et la destination. Outre les anciennes technologies de transport (par exemple la commutation multiprotocole par étiquette), les systèmes IMT-2020 utilisent désormais la technologie SDN pour que le transport soit plus rapide et qu'il soit plus facile de s'adapter aux exigences des services.
- Couche réseau: comprend le réseau d'accès et le réseau central. Le premier permet à l'équipement UE d'accéder aux réseaux IMT-2020. Le second est conçu sur le modèle d'une architecture SBA pour favoriser l'extensibilité et la simplicité. Il est composé d'un certain nombre de fonctions de réseau pour assurer la connectivité des données et le déploiement des services. Ces fonctions comprennent, par exemple, les fonctions de serveur d'authentification (AUSF), de gestion des accès et de la mobilité (AMF) et de gestion de session (SMF).
- Couche service: comprend les applications qui s'exécutent au-dessus du système IMT-2020, par exemple les applications eMBB, mMTC ou URLLC.
- Plan de gestion: responsable de la gestion des réseaux et de l'orchestration des services.

6.3 Domaines des systèmes IMT-2020

La sécurité des IMT-2020 devrait être définie en fonction des domaines, des couches, des exigences de sécurité et des capacités de sécurité.

Un domaine est un groupe d'entités de réseau suivant des aspects physiques ou logiques qui se rapportent à un réseau IMT-2020. Le concept de domaine de tranche sert à rendre compte des aspects liés au découpage de réseau. Celui-ci peut représenter différentes fonctionnalités, différents services et différents acteurs dans les réseaux IMT-2020. La Figure 3 représente les domaines types des IMT-2020.

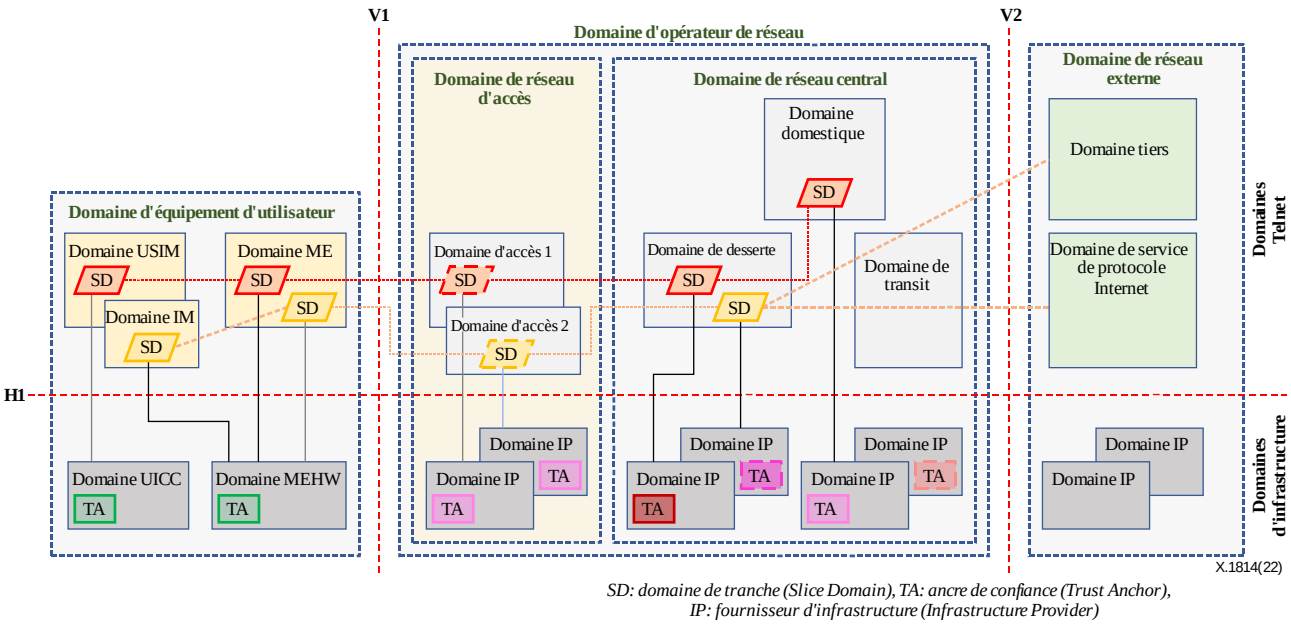

Figure 3 – Domaines types des IMT-2020

Les éléments de réseau situés au-dessus de la ligne H1 dans la Figure 3 représentent des aspects du réseau logique, appelés domaines de locataires, et ceux situés au-dessous de la ligne H1 représentent des aspects du réseau physique, appelés domaines d'infrastructure. La ligne V1 sépare le domaine d'équipement d'utilisateur (UE) du domaine du réseau d'accès et la ligne V2 sépare ensuite le domaine du réseau central du domaine du réseau externe, par exemple les services du protocole Internet utilisés par le réseau de l'opérateur.

Les domaines d'infrastructure contiennent des éléments de réseau mis en œuvre à l'aide de "matériel" et de logiciels et agissent en tant que fournisseur d'infrastructure. Ils comprennent des hyperviseurs (des logiciels qui créent et exécutent des machines virtuelles) ainsi que des ancres de confiance (TA) (une entité faisant autorité pour laquelle la confiance est prise pour hypothèse et qui n'est pas dérivée) [b-UIT-T X.509].

Du côté de l'équipement d'utilisateur au-dessous de la ligne H1, les domaines de l'équipement d'utilisateur se composent de la carte à circuit intégré universelle (UICC), offrant un module inviolable, et d'un domaine matériel d'équipement mobile (MEHW), offrant un support matériel, y compris un environnement d'exécution fiable.

Du côté réseau au-dessous de la ligne H1, un domaine de fournisseur d'infrastructure (IP, infrastructure provider) qui se compose du matériel propre à l'accès (radioélectrique) ainsi que du matériel nécessaire pour le calcul, le stockage et le réseau pour la fonctionnalité principale.

Les ancres de confiance servent à garantir la fiabilité des systèmes virtualisés. Elles garantissent notamment l'intégrité du domaine du locataire et veillent à exécuter le domaine de locataire sur une infrastructure désignée et fiable. Elles peuvent également servir à vérifier l'intégrité d'un domaine d'infrastructure et à relier des domaines de locataires à des domaines d'infrastructure.

Les domaines des locataires contiennent plusieurs domaines logiques qui utilisent des domaines d'infrastructure, par exemple pour exécuter leurs fonctions. Du point de vue de l'équipement d'utilisateur, ils se composent d'un équipement mobile, d'un module d'identité d'abonné universel (USIM), de l'une de plusieurs applications logicielles qui résident dans la partie matériel, appelée carte UICC, qui stocke les informations relatives à l'abonné et met en œuvre les fonctions de sécurité

relatives à l'authentification et au chiffrement du côté de l'utilisateur et du domaine de gestion d'identité. Côté réseau, les domaines de locataires comprennent les domaines d'accès (A), de desserte (S), de rattachement (H), de transit (T), de tiers (3P), de service de protocole Internet et de gestion (M).

6.4 Exigences et capacités générales en matière de sécurité

Le présent paragraphe résume les aspects (exigences) d'ordre général en matière de sécurité figurant dans la Recommandation [b-UIT-T X.805]. Il a pour objectif de constituer le fondement des capacités en matière de sécurité pour les systèmes IMT-2020. L'Appendice I décrit l'architecture générique de sécurité de réseau pour assurer la sécurité du réseau de bout en bout.

Une couche de sécurité désigne une hiérarchie d'équipements de réseau et de groupements d'installations [b-UIT-T X.805].

Elle est constituée d'un groupement de protocoles, de données et de fonctions associées à un aspect des services fournis par un ou plusieurs domaines. La couche de l'architecture de sécurité des IMT-2020 offre une vue de haut niveau des protocoles, des données et des fonctions qui sont liés, en ce sens que ceux-ci sont exposés à un environnement présentant des menaces courantes et sont régis par des exigences de sécurité analogues. Le brouillage radioélectrique, les fausses attaques par station de base, l'injection de données dans le plan utilisateur par voie hertzienne, et les messages de contrôle des ressources radioélectriques avec usurpation d'identité représentent des menaces courantes pour la communication entre les équipements d'utilisateur et un réseau d'accès radioélectrique. D'autre part, le suivi des identificateurs d'abonnement, l'usurpation d'identité des messages dans le plan de commande et l'altération des capacités de sécurité, entre autres, représentent des menaces courantes pour la communication entre les équipements d'utilisateur et le réseau central. Parmi les exemples de menaces courantes qui pèsent sur les services de gestion dans les réseaux IMT-2020 figurent l'exposition à des modifications de configuration non autorisées, la compromission des clés et certificats de réseau et l'ajout à la volée de fonctions de réseau malveillant. La couche de gestion comprend les aspects liés à la gestion du réseau classique (configuration, mises à niveau logicielles, gestion des comptes utilisateur-système, collecte/analyse de journaux, etc.) et, en particulier, les aspects de gestion de la sécurité (audit de surveillance de la sécurité, gestion des clés et des certificats, etc.). En outre, les aspects liés à la gestion de la virtualisation et de la création/composition de services (orchestration, gestion de tranche de réseau, isolation et gestion de machines virtuelles, etc.) appartiennent à cette strate.

Une zone de sécurité permet d'étendre les domaines de sécurité et est assujettie aux exigences de sécurité d'une ou de plusieurs couches ou domaines.

On entend généralement par capacité de sécurité une grande catégorie de contrôles techniques, administratifs ou organisationnels destinés à gérer les risques en matière de confidentialité, d'intégrité, de disponibilité et de responsabilité des données et systèmes [b-ISO 81001-1]. Il s'agit d'un ensemble de fonctions et de mécanismes de sécurité (y compris des garanties et des contre-mesures) relatifs à un seul aspect de la sécurité, par exemple l'intégrité. Une capacité contient des fonctions et des mécanismes de sécurité permettant d'éviter, de détecter, de déceler, de contrecarrer et de réduire au minimum les risques pour les réseaux IMT-2020, en particulier les risques pour l'infrastructure physique et logique d'un réseau, ses services, l'équipement d'utilisateur, la signalisation et les données. Le Tableau 1 présente les exigences de sécurité relatives aux domaines de sécurité.

Tableau 1 – Exigences de sécurité relatives à chaque zone de sécurité

Zone de sécurité	Exigences de sécurité
Réseau d'accès	Les exigences de sécurité relatives à la couche d'accès et au domaine d'accès sont identifiées pour remédier aux menaces associées à ce domaine. Elles comprennent la confidentialité et la protection de l'intégrité des données du plan d'utilisateur et du plan de commande ainsi que la mobilité sécurisée.
Application ou service	Les exigences de sécurité pour la couche application fournissant l'application et le service à l'utilisateur final (par exemple VoIP, VoLTE) sont identifiées pour remédier aux menaces relatives à ce domaine, par exemple: l'authentification et l'autorisation de l'utilisateur pour l'utilisation d'une application et la découverte sécurisée de service.
Gestion	Les exigences de sécurité pour la couche de gestion et le domaine de gestion sont identifiées pour remédier aux menaces liées à ce domaine, y compris la gestion de la sécurité (par exemple, mises à niveau sécurisées, orchestration sécurisée) et la gestion de la sécurité (par exemple, surveillance, gestion de clé et d'accès).
Équipement d'utilisateur	Les exigences de sécurité relatives au domaine de l'équipement d'utilisateur, y compris le contrôle d'accès du dispositif, sont identifiées pour remédier aux menaces associées à ce domaine. On citera à titre d'exemple l'authentification mutuelle avec le réseau et le stockage sécurisé du contexte de sécurité.
Réseau	Les exigences de sécurité relatives au réseau central et aux communications entre le réseau de l'opérateur et les réseaux externes sont identifiées, y compris les aspects liés à l'échange sécurisé de données de signalisation et d'utilisateur final entre les nœuds d'un opérateur et les domaines de réseau externes. On citera à titre d'exemple la sécurité du réseau, la confidentialité des abonnés et l'authentification des abonnés.
Infrastructure et virtualisation	Les exigences de sécurité du domaine du fournisseur d'infrastructure sont identifiées, par exemple, pour les attestations, le découpage/l'isolation sécurisé et les problèmes de confiance entre les domaines du locataire ainsi qu'entre les domaines du locataire et les domaines d'infrastructure.

Le Tableau 2 décrit les capacités de sécurité associées à chaque mesure de sécurité [b-UIT-T X.805]. Sept d'entre elles ont été adoptées à partir de [b-UIT-T X.805]: gestion de l'identité et de l'accès, authentification, non-répudiation, confidentialité, intégrité et disponibilité et confidentialité. Les trois mesures restantes, à savoir audit [b-UIT-T X.800], confiance et assurance, et conformité sont tirées de l'architecture de sécurité des IMT-2020.

Tableau 2 – Capacités de sécurité

Mesures de sécurité	Capacités de sécurité
Gestion de l'identité et de l'accès	Cette capacité de sécurité désigne un ensemble de fonctions et de mécanismes de sécurité (y compris des garanties et des contre-mesures) relatifs au contrôle d'accès et la gestion des justificatifs d'identité et des rôles.
Authentification	Cette capacité de sécurité désigne un ensemble de fonctions et de mécanismes de sécurité (y compris des garanties et des contre-mesures) relatifs à l'authentification, qui permettent de vérifier la validité des attributs d'authentification d'un utilisateur, par exemple l'identité déclarée.
Non-répudiation	Cette capacité de sécurité désigne un ensemble de fonctions et de mécanismes de sécurité (y compris des mécanismes de protection et des contre-mesures) relatifs à service de non-répudiation qui protège contre un faux déni de participation à une action donnée.

Tableau 2 – Capacités de sécurité

Mesures de sécurité	Capacités de sécurité
Confidentialité	Cette capacité de sécurité désigne un ensemble de fonctions et de mécanismes de sécurité (y compris des mécanismes de protection et des contre-mesures) relatifs à un service confidentiel qui protège les données contre toute divulgation non autorisée.
Intégrité	Cette capacité de sécurité désigne un ensemble de fonctions et de mécanismes de sécurité (y compris des garanties et des contre-mesures) relatifs à un service d'intégrité qui protège les données contre la création ou la modification.
Disponibilité	Cette capacité de sécurité désigne un ensemble de fonctions et de mécanismes de sécurité (y compris des mécanismes de protection et des contre-mesures) relatifs à la disponibilité des ressources, même en cas d'attaque. Les mécanismes de reprise après sinistre sont inclus dans la classification.
Confidentialité	Cette capacité de sécurité désigne un ensemble de fonctions et de mécanismes de sécurité (y compris des mécanismes de protection et des contre-mesures) relatifs à un service de confidentialité qui permet à des entités de déterminer dans quelle mesure elles interagiront et partageront leurs informations d'identification personnelle.
Audit	Cette capacité de sécurité désigne un ensemble de fonctions et de mécanismes de sécurité (y compris des garanties et des contre-mesures) relatifs à un service d'audit qui fournit l'étude et l'examen des enregistrements et des activités d'un système afin de déterminer si les capacités du système sont adéquates et de détecter les infractions à la sécurité et aux capacités du système.
Confiance et assurance	Cette capacité de sécurité désigne un ensemble de fonctions et de mécanismes de sécurité (y compris des garanties et des contre-mesures) relatifs à un service de confiance et de garantie servant à acheminer des informations sur la fiabilité d'un système.
Conformité	Cette capacité de sécurité désigne un ensemble de fonctions et de mécanismes de sécurité (y compris des garanties et des contre-mesures) relatifs à un service de conformité qui permet à une entité ou à un système de satisfaire à ses obligations contractuelles ou juridiques.

7 Composants et fiabilité des systèmes de communication IMT-2020

7.1 Composants des systèmes IMT-2020

Les dispositifs IoT connectés et les applications mobiles nécessitent un accès au réseau hertzien résilient, sûr et à même de protéger la vie privée des utilisateurs. Les systèmes de communication IMT-2020 devraient être conçus de manière à satisfaire aux exigences décrites aux § 7.8 et 7.9 de [b-UIT-T Y.3101]. Un réseau IMT-2020 comprend quatre composants, à savoir l'équipement d'utilisateur (UE), le réseau d'accès radioélectrique, le réseau de transport et le réseau central, qui sont représentés sur la Figure 4.

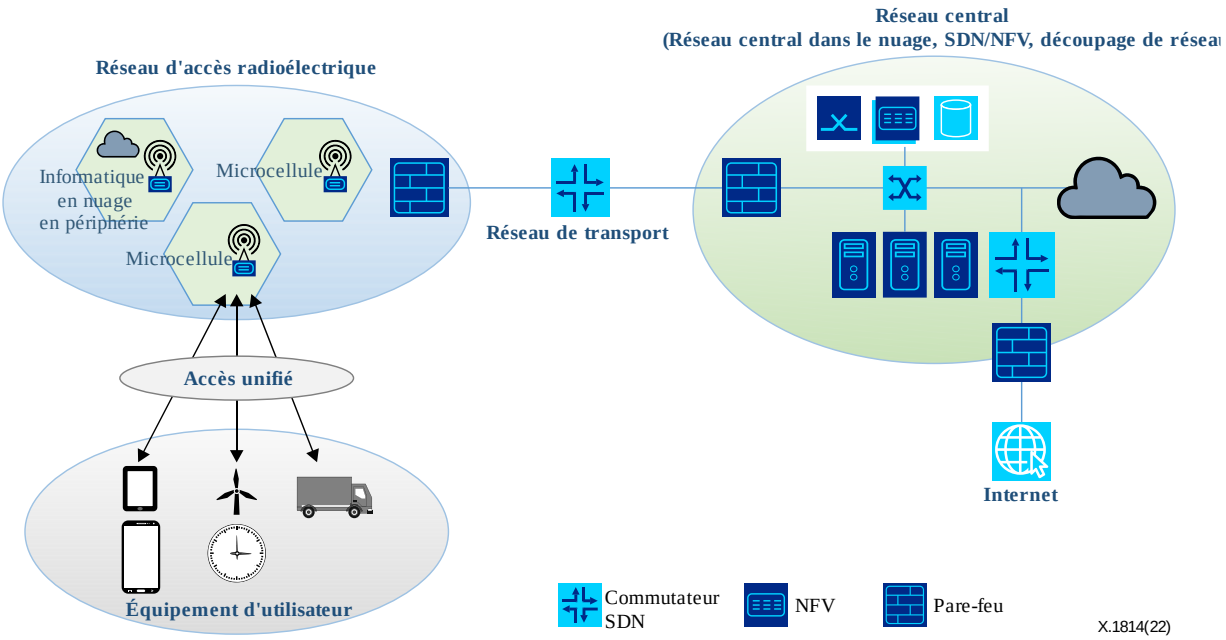

Figure 4 – Réseau de communication IMT-2020 (adapté à partir de l'[atelier b-UIT])

Le système IMT-2020 reposera sur l'informatique en nuage, les réseaux pilotés par logiciel (SDN), la virtualisation NFV et le découpage de réseau pour relever les défis de la connectivité massive, de la souplesse et de la réduction des coûts. Il est donc nécessaire de définir des mécanismes de sécurité pour la virtualisation NFV, le découpage du réseau et l'informatique en nuage en périphérie.

La virtualisation NFV sépare les fonctions de réseau des équipements matériels propriétaires et les exécute comme des logiciels dans les machines virtuelles (VM).

Une fonction de réseau virtuelle (VNF) est un résultat logique de la virtualisation NFV, une fonction de réseau dont le logiciel fonctionnel est découplé du matériel et exécuté sur la ou les machines virtuelles [b-UIT-T Y.3100]. Les fonctions VNF assurent des fonctions de réseau spécifiques telles que les pare-feu, la commutation, les systèmes de détection des intrusions et les systèmes de protection contre les intrusions.

Le découpage de réseau est une forme d'architecture de réseau virtuel qui utilise les principes qui sous-tendent les technologies SDN et NFV dans les réseaux fixes. Les réseaux IMT-2020 sont subdivisés en réseaux virtuels, chacun optimisé pour un cas économique donné, appelé tranche de réseau. Ils peuvent s'étendre à plusieurs domaines de réseau, y compris l'accès, le réseau central et le transport, et être déployés entre plusieurs opérateurs, comme le montre la Figure 5.

Les réseaux SDN offrent une architecture qui vise à rendre les réseaux agiles et souples. L'objectif de ces réseaux est d'améliorer la commande de réseau en permettant aux entreprises et aux fournisseurs de services de réseau de répondre rapidement à l'évolution des besoins commerciaux.

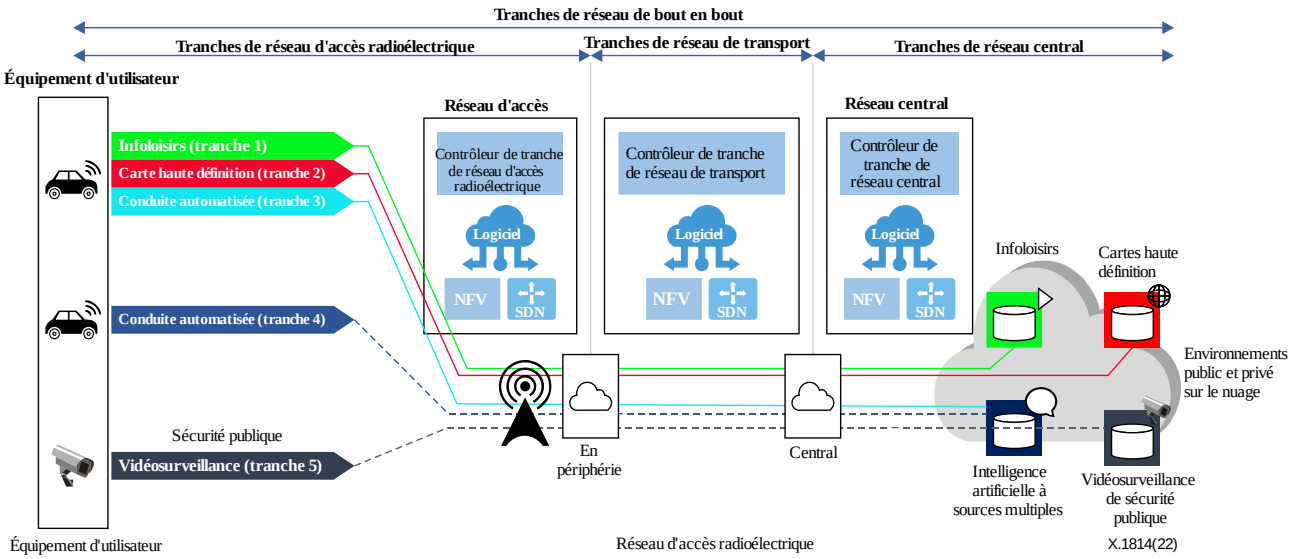

Figure 5 – Tranches des réseaux IMT-2020

Un réseau de transport IMT-2020 est une infrastructure de transport IP qui fournit des IMT-2020 mobiles.

L'informatique en périphérie met les capacités de l'informatique en nuage à la périphérie du réseau IMT-2020. Elle constitue un modèle informatique réparti dans lequel les calculs sont effectués, en grande partie ou en totalité, sur des nœuds de dispositif répartis appelés dispositifs intelligents ou dispositifs d'extrémité, par opposition à un environnement de nuage centralisé. L'informatique en périphérie permet le traitement et le stockage des données à proximité de l'équipement, ce qui permet aux dispositifs IoT de fournir leurs services avec de faibles temps de latence.

7.2 Fiabilité des systèmes de communication IMT-2020

Cinq facteurs permettent de garantir la fiabilité des systèmes de communication IMT-2020: la résilience, la sécurité des communications, la gestion d'identité, la confidentialité et la garantie de la sécurité:

- Résilience: capacité d'une organisation à éviter d'être affectée par les perturbations. L'intégration de diverses fonctionnalités complémentaires se chevauchant partiellement dans les IMT-2020 peut contribuer à rendre un système de communication IMT-2020 plus résistant aux cyberattaques et aux incidents d'origine non malveillante.
- Sécurité des communications: appliquée à la communication de données sur les réseaux IMT-2020. Dans un système de communication IMT-2020, il est primordial de garantir la sécurité des communications, aussi bien pour les appareils que pour l'infrastructure du système lui-même.
- Gestion d'identité: politiques et processus relatifs à la gestion du cycle de vie et valeur, type et métadonnées facultatives des attributs dans les identités connues au sein d'un domaine IMT-2020. Une gestion d'identité sûre devrait être prévue pour identifier et authentifier les abonnés, qu'ils se trouvent ou non en itinérance, et pour faire en sorte que seuls les abonnés réels puissent accéder aux services de réseau. Elle devrait se baser sur des primitives cryptographiques et sur des caractéristiques de sécurité fortes.

- Confidentialité: la confidentialité des données est définie comme les droits et obligations des personnes physiques et des organisations concernant le recueil, l'utilisation, la conservation, la divulgation et la suppression des informations personnelles dans la norme [b ISO/TS 21719-2]. La confidentialité consiste à protéger les informations d'identification personnelle (PII) pouvant être utilisées par des parties non autorisées pour identifier les abonnés.
- Garantie de la sécurité: motifs justifiant la confiance dans le fait qu'une affirmation selon laquelle les objectifs de sécurité ont été atteints s'est avérée ou s'avèrera. La garantie de la sécurité est un moyen de garantir que les équipements de réseau répondent aux exigences de sécurité et que des processus sûrs de développement et de cycle de vie des produits ont été mis en œuvre pour leur conception.

8 Menaces visant les composants et les fonctions

La Figure 6 illustre des exemples de menaces visant les systèmes IMT-2020. Ces menaces sont classées dans les trois catégories suivantes: menaces bien connues découlant de vulnérabilités logicielles, d'erreurs de configuration et d'attaques par inondation; menaces résultant de la mutualisation des infrastructures; et menaces liées au SDN, à la NFV, au découpage de réseau et à l'informatique en nuage.

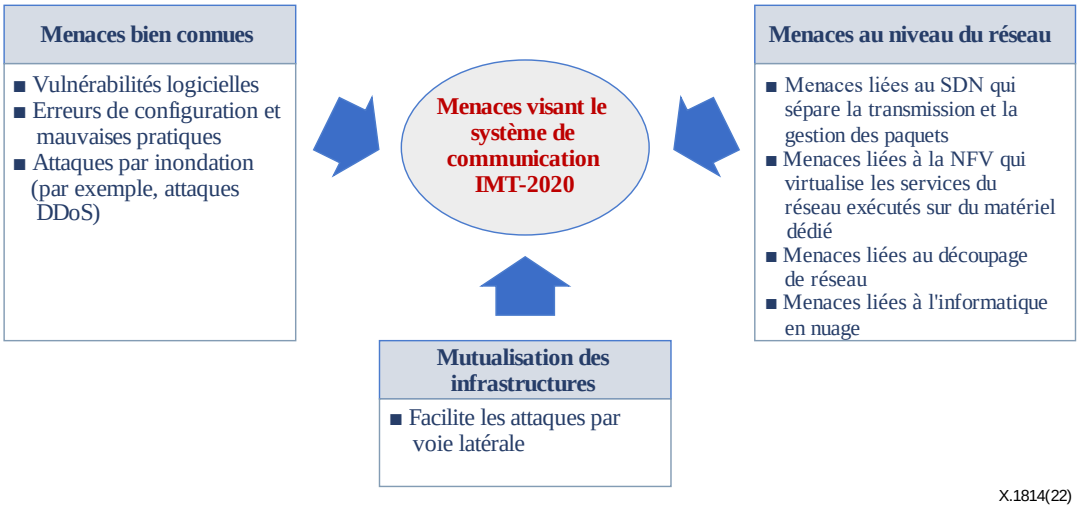

Figure 6 – Exemples de menaces visant le système IMT-2020 [b-UIT workshop]

8.1 Menaces génériques

Les menaces génériques suivantes ont été identifiées dans le document [b-ENISA]:

- **Déni de service (DoS)** [b-ENISA]: ce type d'attaque vise à rendre les ressources d'un réseau inaccessible à ses utilisateurs en inondant le service du réseau avec un grand nombre de requêtes de sorte à le compromettre ou à le perturber temporairement ou indéfiniment. Plusieurs types de ces menaces, qui prennent notamment la forme d'attaques par inondation, par amplification, par signalisation massive et par saturation, peuvent conduire à une attaque DoS. Parmi les attaques DoS les plus courantes, on peut citer les suivantes: 1) attaques par débordement de tampon, qui constituent les attaques DoS les plus répandues. Elles consistent à envoyer à un réseau ciblé plus de données que son système n'a été conçu pour en recevoir. Elle comprend les attaques ci-dessous ainsi que d'autres qui visent à exploiter des failles propres à certaines applications ou certains réseaux; 2) inondations ICMP. Ces menaces visent les dispositifs réseau mal configurés et consistent à envoyer non pas à une seule machine, mais à tous les ordinateurs du réseau ciblé, des paquets usurpés constituant autant de requêtes ping. Le réseau est ensuite incité à augmenter le trafic. Cette attaque est aussi

connue sous le nom d'"attaque par réflexion" ou de "ping de la mort"; 3) inondations SYN. Ces menaces consistent à envoyer continuellement des demandes de connexion à un serveur, sans terminer le processus de connexion, jusqu'à ce que tous les ports ouverts s'en trouvent saturés et qu'aucun port ne soit disponible pour permettre aux utilisateurs légitimes de se connecter.

- **Déni de service réparti (DDoS)** [b-ENISA]: une attaque DDoS est une attaque DoS lancée à l'aide de plusieurs systèmes qui ciblent un seul système. En d'autres termes, ces systèmes orchestrent une attaque DoS synchronisée visant une seule cible. La principale différence entre une attaque DoS et DDoS réside dans le fait que l'attaque n'est non pas menée depuis un seul endroit, mais depuis plusieurs endroits à la fois.
- **Violation, fuite, vol, destruction et manipulation de données** [b-ENISA]: cela inclut le vol d'informations d'identification personnelle (PII) par l'accès sans autorisation aux systèmes ou aux réseaux, ainsi que l'accès non autorisé à des données personnelles, biométriques ou médicales, ou encore aux informations confidentielles d'organisations et relatives à des états ou à des gouvernements, et leur éventuelle publication. Le vol, la violation ou la fuite d'autres types de données, comme les identifiants d'utilisateurs, les clés de chiffrement, les journaux relatifs à la sécurité du réseau ou la configuration logicielle, peuvent aider des personnes malintentionnées à mener différents types d'attaques.
- **Écoute illicite** [b-ENISA]: on entend par "écoute illicite" l'interception non autorisée d'informations. Cette menace consiste pour un intrus à s'introduire dans les couches d'application et de communication des différents éléments de réseau du système IMT-2020 (contrôleur SDN, fonction de réseau, nœud d'extrémité et orchestrateur de la virtualisation). Cela comprend la récupération des données et de l'emplacement des abonnés, d'informations confidentielles, de l'heure du système, de messages électroniques et des signaux transmis sur le réseau. L'auteur de la menace surveille, espionne ou écoute clandestinement des organisations pour suivre l'emplacement de personnes ou accéder à des informations sensibles.
- **Exploitation de vulnérabilités logicielles et matérielles** [b-ENISA]: ce type de menace permet à une personne malintentionnée de mener une attaque en exploitant des failles logicielles ou matérielles inconnues (du fournisseur ou de l'utilisateur) ou des failles connues, mais qui n'ont pas encore été corrigées. En ce qui concerne l'exploitation de failles logicielles et matérielles connues, on peut citer la vulnérabilité Meltdown et le débordement de tampon. Cela inclut également l'exploitation d'autres vulnérabilités connues propres aux systèmes de télécommunication mobiles de générations précédentes.
- **Code et logiciels malveillants** [b-ENISA]: on entend par "code malveillant" toute partie d'un système logiciel ou tout script conçu pour avoir des effets indésirables sur un système, compromettre sa sécurité ou l'endommager. Cette menace comprend l'installation et la distribution de logiciels malveillants ou l'implantation d'extraits de code ou de logiciels dans un produit ou des mises à jour. Parmi les exemples de logiciels ou de code malveillants, on peut citer les rançongiciels, les virus, les vers, les chevaux de Troie, les injections SQL (langage de requête structuré) [b-SQL], les logiciels de sécurité malveillants, les logiciels escrocs ou les *careware*. Dans le contexte du système IMT-2020, les logiciels malveillants désignent des VNF non autorisées qui peuvent s'installer ou s'enregistrer sur le réseau central pour exposer des API malveillantes.

- **Chaîne d'approvisionnement, fournisseurs et prestataires de services compromis** [b-ENISA]: si une chaîne d'approvisionnement, des fournisseurs et des prestataires de services sont compromis, cela permet aux fournisseurs de cacher du matériel ou bien d'installer des logiciels malveillants ou des failles logicielles dans un produit. Cela permet aussi de mettre en œuvre des mises à jour logicielles non contrôlées, de manipuler des fonctionnalités ou bien d'ajouter des fonctions pour contourner les mécanismes d'audit et des portes dérobées.

  Si des tiers non fiables participent aux tests, à la maintenance et à la configuration et au fonctionnement du produit, ils pourront accéder au système de gestion du réseau (sur place ou à travers une interface de commande à distance), afin de mener des activités de maintenance et de fournir une assistance technique. Toutefois, cet accès privilégié aux fonctions d'exploitation, d'administration et de gestion (OAM) du réseau leur permet aussi d'accéder à différents types de données, telles que les données d'abonnés, du système, de configuration du réseau et de télémesure.
- **Menaces ciblées** [b-ENISA]: les menaces ciblées émanent de logiciels malveillants destinés à une organisation ou à un secteur particulier. Mises à exécution à l'aide de logiciels criminels, ces menaces suscitent une grande préoccupation car elles sont conçues pour dérober des informations sensibles. Des attaques extrêmement complexes ou des menaces persistantes avancées peuvent cibler des informations sensibles ou nuire à la disponibilité de services sensibles ou d'importance critique.
- **Exploitation des failles de sécurité, de gestion et de procédures opérationnelles** [b-ENISA]: bien que cette menace ne soit pas directement liée au système IMT-2020, elle constituera une menace à part entière lorsqu'il s'agira de faire face à la complexité de la technologie et de répondre à la nécessité de mettre en place des procédures de gestion du réseau. Cette menace comprend, sans toutefois s'y limiter, l'exploitation des failles des systèmes opérationnels et de gestion de la sécurité du réseau, de configurations, de mises à jour et de fonctionnalités de gestion des correctifs des logiciels. Les erreurs découlant de l'absence de procédures opérationnelles et de sécurité ou de leur mauvaise conception peuvent affecter l'intégrité et la disponibilité du réseau.
- **Abus d'authentification** [b-ENISA]: cette menace peut viser plusieurs points d'entrée d'un réseau, tels que les équipements des utilisateurs (dispositifs mobiles et Internet des objets), les interfaces d'exploitation et de gestion, l'itinérance et les services verticaux. Elle se manifeste par le vol d'identifiants d'utilisateurs, le piratage de comptes d'utilisateurs par force brute, le cassage de mots de passe, le masquage de l'identité des utilisateurs et la perturbation de l'authentification de groupes d'appareils sur l'Internet des objets. Les auteurs de ce genre de menace recourent à ces techniques pour utiliser de manière abusive les systèmes d'authentification du système IMT-2020.
- **Usurpation d'identité** [b-ENISA]: l'usurpation d'identité désigne l'utilisation intentionnelle de l'identité d'autrui. Cela peut constituer une menace lorsqu'une personne malintentionnée parvient à récupérer l'identité d'une personne ou d'une organisation légitime, puis se fait passer pour elle en vue de lancer d'autres attaques. On entend par "usurpation d'identité" le vol de l'identité d'une personne ou d'une organisation en vue d'atteindre un objectif. L'usurpation d'identité est une menace qui peut avoir des conséquences sur tout composant logiciel ou tout agent humain. Au cours d'une telle attaque, une personne malintentionnée usurpe l'identité d'un contrôleur et interagit avec les fonctions du réseau contrôlées par celui-ci (c'est-à-dire par des éléments du plan de données) pour déclencher plusieurs autres attaques de type différent (ouvrir des flux de réseau, détourner le trafic du réseau, etc.). Le cassage de mots de passe et de comptes d'utilisateur par des méthodes d'ingénierie sociale et par force brute peut aussi permettre d'usurper ou de dérober les identifiants d'utilisateurs. Par exemple, les attaques visant à intercepter l'identité internationale d'abonné mobile (IMSI) permettent de révéler l'identité d'un abonné ou celle de l'équipement qu'il utilise. De telles attaques

peuvent également être lancées en configurant une station de base factice privilégiée par l'équipement d'un utilisateur qui a perdu l'accès à une identité temporaire d'abonné mobile (TMSI). L'abonné répondra en transmettant son IMSI. De plus, les réseaux IMT-2020 comprennent différents acteurs comme les opérateurs de réseau virtuel mobile (VMNO), les fournisseurs de services de communication (CSP) et les fournisseurs d'infrastructure réseau.

8.2 Menaces visant les équipements d'utilisateurs

Les menaces de sécurité suivantes visant les équipements d'utilisateurs ont été identifiées:

- **Infection à l'aide de logiciels malveillants** [b-ENISA]: si un logiciel malveillant est installé sur un équipement d'utilisateur, une personne malintentionnée peut manipuler l'équipement afin de lancer une attaque (par exemple, une attaque DDoS), notamment en vue de voler les données de l'équipement ou bien d'infecter d'autres équipements. Parmi les exemples de logiciels malveillants, on peut citer les rançongiciels, les virus, les vers, les chevaux de Troie et les logiciels de sécurité malveillants. Une fois que le logiciel malveillant a infecté l'équipement d'utilisateur, le point d'extrémité mobile est inclus comme un botnet.
- **Menace émanant des botnets** [b-Khan]: les botnets sont un type de logiciels malveillants qui peuvent contrôler plusieurs dispositifs connectés à l'Internet. Les botnets mobiles peuvent cibler plusieurs points d'extrémité mobiles pour lancer automatiquement une variété d'attaques (par exemple des attaques DoS) visant des systèmes IMT-2020. Ces menaces se répandent à mesure que les systèmes IMT-2020 interconnectent des téléphones mobiles dotés d'une puissance de calcul élevée. En outre, la connexion de dispositifs connectés à l'Internet des objets ouvre la voie à de nouvelles menaces, les rendant ainsi vulnérables à l'attaque de botnets qui sont très nombreux sur l'Internet des objets. On peut notamment citer l'exemple du botnet Mirai, qui a ciblé des millions de caméras IP en 2016.
- **Menaces émanant de logiciels malveillants mobiles** [b-Khan]: les logiciels malveillants mobiles peuvent permettre à des personnes malintentionnées de voler des informations d'identification personnelle stockées sur des dispositifs mobiles, voire de lancer des attaques (comme des attaques DoS) contre d'autres systèmes, tels que des équipements d'utilisateurs, des réseaux d'accès mobiles et des réseaux centraux d'opérateurs mobiles.
- **Accès non autorisé aux données d'utilisateurs et de signalisation, et destruction, divulgation ou modification de ces dernières:** un attaquant peut accéder sans autorisation aux données d'utilisateurs et de signalisation transmises entre les équipements des utilisateurs et les stations de base nœud B de dernière génération, ou procéder à leur destruction, divulgation ou modification.
- **Altération des identifiants d'abonnement:** un attaquant peut altérer les identifiants d'abonnement utilisés à des fins d'authentification et de confidentialité.

8.3 Menaces liées aux réseaux d'accès

Les menaces de sécurité suivantes pesant sur les réseaux d'accès ont été identifiées:

- **Trafic élevé malveillant ou accidentel** [b-NGMN]: compte tenu de l'augmentation des capacités de réseau et du nombre d'équipements d'utilisateurs, la forme que prendront les trafics de réseau malveillants ou accidentels découlant d'évènements importants risque fortement d'évoluer de manière significative. À cette échelle, étant donné qu'il est impossible de déterminer la nature de telles surcharges de réseau, l'objectif principal est d'empêcher la tenue d'évènements organisés dans le but de nuire (cela inclut toutefois les deux cas de figure).

- **Fuite de clés entre les liens d'opérateurs** [b-NGMN]: la clé de chiffrement (et parfois d'intégrité) de l'interface radioélectrique est calculée sur le réseau central de rattachement, puis transmise au réseau hertzien visité à l'aide d'une liaison, notamment du système SS7 (système de signalisation N° 7) [b-UIT-T Q700] ou du protocole Diameter [b-RFC 3588]. Il s'agit d'un point faible évident qui illustre comment la clé est récupérée lors d'une fuite.
- **Compromission de l'intégrité du plan utilisateur** [b-NGMN]: il existe un risque que la session soit entièrement interceptée et utilisée pour insérer des données erronées dans la connexion mobile (ou que les données soient perdues lorsqu'elles sont transmises au point d'extrémité du service).
- **Mise en œuvre facultative de la sécurité** [b-Khan], [b-NGMN]: cette menace émane de la mise en œuvre facultative de la sécurité. De nombreuses dispositions de sécurité n'ont aucune incidence sur l'interopérabilité (notamment avec les équipements d'utilisateurs). Historiquement, ces options ont été traitées comme des options de déploiement. Ce genre d'options peut créer des situations dans lesquelles l'opérateur est malgré lui inévitablement affecté par les actions d'autres opérateurs. Cela compromet également les hypothèses relatives à la sécurité des systèmes. Sans cette étape d'authentification, l'étage de la clé ne peut pas remplir l'un de ses objectifs, qui est de protéger les abonnés contre les stations de base défectueuses.
- **Menaces liées aux faux rapports d'état de tampon** [b-Khan]: les attaquants peuvent exploiter les rapports d'état du tampon de composants de réseaux d'accès, notamment ceux de stations de base, pour obtenir des informations, telles que les algorithmes d'ordonnancement des paquets, d'équilibrage des charges et de commande d'admission, et ainsi mettre en œuvre leurs mauvaises intentions. Les attaquants peuvent ensuite envoyer de faux rapports d'état de tampon en se faisant passer pour un équipement d'utilisateur légitime afin de compromettre diverses opérations.
- **Menaces découlant d'insertions de message** [b-Khan]: une insertion de message peut permettre de lancer des attaques DoS sur les réseaux IMT-2020. Par exemple, un appareil SDN dont le tableau de flux a été incorrectement mis à jour risque d'être surchargé. Un attaquant peut aussi injecter des unités de données de protocole de commande (C-PDU) dans le système pendant que ce dernier sort du mode veille pour lancer des attaques DoS sur les nouveaux équipements d'utilisateurs qui s'y connectent.
- **Menaces émanant de microcellules** [b-Kahn]: les stations de base ont été considérablement miniaturisées et sont placées en intérieur, notamment dans des centres commerciaux, des espaces publics, des stades et des hôpitaux. De plus, les nouvelles fréquences, comme les ondes millimétriques, faciliteront également l'utilisation de ces microstations de base. Cependant, elles ne sont pas, d'un point de vue physique, aussi sûres que les macrostations de base utilisées dans les réseaux pré-IMT-2020. En outre, l'essor des stations de base augmentera le nombre de vulnérabilités potentielles des réseaux IMT-2020.
- **Détournement de session** [b-ENISA]: le détournement d'une session à travers l'interface radioélectrique consiste pour un attaquant à prendre le contrôle d'une session d'utilisateur. Si une session authentifiée légitime est détournée, l'attaquant peut contrôler l'intégralité de la session d'un flux de données spécifique afin de lancer un autre type d'attaque.
- **Menaces émanant de faux réseaux d'accès** [b-ENISA]: si une station de base est compromise, un attaquant peut se faire passer pour une station de base légitime et mener une attaque par hôte interposé ou modifier le trafic du réseau. Cette menace conduit à l'altération des communications entre les équipements d'utilisateurs mobiles et le réseau, et permet ainsi de lancer d'autres types d'attaques.

- **Manipulation des données de configuration des réseaux d'accès** [b-ENISA]: si un élément de réseau d'accès, tel qu'une station de base, est compromis, l'attaquant peut produire de fausses données de configuration et ainsi lancer d'autres attaques (par exemple des attaques DoS).
- **Menaces émanant de l'usurpation d'identité (IMSI)** [b-ENISA]: si un attaquant exploite les protocoles de radiomessagerie cellulaire, il peut associer l'identité virtuelle de la victime à l'occasion de radiorecherche. Il peut ensuite vérifier les informations d'emplacement de la victime, injecter des messages de radiorecherche contrefaits et lancer des attaques par déni de service.
- **Perturbation de service provoquée par une demande de connexion RRC altérée**: si un attaquant altère le message de demande de connexion RRC transmis sous forme de texte brut, il peut utiliser les informations d'identification temporaires de la victime pour l'empêcher de se connecter au réseau. Le scénario de l'attaque est détaillé dans l'Appendice II.

8.4 Menaces visant les réseaux pilotés par logiciel (SDN)

Les menaces qui pèsent sur les réseaux SDN sont décrites dans le document [UIT-T X.1038].

8.5 Menaces visant les réseaux centraux

Les menaces de sécurité suivantes visant les réseaux centraux ont été identifiées:

- **DDoS** [b-Khan]: des attaques DDoS peuvent être lancées sous la forme d'une amplification des signaux et d'une saturation des fonctions AUSF et UDM à l'aide de botnets commandant plusieurs équipements d'utilisateurs infectés.
- **Menaces liées à la sécurité de la couche de transport (TLS)/couche de connexion sécurisée (SSL)** [b-Khan]: les systèmes de communications reposant sur les protocoles TLS/SSL utilisés sur les réseaux centraux pilotés par logiciel sont vulnérables à différentes attaques, telles que les attaques DDoS TCP/SYN (synchronisées), celles qui exploitent les biais de l'algorithme RC4 utilisé par le protocole TLS, les attaques BEAST (exploitation du navigateur contre les protocoles SSL/TLS), CRIME (fuite d'informations facilitée par le rapport de compression), LUCKY 13 [b-Goodin], et POODLE (attaque par oracle de bourrage sur des algorithmes de chiffrement obsolètes) [b-Möller].
- **Analyse des réseaux SDN** [b-Khan]: un attaquant peut analyser le flux de réseaux pilotés par logiciel (SDN) et recueillir manuellement des informations les concernant, comme le protocole de l'infrastructure et des éléments clés de réseau du contrôleur SDN. Les informations recueillies peuvent être utilisées pour lancer différentes attaques telles que des attaques DoS, de réinitialisation TCP, par répétition et par usurpation d'identité.
- **Détournement malveillant du trafic** [b-ENISA]: en compromettant un élément de réseau, un attaquant peut détourner le trafic du réseau et écouter les données qui y transitent. Le détournement du trafic est une menace visant les éléments de réseau du plan de données. La violation des tranches de réseau est un parfait exemple de détournement du trafic des réseaux virtualisés. Cette menace peut se concrétiser lorsque l'isolation entre les tranches est compromise dans un nœud actif ou que l'accès à une tranche d'un équipement d'extrémité est contourné ou mal configuré.
- **Utilisation abusive des outils d'audit** [b-ENISA]: les outils d'audit sont utilisés par les opérateurs pour suivre l'activité du réseau et recueillir des informations à diverses fins, notamment d'optimisation, de sécurité et commerciales. Ce genre d'outils logiciels peut permettre à des attaquants d'effectuer une reconnaissance en vue d'une attaque. Ces attaquants agissent généralement avec des personnes qui travaillent pour l'opérateur de réseau mobile et qui disposent d'un accès privilégié à ces outils pour récupérer des informations sensibles.

- **Fuite de clés de longue durée destinées à l'authentification des utilisateurs/aux données d'autorisation** [b-ENISA]: cette menace se rapporte à la divulgation, par un initié ou un membre hostile ou non fiable du personnel gérant un réseau central, de clés de longue durée destinées à l'authentification et aux contrôles de sécurité.
- **Exploitation de systèmes/réseaux mal configurés** [b-ENISA]: si des systèmes ou des réseaux sont mal configurés, un attaquant peut accéder à des ressources d'importance critique. En exploitant un système qui a été mal configuré par inadvertance, un attaquant peut accéder aux ressources importantes d'un réseau. Des erreurs de configuration peuvent survenir à diverses étapes de la mise en œuvre de la solution, notamment à l'installation du produit et lors de sa maintenance.
- **Reniflage de trafic** [b-ENISA]: un renifleur est un outil logiciel ou matériel permettant à un attaquant d'intercepter, d'enregistrer et d'analyser le trafic du réseau et les données qui y transitent. Grâce à ce procédé, l'attaquant peut écouter de manière illicite les données transmises entre les éléments de réseau ou accéder à des informations sensibles et les voler. La menace de reniflage peut se concrétiser lorsque le trafic d'un réseau est constant.
- **Enregistrement de fonctions de réseau malveillantes** [b-ENISA]: cette menace se caractérise par le déploiement de fonctions de réseau malveillantes sur des réseaux IMT-2020. Une fonction de réseau non autorisée ou intégrant un cheval de Troie, introduite sur le réseau par un initié (travaillant pour l'opérateur de réseau mobile) ou un fournisseur/prestataire de services, peut être installée dans l'architecture fondée sur les services (SBA) et enregistrée sur le réseau central à l'aide d'une fonction de référentiel de réseau (NRF) afin d'exposer d'autres API malveillantes. En installant ou en activant une fonction de réseau (NF), l'attaquant peut avoir accès à des ressources sensibles du réseau afin de mener d'autres types d'attaques, telles que des attaques DoS, distribuer des logiciels malveillants ou voler des informations sensibles.
- **Exposition de fonctions de réseau non sécurisées pour des fonctions d'applications de tiers** [b-Ta-Hao Ting]: l'exposition de fonctions de réseau entre des réseaux internes et externes permet de déployer de manière dynamique et souple les systèmes IMT-2020. Si un message est détourné ou altéré, cela endommagera tout le réseau central.
- **Interfaces non sécurisées fondées sur les services** [b-TS 33.501]: si un message transmis entre les éléments de réseau par l'intermédiaire d'une interface fondée sur les services (SBI) est détourné ou altéré, il peut être modifié et divulgué.

8.6 Menaces visant le découpage de réseau

Les menaces suivantes visant le découpage de réseau ont été identifiées:

- **Menaces visant la communication entre les tranches interréseaux** [b-Khan]: un attaquant peut perturber la communication entre les tranches afin d'empêcher la gestion adéquate du cycle de vie des tranches.
- **Attaque par usurpation d'identité** [b-Khan]: un attaquant peut se faire passer pour une plate-forme d'hébergement physique pour attribuer des ressources non disponibles. Il peut aussi se faire passer pour un gestionnaire de tranches de réseau pour voler les paramètres de création des tranches de réseau.
- **Absence de concordance entre les politiques de sécurité** [b-Khan]: les divergences entre les politiques et les protocoles de sécurité de différentes tranches permettent aux attaquants d'accéder au système de découpage du réseau et aux entités de commande par l'intermédiaire d'une tranche moins sécurisée.
- **Attaque DoS** [b-Khan]: une personne malintentionnée peut lancer une attaque DoS sur un réseau virtualisé ou des ressources physiques afin d'épuiser les ressources de réseau disponibles d'autres tranches.

- **Attaque par voie latérale** [b-Khan]: un attaquant obtient l'accès à une tranche et attaque un ensemble de tranches qui partagent le même matériel principal.
- **Fuite de données confidentielles** [b-Khan]: les fournisseurs d'infrastructure ou de fonctions de réseau virtualisées (VNF) volent des informations d'utilisateurs stockées sur différentes tranches.
- **Menaces liées à l'hyperviseur** [b-Khan]: il s'agit d'attaques visant l'hyperviseur en vue de compromettre la virtualisation des ressources. Ces attaques incluent l'introduction d'erreurs logicielles dans l'hyperviseur, la mise en place d'une porte dérobée par l'intermédiaire du système d'exploitation du serveur, des attaques DoS et des attaques visant les ressources matérielles.

8.7 Menaces visant l'informatique en périphérie à accès multiples

Les menaces suivantes visant l'informatique en périphérie ont été identifiées:

- **Passerelle MEC fausse ou malveillante** [b-ENISA]: étant donné qu'elles sont ouvertes, les passerelles d'extrémité peuvent subir une attaque au cours de laquelle l'attaquant peut déployer ses dispositifs passerelles. Cette menace a les mêmes conséquences qu'une attaque par intercepteur.
- **Surcharge de nœud d'extrémité** [b-ENISA]: si des applications mobiles ou des dispositifs IoT inondent le nœud d'extrémité de demandes ou de données, ce dernier peut se retrouver surchargé au niveau local ou des services. Cette attaque est lancée depuis des réseaux périphériques composés de dispositifs IoT qui perturbent les nœuds voisins du réseau affecté.
- **Utilisation abusive des API périphériques ouvertes** [b-ENISA]: si les vulnérabilités d'applications d'informatique en périphérie de réseau mobile (MEC) sont exploitées, les API ouvertes MEC peuvent faire l'objet d'une utilisation abusive. Le recours aux API MEC ouvertes permet principalement d'assurer la prise en charge de services fédérés et des interactions avec les différents fournisseurs et créateurs de contenu. Cette menace peut être associée à des attaques DoS ou par intercepteur, à des fuites de données confidentielles et à la manipulation de machines virtuelles.
- **Intrusion physique dans des dispositifs**: plus les ressources de calcul de l'architecture d'informatique en périphérie sont proches d'un attaquant, plus ce dernier est susceptible de s'introduire dans des dispositifs. L'attaquant peut détruire les nœuds d'extrémité, puis compromettre l'efficacité de l'intégralité du réseau.

8.8 Menaces visant la virtualisation des fonctions de réseau

Les menaces suivantes visant la virtualisation des fonctions de réseau ont été identifiées:

- **Utilisation abusive du protocole d'interconnexion des centres de données (DCI)** [b-ENISA]: si un attaquant exploite les vulnérabilités des protocoles DCI, il peut créer un trafic usurpé. Si les systèmes virtualisés sont déployés dans des centres de données, ces derniers peuvent se retrouver menacés. Ces menaces doivent ensuite être examinées.
- **Utilisation abusive des ressources de calcul en nuage** [b-ENISA]: si un attaquant utilise un processus simple d'enregistrement sur un service d'informatique en nuage, il peut utiliser de manière abusive la puissante infrastructure de calcul, y compris les composants logiciels et matériels. L'attaquant tire parti de la puissance de calcul propre aux réseaux en nuage et peut lancer des attaques en peu de temps. Par exemple, il peut mener des attaques par force brute et des attaques DoS en exploitant la puissance de calcul des services informatiques en nuage.

- **Contournement de la virtualisation de réseau** [b-ENISA]: les problèmes liés à la mauvaise mise en œuvre et configuration du découpage de réseau, ou à une mauvaise isolation des tranches de réseau, peuvent entraîner la violation de la confidentialité des données (données ou trafic interceptés par des entités d'autres tranches). Il est essentiel que seules des données légitimes transitent par les tranches d'un réseau utilisé par différents locataires, mais aussi que tout élément de commutation garantisse l'isolation du trafic et en vérifie l'état en instaurant des règles visant à assurer un flux de données légitimes de sorte à empêcher tout accès non autorisé aux tranches de réseau. Au niveau du réseau central, l'auteur d'une attaque pourrait exploiter les vulnérabilités de l'hyperviseur et la configuration des règles de flux pour contourner l'isolation des tranches et ainsi divulguer des données appartenant à d'autres locataires.
- **Utilisation abusive de serveurs virtualisés** [b-ENISA]: si des applications s'exécutent sur des serveurs virtualisés, cela peut entraîner une utilisation abusive des ressources d'un environnement virtualisé. Dans les environnements virtuels, où les ressources physiques sont partagées entre les locataires, certains comportements peuvent entraîner la divulgation d'informations sensibles. En effet, le risque de divulgation de données par balayage est plus grand dans les environnements virtualisés que sur des systèmes physiques. Bien que l'interception soit une menace courante pour les systèmes physiques (par exemple, les environnements de réseau), ses effets sont exacerbés dans les environnements virtuels, car ces derniers permettent d'effectuer l'inspection croisée des différents flux de données des locataires et de déduire la topologie du réseau, afin de préparer une attaque DoS.
- **Menace visant l'intégrité de l'infrastructure** [b-Alwakeel]: un attaquant se fait passer pour un prestataire proposant de vrais services de virtualisation des fonctions de réseau (NFV) afin d'obtenir l'accès aux données des utilisateurs.
- **Utilisation abusive des ressources** [b-Alwakeel]: un attaquant libère certaines ressources et les utilise pour son propre compte.
- **Modification de la définition des fonctionnalités de virtualisation des fonctions de réseau** [b-Alwakeel]: un attaquant modifie certaines des opérations de virtualisation des fonctions de réseau ou leur définition, ou lance même des attaques DoS. Cela est généralement réalisé par injection.
- **Modification des privilèges** [b-Alwakeel]: un attaquant ne visant pas les données de contrôle modifie les privilèges des utilisateurs en leur octroyant ou en leur retirant, sans autorisation, des droits d'accès aux entités du système.
- **Attaque visant la confidentialité et reposant sur les ressources partagées** [b-Alwakeel]: en lançant une attaque par voie latérale, un attaquant peut récupérer des informations privées concernant d'autres utilisateurs en se servant sans autorisation d'un service partagé.
- **Initié malveillant** [b-Alwakeel]: les membres supposés fiables d'une organisation abusent de leurs fonctions pour accéder sans autorisation aux données privées des utilisateurs.

8.9 Menaces visant les fonctionnalités de gestion

Les menaces suivantes visant les fonctionnalités de gestion ont été identifiées:

- **Interface de gestion non sécurisée** [b-TR 33.811]: cette menace se manifeste lorsque l'interface n'est pas sécurisée. Cela permet aux attaquants d'obtenir l'accès aux fonctionnalités de gestion du réseau sans autorisation et de créer des instances de tranches de réseau qui requièrent des ressources réseau considérables ou un grand nombre d'instances de tranches de réseau.

- **Divulgation des données de supervision et de rapport liées aux fonctionnalités de gestion** [b-TR 33.811]: cette menace se concrétise quand les données de supervision et de rapport ne sont pas protégées de manière adéquate. Cela peut permettre à un attaquant d'altérer les résultats de supervision/rapport, d'écouter de manière illicite la transmission de données de supervision et de rapport, et d'extraire des informations sensibles pouvant servir à lancer des attaques consistant à exécuter des instances de tranches de réseau.
- **Accès non autorisé à l'interface d'exposition des fonctionnalités de gestion** [b-Ta-Hao Ting]: si l'interface est compromise car un attaquant y a accédé sans autorisation, les fonctions de réseau, telles que les fonctions SDN, NFV et de découpage de réseau, peuvent subir des dysfonctionnements préjudiciables, comme le remplacement non autorisé et la modification des fonctions de réseau, et la création de configurations de réseau inappropriées.

9 Exigences applicables aux capacités de sécurité concernant les composants et les fonctions

9.1 Capacités de sécurité concernant les équipements d'utilisateur

Les capacités de sécurité suivantes concernant les équipements d'utilisateur devraient être prises en charge:

- **Capacité de lutte contre les logiciels malveillants permettant de sécuriser les équipements d'utilisateur**: il existe des programmes logiciels conçus pour prévenir, détecter et supprimer les logiciels malveillants des équipements d'utilisateur. Trois méthodes, à savoir la détection des logiciels malveillants basée sur la signature, la détection des logiciels malveillants basée sur le comportement et la mise en place d'un environnement sécurisé (sandboxing), sont utilisées pour protéger les équipements d'utilisateur contre toute infection par un logiciel malveillant.
- **Capacité de sécurité de l'IMSI permettant de sécuriser l'identité d'abonné par le biais du chiffrement**: l'IMSI devrait être chiffrée par la clé de chiffrement éphémère au moyen d'un algorithme symétrique de cryptographie. La condition préexistante consiste en ce que l'équipement d'utilisateur dispose de sa propre IMSI et en ce que la clé asymétrique publique du réseau domestique et chaque opérateur mobile (ici le réseau domestique) disposent d'une paire de clés asymétriques publique et privée. Il est admis que la clé asymétrique privée du réseau domestique est tenue secrète par le réseau domestique, tandis que la clé asymétrique publique du réseau domestique est préconfigurée sur les dispositifs mobiles, au même titre que les IMSI propres à l'abonné.
- **Capacité de vérification de l'identité**: il s'agit de vérifier l'identité de l'utilisateur en ce qui concerne les services d'itinérance et les services en nuage.
- **Capacité de gestion des clés**: il s'agit de prendre en charge la vérification de l'identité de l'utilisateur et l'authentification mutuelle entre l'équipement d'utilisateur et les éléments de réseau.
- **Capacité de sécurité de l'emplacement**: il s'agit de garantir la sécurité de l'emplacement de l'utilisateur.
- **Authentification du réseau de desserte**: les équipements d'utilisateur devraient authentifier l'identificateur du réseau de desserte au moyen d'une authentification par clé implicite. Autrement dit, cette authentification est assurée grâce à l'utilisation réussie des clés résultant de l'authentification et de la concordance de clés dans les procédures ultérieures.

- **Confidentialité et intégrité des données d'utilisateur et des données de signalisation** [b-UIT-T X.1811]: les équipements d'utilisateur peuvent prendre en charge la confidentialité des données au moyen d'algorithmes de chiffrement, ainsi que la protection de l'intégrité et la protection contre les répétitions pour ce qui est des données d'utilisateur entre les équipements d'utilisateur et les nœuds de réseau.
- **Capacité de traitement et de stockage sécurisés des justificatifs d'identité d'abonné** [b-Craven]: les équipements d'utilisateur peuvent assurer la protection de l'intégrité des justificatifs d'identité et des clés à long terme associées au moyen de matériel inviolable. Les clés à long terme doivent systématiquement bénéficier d'un chiffrement en dehors du matériel inviolable. Le programme devrait être exécuté dans le matériel inviolable en utilisant un algorithme d'authentification et des justificatifs d'identité d'abonné.

9.2 Capacités de sécurité concernant les réseaux d'accès

Les capacités de sécurité suivantes concernant les réseaux d'accès devraient être prises en charge:

- **Capacité de sécurité des liaisons**: il s'agit d'assurer la confidentialité et l'intégrité des communications pour les canaux de commande et les canaux de trafic utilisateur à l'aide des équipements d'utilisateur.
- **Capacité d'authentification des équipements d'utilisateur**: le réseau de desserte devrait authentifier l'identificateur permanent d'abonnement lors du processus d'authentification et de concordance de clés entre les équipements d'utilisateur et le réseau.
- **Capacité d'autorisation des équipements d'utilisateur** [b-Craven]: le réseau de desserte devrait autoriser les équipements d'utilisateur en utilisant le profil d'abonnement obtenu auprès du réseau domestique.
- **Capacité d'autorisation de réseau de desserte du réseau domestique** [b-Craven]: il convient de s'assurer que les équipements d'utilisateur soient connectés à un réseau de desserte autorisé par le réseau domestique.
- **Capacité d'autorisation de réseau d'accès** [b-Craven]: un réseau d'accès devrait être autorisé par le réseau de desserte à fournir des services aux équipements d'utilisateur.
- **Capacité de confidentialité des données d'utilisateur et de signalisation** [b-Craven]: le réseau d'accès devrait prendre en charge le chiffrement des données d'utilisateur en transit et pour la signalisation RRC.
- **Capacité d'intégrité des données d'utilisateur et de signalisation** [b-Craven]: les nœuds, comme les équipements d'utilisateur, devraient prendre en charge la protection de l'intégrité et la protection contre les répétitions des données d'utilisateur transmises entre les équipements d'utilisateur et le nœud B de prochaine génération.
- **Capacité de configuration et d'établissement de connexion** [b-Craven]: lors de l'établissement et de la configuration de systèmes d'exploitation et de gestion (O&M), le nœud B de prochaine génération devrait être authentifié et autorisé par une autorité d'enregistrement et une autorité de certification (RA/CA), afin que les attaquants ne puissent pas modifier les configurations logicielles et les paramètres du nœud B de prochaine génération.
- **Capacité de gestion des clés dans le nœud B de prochaine génération** [b-Craven]: il est nécessaire de protéger les différents éléments des clés de chiffrement fournies par le réseau central IMT-2020 au nœud B de prochaine génération.
- **Capacité de traitement du plan d'utilisateur et du plan de commande** [b-Craven]: la capacité de gestion des clés est semblable à celle de traitement du plan d'utilisateur et du plan de commande pour le nœud B de prochaine génération.

- **Capacité d'un environnement sécurisé** [b-Craven]: l'environnement sécurisé dans lequel se trouvent toutes ces données non chiffrées doit également répondre à des exigences, par exemple prendre en charge le stockage sécurisé au moyen de secrets cryptographiques à long terme et de données de configuration essentielle.
- **Capacité de faire face aux menaces d'interruption de service provoquée par des demandes de connexion RRC**: pour éviter toute menace découlant d'une demande de connexion RRC manipulée, la station de base doit maintenir la connexion RRC avec l'utilisateur existant pendant plus longtemps, d'où la nécessité pour la station de base de conserver une connexion pendant plus longtemps que le temporisateur d'attente pour la connexion RRC existante. En outre, les paramètres "limit-time" (délai maximal) et "limit-count" (nombre maximal) au niveau de la station de base devraient être utilisés et un processus de contrôle permettant de vérifier si cette attaque est en cours devrait être ajouté. Le scénario d'attaque détaillé est décrit dans l'Appendice II.

9.3 Capacités de sécurité concernant les réseaux pilotés par logiciel (SDN)

Les capacités de sécurité suivantes concernant les SDN devraient être prises en charge [UIT-T X.1038]:

- **Capacité d'authentification** de l'application SDN permettant d'authentifier le contrôleur SDN/l'utilisateur/l'administrateur.
- **Capacité d'autorisation** de l'application SDN permettant d'autoriser l'utilisateur/l'administrateur à accéder aux informations du système.
- **Capacité de confidentialité des données** de l'application SDN permettant de protéger la confidentialité des informations du système stockées dans la plate-forme d'application d'une part, et le transport des données dans l'interface application-commande d'autre part.
- **Capacité de gestion des clés/certificats** de l'application SDN permettant de gérer les clés/certificats.
- **Capacité de gestion de la sécurité** de l'application SDN permettant de prendre en charge les journaux et les audits.
- **Capacité de protection d'application** de l'application SDN permettant de mettre en place des mesures de protection contre les vulnérabilités de l'application.
- **Capacité d'intégrité des données** de l'application SDN permettant de prendre en charge la protection de l'intégrité du transport des données dans l'interface application-commande.
- **Capacité d'authentification** du contrôleur SDN permettant d'authentifier les administrateurs/l'application SDN/le commutateur SDN.
- **Capacité d'autorisation** du contrôleur SDN permettant d'autoriser les administrateurs/l'application SDN à gérer le contrôleur SDN.
- **Capacité de gestion de l'authentification et de la sécurité** du contrôleur SDN permettant de mettre en place des mesures de protection contre des attaques DoS.
- **Capacité d'intégrité des données** du contrôleur SDN permettant de protéger l'intégrité des données de configuration et des données d'utilisateur stockées dans le contrôleur SDN d'une part, et le transport des données dans l'interface application-commande et dans l'interface ressources-commande d'autre part.
- **Capacité de gestion des clés/certificats** du contrôleur SDN permettant de gérer les clés/certificats.
- **Capacité de confidentialité des données du contrôleur SDN** permettant de protéger la confidentialité des données de configuration et des données d'utilisateur stockées dans le contrôleur SDN d'une part, et le transport des données dans l'interface application-commande et dans l'interface ressources-commande d'autre part.

- **Capacité de renforcement du système d'exploitation du contrôleur SDN** permettant de prendre en charge la fonctionnalité de renforcement du système d'exploitation.
- **Capacité d'authentification de la couche ressource du réseau SDN** permettant d'authentifier les administrateurs/le contrôleur SDN.
- **Capacité d'autorisation de la couche ressource du réseau SDN** permettant d'autoriser les administrateurs à gérer les commutateurs SDN.
- **Capacité de gestion de la sécurité de la couche ressource du réseau SDN** permettant de prendre en charge les journaux et les audits.
- **Capacité d'intégrité des données de la couche ressource du réseau SDN** permettant de protéger l'intégrité des données de configuration stockées dans le commutateur SDN et le transport des données entre les commutateurs SDN et dans l'interface ressources-commande.
- **Capacité de gestion des clés/certificats de la couche ressource du réseau SDN** permettant de gérer les clés/certificats.
- **Capacité de confidentialité des données de la couche ressource du réseau SDN** permettant de protéger la confidentialité des données de configuration stockées dans le commutateur SDN d'une part, et le transport des données entre les commutateurs SDN et dans l'interface ressources-commande d'autre part.
- **Capacité de prévention des dépassements de capacité du tableau de flux de la couche ressource du réseau SDN**. Le contrôleur SDN doit dynamiquement tenir à jour le tableau de flux en insérant et en supprimant des entrées de flux.

9.4 Capacités de sécurité concernant le réseau central

Les capacités de sécurité suivantes devraient être prises en charge:

- **Capacité de détection d'attaques DoS/DDoS et de protection contre ces attaques** permettant de protéger le point de contrôle centralisé dans un réseau SDN.
- **Capacité de vérification de la configuration** permettant de vérifier les règles de flux dans les éléments de réseau SDN.
- **Capacité de contrôle d'accès** permettant de limiter l'accès au réseau SDN et aux éléments de réseau central.

Les capacités de sécurité suivantes concernant la fonction d'exposition de réseau et l'interface fondée sur les services devraient être prises en charge:

- **Capacités de fonctions d'exposition de réseau sécurisées** [b-TS 33.501]: l'authentification mutuelle fondée sur des certificats de client et de serveur devrait être effectuée entre la fonction d'exposition de réseau et la fonction d'application de fonctions d'application tierces situées en dehors du domaine d'un opérateur de réseau IMT-2020, qui est assurée par un tunnel sécurisé de type TLS, par exemple. Le trafic entre la fonction d'exposition de réseau (NEF) et la fonction d'application doit être utilisé pour assurer la protection de l'intégrité, la protection contre les répétitions et la protection de la confidentialité.
- **Confidentialité, intégrité des données et authentification des éléments de réseau à travers une interface fondée sur les services** [b-TS 33.501]: le trafic entre les éléments de réseau par le biais de l'indicateur SBI devrait assurer la protection de l'intégrité, la protection contre les répétitions et la protection de la confidentialité des données et l'authentification des éléments de réseau à travers un tunnel sécurisé de type TLS, par exemple.

9.5 Capacités de sécurité concernant le découpage de réseau

Les capacités de sécurité suivantes concernant le cycle de vie des tranches devraient être prises en charge [b-Olimid]:

- **Capacité de sécurité du cycle de vie des tranches**: la sécurité devrait être assurée au cours des quatre phases, car une vulnérabilité dans une phase peut introduire des vulnérabilités dans d'autres phases.
- **Capacité appropriée de journalisation et d'audit**: différents niveaux de journalisation devraient être mis en œuvre dans des tranches de réseau distinctes, en fonction de divers facteurs tels que la réglementation, le niveau de sécurité ciblé pour les services consommateur et le type dédié de dispositifs client (par exemple, l'utilisation par l'homme ou la machine). Les résultats des journaux et des rapports devraient être protégés, car leur exposition entraînerait une divulgation d'informations sensibles.
- **Capacité de sécurité du modèle de tranche de réseau**: la confidentialité et l'intégrité devraient être assurées pendant la transmission et le stockage, et la source du modèle devrait être authentifiée.
- **Capacité de sécurité en matière d'orchestration**: les services de sécurité personnalisés devraient être orchestrés et déployés conformément aux exigences de sécurité des différents secteurs verticaux [b-UIT-T X.1047].
- **Capacité d'isolation des tranches**: l'isolation devrait être assurée lors de la création et du suivi des tranches et, au besoin, mise à jour pendant l'exécution [b-UIT-T X.1047].
- **Capacité de sécurité des API**: les API devraient être sécurisées en matière de droits d'exploitation et d'accès et ne devraient pas exposer de données de trafic. Elles devraient uniquement autoriser l'accès aux données et aux capacités, comme convenu entre les parties par des moyens légaux.
- **Capacité de mise hors service**: au moment de la mise hors service, les données sensibles devraient être détruites (ou, au cas par cas, stockées de manière sécurisée) et les ressources et les fonctions de réseau devraient être libérées.

Les capacités de sécurité suivantes concernant la sécurité des tranches devraient être prises en charge:

- **Capacité de sécurité de bout en bout**: les tranches étant des réseaux logiques de bout en bout, la sécurité de bout en bout devrait être prise en charge [b-UIT-T X.1047].
- **Capacité d'utilisation adéquate de mécanismes de sécurité**: toutes les communications (par exemple, entre la tranche et la couche ressource, la tranche et le gestionnaire de tranches, les sous-tranches d'une tranche, le dispositif client et le point d'accès dans le réseau) devraient utiliser des mécanismes adéquats pour protéger le niveau de sécurité souhaité; les exigences minimales devraient couvrir la confidentialité, l'intégrité, l'authenticité des données et l'authentification mutuelle entre les pairs.
- **Capacité d'authentification des équipements d'utilisateur**: les dispositifs client du réseau IMT-2020 devraient bénéficier d'une authentification forte au moyen d'une authentification primaire et de préférence secondaire.
- **Capacité de consommation de fonctions de ressources sécurisées**: toutes les ressources et fonctions réseau consommées par une tranche devraient être sécurisées.
- **Capacité de sécurité des locataires**: les nouvelles fonctionnalités introduites par les locataires (par exemple, services, configuration et fonctions de réseau) et leur intégration devraient être sécurisées de manière appropriée, afin de prévenir des failles susceptibles d'être exploitées ultérieurement.
- **Capacité de sécurité de l'identité**: les identifiants sensibles devraient être protégés et aucune corrélation entre les identifiants ne devrait être divulguée.

- **Interception légale**: cette capacité devrait être accessible au niveau des couches de tranche et de service.
- **Capacités de configuration, de droits et d'accès des locataires**: ces éléments devraient être conformes aux accords juridiques conclus entre les parties.

Les capacités de sécurité suivantes concernant la communication entre tranches devraient être prises en charge:

- Un niveau de sécurité minimal devrait être accordé pour chaque tranche.
- **Capacité d'isolation des tranches**: l'isolation entre les tranches devrait être suffisamment robuste pour empêcher toute attaque par le biais des tranches les moins sécurisées [b-UIT-T X.1047].
- **Capacité de sécurité de communication minimale**: la communication entre les tranches devrait être réduite au minimum, définie par des règles strictes et mise en œuvre par le biais de canaux sécurisés.
- **Capacité de gestion des clés**: les clés cryptographiques (et d'autres paramètres sensibles) ne devraient pas être partagés entre des tranches.
- **Capacité d'attribution minimale des ressources**: l'attribution des ressources devrait garantir un niveau minimal de disponibilité pour chaque tranche, et des mécanismes de sécurité devraient notamment être en mesure de s'exécuter indépendamment de la consommation de ressources.
- Les tranches dont les niveaux de sécurité sont très différents ne devraient pas partager de ressources ou de fonctions réseau; il convient notamment de ne jamais exécuter de tranches en mode d'essai avec des tranches en phase d'exécution.
- **Capacité de sécurité indépendante**: les mécanismes d'authentification, d'autorisation et de contrôle d'accès distincts devraient être indépendants pour chaque tranche.

9.6 Capacités de sécurité concernant l'informatique en périphérie à accès multiples

Les capacités de sécurité suivantes devraient être prises en charge:

- **Capacité d'atténuation des effets d'attaques DDoS** permettant de protéger les services web en nuage.
- **Capacité de contrôle d'accès** permettant de limiter l'accès aux éléments de réseau de l'informatique en périphérie à accès multiples.
- **Capacité de vérification de l'intégrité** permettant de sécuriser les données et le système de stockage dans l'informatique en nuage.
- **Capacité de contrôle d'accès aux services** permettant de limiter les éléments d'informatique en nuage fondés sur les services.
- **Capacité de sécurité physique**: il convient de garantir la sécurité physique de tout nœud d'extrémité n'étant pas placé dans des centres de données périphériques hautement sécurisés, tels que ceux qui ont recours à des techniques de protection physique supplémentaires pendant la fabrication ou la mise en œuvre de mécanismes de verrouillage et d'autres mesures de protection physiques sur le terrain.

9.7 Capacités de sécurité concernant la virtualisation des fonctions de réseau

Les capacités de sécurité suivantes devraient être prises en charge:

- **Capacité d'isolation du trafic:** capacité permettant de protéger les tranches virtuelles et les fonctions de réseau virtuel.

- **Capacité de prévention des attaques DoS** [b-Alwakeel]: des éléments de réseau, comme les pare-feu et les répartiteurs de charge, devraient être utilisés pour atténuer les effets d'attaques DoS/DDoS.
- **Capacité d'intégrité de l'infrastructure** [b-Alwakeel]: une chaîne de confiance et un module de plate-forme fiable (TPM) devraient être utilisés pour garantir la sécurité des différents fournisseurs de VNF.
- **Capacité d'atténuation des effets de l'utilisation abusive de ressources** [b-Alwakeel]: un planificateur d'hyperviseur avancé assurant une répartition équitable entre les processus et limitant les capacités maximales autorisées pour chaque service virtuel devrait être fourni.
- **Capacité de protection contre des modifications de la définition des fonctions de réseau virtualisées** [b-Alwakeel]: une copie des services virtuels d'utilisateur devrait être conservée sur un support de stockage distinct pour empêcher toute attaque par injection d'un logiciel malveillant. Une table d'allocation des fichiers (FAT) contient des informations sur les services et les logiciels en cours d'exécution par l'utilisateur.
- **Capacité de prévention des modifications de privilèges** [b-Alwakeel]: une protection de l'entité de virtualisation contre tout accès non autorisé au moyen de l'ajout de politiques restrictives quant à l'accès aux ressources devrait être assurée.
- **Capacité d'atténuation des effets des ressources partagées** [b-Alwakeel]: une capacité d'atténuation des effets d'attaques par voie latérale devrait être utilisée pour restreindre l'accès aux images de la machine virtuelle et aux composants de l'infrastructure de virtualisation des fonctions de réseau (NFVI) et pour contrôler l'utilisation des ressources. Pour ce faire, on peut utiliser un pare-feu virtuel pour empêcher tout accès non autorisé au système.
- **Capacité d'atténuation des effets d'attaques malveillantes de l'intérieur** [b-Alwakeel]: il est possible d'atténuer les effets d'attaques de l'intérieur au moyen de diverses capacités, l'une d'elles étant la journalisation des accès au sein de l'environnement NFV, qui peuvent ensuite être utilisées dans le cadre d'audits internes pour détecter toute activité suspecte. Un autre mécanisme vise à mettre en place des politiques strictes en matière d'authentification et d'autorisation des utilisateurs disposant de droits d'accès.

9.8 Capacités de sécurité concernant la fonction de gestion

Les capacités de sécurité suivantes [b-TR 33.811] devraient être prises en charge:

- **Capacité d'authentification mutuelle** entre le consommateur de service de gestion et le producteur de service de gestion au moyen d'un tunnel sécurisé de type TLS, par exemple, sur la base soit 1) des certificats de client et de serveur, soit 2) de clés prépartagées (PSK) avec le protocole PSK TLS.
- **Capacité de protection de l'intégrité, de protection contre les répétitions et de protection de la confidentialité** concernant l'interface entre le producteur de service de gestion et le consommateur de service de gestion située à l'extérieur du domaine de confiance avec TLS de l'opérateur 3GPP.
- **Capacité de sécurité des API liées aux interfaces de gestion**: les API devraient être sécurisées en matière de droits d'exploitation et d'accès et ne devraient pas exposer de données de trafic. Les API liées aux interfaces de gestion devraient uniquement autoriser l'accès aux données et aux capacités, comme convenu entre les parties par des moyens légaux.

Annexe A

Architecture de sécurité du système de communication IMT-2020

(La présente annexe fait partie intégrante de la présente Recommandation.)

La Figure 4-1 présentée dans [b-TS 33.501] donne une vue d'ensemble de l'architecture de sécurité du système de communication IMT-2020.

La Figure 4-1 présentée dans [b-TS 33.501] illustre les domaines de sécurité suivants:

– Sécurité de l'accès au réseau (I): ensemble des fonctions de sécurité qui permettent aux équipements d'utilisateur d'authentifier des services et d'y accéder par le biais du réseau de façon sécurisée, y compris par le biais du réseau d'accès 3GPP et du réseau d'accès non 3GPP, et en particulier d'assurer une protection contre les attaques se produisant sur les interfaces (radioélectriques). Il s'agit également de la sécurité de contexte de remise en provenance du réseau de desserte (SN) jusqu'au réseau d'accès (AN) en ce qui concerne la sécurité d'accès.

– Sécurité dans le domaine de réseau (II): ensemble des fonctions de sécurité qui permettent à des nœuds du réseau d'échanger en toute sécurité des données de signalisation et des données sur le plan utilisateur.

– Sécurité dans le domaine de l'utilisateur (III): ensemble des fonctions de sécurité qui sécurisent l'accès de l'utilisateur aux équipements mobiles.

– Sécurité dans le domaine de l'application (IV): ensemble des fonctions de sécurité qui permettent à des applications dans le domaine de l'utilisateur et dans le domaine du fournisseur d'échanger des messages en toute sécurité. La sécurité dans le domaine de l'application n'entre pas dans le cadre de la présente Recommandation.

– Sécurité dans le domaine de l'architecture SBA (V): ensemble des fonctions de sécurité qui permettent aux fonctions de réseau de l'architecture SBA de communiquer en sécurité au sein du domaine du réseau SN et avec d'autres domaines du réseau. Ces fonctions incluent l'enregistrement des fonctions de réseau, les aspects de sécurité de découverte et d'autorisation ainsi que la protection des interfaces fondées sur les services. La sécurité dans le domaine de l'architecture SBA est une nouvelle fonction de sécurité par rapport à la norme [b-TS 33.401].

– Visibilité et configurabilité de la sécurité (VI): ensemble des fonctions qui permettent à l'utilisateur de savoir si une fonction de sécurité fonctionne ou non.

Appendice I

Architecture générique de sécurité de réseau pour assurer la sécurité du réseau de bout en bout

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

Le présent Appendice décrit une architecture générique de sécurité de réseau pour assurer la sécurité du réseau de bout en bout, comme décrite dans [b-UIT-T X.805], qui constitue la base de la présente Recommandation.

Une architecture de sécurité de réseau permettant d'assurer la sécurité du réseau de bout en bout est définie dans [b-UIT-T X.805]. Cette architecture peut s'appliquer, indépendamment de la technologie sous-jacente du réseau, à divers types de réseaux où la sécurité de bout en bout est primordiale. [b-UIT-T X.805] définit les éléments architecturaux liés à la sécurité générale, qui sont nécessaires pour assurer la sécurité de bout en bout. [b-UIT-T X.805] a pour objet d'établir les fondements devant permettre l'élaboration de Recommandations détaillées relatives à la sécurité du réseau de bout en bout.

La Recommandation [b-UIT-T X.805] définit huit dimensions de sécurité:

1) contrôle d'accès;
2) authentification;
3) non-répudiation;
4) confidentialité des données;
5) sécurité de la communication;
6) intégrité des données;
7) disponibilité;
8) respect de la vie privée.

La Recommandation [b-UIT-T X.805] définit également trois couches de sécurité qui, ensemble, permettent d'offrir des solutions fondées sur le réseau:

1) la couche de sécurité relative à l'infrastructure;
2) la couche de sécurité relative aux services;
3) la couche de sécurité relative aux applications.

En outre, [b-UIT-T X.805] définit trois plans de sécurité:

1) le plan de gestion;
2) le plan de commande;
3) le plan de l'utilisateur final.

Appendice II

Menace d'interruption de service due à une demande de connexion de contrôle des ressources radioélectriques (RRC) manipulée et capacités associées

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

II.1 Vue d'ensemble

Une demande de connexion RRC est un message transmis en clair lorsqu'un équipement d'utilisateur accède à un réseau. Elle contient un identificateur temporaire unique à l'échelle mondiale (GUTI) ou une S-TMSI, c'est-à-dire des informations d'identification temporaires de l'équipement d'utilisateur. Il existe plusieurs moyens de découvrir les informations d'identification temporaires d'un utilisateur donné. Si un attaquant intercepte cette demande de connexion RRC et modifie le message transmis en clair à l'étape précédente, les informations d'identification temporaires de la victime peuvent être utilisées pour bloquer en continu la connexion au réseau de la victime.

II.2 Scénario d'attaque

Un attaquant peut intercepter le message de demande de connexion RRC transmis en clair et identifier le GUTI ou la S-TMSI, qui fournissent des informations d'identification temporaires. Lors de l'envoi d'un message de demande de connexion RRC falsifié, l'attaquant utilise à mauvais escient les informations d'identification temporaires et le message est considéré à tort comme étant envoyé depuis l'équipement d'utilisateur de la victime. Bien que la connexion RRC de l'attaquant soit libérée en raison d'un échec d'authentification du code d'authentification de message (MAC) pendant la signalisation de la strate hors accès (NAS), l'attaquant peut bloquer en continu la connexion radioélectrique de la victime en envoyant à nouveau le même message falsifié. En outre, des informations d'identification temporaires sont nouvellement créées à intervalles réguliers, conformément à des règles spécifiques fondées sur l'IMSI. Si l'identité S-TMSI est modifiée, l'attaquant peut détecter la modification et envoyer à nouveau un message d'attaque. Pour bloquer l'accès radioélectrique à l'équipement d'utilisateur de la victime, l'attaquant doit envoyer un message de demande de connexion RRC falsifié. Deux conditions préalables doivent être remplies pour qu'il soit procédé à cette attaque: 1) l'attaquant doit placer son dispositif mobile dans la même cellule que l'équipement d'utilisateur de la victime pour intercepter le trafic radioélectrique; et 2) l'attaquant doit disposer d'un équipement d'utilisateur qui peut envoyer un message falsifié.

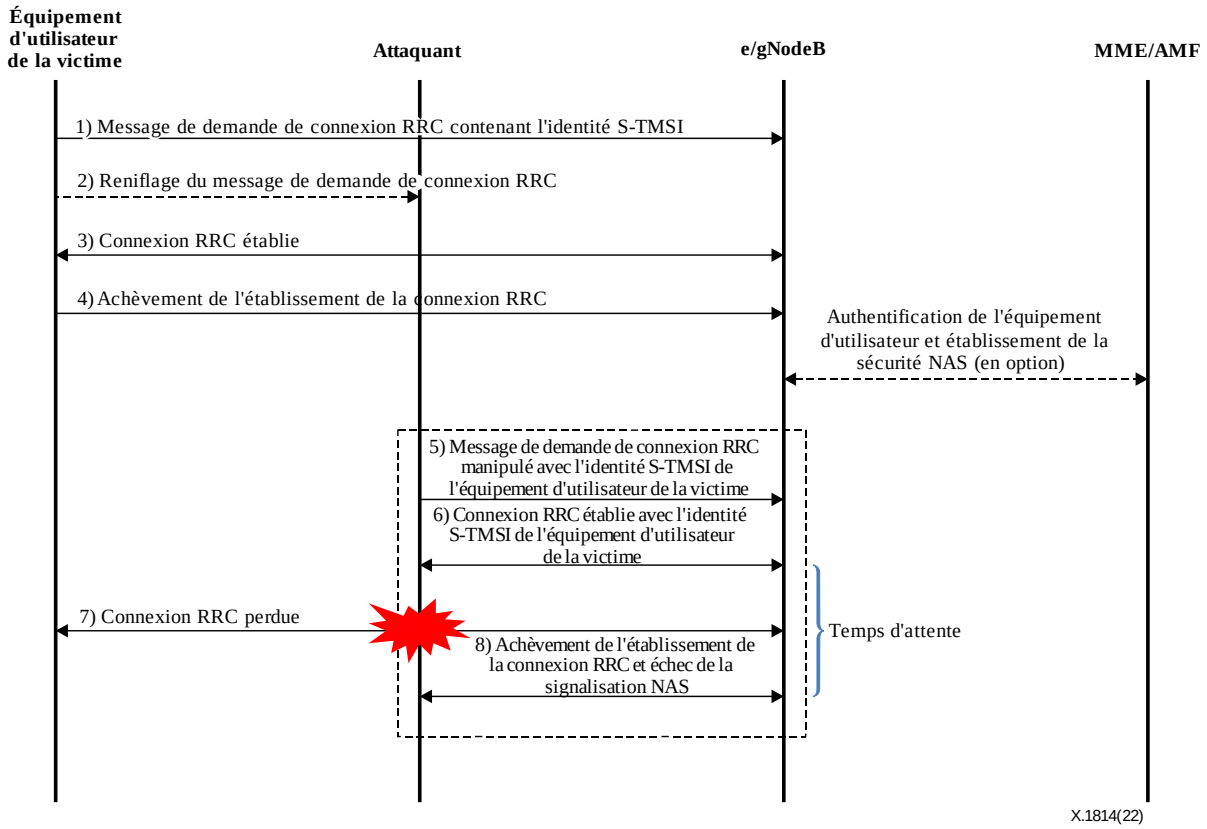

Figure II.1 – Scénario d'attaque de demande de connexion RRC manipulée

II.3 Conséquence

En raison de cette vulnérabilité, si rien n'est fait pour vérifier que le message a été altéré, l'équipement de réseau radioélectrique (e/gNodeB) déconnecte la connexion existante avec l'équipement d'utilisateur de la victime en fonction du message envoyé par l'attaquant et se connecte à l'équipement d'utilisateur de l'attaquant. L'équipement d'utilisateur de la victime peut rester dans un état où il ne peut pas accéder normalement au réseau.

II.4 Contre-mesures

La contre-mesure la plus simple et la plus efficace vise à ce que la station de base maintienne la connexion RRC avec l'utilisateur existant pendant un certain temps. Après que l'attaquant a établi la connexion RRC en utilisant l'identificateur volé de la victime, la connexion est libérée en cas d'échec du processus de signalisation NAS. Par conséquent, si la connexion existante de la victime est maintenue jusqu'à ce que la connexion RRC de l'attaquant soit libérée, la connexion radioélectrique peut être maintenue. Habituellement, le temps qui s'écoule entre le moment où un attaquant tente d'établir la connexion RRC et le moment où la connexion RRC est libérée en raison d'un échec du processus de signalisation NAS correspond à la durée pendant laquelle la station de base transmet l'information d'établissement de la connexion RRC et attend que l'établissement de la connexion RRC soit achevé. Ce faisant, le "temporisateur d'attente"[1] est mis en œuvre dans l'équipement e/gNodeB pour compter le temps écoulé depuis l'envoi à l'équipement d'utilisateur de l'information d'établissement de la connexion RRC jusqu'à la réception de cette information. Il convient d'ajouter un processus pour que la station de base maintienne une connexion plus longue que le temporisateur d'attente pour la connexion RRC existante, qui envoie à présent une demande avec un identificateur en double et maintient la connexion existante lorsqu'une nouvelle connexion est libérée dans les délais

[1] Par exemple T352 comme défini dans la norme 3GPP TS 25.331.

correspondants. La durée de maintenance doit être réduite au minimum compte tenu de son influence sur la qualité de fonctionnement des équipements et du service de communication.

En outre, un attaquant peut envoyer de façon répétée des demandes de connexion RRC à la station de base en vue de maintenir le statut d'interruption de service causée à une victime. Pour atténuer les effets de cette situation, des composantes "limit-time" (délai maximal) et "limit-count" (nombre maximal) au niveau de l'équipement e/gNodeB devraient être définis, si la connexion et la libération RRC sont effectuées de façon répétée dans le délai maximal et dans la limite fixée par la composante *count*, en ajoutant un processus afin que la station de base alerte l'opérateur de réseau pour surveiller les attaques.

Bibliographie

[b-UIT-T Q.700] Recommandation UIT-T Q.700 (1993), *Introduction au système de signalisation N° 7 du CCITT*.

[b-UIT-T X.509] Recommandation UIT-T X.509 (2019), *Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: cadre général des certificats de clé publique et d'attribut*.

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

[b-UIT-T X.1047] Recommandation UIT-T X.1047 (2021), *Exigences et architecture de sécurité pour la gestion et l'orchestration des tranches de réseau*.

[b-UIT-T X.1401] Recommandation UIT-T X.1401 (2019), *Menaces de sécurité pour la technologie des registres distribués.*

[b-UIT-T X.1406] Recommandation UIT-T X.1406 (2021), *Menaces de sécurité contre le vote en ligne à l'aide de la technologie des registres distribués.*

[b-UIT-T X.1408] Recommandation UIT-T X.1408 (2021), *Menaces et exigences de sécurité relatives à l'accès aux données et au partage de données reposant sur la technologie des registres distribués.*

[b-UIT-T X.1811] Recommandation UIT-T X.1811 (2021), *Lignes directrices en matière de sécurité relatives à l'utilisation d'algorithmes à l'épreuve des attaques quantiques dans les systèmes IMT-2020*.

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

[b-UIT-T Y.3101] Recommandation UIT-T Y.3101 (2018), *Exigences relatives aux réseaux IMT-2020*.

[b-UIT-T Y.3150] Recommandation UIT-T Y.3150 (2020), *Caractéristiques techniques de haut niveau de la logiciellisation des réseaux IMT-2020.*

[b-UIT-T Y.4807] Recommandation UIT-T Y.4807 (2020), *Intégration de l'agilité dès la conception pour la sécurité des systèmes de télécommunication/TIC utilisés dans l'Internet des objets*.

[b-UIT workshop] Troisième édition de la journée annuelle atelier et démonstration sur les IMT-2020/5G organisée par l'UIT (18 juillet 2018), *5G security activities and future plan in UIT-T SG17 (Activités relatives à la sécurité de la 5G et programme futur au sein de la CE 17 de l'UIT-T).*

[b-ISO 10393] ISO 10393:2013, *Rappel de produits de consommation – Lignes directrices pour les fournisseurs*.

[b-ISO 81001-1] ISO 81001-1:2021, *Sécurité, efficacité et sûreté des logiciels de santé et des systèmes TI de santé — Partie 1: Principes et concepts*

[b-ISO/IEC 27000] ISO/CEI 27000:2016, *Technologies de l'information – Techniques de sécurité – Systèmes de management de la sécurité de l'information – Vue d'ensemble et vocabulaire*.

[b-ISO/TS 21719-2] ISO/TS 21719-2:2018, *Perception de télépéage – Personnalisation des équipements embarqués – Partie 2: Utilisation des communications dédiées à courte portée.*

[b-RFC 3588] IETF RFC 3588 (2003), *Diameter base protocol (Protocole au niveau d'un diamètre de serveur)*.

[b-TR 33.811] 3GPP TR 33.811 (2018), *Study on security aspects of 5G network slicing management (Étude sur les aspects liés à la sécurité de la gestion du découpage de réseau 5G)*.

[b-TS 33.401] 3GPP TS 33.401 (2021), *3GPP System Architecture Evolution (SAE); Security architecture (Évolution de l'architecture système (SAE) 3GPP – Architecture de sécurité)*.

[b-TS 33.501] 3GPP TS 33.501 (2022), *Security architecture and procedures for 5G System (Architecture et procédures de sécurité pour les systèmes 5G)*.

[b-Alwakeel] Alwakeel, A.M., Alnaim, A., and Fernández, E.B., *A Survey of Network Function Virtualization Security (Enquête sur la sécurité de la virtualisation des fonctions de réseau)*, IEEE Southeast Conf. 2018. https://www.researchgate.net/publication/328146655_A_Survey_of_Network_Function_Virtualization_Security

[b-Craven] Craven, C., *5G Security Standards: What Are They? (Normes de sécurité pour la 5G: de quoi s'agit-il?)*, 10 juin 2020. https://www.sdxcentral.com/5g/definitions/5g-security-standards/

[b-ENISA] Agence de l'Union européenne pour la cybersécurité (ENISA) (2019), *ENISA Threat Landscape for 5G Networks (État des lieux des menaces de l'ENISA concernant les réseaux 5G)*.

[b-Goodin] Goodin, D. (2013), *Lucky Thirteen attack snarfs cookies protected by SSL encryption (Une attaque Lucky Thirteen a permis de dérober des cookies protégés par un chiffrement SSL*), Ars Technica. https://arstechnica.com/security/2013/02/lucky-thirteen-attack-snarfs-cookies-protected-by-ssl-encryption/

[b-Khan] Khan, R., Kumar, P., Jayakody, D.N.K, and Liyanage, M. (2019), *A Survey on Security and Privacy of 5G Technologies: Potential Solutions, Recent Advancements and Future Directions (Enquête sur la sécurité et la confidentialité des technologies 5G – Solutions potentielles, avancées récentes et orientations futures)*, IEEE Communications Surveys and Tutorials, Vol. 22, No. 1, Juillet, 196-248.

[b-Möller] Möller, B, Duong, T, and Kotowicz, K. (2014), *This POODLE Bites: Exploiting The SSL 3.0 Fallback (Cette attaque POODLE fait mal: exploitation des vulnérabilités du protocole SSL 3.0)*. https://www.openssl.org/~bodo/ssl-poodle.pdf

[b-NGMN] The Next Generation Mobile Networks Alliance (NGMN Alliance) (2016), *5G Security Recommendations Package (Ensemble de recommandations en matière de sécurité pour la 5G)*.

[b-Olimid] Olimid, R., and Nencioni, G. (2020) *5G Network Slicing: A Security Overview (Découpage en tranches de réseau 5G – Vue d'ensemble de la sécurité)*, IEEE Access, Vol. 8, juin, 99999–100009.

[b-SQL] OWASP, *SQL injection (Attaque par injection SQL)*. https://owasp.org/www-community/attacks/SQL_Injection

[b-Ta-Hao Ting] Ta-Hao Ting, Tsung-Nan Lin, Shan-Hsiang Shen, and Yu-Wei Chang (2019), *Guidelines for 5G end to end architecture and security issues (Lignes directrices relatives aux questions de sécurité et d'architecture 5G de bout en bout)*. https://arxiv.org/abs/1912.10318

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, 2022