Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

X.1361

(09/2018)

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

Applications et services sécurisés (2) – Sécurité de l'Internet des objets (IoT)

Cadre de sécurité applicable à l'Internet des objets fondé sur le modèle passerelle

Recommandation UIT-T X.1361

RECOMMANDATIONS UIT-T DE LA SÉRIE X

RÉSEAUX DE DONNÉES, COMMUNICATION ENTRE SYSTÈMES OUVERTS ET SÉCURITÉ

RÉSEAUX PUBLICS DE DONNÉES	X.1–X.199
INTERCONNEXION DES SYSTÈMES OUVERTS	X.200–X.299
INTERFONCTIONNEMENT DES RÉSEAUX	X.300–X.399
SYSTÈMES DE MESSAGERIE	X.400–X.499
ANNUAIRE	X.500–X.599
RÉSEAUTAGE OSI ET ASPECTS SYSTÈMES	X.600–X.699
GESTION OSI	X.700–X.799
SÉCURITÉ	X.800–X.849
APPLICATIONS OSI	X.850–X.899
TRAITEMENT RÉPARTI OUVERT	X.900–X.999
SÉCURITÉ DE L'INFORMATION ET DES RÉSEAUX	
Aspects généraux de la sécurité	X.1000–X.1029
Sécurité des réseaux	X.1030–X.1049
Gestion de la sécurité	X.1050–X.1069
Télébiométrie	X.1080–X.1099
APPLICATIONS ET SERVICES SÉCURISÉS (1)	
Sécurité en multidiffusion	X.1100–X.1109
Sécurité des réseaux domestiques	X.1110–X.1119
Sécurité des télécommunications mobiles	X.1120–X.1139
Sécurité de la toile	X.1140–X.1149
Protocoles de sécurité (1)	X.1150–X.1159
Sécurité d'homologue à homologue	X.1160–X.1169
Sécurité des identificateurs en réseau	X.1170–X.1179
Sécurité de la télévision par réseau IP	X.1180–X.1199
SÉCURITÉ DU CYBERESPACE	
Cybersécurité	X.1200–X.1229
Lutte contre le spam	X.1230–X.1249
Gestion des identités	X.1250–X.1279
APPLICATIONS ET SERVICES SÉCURISÉS (2)	
Communications d'urgence	X.1300–X.1309
Sécurité des réseaux de capteurs ubiquitaires	X.1310–X.1319
Sécurité des réseaux électriques intelligents	X.1330–X.1339
Courrier certifié	X.1340–X.1349
Sécurité de l'Internet des objets (IoT)	**X.1360–X.1369**
Sécurité des systèmes de transport intelligents	X.1370–X.1389
Sécurité de la technologie des registres distribués	X.1400–X.1429
Protocoles de sécurité (2)	X.1450–X.1459
ECHANGE D'INFORMATIONS SUR LA CYBERSÉCURITÉ	
Aperçu général de la cybersécurité	X.1500–X.1519
Echange concernant les vulnérabilités/les états	X.1520–X.1539
Echange concernant les événements/les incidents/l'heuristique	X.1540–X.1549
Echange de politiques	X.1550–X.1559
Heuristique et demande d'informations	X.1560–X.1569
Identification et découverte	X.1570–X.1579
Echange garanti	X.1580–X.1589
SÉCURITÉ DE L'INFORMATIQUE EN NUAGE	
Aperçu de la sécurité de l'informatique en nuage	X.1600–X.1601
Conception de la sécurité de l'informatique en nuage	X.1602–X.1639
Bonnes pratiques et lignes directrices concernant la sécurité de l'informatique en nuage	X.1640–X.1659
Mise en œuvre de la sécurité de l'informatique en nuage	X.1660–X.1679
Sécurité de l'informatique en nuage (autres)	X.1680–X.1699

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

Recommandation UIT-T X.1361

Cadre de sécurité applicable à l'Internet des objets fondé sur le modèle passerelle

Résumé

La Recommandation UIT-T X.1361 décrit un cadre de sécurité applicable à l'Internet des objets qui s'appuie sur des passerelles de sécurité. L'Internet des objets est une infrastructure mondiale pour la société de l'information, qui permet de disposer de services évolués en interconnectant des objets (physiques ou virtuels) grâce aux technologies de l'information et de la communication interopérables existantes ou en évolution.

La présente Recommandation analyse les menaces et les problèmes de sécurité dans l'environnement de l'Internet des objets et décrit les capacités qui pourraient permettre d'y faire face et de les atténuer. Elle présente une méthode générale permettant de déterminer quelles capacités de sécurité sont requises pour faire face à ces menaces et à ces problèmes et les atténuer dans le cadre de l'Internet des objets.

Historique

Edition	Recommandation	Approbation	Commission d'études	Identifiant unique*
1.0	UIT-T X.1361	07-09-2018	17	11.1002/1000/13607

Mots clés

Cadre de sécurité, exigences de sécurité, Internet des objets.

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

AVANT-PROPOS

L'Union internationale des télécommunications (UIT) est une institution spécialisée des Nations Unies dans le domaine des télécommunications et des technologies de l'information et de la communication (ICT). Le Secteur de la normalisation des télécommunications (UIT-T) est un organe permanent de l'UIT. Il est chargé de l'étude des questions techniques, d'exploitation et de tarification, et émet à ce sujet des Recommandations en vue de la normalisation des télécommunications à l'échelle mondiale.

L'Assemblée mondiale de normalisation des télécommunications (AMNT), qui se réunit tous les quatre ans, détermine les thèmes d'étude à traiter par les Commissions d'études de l'UIT-T, lesquelles élaborent en retour des Recommandations sur ces thèmes.

L'approbation des Recommandations par les Membres de l'UIT-T s'effectue selon la procédure définie dans la Résolution 1 de l'AMNT.

Dans certains secteurs des technologies de l'information qui correspondent à la sphère de compétence de l'UIT-T, les normes nécessaires se préparent en collaboration avec l'ISO et la CEI.

NOTE

Dans la présente Recommandation, l'expression "Administration" est utilisée pour désigner de façon abrégée aussi bien une administration de télécommunications qu'une exploitation reconnue.

Le respect de cette Recommandation se fait à titre volontaire. Cependant, il se peut que la Recommandation contienne certaines dispositions obligatoires (pour assurer, par exemple, l'interopérabilité et l'applicabilité) et on considère que la Recommandation est respectée lorsque toutes ces dispositions sont observées. Le futur d'obligation et les autres moyens d'expression de l'obligation comme le verbe "devoir" ainsi que leurs formes négatives servent à énoncer des prescriptions. L'utilisation de ces formes ne signifie pas qu'il est obligatoire de respecter la Recommandation.

DROITS DE PROPRIÉTÉ INTELLECTUELLE

L'UIT attire l'attention sur la possibilité que l'application ou la mise en œuvre de la présente Recommandation puisse donner lieu à l'utilisation d'un droit de propriété intellectuelle. L'UIT ne prend pas position en ce qui concerne l'existence, la validité ou l'applicabilité des droits de propriété intellectuelle, qu'ils soient revendiqués par un membre de l'UIT ou par une tierce partie étrangère à la procédure d'élaboration des Recommandations.

A la date d'approbation de la présente Recommandation, l'UIT n'avait pas été avisée de l'existence d'une propriété intellectuelle protégée par des brevets à acquérir pour mettre en œuvre la présente Recommandation. Toutefois, comme il ne s'agit peut-être pas de renseignements les plus récents, il est vivement recommandé aux développeurs de consulter la base de données des brevets du TSB sous http://www.itu.int/ITU-T/ipr/.

TABLE DES MATIÈRES

Recommandation UIT-T X.1361

Cadre de sécurité applicable à l'Internet des objets fondé sur le modèle passerelle

1 Domaine d'application

La présente Recommandation décrit un cadre de sécurité applicable à l'Internet des objets qui s'appuie sur des passerelles de sécurité.

La présente Recommandation analyse les menaces et les problèmes de sécurité dans l'environnement de l'Internet des objets et décrit les capacités qui permettent d'y faire face et de les atténuer. Elle présente une méthode générale permettant de déterminer quelles capacités de sécurité sont requises pour faire face à ces menaces et à ces problèmes et les atténuer dans le cadre de l'Internet des objets.

La présente Recommandation porte essentiellement sur les capacités de sécurité IoT fondées sur des passerelles de sécurité et traite du modèle de référence décrit dans [b-UIT-T Y.4401] du point de vue des aspects techniques et non de la gestion.

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. Toutes les Recommandations et autres références étant sujettes à révision, les utilisateurs de la présente Recommandation sont invités à rechercher la possibilité d'appliquer les éditions les plus récentes des Recommandations et autres références énumérées ci-dessous. Une liste des Recommandations UIT-T en vigueur est publiée périodiquement. La référence à un document figurant dans la présente Recommandation ne donne pas à ce document en tant que tel le statut de Recommandation.

[UIT-T Y.4100] Recommandation UIT-T Y.4100/Y.2066 (2014), *Exigences communes relatives à l'Internet des objets*.

3 Définitions

3.1 Termes définis ailleurs

La présente Recommandation utilise les termes suivants définis ailleurs:

3.1.1 attaque [b-ISO 13491-1]: tentative d'obtention ou de modification d'informations sensibles ou d'un service sur un dispositif, par un adversaire qui n'y est pas autorisé.

3.1.2 authentification [b-NIST-SP-800-53]: vérification de l'identité d'un utilisateur, d'un processus ou d'un dispositif, souvent indispensable pour pouvoir accéder aux ressources d'un système d'information.

3.1.3 capacité [b-ISO 19440]: construction qui représente l'ensemble des caractéristiques d'une capacité (appelées attributs d'une capacité) soit d'une ressource (sa capacité fournie) soit d'une activité d'une entreprise (sa capacité requise).

NOTE – Les capacités peuvent être regroupées.

3.1.4 contexte [b-UIT-T X.1252]: environnement avec des frontières définies dans lequel des entités existent et interagissent.

3.1.5 algorithme de chiffrement [b-ISO/CEI 19790]: procédure de calcul bien définie qui, à partir de variables d'entrée, pouvant inclure des clés de chiffrement, produit un résultat.

3.1.6 nombre aléatoire de qualité cryptographique [b-UIT-T X.667]: nombre aléatoire ou pseudo-aléatoire généré par un mécanisme qui garantit une dispersion suffisante de valeurs générées de façon répétitive pour que ces valeurs soient acceptables pour utilisation dans des travaux cryptographiques (et qui est utilisé dans de tels travaux).

3.1.7 cryptographie [b-UIT-T X.800]: discipline incluant les principes, moyens et méthodes de transformation des données, dans le but de cacher leur contenu, d'empêcher que leur modification passe inaperçue et/ou d'empêcher leur utilisation non autorisée.

NOTE – La cryptographie détermine les méthodes de chiffrement et de déchiffrement. Une attaque portant sur les principes, moyens et méthodes de cryptographie est appelée analyse cryptographique.

3.1.8 système de chiffrement [b-ISO 11568-1]: ensemble de primitives de chiffrement utilisées pour fournir des services de sécurité de l'information.

3.1.9 dispositif [b-UIT-T Y.4000]: dans l'Internet des objets, équipement doté obligatoirement de capacités de communication et éventuellement de capacités de détection, d'actionnement, de saisie de données, de stockage de données et de traitement de données.

3.1.10 gestion d'identité [b-UIT-T X.1250]: ensemble de fonctions et de capacités (par exemple, l'administration, la gestion et la tenue à jour, la découverte, les échanges de communication, la corrélation et les liens, l'application des politiques, l'authentification et les assertions) utilisées pour:

– garantir les informations d'identité (par exemple, les identificateurs, les justificatifs d'identité, les attributs);

– garantir l'identité d'une entité (par exemple les utilisateurs/abonnés, les groupes, les dispositifs d'utilisateur, les organisations, les fournisseurs de réseau et de service, les éléments et objets de réseau et les objets virtuels); et

– permettre des applications commerciales et liées à la sécurité.

3.1.11 Internet des objets (IoT) [b-UIT-T Y.4000]: infrastructure mondiale pour la société de l'information, qui permet de disposer de services évolués en interconnectant des objets (physiques ou virtuels) grâce aux technologies de l'information et de la communication interopérables existantes ou en évolution.

NOTE 1 – En exploitant les capacités d'identification, de saisie de données, de traitement et de communication, l'IoT tire pleinement parti des objets pour offrir des services à toutes sortes d'applications, tout en garantissant le respect des exigences de sécurité et de confidentialité.

NOTE 2 – Dans une optique plus large, l'IoT peut être considéré comme un concept ayant des répercussions sur les technologies et la société.

3.1.12 détection des intrusions [b-ISO/CEI 27039]: processus formel de détection des intrusions, qui se caractérise généralement par la collecte de connaissances sur les profils d'utilisation anormaux, sur le type de vulnérabilité qui a été exploité ainsi que sur la manière et le moment où elle a été exploitée.

3.1.13 système de détection des intrusions [b-ISO/CEI 27039]: systèmes d'information utilisés pour déterminer qu'une tentative d'intrusion a eu lieu ou qu'une intrusion est en cours ou a eu lieu.

3.1.14 prévention des intrusions [b-ISO/CEI 27033-1]: processus formel consistant à intervenir de manière active pour prévenir les intrusions.

3.1.15 système de prévention des intrusions [b-ISO/CEI 27039]: variante des systèmes de détection des intrusions conçue précisément pour fournir une capacité de réponse active.

3.1.16 gestion de clés [b-UIT-T X.800]: production, stockage, distribution, suppression, archivage et application de clés conformément à la politique de sécurité.

3.1.17 cryptographie pour environnements contraints [b-ISO/CEI 29192-1]: cryptographie adaptée en vue de sa mise en œuvre dans des environnements contraints.

3.1.18 logiciel malveillant [b-ISO/CEI 27033-1]: logiciel conçu expressément pour endommager ou perturber un système, et nuire à la confidentialité, à l'intégrité et/ou à la disponibilité.

NOTE – Les virus et les chevaux de Troie sont des exemples de logiciels malveillants.

3.1.19 surveillance du réseau [b-ISO/CEI 27033-1]: processus consistant à observer et examiner en permanence, d'une part, les données enregistrées concernant l'activité et les opérations sur un réseau, y compris les journaux d'audit et les alertes, et, d'autre part, les analyses connexes.

3.1.20 information d'identification personnelle (PII) [b-ISO/CEI 29100]: toute information qui a) peut être utilisée pour identifier la personne à laquelle elle se rapporte; ou b) est ou peut être directement ou indirectement liée à une personne.

NOTE – Pour déterminer si la personne à laquelle les informations se rapportent peut être identifiée, il convient de tenir compte de tous les moyens qui peuvent être raisonnablement utilisés par la partie intervenant dans la protection de la vie privée et détenant les données ou par toute autre partie pour identifier cette personne.

3.1.21 association de sécurité avec gabarit (SAM) [b-UIT-T X.1362]: ensemble de paramètres propres à un protocole de sécurité. L'association SAM définit les services et les mécanismes nécessaires pour protéger le trafic en appliquant la méthode de chiffrement avec données de gabarit associées (EAMD). C'est le protocole associé à une association SAM qui redirige vers elle, en fonction des couches du protocole telles que la couche transport ou la couche du protocole Internet (IP). Il est possible d'inclure, dans ces paramètres, des identificateurs d'algorithmes, des modes, des identificateurs de couche à laquelle est appliqué le chiffrement EAMD ainsi que des clés de chiffrement.

3.1.22 capteur [b-UIT-T Y.4105]: dispositif électronique qui détecte une condition physique ou un composé chimique et fournit un signal électronique proportionnel à la caractéristique observée.

3.1.23 objet [b-UIT-T Y.4000]: dans l'Internet des objets, objet du monde physique (objet physique) ou du monde de l'information (objet virtuel), pouvant être identifié et intégré dans des réseaux de communication.

3.1.24 menace [b-ISO/CEI 27000]: cause potentielle d'un incident indésirable, qui peut nuire à un système ou à un organisme.

3.1.25 vulnérabilité [b-ISO/CEI 27000]: faille dans un actif ou dans une mesure de sécurité qui peut être exploitée par une ou plusieurs menaces.

3.2 Termes définis dans la présente Recommandation

La présente Recommandation définit les termes suivants:

3.2.1 négociation de l'algorithme de chiffrement: mécanisme permettant de déterminer le type d'algorithme de chiffrement et la longueur des clés de chiffrement à utiliser dans une session de communication chiffrée et intégrée et de découvrir l'algorithme de chiffrement le mieux adapté disponible aux deux extrémités.

3.2.2 gestion des correctifs: processus comprenant l'acquisition, le test et l'installation de multiples correctifs pour les systèmes d'information.

NOTE – Une capacité de gestion des vulnérabilités pourrait être envisagée.

3.2.3 atteinte aux informations PII: situation dans laquelle des informations d'identification personnelle sont traitées de manière non conforme à une ou plusieurs exigences de protection des informations PII.

3.2.4 modèle de préférence en matière de protection de la vie privée: modèle qui permet aux sites web de déclarer l'utilisation prévue des données qu'ils rassemblent sur les personnes afin que ces personnes aient davantage de contrôle sur leurs informations personnelles.

3.2.5 configuration sécurisée: processus grâce auquel les dispositifs de réseau devraient être configurés pour réduire le niveau des vulnérabilités inhérentes et fournir uniquement les services nécessaires pour s'acquitter de leur fonction.

NOTE – Ce processus comprend la suppression ou la désactivation des comptes d'utilisateur inutiles et des logiciels inutiles, le remplacement des mots de passe par défaut par un autre mot de passe fort, l'activation des pare-feu et la configuration pour désactiver (bloquer) les connexions non approuvées par défaut et la désactivation de la fonction auto-exécution.

3.2.6 passerelle de sécurité: point de connexion entre des réseaux, ou entre des sous-groupes à l'intérieur de réseaux, ou entre des applications logicielles à l'intérieur de domaines de sécurité différents dont le rôle est de protéger un réseau conformément à une politique de sécurité donnée dans l'environnement de l'Internet des objets.

NOTE – Cette définition est adaptée de [b-ISO/CEI 27033-1]; on parle de "passerelle" dans la présente Recommandation.

3.2.7 attaque par voie latérale: attaque utilisant des informations obtenues auprès de la mise en œuvre physique d'un système de chiffrement.

NOTE – Les informations sur les plages horaires de fonctionnement, la consommation électrique et les fuites électromagnétiques peuvent être utilisées pour percer le système de chiffrement.

3.2.8 gestion des vulnérabilités: processus consistant à identifier, à classer, à résoudre et à atténuer les vulnérabilités.

4 Abréviations et acronymes

La présente Recommandation utilise les abréviations et acronymes suivants:

DoS déni de service (*denial of service*)

EAMD chiffrement avec données de gabarit associées (*encryption with associated mask data*)

IDS système de détection des intrusions (*intrusion detection system*)

IoT Internet des objets (*Internet of things*)

IP protocole Internet (*Internet protocol*)

IPS système de prévention des intrusions (*intrusion prevention system*)

PII information d'identification personnelle (*personally identifiable information*)

5 Conventions

Aucune.

6 Aperçu

L'Internet des objets (IoT) est défini comme étant une infrastructure mondiale pour la société de l'information, qui permet de disposer de services évolués en interconnectant des objets (physiques ou virtuels) grâce aux technologies de l'information et de la communication interopérables existantes ou en évolution.

Un exemple de déploiement type de l'Internet des objets sera composé de dispositifs d'extrémité dotés de capteurs installés sur un réseau filaire ou hertzien, qui envoient des données via une passerelle vers un nuage public ou privé. Les aspects de la topologie varieront considérablement d'une application à l'autre; par exemple, dans certains cas, la passerelle pourra être située sur le dispositif. Les dispositifs fondés sur ce type de topologies pourront être des dispositifs créés de toutes pièces pour fonctionner avec l'Internet des objets ou des dispositifs existants auxquels des capacités IoT ont été ajoutées après leur déploiement.

7 Architecture et cadre fonctionnels

La présente Recommandation repose sur l'architecture fonctionnelle de l'Internet des objets décrite dans la Figure 1.

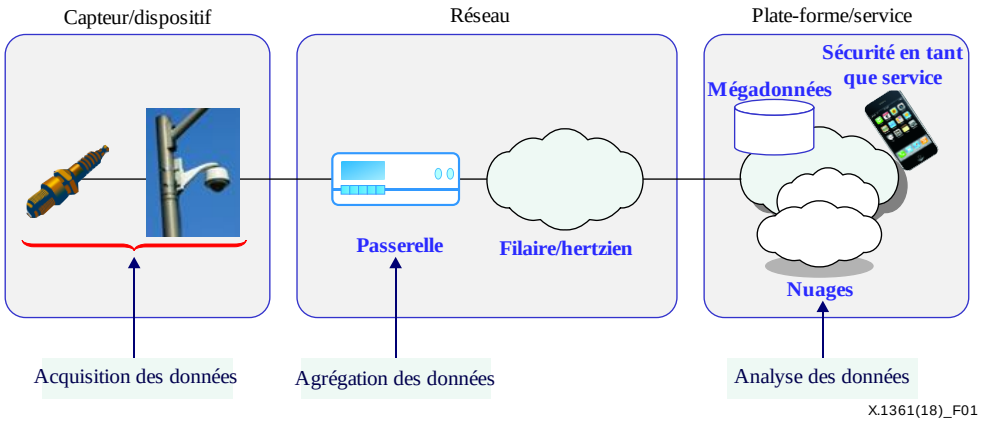

Figure 1 – Architecture fonctionnelle de l'Internet des objets (simplifiée)

Les données entre un point d'extrémité IoT (capteur ou dispositif) et une passerelle peuvent être acheminées sur deux types de réseaux de communication: un réseau fondé sur le protocole Internet (IP) ou un réseau non fondé sur le protocole IP. On part du principe que la communication entre la passerelle et le composant IoT de la plate-forme IoT, déployée dans un centre de données, devrait être acheminée grâce à un protocole fondé sur IP. Par conséquent, dans le cas d'un réseau non IP, il convient de mettre fin à la connexion de communication établie sur le réseau non IP et d'en établir une nouvelle sur un réseau IP au niveau de la passerelle.

L'architecture fonctionnelle peut être élaborée comme indiqué dans la Figure 2.

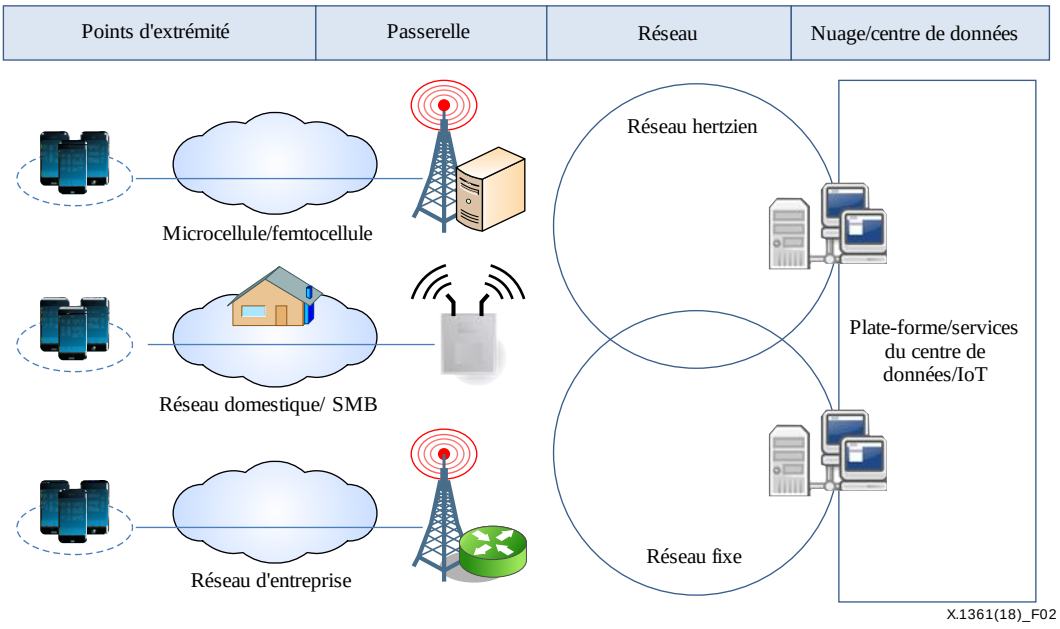

Figure 2 – Architecture fonctionnelle pratique

Par exemple, dans un système de transport intelligent, la passerelle, figurant dans Figure 2, pourrait servir de passerelle mobile embarquée pour connecter un réseau local interne (voiture) et un réseau ouvert extérieur.

Une capacité de pare-feu devrait être en place dans la passerelle afin de contrôler le trafic dont le point de terminaison est le dispositif. Certaines dispositifs IoT ont des protocoles de transport particuliers, différents du protocole de commande de transmission/des protocoles IP. Il est possible d'utiliser des protocoles propriété pour régir les communications entre dispositifs IoT. Ainsi, des capacités de filtrage des protocoles privés devraient être en place afin d'identifier les données utiles malveillantes qui pourraient éventuellement se cacher dans des protocoles non IP.

La passerelle devrait mettre en œuvre une fonction pour filtrer certaines données dont le point de terminaison est ce dispositif afin d'utiliser au mieux les ressources de calcul limitées disponibles.

La passerelle est un élément avec un rôle unique dans l'architecture fonctionnelle. Elle est en effet souvent le premier point de sécurité fiable dans un système IoT, car les points d'extrémité sont particulièrement vulnérables aux altérations physiques. Le rôle que joue la passerelle dans l'Internet des objets fait d'elle un élément de sécurité particulier, à part du réseau. La passerelle devrait tenir compte des contraintes auxquelles les nœuds de sécurité sont soumis. Souvent, elle peut s'acquitter de certaines fonctions de sécurité au nom des points d'extrémité soumis à des contraintes, comme la gestion des clés, la négociation des suites de chiffrement ou la prévention des intrusions.

Les capacités de sécurité d'une passerelle varieront considérablement en fonction de facteurs comme la puissance et les capacités des points d'extrémité, la conception du service, la conception du réseau, l'emplacement physique et le contexte d'utilisation.

8 Menaces pour la sécurité de l'Internet des objets

8.1 Menaces pour la sécurité des capteurs/dispositifs IoT

Menaces propres aux capteurs/dispositifs:

– Détournement du dispositif: s'applique à un dispositif qui est physiquement compromis ou pour lequel les clés sont perdues.

– Attaque du puits (sinkhole): désigne une attaque dans laquelle un dispositif compromis attire le trafic de communication pour former un trou noir ou mettre en place une retransmission sélective. Dans ce type d'attaque, un intrus compromet un dispositif ou introduit un dispositif de contrefaçon dans le réseau et l'utilise pour lancer une attaque du puits. Le dispositif compromis essaie d'attirer la totalité du trafic de données provenant des nœuds voisins sur la base des paramètres de routage utilisés dans le protocole de routage. Une fois cette opération réussie, le dispositif compromis lancera une attaque. Il s'agit d'une forme d'attaque de la couche réseau dans laquelle un dispositif compromis envoie de fausses informations de routage aux entités voisines pour attirer à lui le trafic de réseau. En raison de la présence de réseaux ad hoc et des schémas de communication multipoint à point utilisés par les réseaux sans fil où de nombreux de nœuds envoient des données à une seule station de base, les réseaux sans fil sont particulièrement vulnérables à ce type d'attaque. Vu les flux de communication dans un réseau sans fil, le puits n'a pas besoin de cibler tous les nœuds du réseau, mais uniquement ceux proches de la station de base.

– Attaque Sybil: désigne une attaque dans laquelle un dispositif malveillant prend de multiples identités de manière illégitime. On appelle nœud Sybil une identité supplémentaire du dispositif malveillant. Cette attaque est menée en même temps que d'autres attaques pour réduire l'efficacité des mécanismes tolérant les dérangements comme le stockage réparti, le routage multi-trajets et la maintenance de la topologie.

– Attaques par inondation: type d'attaque par déni de service (DoS) dans laquelle l'auteur de l'attaque envoie une succession de paquets "hello" à un dispositif visé afin de consommer une part suffisante des ressources du dispositif pour que celui-ci ne puisse plus répondre au trafic légitime.
– Attaque par retransmission sélective: attaque dans laquelle un nœud compromis filtre de manière aléatoire les paquets reçus et en retransmet certains au nœud suivant. On parle d'attaque par trou noir lorsque le nœud filtre (écarte) tous les paquets qu'il reçoit.
– Attaque par trou de ver: une attaque par trou de vers se produit lorsque deux nœuds malveillants/compromis font croire que le trajet les reliant est très court. Un tunnel est un trajet de données entre deux dispositifs en réseau qui est établi à l'intérieur d'une infrastructure de réseau existante. Un réseau qui envoie des données vers un autre réseau via un tunnel obtient les données auprès d'un réseau et les réplique vers un autre réseau en passant par le tunnel et cette action peut perturber le réseau. Un hackeur peut alors entrer facilement dans le réseau et l'utiliser de manière illégitime. Associée à une attaque du puits et à une attaque Sybil, cette attaque peut aboutir à une retransmission sélective ou à la création d'un puits.
– Usurpation de l'identité du capteur/dispositif: désigne une attaque dans laquelle l'auteur de l'attaque réussit à se faire passer pour un capteur/dispositif légitime.

8.2 Menaces pour la sécurité des passerelles IoT

Menaces propres aux passerelles:

– Accès non autorisé: l'accès non autorisé à une passerelle peut entraîner la divulgation d'informations sensibles, la modification de données, des dénis de service et l'utilisation illicite de ressources. Par exemple, dès lors qu'il a réussi à accéder à une passerelle, l'auteur d'une attaque peut surveiller les données qui ne sont donc plus chiffrées, les noms d'utilisateurs, les mots de passe et les données de configuration sécurisée étant alors compromis.
– Passerelle malveillante: même si toutes les passerelles hertziennes sont sécurisées, il est facile pour l'auteur d'une attaque de déployer sa propre passerelle malveillante. Par exemple, un employé trop "enthousiaste" pourrait installer un point d'accès hertzien dans son bureau sans se soucier de la sécurité, contournant ainsi, dans la pratique, nombre des mesures de sécurité en place et risquant même de causer des brouillages radioélectriques à l'installation officielle de l'organisation et/ou de l'entreprise. De même, un point d'accès hertzien malveillant pourrait être installé de manière délibérée et en secret afin de permettre à l'auteur d'une attaque d'accéder facilement au réseau, localement ou à distance. L'auteur de cette attaque (appelé "double maléfique") pourrait remplacer un point d'accès hertzien existant par un point dont il maîtrise entièrement la configuration et la gestion, voire configurer un point d'accès hertzien malveillant, avec des paramètres analogues mais avec un rapport de puissance plus élevé permettant de couvrir le signal du point d'accès hertzien légitime. Dès qu'un dispositif légitime est trompé et se connecte à une passerelle malveillante, il est possible de rassembler des informations confidentielles sur les connexions.
– Attaque par déni de service: une attaque par déni de service sature la mémoire et/ou la capacité informatique de sa cible afin que celle-ci ralentisse de manière significative voire interrompe la fourniture des services. La cible est occupée à répondre au trafic illégitime que l'auteur de l'attaque lui envoie. Les réseaux de capteurs sans fil sont particulièrement vulnérables aux attaques par déni de service en raison de leurs caractéristiques de support ouvert dont la topologie évolue de manière dynamique et de l'absence de stratégie de défense claire. Les attaques par déni de service constituent un problème de plus en plus important pour les réseaux d'aujourd'hui. Nombre des techniques de défense mises au point pour les réseaux filaires fixes ne peuvent être appliquées dans les environnements des réseaux mobiles.

8.3 Menaces pour la sécurité du réseau

Menaces propres au réseau:

– Accès non autorisé: l'accès non autorisé à un réseau de capteurs sans fil peut entraîner la divulgation d'informations sensibles, la modification de données, des dénis de service et l'utilisation illicite de ressources. Par exemple, dès lors qu'il a réussi à accéder à un réseau de capteurs, l'auteur d'une attaque peut surveiller les données qui ne sont donc plus chiffrées, les noms d'utilisateurs et les mots de passe étant alors compromis.

– Reniflage des paquets: dans le cas des réseaux de capteurs sans fil qui n'ont pas de capacités de chiffrement, il est généralement facile pour l'auteur du attaque d'écouter clandestinement les communications sur le réseau. Pour ce faire, il faut une antenne, ainsi que des outils de réseaux hertziens normaux et un renifleur de paquets. Un renifleur de paquets est un outil qui met la carte réseau en "mode promiscuité", ce qui signifie que l'interface recevra et traitera la totalité du trafic et non uniquement le trafic qui lui est destiné. Le renifleur montrera à son utilisateur tous les paquets du réseau et les décodera pour en faciliter la lecture. Le trafic en texte clair est facile à comprendre et il est possible de définir des filtres pour rechercher certains mots clés ou certaines valeurs.

– Bluejacking: il s'agit d'une attaque visant les dispositifs mobiles dotés d'une fonction Bluetooth, comme les téléphones cellulaires. L'auteur de l'attaque envoie des messages non sollicités aux utilisateurs de dispositifs Bluetooth. Les messages envoyés n'endommagent pas le dispositif visé, mais peuvent amener l'utilisateur à répondre d'une certaine manière ou à ajouter de nouveau contact dans son répertoire.

– Bluesnarfing: cette attaque permet d'accéder sans autorisation à des informations contenues dans un dispositif sans fil cible grâce à une connexion Bluetooth, souvent entre téléphones, ordinateurs de bureau, ordinateurs portables et assistants numériques personnels (PDA). Lorsqu'elle est réussie, cette attaque peut permettre d'accéder sans autorisation à des informations privées et confidentielles stockées sur ces dispositifs.

8.4 Menaces pour la sécurité des plates-formes/services

Dans l'Internet, la couche application est principalement chargée de rassembler et de traiter un volume important de données d'utilisateur, comprenant des informations personnelles sur les utilisateurs ou des informations confidentielles se rapportant à diverses transactions. Les données sont la cible principale de l'auteur d'une attaque, et peuvent être volées, altérées ou endommagées. Il est nécessaire de les protéger en utilisant des mécanismes de protection de la confidentialité. Les menaces visant la couche application sont les suivantes: traitement de données de masse, dispositifs intelligents dont on a perdu le contrôle, intervention humaine non autorisée et dispositifs dont on a perdu le contrôle incapables de se rétablir après une catastrophe.

Menaces propres aux plates-formes/services:

– Profilage: processus d'exploration utilisé pour rassembler des informations sur la plate-forme/les services.

– Déni de service: attaque dans le cadre de laquelle la plate-forme/le service est submergé(e) par un très grand nombre de demandes de services et est de ce fait trop occupé(e) pour répondre aux demandes des clients légitimes.

– Exécution d'un code arbitraire: attaque consistant à tenter d'exécuter un code malveillant sur une plate-forme/un service afin de compromettre les ressources de la plate-forme/du service et de lancer ensuite d'autres attaques.

– Exécution d'un code malveillant: tout élément d'un système logiciel ou d'un script visant à causer des effets non désirés, des atteintes à la sécurité ou aux informations d'identification personnelles (PII) et des dégâts dans un système. Les exemples types sont les virus, les vers et les chevaux de Troie.

– Élévation des privilèges: attaque dans le cadre de laquelle un code est exécuté, au moyen d'un compte de traitement des privilèges, afin d'élever les privilèges de l'auteur de l'attaque.
– Injection d'éléments en langage de requête structurée (SQL): attaque qui exploite les vulnérabilités dans le code de validation des données d'entrée et d'accès aux données d'une application pour exécuter des commandes arbitraires qui injectent ou extraient des informations.
– Écoute illicite du réseau: attaque consistant à intercepter des paquets transmis depuis le réseau et à lire les données qu'ils contiennent pour trouver des informations sensibles comme des mots de passe, des jetons de session ou tout type d'informations confidentielles.
– Accès non autorisé: attaque consistant à obtenir l'accès à une plate-forme/un service en utilisant le compte d'un tiers ou une autre méthode d'accès. Par exemple, le cas d'une personne qui réussit à deviner le mot de passe ou le nom d'utilisateur pour un compte qui ne lui appartenait pas avant d'avoir réussi à y accéder est considéré comme un accès non autorisé.
– Force brute: attaque consistant à essayer de manière systématique toutes les clés possibles jusqu'à ce qu'une clé correcte soit trouvée.
– Attaque par dictionnaire pour les noms d'utilisateur/mots de passe: attaque visant à neutraliser de manière systématique les mécanismes de chiffrement ou d'authentification en essayant de manière répétée des mots de passe en utilisant les mots figurant dans un dictionnaire.
– Utilisation de noms d'utilisateur et de mots de passe par défaut/utilisation de mots de passe faibles: attaque consistant à exploiter des noms d'utilisateurs et mots de passe par défaut/mots de passe faibles pour accéder à une plate-forme/des services.
– Attaque par inférence: attaque dans le cadre de laquelle un utilisateur est en mesure d'obtenir par déduction des informations protégées à partir d'éléments d'information légitimement accessibles avec une classification inférieure.
– Fuite d'informations PII: publication intentionnelle ou non d'informations PII dans un environnement non sécurisé.

9 Exigences pour l'Internet des objets

La présente Recommandation repose sur les exigences de haut niveau décrites dans [UIT-T Y.4100], comme indiqué dans l'Annexe A.

10 Capacités de sécurité pour l'Internet des objets

10.1 Aperçu

La présente Recommandation traite uniquement des exigences relatives à la sécurité et tient compte de la fiabilité et de la qualité des services. Les capacités de sécurité pour l'Internet des objets découlent de celles décrites dans [b-UIT-T Y.4401].

Capacités générales

L'architecture IoT devrait avoir les capacités suivantes:

– une capacité de communication sécurisée pour la prise en charge des communications de manière sécurisée et sûre avec protection de la vie privée;
– une capacité de gestion sécurisée des clés pour la prise en charge de communications sécurisées;
– une capacité de gestion sécurisée des données pour assurer la gestion des données de manière sécurisée et sûre avec protection de la vie privée;
– une capacité d'authentification pour authentifier les dispositifs;
– une capacité d'autorisation (contrôle d'accès) pour autoriser les dispositifs;

– une capacité d'audit pour surveiller l'accès aux données ou les tentatives d'accès aux applications IoT de manière parfaitement transparente, traçable et reproductible, conformément aux réglementations et législations pertinentes;
– une capacité de fourniture sécurisée de services pour fournir des services de manière sécurisée et sûre avec protection de la vie privée;
– une capacité d'intégration sécurisée pour intégrer les différentes politiques et techniques de sécurité se rapportant aux différents composants fonctionnels IoT;
– une capacité pour mettre en œuvre des protocoles sécurisés utilisant des algorithmes de chiffrement grand public et normalisés;
– une capacité pour mettre en œuvre des protocoles sécurisés fondés sur une cryptographie pour environnements contraints;
– une capacité de mise à jour logicielle sécurisée et solide pour mettre à jour les modules ou applications logiciels;
– une capacité de gestion des identités pour les dispositifs/capteurs IoT, les passerelles et les plates-formes/services;
– une capacité d'analyse des vulnérabilités;
– une capacité pour surveiller l'accès aux données ou les tentatives d'accès aux applications IoT de manière parfaitement transparente, traçable et reproductible;
– une capacité de sécurité installée sur le matériel (par exemple, module de plate-forme sécurisé) pour empêcher les risques liés à la sécurité physique associés à la virtualisation des réseaux et des passerelles;
– une capacité de routage par trajets multiples pour empêcher les attaques par retransmission sélective;
– une capacité de protection des informations PII contre les atteintes tout au long de leur cycle de vie;
– une capacité de configuration sécurisée;
– une capacité utilisant une cryptographie pour environnements contraints; et
– une capacité de chiffrement simple avec chiffrement avec données de gabarit associées (EAMD) [b-UIT-T X.1362] pour communiquer avec d'autres entités, y compris la passerelle.

Capacités liées à l'algorithme de chiffrement

L'architecture IoT devrait avoir les capacités suivantes:

– une capacité pour produire un nombre aléatoire de qualité cryptographique pour la prise en charge de la gestion des clés [b-IETF RFC 4086];
– une capacité de mise à jour périodique des clés de chiffrement nécessaires pour les flux de radiodiffusion; et
– une capacité utilisant des algorithmes de chiffrement normalisés.

Capacités liées au contexte

L'architecture IoT devrait avoir les capacités suivantes:

– une capacité pour résister aux attaques par voie latérale;
– une capacité pour prendre en charge des pratiques de codage sécurisées qui appliquent des données d'entrée rigoureuses pour la validation des données dans les systèmes et services, les applications de bases de données et les services web; et
– une capacité pour effectuer une évaluation des risques prévus afin de déterminer les risques dans les différents contextes opérationnels.

10.2 Capacités de sécurité pour les capteurs/dispositifs

Les capteurs/dispositifs IoT devraient avoir les capacités suivantes:

– une capacité de gestion des clés;

– une capacité de négociation de l'algorithme de chiffrement;

– une capacité de chiffrement des données et, dans certains cas, des données dans les plans de signalisation, de commande et de gestion pour atténuer les problèmes de sécurité liés à la confidentialité des données transmises par l'intermédiaire de réseaux hertziens;

– une capacité de protection de l'intégrité des données transmises par l'intermédiaire de réseaux hertziens en utilisant des mécanismes de protection de l'intégrité appropriés qui donnent des assurances que les données d'utilisateurs ou les données de signalisation, de commande ou de gestion n'ont pas été modifiées ou altérées;

– une capacité d'authentification de l'origine des données ou de l'identité des capteurs/dispositifs IoT ainsi que des administrateurs et du personnel de maintenance des réseaux de capteurs;

– une capacité pour gérer les correctifs, y compris pour la mise à jour ou de mise à niveau des modules logiciels sécurisés;

– une capacité pour mettre en œuvre des protocoles sécurisés fondés sur une cryptographie pour environnements contraints;

– une capacité de contrôle d'accès pour garantir que seuls le personnel et les dispositifs autorisés puissent accéder aux éléments de réseau, aux informations stockées, aux flux d'informations, aux services et aux applications;

– une capacité de détection et/ou de prévention des altérations;

– une capacité pour produire des nombres aléatoires de qualité cryptographique pour la prise en charge de la gestion des clés;

– une capacité pour résister aux attaques par voie latérale;

– une capacité de détection et de protection contre les logiciels malveillants; et

– une capacité de protection des informations PII contre la fuite de ces informations.

Les dispositifs IoT devraient avoir les capacités suivantes:

– une capacité pour vérifier l'authenticité et l'intégrité des logiciels sur un dispositif utilisant des signatures numériques générées de manière cryptographique [b-ISO/CEI 9796-3];

– une capacité de pare-feu, de détection des intrusions, de protection contre les intrusions ou d'inspection approfondie des paquets pour contrôler le trafic dont le point de terminaison est le dispositif; et

– une capacité pour mettre en place des configurations sécurisées.

10.3 Capacités de sécurité pour les passerelles

Les passerelles devraient avoir les capacités suivantes:

– une capacité de système de détection des intrusions (IDS)/système de prévention des intrusions (IPS);

– une capacité de gestion des clés;

– une capacité pour mettre en place des configurations sécurisées;

– une capacité de négociation de l'algorithme de chiffrement;

– une capacité de chiffrement des données et, dans certains cas, des données dans les plans de signalisation, de commande et de gestion avec les dispositifs et composants IoT du centre de données pour atténuer les problèmes de sécurité liés à la confidentialité des données transmises par l'intermédiaire de réseaux hertziens
– une capacité de protection de l'intégrité des données transmises par l'intermédiaire de réseaux hertziens en utilisant des mécanismes de protection de l'intégrité appropriés qui donnent des assurances que les données d'utilisateurs ou les données de signalisation, de commande ou de gestion n'ont pas été modifiées ou altérées;
– une capacité disponible pour faire face aux attaques par déni de service capable d'utiliser des techniques de codage source sécurisé, d'analyser le code source et de tester de les vulnérabilités ou encore d'utiliser un système IDS/IPS installé sur un réseau ou un serveur;
– une capacité d'authentification de l'origine des données ou de l'identité des capteurs/dispositifs IoT ainsi que des administrateurs et du personnel de maintenance des réseaux de capteurs;
– une capacité de contrôle d'accès pour garantir que seuls le personnel et les dispositifs autorisés puissent accéder aux éléments de réseau, aux informations stockées, aux flux d'informations, aux services et aux applications; et
– une capacité de traçabilité des dispositifs IoT pour garantir qu'en cas de violation de la politique, il sera possible de retrouver le dispositif qui en est à l'origine.

La passerelle doit pouvoir prendre en charge une capacité de mise à jour des modules logiciels sécurisés.

10.4 Capacités de sécurité du réseau

Les capacités de sécurité du réseau ne relèvent pas du domaine d'application de la présente Recommandation.

NOTE – Des capacités de sécurité permettant de mettre en œuvre les mesures de sécurité décrites dans [b-UIT-T X.805] pourraient être utilisées.

10.5 Capacités de sécurité des plates-formes/services

Les plates-formes/services devraient avoir les capacités suivantes:

– une capacité pour protéger un justificatif pour les opérations de chiffrement, qui est un ensemble de données présentées pour prouver une identité ou des privilèges revendiqués;
– une capacité pour modifier les noms d'utilisateur et les mots de passe par défaut lors de l'établissement de la connexion initiale;
– une capacité pour mettre en œuvre des mots de passe forts et une politique de contrôle d'accès granulaire;
– une capacité pour rendre les ports inutiles non disponibles;
– une capacité pour prendre en charge une configuration sécurisée, par exemple, pour supprimer les services et les logiciels inutiles;
– une capacité de protection contre les infections par des logiciels malveillants grâce à l'utilisation de logiciels de protection contre les logiciels malveillants;
– une capacité pour mettre en œuvre des politiques de gestion des correctifs;
– une capacité de gestion des vulnérabilités;
– une capacité pour mettre à jour les modules et applications logiciels sécurisés;
– une capacité de gestion des clés pour le transfert sécurisé de messages entre une passerelle et une plate-forme/un service;

– une capacité de négociation de l'algorithme de chiffrement pour établir une tunnellisation sécurisée entre la passerelle et la plate-forme/le service, au cas où il serait nécessaire de transférer de manière sécurisée des messages entre la passerelle et la plate-forme/le service;
– une capacité disponible pour faire face aux attaques par déni de service;
– une capacité pour surveiller le réseau;
– une capacité de protection des informations PII en mode veille;
– une capacité de sécurité au niveau des applications pour prévenir les menaces et attaques au niveau des applications décrites au § 8.4; et
– une capacité pour permettre d'atténuer les attaques par inférence.

Annexe A

Exigences concernant la sécurité et la protection de la vie privée décrites dans UIT-T Y.4100/Y.2066

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

Les exigences concernant la sécurité et la protection de la vie privée renvoient aux exigences fonctionnelles à respecter lors de la saisie, du stockage, du transfert, de l'agrégation et du traitement des données des objets, ainsi qu'à la fourniture de services faisant intervenir des objets. Ces exigences concernent tous les acteurs IoT.

La présente annexe énumère les exigences de haut niveau en matière de sécurité et de protection de la vie privée décrites dans l'Annexe A de [UIT-T Y.4100]. L'élément entre crochets donné dans chaque paragraphe ci-dessous renvoie à l'élément correspondant décrit dans l'Annexe A de [UIT-T Y.4100].

A.1 Sécurité des communications

Il faut une capacité de communication sécurisée et sûre avec protection de la vie privée afin de pouvoir interdire l'accès non autorisé au contenu des données, garantir l'intégrité des données et protéger le contenu des données se rapportant à la vie privée lors de la transmission ou du transfert des données dans l'Internet des objets [SP1].

A.2 Sécurité de la gestion des données

Il faut une capacité de gestion des données sécurisée et sûre avec protection de la vie privée afin de pouvoir interdire l'accès non autorisé au contenu des données, garantir l'intégrité des données et protéger le contenu des données se rapportant à la vie privée lors du stockage ou du traitement des données dans l'Internet des objets [SP2].

A.3 Sécurité de la fourniture des services

Il faut une capacité de fourniture des services sécurisée et sûre avec protection de la vie privée afin de pouvoir interdire l'accès non autorisé au service et la fourniture de services frauduleux et protéger les informations se rapportant à la vie privée des utilisateurs IoT [SP3].

A.4 Intégration des politiques et des techniques de sécurité

Il faut pouvoir intégrer différentes politiques et techniques de sécurité afin de garantir des contrôles de sécurité cohérents sur les différents dispositifs et réseaux utilisateurs dans l'Internet des objets [SP4].

A.5 Authentification et autorisation mutuelles

Avant qu'un dispositif (ou un utilisateur IoT) puisse accéder à l'Internet des objets, une authentification et une autorisation mutuelles entre le dispositif (ou l'utilisateur IoT) et l'Internet des objets doivent avoir lieu selon des politiques de sécurité définies au préalable [SP5].

A.6 Audit de sécurité

Les audits de sécurité doivent être pris en charge dans l'Internet des objets. L'accès aux données et les tentatives d'accès aux applications IoT doivent être parfaitement transparents, traçables et reproductibles conformément aux réglementations et aux législations pertinentes. En particulier, l'Internet des objets doit prendre en charge les audits de sécurité concernant la transmission, le stockage et le traitement des données, et l'accès aux données par les applications [SP6].

Appendice I

Capacités de sécurité et de protection de la vie privée décrites dans UIT-T Y.4401/Y.2068

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

Le présent appendice donne les capacités de sécurité et de protection de la vie privée de haut niveau décrites dans [b-UIT-T Y.4401] et l'élément entre crochets donné dans chaque paragraphe ci-dessous renvoie à l'élément correspondant décrit dans l'Annexe A de [b-UIT-T Y.4401].

I.1 Capacité de sécurité des communications

La capacité de sécurité des communications fait intervenir les fonctions permettant de prendre en charge les communications de manière sécurisée et sûre avec protection de la vie privée [C-7-1].

I.2 Capacité de sécurité de la gestion des données

La capacité de sécurité de la gestion des données fait intervenir les fonctions permettant d'assurer la gestion des données de manière sécurisée et sûre avec protection de la vie privé [C-7-2].

I.3 Capacité de sécurité de la fourniture des services

La capacité de sécurité de la fourniture des services fait intervenir les fonctions permettant d'assurer la fourniture des services de manière sécurisée et sûre avec protection de la vie privé [C-7-3].

I.4 Capacité d'intégration de la sécurité

La capacité d'intégration de la sécurité fait intervenir les fonctions permettant d'intégrer les différentes politiques et techniques de sécurité se rapportant aux divers composants fonctionnels de l'Internet des objets [C-7-4].

I.5 Capacité d'authentification et d'autorisation mutuelles

La capacité d'authentification et d'autorisation mutuelles fait intervenir les fonctions permettant d'authentifier et d'autoriser chaque dispositif avant qu'il accède à l'Internet des objets sur la base de politiques de sécurité définies au préalable [C-7-5].

I.6 Capacité d'audit de sécurité

La capacité d'audit de sécurité fait intervenir les fonctions permettant de surveiller l'accès aux données ou les tentatives d'accès aux applications IoT de manière parfaitement transparente, traçable et reproductible conformément aux réglementations et aux législations pertinentes [C-7-6].

NOTE – Ces capacités de sécurité et de protection de la vie privée comprennent également la capacité de faire face aux problèmes de sécurité et de protection de la vie privée pour les opérations dans les différents domaines.

Appendice II

Vue de la mise en œuvre du cadre fonctionnel de l'Internet des objets fondée sur l'architecture fonctionnelle des réseaux de prochaine génération décrite dans UIT-T Y.4401/Y.2068

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

La Figure II.1 montre une vue de la mise en œuvre du cadre fonctionnel de l'Internet des objets, reposant sur les entités fonctionnelles décrites dans l'architecture fonctionnelle des réseaux de prochaine génération (NGN) figurant dans [b-UIT-T Y.4401], qui se rapporte au cadre fonctionnel de sécurité défini dans la présente Recommandation. La présente Recommandation donne les capacités pour la couche prise en charge du service et la couche dispositif décrites dans la Figure 7-2 de [b-UIT-T Y.4401].

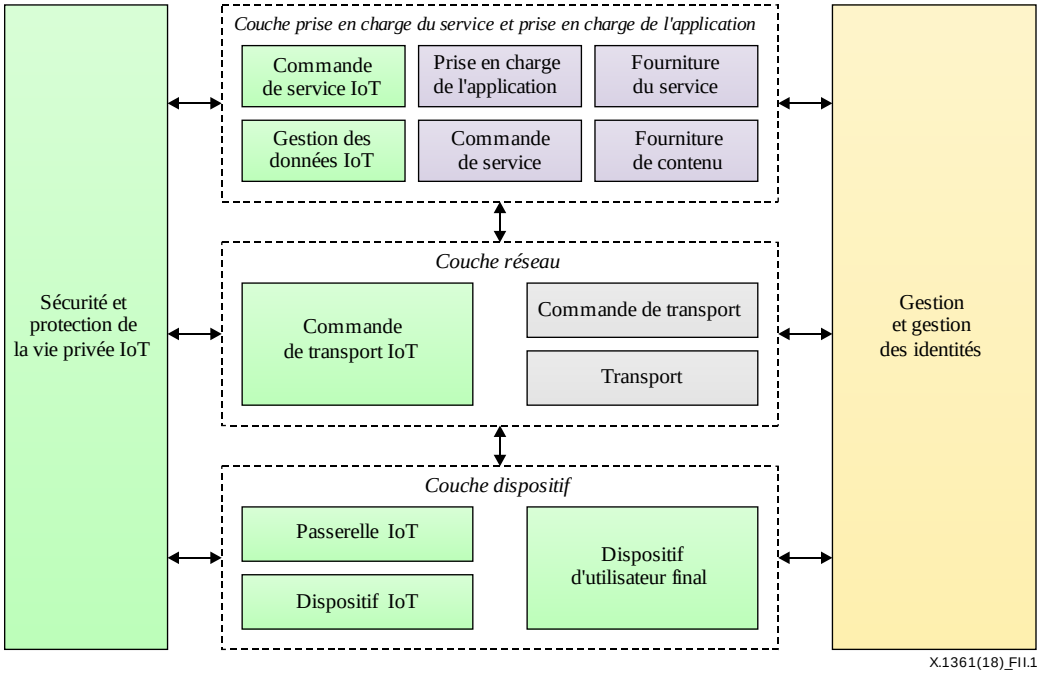

Figure II.1 – Vue de la mise en œuvre du cadre fonctionnel de l'Internet des objets fondée sur l'architecture fonctionnelle NGN

Bibliographie

[b-UIT-T X.667] Recommandation UIT-T X.667 (2012), *Technologies de l'information – Procédures opérationnelles des autorités d'enregistrement des identificateurs d'objet: génération des identificateurs uniques universels et utilisation de ces identificateurs dans les identificateurs d'objet.*

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

[b-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.1250] Recommandation UIT-T X.1250 (2009), *Capacités de base pour l'amélioration de l'interopérabilité globale dans la gestion d'identité.*

[b-UIT-T X.1252] Recommandation UIT-T X.1252 (2010), *Termes et définitions de base relatifs à la gestion d'identité.*

[b-UIT-T X.1311] Recommandation UIT-T X.1311 (2011) | ISO/CEI 29180:2012, *Technologies de l'information – Cadre de sécurité des réseaux de capteurs ubiquitaires.*

[b-UIT-T X.1362] Recommandation UIT-T X.1362 (2017), *Procédure de chiffrement simple pour les environnements de l'Internet des objets (IoT).*

[b-UIT-T Y.4000] Recommandation UIT-T Y.4000/Y.2060 (2012), *Présentation générale de l'Internet des objets.*

[b-UIT-T Y.4050] Recommandation UIT-T Y.4050/Y.2069 (2012), *Termes et définitions applicables à l'Internet des objets.*

[b-UIT-T Y.4105] Recommandation UIT-T Y.4105/Y.2221 (2010), *Prescriptions de prise en charge pour les applications et services de réseaux de capteurs ubiquitaires dans l'environnement des réseaux de prochaine génération.*

[b-UIT-T Y.4113] Recommandation UIT-T Y.4113 (2016), *Exigences applicables au réseau pour l'Internet des objets.*

[b-UIT-T Y.4400] Recommandation UIT-T Y.4400/Y.2063 (2012), *Cadre applicable au web des objets.*

[b-UIT-T Y.4401] Recommandation UIT-T Y.4401/Y.2068 (2015), *Cadre fonctionnel et capacités de l'Internet des objets.*

[b-IETF RFC 4086] IETF RFC 4086 (2005), *Randomness Requirements for Security.*

[b-ISO 11568-1] ISO 11568-1:2005, *Banque – Gestion de clés (services aux particuliers) – Partie 1: Principes.*

[b-ISO 13491-1] ISO 13491-1:2016, *Services financiers – Dispositifs cryptographiques de sécurité (services aux particuliers) – Partie 1: Concepts, exigences et méthodes d'évaluation.*

[b-ISO 19440] ISO 19440:2007, *Entreprise intégrée – Constructions pour la modélisation d'entreprise.*

[b-ISO/CEI 9796-3] ISO/CEI 9796-3:2006, *Technologies de l'information – Techniques de sécurité - Schémas de signature numérique rétablissant le message – Partie 3: Mécanismes basés sur les logarithmes discrets.*

[b-ISO/CEI 19790] ISO/CEI 19790:2012, *Technologies de l'information – Techniques de sécurité – Exigences de sécurité pour les modules cryptographiques.*

[b-ISO/CEI 27000] ISO/CEI 27000:2018, *Technologies de l'information – Techniques de sécurité – Systèmes de management de la sécurité de l'information – Vue d'ensemble et vocabulaire.*

[b-ISO/CEI 27033-1] ISO/CEI 27033-1:2015, *Technologies de l'information – Techniques de sécurité – Sécurité de réseau – Partie 1: Vue d'ensemble et concepts.*

[b-ISO/CEI 27033-6] ISO/CEI 27033-6:2016, *Technologies de l'information – Techniques de sécurité – Sécurité de réseau – Partie 6: Sécurisation de l'accès réseau IP sans fil.*

[b-ISO/CEI 27039] ISO/CEI 27039:2015, *Technologies de l'information – Techniques de sécurité – Sélection, déploiement et opérations des systèmes de détection et prévention d'intrusion.*

[b-ISO/CEI 29100] ISO/CEI 29100:2011, *Technologies de l'information – Techniques de sécurité – Cadre privé.*

[b-ISO/CEI 29192-1] ISO/CEI 29192-1:2012, *Technologies de l'information – Techniques de sécurité – Cryptographie pour environnements contraints – Partie 1: Généralités.*

[b-NIST SP 800-53] NIST Special Publication 800-53 (2013), *Security and Privacy Controls for Federal Information Systems and Organizations.*

[b-ZT] Zhang Li, Tong Xin (2013), *Threat Modeling and Countermeasures Study for the Internet of Things, Journal of Convergence Information Technology (JCIT), Vol. 8, No. 5, mars.*

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, 2019