Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

X.1352

(09/2022)

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

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

Exigences de sécurité applicables aux dispositifs et aux passerelles de l'Internet des objets

Recommandation UIT-T X.1352

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 (DLT)	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.1352

Exigences de sécurité applicables aux dispositifs et aux passerelles de l'Internet des objets

Résumé

La Recommandation ITU-T X.1352 définit des exigences détaillées concernant les cinq dimensions de sécurité applicables aux dispositifs et aux passerelles de l'Internet des objets (IoT): authentification, cryptographie, sécurité des données, sécurité de la plate-forme du dispositif et sécurité physique. Ces exigences de sécurité reposent sur le modèle de référence de l'IoT défini dans la Recommandation UIT-T Y.4100 et sur le cadre de sécurité de l'IoT décrit dans la Recommandation UIT-T X.1361.

La dimension liée à l'authentification comprend l'authentification de l'utilisateur, l'utilisation sécurisée des justificatifs d'authentification et l'authentification des dispositifs. La dimension cryptographique comprend l'utilisation de la cryptographie sécurisée, la gestion sécurisée des clés et la génération sécurisée de nombres aléatoires. La dimension liée à la sécurité des données comprend la transmission et le stockage sécurisés, le contrôle des flux d'informations, la gestion sécurisée des sessions et la gestion des informations d'identification personnelle (PII). La dimension liée à la sécurité de la plate-forme du dispositif comporte cinq éléments: sécurité logicielle; mises à jour sécurisées; gestion de la sécurité; journalisation et horodatage. De même, la dimension liée à la sécurité physique comprend une interface physique sécurisée et une fonction d'inviolabilité.

Historique

Édition	Recommandation	Approbation	Commission d'études	ID unique*
1.0	UIT-T X.1352	02-09-2022	17	11.1002/1000/14990

Mots clés

Authentification, cryptographie, sécurité des données, sécurité de la plate-forme du dispositif, sécurité des dispositifs et des passerelles de l'IoT, passerelle de l'IoT, évaluation de la sécurité de l'IoT et sécurité physique.

* 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.

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 développeurs 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

Recommandation UIT-T X.1352

Exigences de sécurité applicables aux dispositifs et aux passerelles de l'Internet des objets

1 Champ d'application

La présente Recommandation définit des exigences détaillées concernant les cinq dimensions de sécurité applicables aux dispositifs et aux passerelles de l'Internet des objets (IoT): authentification, cryptographie, sécurité des données, sécurité de la plate-forme du dispositif et sécurité physique. Ces exigences de sécurité reposent sur le modèle de référence de l'IoT défini dans [UIT-T Y.4100] et sur le cadre de sécurité de l'IoT décrit dans [UIT-T X.1361].

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 est sujette à révision; les utilisateurs de la présente Recommandation sont donc invités à rechercher la possibilité d'appliquer les éditions les plus récentes des Recommandations et autres références indiquées ci-après. 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 d'une Recommandation.

[UIT-T X.1361] Recommandation UIT-T X.1361 (2018), *Cadre de sécurité applicable à l'Internet des objets fondé sur le modèle passerelle*.

[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 authentification [b-UIT-T X.1254]: attestation de l'identité revendiquée par une entité.

3.1.2 capacité [b-ISO 16100-1]: ensemble de fonctions et de services assorti d'un ensemble de critères visant à évaluer la qualité offerte par un fournisseur de capacité.

3.1.3 confidentialité [b-UIT-T X.800]: propriété d'une information qui n'est ni disponible, ni divulguée aux personnes, entités ou processus non autorisés.

3.1.4 justificatif [b-UIT-T X.1252]: ensemble de données présentées comme preuve d'une identité déclarée et/ou de droits.

3.1.5 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).

3.1.6 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.

3.1.7 intégrité des données [b-UIT-T X.800]: propriété assurant que des données n'ont pas été modifiées ou détruites de façon non autorisée.

3.1.8 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.

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

3.1.10 gestion des correctifs [UIT-T X.1361]: 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.

3.1.11 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.

3.1.12 sécurité physique [b-UIT-T X.800]: mesures prises pour assurer la protection physique des ressources contre des menaces délibérées ou accidentelles.

3.1.13 configuration sécurisée [UIT-T X.1361]: 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.

3.1.14 passerelle de sécurité [UIT-T X.1361]: 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 – Ce terme est parfois appelé simplement "passerelle". La définition est adaptée de [b-ISO/IEC 27033-1].

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

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

3.1.17 gestion des vulnérabilités [UIT-T X.1361]: processus consistant à identifier, à classer, à résoudre et à atténuer les vulnérabilités.

3.2 Termes définis dans la présente Recommandation

La présente Recommandation définit les termes suivants:

3.2.1 dimension de sécurité: ensemble de mesures de sécurité destinées à traiter un aspect particulier de la sécurité dans le réseau.

3.2.2 sécurité de la plate-forme du dispositif: ensemble de sécurité pour les microgiciels doté d'une capacité de mise à jour et de gestion d'un logiciel tiers et d'une capacité d'audit pour les dispositifs et passerelles IoT.

NOTE – Le microgiciel est remplacé par un logiciel sur un système d'exploitation, en fonction des capacités matérielles.

3.2.3 obfuscation: effet d'une opération effectuée sur le code de programme ou les données des applications dont les résultats entraînent en quelque sorte une dissimulation ou un obscurcissement des applications sans affecter la sortie du code.

4 Abréviations et acronymes

La présente Recommandation utilise les abréviations et acronymes suivants:

API interface de programmation d'application (*application programming interface*)

CAPTCHA	test public de Turing entièrement automatisé visant à distinguer les ordinateurs des humains (*completely automated public turing test to tell computers and humans apart*)
CoAP	protocole d'application avec contraintes (*constrained application protocol*)
DoS	déni de service (*denial of service*)
F/W	micrologiciel (*firmware*)
FTP	protocole de transfert de fichiers (*file transfer protocol*)
H/W	matériel (*hardware*)
ID	identificateur (*identifier*)
IDS	système de détection des intrusions (*intrusion detection system*)
IMEI	identité internationale d'équipement mobile (*international mobile equipment identity)*
IoT	Internet des objets (*internet of things*)
IPS	système de prévention des intrusions (*intrusion prevention system*)
LwM2M	de machine à machine simple
MAC	contrôle d'accès au support (*media access control*)
MCU	microcontrôleur (*microcontroller unit*)
MQTT	transport avec télémesure de mise en file d'attente du message (*message queuing telemetry transport*)
OS	système d'exploitation (*operating system*)
PII	information d'identification personnelle (*personally identifiable information*)
PIN	numéro d'identification personnel (*personal identification number*)
S/W	logiciel (*software*)
SD	numérique sécurisé (*secure digital*)
SHA	algorithme de hachage sécurisé (*secure hash algorithm*)
SNMP	protocole simple de gestion de réseau (*simple network management protocol*)
SSA	attaque par-dessus l'épaule (*shoulder-surfing attack*)
SWD	débogage série par câble (*serial wire debug*)
TLS	sécurité de la couche de transport (*transport layer security*)
UART	émetteur-récepteur asynchrone universel (*universal asynchronous receiver/transceiver*)
UID	identifiant unique (*unique identifier*)
UPnP	dispositif universel prêt à fonctionner (*universal plug and play*)
USB	bus série universel (*universal serial bus*)

5 Conventions

La présente Recommandation utilise les conventions suivantes:

L'expression "il est recommandé" indique une exigence qui est recommandée, mais qui n'est pas absolument nécessaire.

L'expression "il est obligatoire" indique une exigence qui doit être strictement suivie et par rapport à laquelle aucun écart n'est permis pour pouvoir déclarer la conformité à la présente Recommandation.

Dans le corps de la présente Recommandation, le mot "peut" apparaît à quelques occasions. Il doit alors être interprété comme "est en mesure de".

L'expression "il est recommandé" dans l'Appendice I est dépourvue d'intention normative.

6 Présentation générale

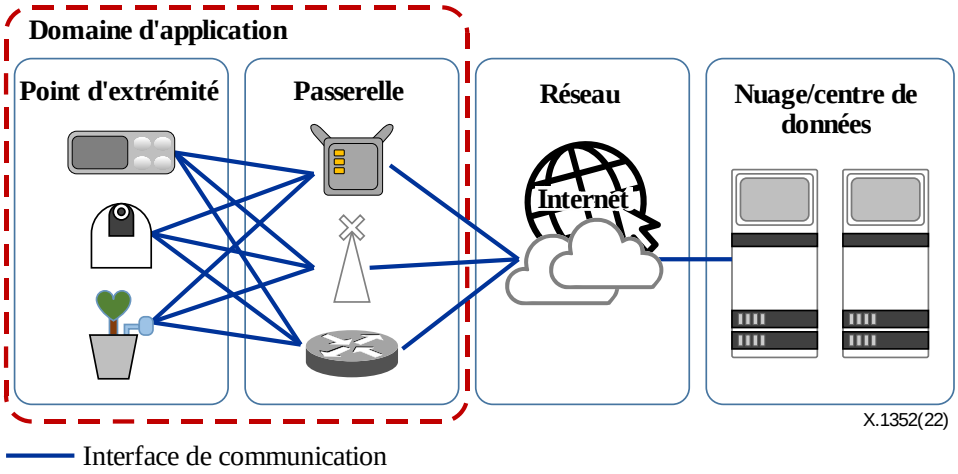

Figure 1 – Domaine d'application des exigences de sécurité

Sur la base des capacités de sécurité proposées dans les Recommandations [UIT-T X.1361] et [UIT-T Y.4100], et comme indiqué dans l'Appendice II, les exigences en matière de sécurité permettant de faire face aux enjeux et aux menaces qui pèsent sur les dispositifs et les passerelles IoT (à l'exception des systèmes et des plates-formes de réseau) sont présentées pour cinq dimensions de sécurité, à savoir l'authentification, la cryptographie, la sécurité des données, la sécurité de la plate-forme du dispositif et la sécurité physique.

La dimension liée à l'authentification comprend l'authentification de l'utilisateur, l'utilisation sécurisée des justificatifs d'authentification et l'authentification des dispositifs.

La dimension cryptographique comprend l'utilisation d'algorithmes cryptographiques sécurisés, la gestion sécurisée des clés et la génération sécurisée de nombres aléatoires.

La dimension liée à la sécurité des données comprend la protection des données durant la transmission et hors transmission, le contrôle des flux d'informations, la gestion sécurisée des sessions et la protection des informations d'identification personnelle (PII).

La dimension liée à la sécurité de la plate-forme du dispositif comporte cinq éléments: sécurité logicielle; mises à jour sécurisées; gestion de la sécurité; journalisation et horodatage.

De même, pour la dimension liée à la sécurité physique, une interface physique sécurisée et une défense contre l'altération volontaire ont été définies.

La Figure 2 montre les éléments cibles des dimensions de sécurité pour un dispositif et une passerelle IoT. Un dispositif et une passerelle IoT sont généralement constitués d'un microcontrôleur, d'un module de communication, d'une mémoire et de ports d'entrée/sortie. Un élément sécurisé existe sous une forme matérielle ou logicielle. Le microcontrôleur comporte un micrologiciel, des interfaces physiques et une mémoire. Dans ce cas, un logiciel doté d'un système d'exploitation peut être remplacé par un micrologiciel. Le module de communication nécessite d'assurer la cryptographie et la sécurité des données durant la transmission. Les données des dispositifs de mémoire flash sont stockées en toute sécurité au niveau de l'authentification, de la cryptographie et de la confidentialité/l'intégrité des données. L'accès aux interfaces physiques comme les émetteurs/récepteurs universels asynchrones (UART) exige également l'authentification des utilisateurs. Les interfaces matérielles superflues doivent être supprimées ou désactivées.

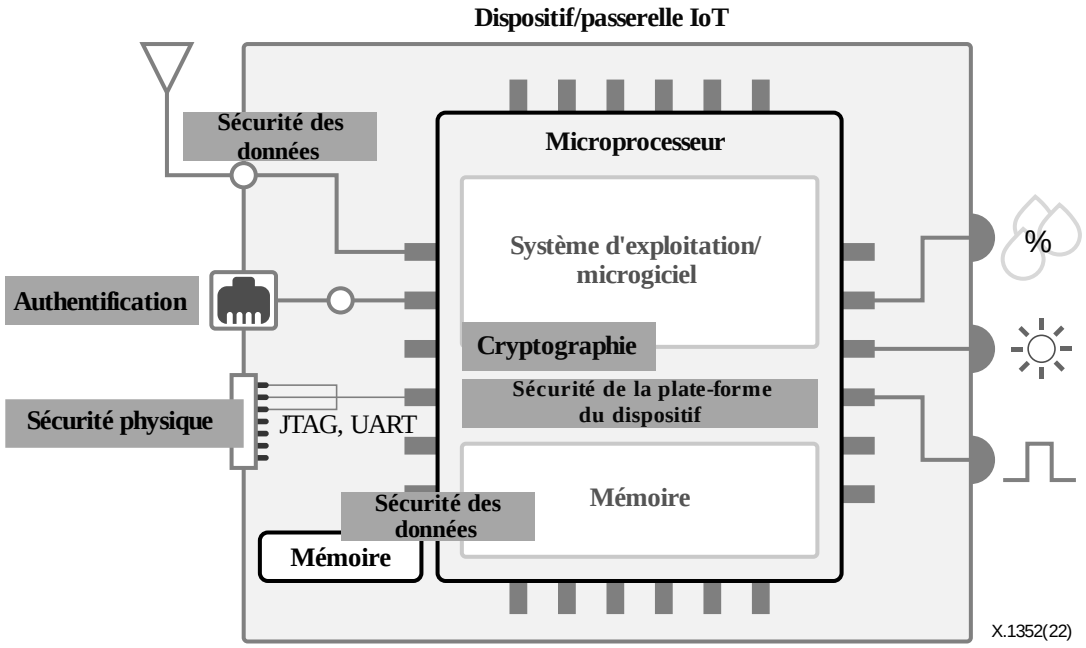

Figure 2 – Exemple de dimensions de sécurité appliquées à des dispositifs et à des passerelles IoT

7 Menaces/vulnérabilités pour la sécurité des dispositifs et des passerelles IoT

Les menaces/vulnérabilités pour la sécurité des dispositifs et des passerelles IoT, qui peuvent en faire des cibles potentielles pour les cyberattaques, sont décrites aux paragraphes 7.1 et 7.2. Les menaces pour la sécurité des passerelles englobent les menaces pour les dispositifs IoT.

7.1 Menaces/vulnérabilités pour la sécurité des dispositifs IoT

Les menaces/vulnérabilités particulières auxquelles sont exposés les dispositifs sont les suivantes:

– ST-D-1: Contournement de l'authentification: un utilisateur non autorisé obtient un accès à un dispositif et est également en mesure d'accéder à des données essentielles, notamment aux données de l'utilisateur et aux fichiers de configuration stockés sur le dispositif.

– ST-D-2: Connexion non autorisée au dispositif: un dispositif est exposé à un autre dispositif non autorisé ou ses données, comme les données d'utilisateur, peuvent être transmises à un autre dispositif non autorisé.

– ST-D-3: Privilèges excessifs: le fait de conférer des privilèges excessifs ou superflus permet à l'auteur d'une attaque d'accéder à toutes les opérations acceptables et les données contrôlées, y compris les données d'utilisateur d'un dispositif.

– ST-D-4: Tentatives d'authentification répétées sans restrictions: un utilisateur non autorisé effectuant des tentatives d'authentification répétées peut obtenir un accès à un compte utilisateur authentique.

– ST-D-5: Erreur due à un accès concurrent: un accès concurrent de plusieurs comptes administrateurs peut entraîner des modifications non coordonnées au niveau de la configuration des fonctionnalités essentielles.

– ST-D-6: Exposition et attaque par devinette des informations d'authentification: lorsque les informations d'authentification, comme les mots de passe, sont codées en dur ou stockées en plein texte, ou lorsqu'un mot de passe d'authentification ou un numéro d'identification personnel (PIN) est exposé en plein texte (procédé également connu sous le nom d'attaque par-dessus l'épaule (*Shoulder-surfing attack*)), les informations d'authentification peuvent être exposées par l'auteur d'une attaque, qui peut aussi les deviner.

– ST-D-7: Mot de passe faible: l'auteur d'une attaque peut obtenir une combinaison non sécurisée, concernant par exemple un mot de passe par défaut ou un mot de passe faible, qui peuvent permettre à un attaquant de se faire passer pour un utilisateur légitime.
– ST-D-8: Clé de chiffrement/numéro aléatoire faible: une clé cryptographique insuffisante ou un nombre "aléatoire" prévisible peuvent être insuffisants pour protéger les données essentielles.
– ST-D-9: Algorithme cryptographique faible: l'auteur d'une attaque peut prédire des données essentielles ou découvrir un message chiffré en plein texte (cryptogramme) en analysant le trafic qui utilise un algorithme cryptographique faible.
– ST-D-10: Absence de validation des valeurs d'entrée: une absence de validation des valeurs d'entrée peut entraîner le disfonctionnement d'un dispositif.
– ST-D-11: Exposition des données et manipulation des données: les données essentielles, comme les données de l'utilisateur, la configuration du dispositif ou les clés cryptographiques, qui sont transmises par un dispositif ou stockées sur un dispositif peuvent être exposées à l'auteur d'une attaque, qui peut les exploiter ou les manipuler.
– ST-D-12: détournement de la session de l'utilisateur: l'auteur d'une attaque peut obtenir un accès non autorisé à un compte utilisateur authentique dont la session est anormalement fermée ou exploiter des sessions valides sur plusieurs dispositifs qui utilisent la même clé cryptographique.
– ST-D-13: Mise à jour non sécurisée: un fichier de mise à jour spécifique n'est pas téléchargeable ou un fichier de mise à jour altéré dont la source est non autorisée ou non authentifiée peut être exécutable.
– ST-D-14: Défaillance de la mise à jour: une erreur qui s'est produite durant une mise à jour peut entraîner un fonctionnement anormal du dispositif.
– ST-D-15: Erreur concernant l'intégrité: une manipulation involontaire de codes exécutables ou de valeurs de configuration peut entraîner le dysfonctionnement d'un dispositif.
– ST-D-16: Logiciel malveillant: code qui présente des fonctions involontaires susceptible d'être utilisées à des fins malveillantes.
– ST-D-17: Exploitation des informations résiduelles de la mémoire: la clé cryptographique, le mot de passe et les données sensibles utilisées pour les opérations cryptographiques, l'authentification et les transmissions de données demeurent dans la mémoire et peuvent être exploités.
– ST-D-18: Modification involontaire des configurations essentielles: l'absence de mesures de contrôle de sécurité sur un dispositif peut entraîner des modifications involontaires au niveau des configurations essentielles et la fourniture de services non sécurisés.
– ST-D-19: messages d'erreur non sécurisés: l'absence de détection appropriée d'erreurs et de comportement malveillant sur un dispositif et de réponse face à ces erreurs et comportements peut entraîner la fourniture de services non sécurisée.
– ST-D-20: Développement non sécurisé: des vulnérabilités potentielles sur le plan de la sécurité peuvent trouver leur source dans la conception ou la mise en œuvre d'un dispositif, et l'évaluation de ces vulnérabilités et les solutions apportées durant le processus de test peuvent être absentes ou inappropriées.
– ST-D-21: Système d'exploitation vulnérable: les fonctionnalités du dispositif peuvent être compromises ou contournées en raison de l'environnement vulnérable du système d'exploitation.
– ST-D-22: Utilisation de modules ou de bibliothèques tiers vulnérables: des modules ou des bibliothèques tiers vulnérables peuvent permettre à l'auteur d'une attaque de cibler les éléments à risque.
– ST-D-23: Informations sensibles non sécurisées dans le journal système: les informations sensibles enregistrées dans le journal système peuvent être exposées à une attaque et exploitées par l'auteur d'une attaque.

– ST-D-24: Exposition à des informations essentielles au moyen du débogage: des informations essentielles peuvent être exposées à une attaque et exploitées par l'auteur d'une attaque durant la journalisation et le débogage lorsqu'un dispositif est commercialisé et distribué.
– ST-D-25: Accès physique non autorisé: un dispositif est exposé à un accès physique non autorisé et à des changements involontaires dans sa configuration.

7.2 Menaces/vulnérabilités pour la sécurité des passerelles IoT

Les menaces/vulnérabilités particulières auxquelles sont exposées les passerelles sont notamment les suivantes:

– ST-G-1: Transmission de données non fiables: la transmission de données non fiables peut entraîner un dysfonctionnement du dispositif ou la transmission d'un code malveillant.
– ST-G-2: Déni de service (DOS) ou déni de service réparti (DDos): une attaque par déni de service peut entraîner l'indisponibilité d'un dispositif.

8 Exigences relatives à la sécurité

La présente Recommandation contient les exigences de sécurité pour les dispositifs et les passerelles IoT sur la base de cinq dimensions de sécurité définies au paragraphe 6; un ensemble d'exigences de sécurité est défini à partir des dispositions du modèle de menace et des propriétés fonctionnelles spécifiques de l'IoT, etc. La capacité de sécurité est fondée sur [UIT-T X.1361], comme indiqué dans l'Appendice II.

8.1 Authentification

La dimension liée à l'authentification comprend l'authentification de l'utilisateur, l'utilisation sécurisée des justificatifs d'authentification et l'authentification des dispositifs.

8.1.1 Authentification de l'utilisateur

Le mot de passe d'usine par défaut doit être modifié (AU-1-1).

– Un mot de passe doit être défini au moment de l'authentification initiale ou lorsqu'un changement est nécessaire après l'authentification initiale.
– Il convient de veiller à ce que le mot de passe soit différent de la valeur initiale ou de la valeur précédente.

Un utilisateur doit tout d'abord s'identifier et s'authentifier lorsqu'il accède à la gestion de la sécurité ou aux données sensibles (AU-1-2).

– Pour accéder à la gestion de la sécurité, par exemple pour paramétrer un dispositif IoT, un compte d'utilisateur ou un privilège, l'utilisateur doit être identifié et authentifié.
– Les utilisateurs bénéficiant d'un accès privilégié aux fonctions de gestion de la sécurité ou aux données sensibles doivent faire l'objet d'une gestion distincte par rapport aux utilisateurs normaux.

Le nombre de tentatives d'authentification doit être limité (AU-1-3).

– Un dispositif IoT peut être vulnérable aux attaques en force si les tentatives d'authentification répétées sont autorisées. Il convient donc de prévoir une fonction pour répondre comme il se doit aux tentatives d'authentification continues.
– Cette fonction peut être assurée au moyen de l'une des méthodes suivantes:
    a) limiter le nombre de tentatives d'authentification avant de verrouiller le compte ou de désactiver la fonction d'authentification pour un certain laps de temps (il est recommandé de limiter le nombre de tentatives d'authentification à cinq ou moins et de désactiver la fonction d'identification pendant au moins 5 minutes);

b) considérer le dépassement du nombre défini de tentatives d'authentification comme un trafic réseau non autorisé, et ajouter l'utilisateur à la liste de blocage automatique (il est recommandé de limiter le nombre de tentatives d'authentification à dix ou moins);

c) appliquer un test public de Turing entièrement automatisé visant à distinguer les ordinateurs des humains (*completely automated public turing test to tell computers and humans apart*).

Le mot de passe préinstallé sur le dispositif devrait être unique (AU-1-4).

Il est recommandé de fournir une fonction permettant de gérer les comptes utilisateur et les privilèges (AU-1-5).

– Il devrait être possible de gérer tous les comptes utilisateur (y compris le compte administrateur) utilisés sur un dispositif IoT, par exemple pour ajouter et supprimer des comptes et assigner des privilèges.

– Si un modèle de contrôle d'accès fondé sur les rôles est utilisé, il convient d'indiquer clairement les privilèges d'accès pour toutes les fonctions du dispositif IoT et d'assigner les privilèges en conséquence.

Le principe du moindre privilège devrait être appliqué à tous les comptes utilisateur (AU-1-6).

– Des privilèges fondé sur les rôles devraient être assignés à tous les comptes utilisateur.

L'accès concurrent au compte administrateur devrait être restreint (AU-1-7).

– L'accès concurrent aux services de gestion devrait être limité à un même compte administrateur, et il convient d'assurer une fonction permettant de déconnecter l'accès précédent ou limiter les nouvelles tentatives d'accès.

Un mot de passe sécurisé (longueur, cycle et complexité) devrait être créé (AU-1-8).

– Les dispositifs IoT devraient fournir à l'utilisateur une fonction permettant de créer un mot de passe sécurisé (longueur, cycle et complexité).

8.1.2 Utilisation sécurisée des justificatifs

Les justificatifs codés en dur ne devraient pas être utilisés (AU-2-1).

– Le mot de passe (code PIN, code secret, etc.) ne devrait pas être codé en dur ni stocké en plein texte.

Dans le cadre de l'authentification par mot de passe, le mot de passe devrait être masqué (AU-2-2).

– Si un mot de passe est affiché en plein texte, il peut être vulnérable aux attaques "par-dessus l'épaule". Par conséquent, pour éviter l'affichage des mots de passe lors de la saisie, il convient de masquer les caractères qui composent le mot de passe, par exemple en utilisant des astérisques ("*").

Aucun retour spécifique ne devrait être fourni en cas d'échec de l'authentification (AU-2-3).

8.1.3 Authentification du dispositif

L'identifiant (UID) unique de chaque dispositif matériel doit être conservé (AU-3-1). Voir le Tableau 1.

– Le dispositif IoT doit avoir un identifiant (ID) unique et fixe.

Tableau 1 – Identifiant unique des dispositifs IoT

ID	Description
Adresse de commande d'accès au support (MAC)	Identifiant unique assigné à l'interface réseau pour la communication au niveau de la couche de liaison de données du segment de réseau (48 bits).
Identité internationale d'équipement mobile (IMEI), numéro d'authentification international du terminal mobile	Numéro unique pour les smartphones. Assigné par le fabricant lors de la commercialisation du téléphone. Constitué de 15 chiffres au total, comprenant: un code d'approbation (huit chiffres), le numéro de série du modèle (six chiffres) et un numéro de vérification (un chiffre).

Les dispositifs devraient être mutuellement authentifiés avant que des données sensibles ne soient transmises ou que les dispositifs ne soient interconnectés à des fins de contrôle (AU-3-2).

– Parmi les exemples d'authentification mutuelle, on peut citer:

a) l'utilisation d'une clé privée fondée sur la méthode de chiffrement de clé publique;

b) l'utilisation d'attributs de sécurité (UID, clé, etc.) et de puces de sécurité;

c) l'application de la sécurité de la couche de transport (TLS) (ou datagramme TLS) au protocole léger de communication, par exemple le protocole d'application avec contraintes (CoAP), le protocole de machine à machine simple (LwM2M) ou le transport avec télémesure de mise en file d'attente du message (MQTT).

8.2 Cryptographie

– S'il est difficile d'utiliser des algorithmes cryptographiques généraux en raison de la capacité de mémoire et de stockage limitée, des algorithmes cryptographiques légers doivent être utilisés.

– Il convient d'utiliser des algorithmes cryptographiques pour se prémunir contre les attaques par voie latérale.

Des clés cryptographiques doivent être gérées de façon sécurisée tout au long de leur cycle de vie (CR-1-2).

– Les clés devraient être établies, mises à jour, distribuées, utilisées, stockées et détruites de façon sécurisée.

Un nombre aléatoire devrait être généré par le biais d'un algorithme avec un caractère aléatoire avéré (CR-1-3).

8.3 Sécurité des données

La dimension liée à la sécurité des données comprend la protection des données durant la transmission et hors transmission, le contrôle des flux d'informations, la gestion sécurisée des sessions et la protection des informations d'identification personnelle (PII).

8.3.1 Transmission et stockage sécurisés

Les données transmises doivent être chiffrées (DS-1-1).

– Les données transmises doivent être chiffrées au moyen d'un algorithme cryptographique sécurisé (voir CR-1-1).

Un mode sécurisé devrait être appliqué lorsqu'un canal de données ou de commande est créé (DS-1-2).

– Lorsque les données sont transmises, un protocole de sécurité fiable devrait être utilisé, garantissant la confidentialité et l'intégrité des données transmises et authentifiant les correspondants de départ et de destination.

Les données stockées dans les dispositifs doivent être chiffrées (DS-1-3).

– Les dispositifs de stockage des données doivent être chiffrés au moyen d'un algorithme cryptographique sécurisé (voir CR-1-1).

Les données supprimées ne doivent pas être restaurées (DS-1-4).

– S'il est nécessaire de mettre le dispositif au rebut, de le mettre à jour ou de le remplacer, une fonction de suppression (par exemple la restauration des paramètres d'usine) doit être fournie, afin que les données ne puissent pas être récupérées.

8.3.2 Contrôle des flux d'information

Le trafic réseau non autorisé ne devrait pas être permis (DS-2-1).

8.3.3 Gestion de session sécurisée

La session devrait être terminée après un temps d'inactivité (DS-3-1).

– Si l'utilisateur cherche à réaccéder au service après la fermeture de la session, il est recommandé de procéder à une réauthentification.

L'identifiant de la session devrait être une valeur non prévisible (DS-3-2).

– Un algorithme sécurisé générant des nombres aléatoires devrait être utilisé pour générer l'identifiant de la session.

– Lors de chaque ouverture de session avec authentification, l'identifiant de la session devrait être modifié et les identifiants déjà utilisés devraient être détruits.

8.3.4 Gestion des informations d'identification personnelle

Les informations d'identification personnelle devraient être gérées de façon sécurisée dans le cycle de vie des clés (DS-4-1).

– Les informations d'identification personnelle devraient être recueillies, utilisées, stockées et détruites de façon sécurisée.

8.4 Sécurité de la plate-forme du dispositif

La dimension liée à la sécurité de la plate-forme du dispositif comporte cinq éléments: sécurité logicielle; mises à jour sécurisées; gestion de la sécurité; journalisation et horodatage.

8.4.1 Sécurité logicielle

Un codage sécurisé devrait être appliqué (PL-1-1).

– Les logiciels devraient être conçus et mis en œuvre en tenant compte des questions de sécurité.

Les vulnérabilités connues sur le plan de la sécurité devraient être analysées et éliminées (PL-1-2).

– Si le logiciel a été conçu au moyen de protocoles et de bibliothèques, d'une interface de programmation d'application (API), de progiciels ou de logiciels à code source ouvert comportant des vulnérabilités sur le plan de la sécurité, les micrologiciels et le système d'exploitation peuvent eux aussi comporter ces vulnérabilités.

– Le domaine publique des vulnérabilités de sécurité connues (par exemple [b-CVE]) doit être utilisé pour analyser les vulnérabilités de sécurité du dispositif et les éliminer.

L'obfuscation devrait être appliquée (PL-1-3).

– Ces exigences peuvent être appliquées essentiellement aux applications développées, qui facilitent la restauration du code source.

– Dans la mesure où des outils de rétro-ingénierie ouverts peuvent être utilisés pour extraire des informations logiques importantes ou des informations essentielles, un niveau de protection approprié doit être assuré.

Une fonction de vérification de l'intégrité pour les paramètres de configuration et les codes exécutables devrait être prise en charge (PL-1-4).

– Pour garantir la validité des dispositifs IoT, l'intégrité des paramètres de configuration et des codes exécutables devrait périodiquement faire l'objet de vérifications au niveau du temps de démarrage, de façon automatique ou manuelle.

En cas d'erreur liée à l'intégrité, il convient de mettre en place des mesures appropriées.

8.4.2 Mise à jour sécurisée

La mise à jour doit être effectuée par des utilisateurs autorisés (PL-2-1).

La fonction de retour en arrière devrait être prise en charge en cas d'échec de la mise à jour (PL-2-2).

Une vérification de l'intégrité et de l'authentification devrait être effectuée avant toute mise à jour (PL-2-3).

– Il est recommandé d'authentifier l'utilisateur qui procède à la mise à jour, de réaliser des vérifications de l'intégrité de l'adresse du serveur de mise à jour et de contrôler ces deux éléments par rapport au fichier de mise à jour.

– Il est possible de confirmer l'authenticité d'un utilisateur en procédant à une nouvelle authentification de l'utilisateur immédiatement avant la procédure de mise à jour.

– Un utilisateur autorisé peut vérifier l'intégrité de l'adresse du serveur de mise à jour par une inspection visuelle.

– La vérification de l'intégrité et de l'authenticité des fichiers de mise à jour peut être effectuée par la vérification d'une signature numérique cryptographique.

8.4.3 Gestion de la sécurité

Les dispositifs superflus devraient être désactivés (PL-3-1).

– Les services superflus (Telnet, protocole de transfert de fichier (FTP), dispositifs universels prêts à fonctionner (UPnP), protocole simple de gestion de réseau (SNMP), etc.) devraient être désactivés et les services nécessaires fournis par les dispositifs devraient être précisés.

La gestion à distance devrait s'effectuer dans un environnement fiable (PL-3-2).

Une bibliothèque tierce sécurisée devrait être appliquée (PL-3-3).

– Il convient d'employer la dernière version de la bibliothèque et du module tiers utilisés pour le développement, sans vulnérabilités ou défauts de sécurité connus.

Un autotest devrait être fourni (PL-3-4).

– Il est recommandé de fournir une fonction d'autotest pour la détection des erreurs sur les éléments matériels et logiciels principaux lorsqu'un dispositif IoT est allumé (démarré) ou après son démarrage.

8.4.4 Journalisation

Un journal devrait être généré pour les évènements liés à la sécurité (PL-4-1).

– La journalisation devrait être mise en œuvre, et il devrait être possible de détecter et de suivre tout comportement anormal de la part du dispositif.

Un mécanisme de journalisation sécurisé devrait être fourni (PL-4-2).

– Pour prévenir la perte des journaux et les changements non autorisés (y compris la suppression), il est recommandé de disposer d'un mécanisme de protection des journaux.

8.4.5 Horodatage

Un horodatage fiable devrait être fourni (PL-5-1).

8.5 Sécurité physique

La dimension liée à la sécurité physique comprend la sécurisation des interfaces physiques et la protection des dispositifs IoT contre l'altération volontaire.

8.5.1 Interface physique sécurisée

Toute interface externe superflue devrait être désactivée (PH-1-1).

– Les dimensions et les fonctions de toutes les interfaces externes (réseau local, bus série universel (USB), port de carte numérique sécurisée (SD), etc.) exposées à l'extérieur devraient être indiquées.

– Si nécessaire, l'accès devrait être contrôlé afin de prévenir tout accès non autorisé.

Il convient d'empêcher l'accès non autorisé à l'interface interne (PH-1-2).

– Les dimensions et les fonctions de toutes les interfaces internes (Groupe d'action de test mixte (JTAG), débogage série par câble (SWD), UART, etc.) exposées à l'extérieur doivent être indiquées.

– Si nécessaire, l'accès doit être contrôlé afin de d'empêcher tout accès non autorisé.

8.5.2 Inviolabilité

Une fonction de détection des manipulations physiques non autorisées et de réponse à ces manipulations devrait être prise en charge (par exemple des sceaux à l'épreuve de l'altération, des verrous, des mesures visant à prévenir l'altération, des interrupteurs de remise à zéro et des alarmes) (PH-2-1).

Annexe A

Liste de correspondance entre les exigences de sécurité pour l'Internet des objets et les menaces/vulnérabilités pour la sécurité

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

Les exigences de sécurité pour l'IoT sont énumérées et décrites au paragraphe 8, et les menaces/vulnérabilités pour la sécurité sont indiquées au paragraphe 7. La correspondance entre les exigences de sécurité pour l'IoT et les menaces/vulnérabilités pour la sécurité est présentée dans le Tableau A.1.

Tableau A.1 – Liste de correspondance entre les exigences de sécurité pour l'IoT et les menaces/vulnérabilités pour la sécurité

Numéro de l'exigence	Dimension de l'exigence	Description de l'exigence	Menaces/vulnérabilités pour la sécurité
AU-1-1	Authentification	Le mot de passe d'usine par défaut doit être modifié.	ST-D-6
AU-1-2	Authentification	Un utilisateur doit être identifié et authentifié avant d'accéder à la gestion de la sécurité ou aux données sensibles.	ST-D-1
AU-1-3	Authentification	Le nombre de tentatives d'authentification doit être limité.	ST-D-4 ST-D-5
AU-1-4	Authentification	Le mot de passe préinstallé sur le dispositif devrait être unique.	ST-D-1
AU-1-5	Authentification	Il est recommandé de fournir une fonction de gestion des comptes utilisateur et des privilèges.	ST-D-3
AU-1-6	Authentification	Le principe du moindre privilège devrait être appliqué à tous les comptes utilisateur.	ST-D-3
AU-1-7	Authentification	L'accès concurrent au compte administrateur devrait être restreint.	ST-D-1
AU-1-8	Authentification	Un mot de passe sécurisé (longueur, cycle et complexité) devrait être créé.	ST-D-7
AU-2-1	Authentification	Les justificatifs codés en dur ne devraient pas être utilisés.	ST-D-6
AU-2-2	Authentification	Dans le cadre de l'authentification par mot de passe, le mot de passe devrait être masqué.	ST-D-6
AU-2-3	Authentification	Aucun retour spécifique ne devrait être fourni en cas d'échec de l'authentification.	ST-D-6
AU-3-1	Authentification	L'identifiant (ID) unique de chaque dispositif matériel devrait être conservé.	ST-D-2
AU-3-2	Authentification	Les dispositifs devraient être mutuellement authentifiés avant que des données sensibles ne soient transmises ou faire l'objet d'un contrôle avant l'interconnexion.	ST-D-2

Tableau A.1 – Liste de correspondance entre les exigences de sécurité pour l'IoT et les menaces/vulnérabilités pour la sécurité

Numéro de l'exigence	Dimension de l'exigence	Description de l'exigence	Menaces/vulnérabilités pour la sécurité
CR-1-1	Cryptographie	Des algorithmes de chiffrement sécurisés doivent être utilisés lorsque des données sont transmises ou stockées.	ST-D-8 ST-D-9
CR-1-2	Cryptographie	Les clés cryptographiques doivent être gérées de façon sécurisée tout au long de leur cycle de vie.	ST-D-8
CR-1-3	Cryptographie	Un nombre aléatoire devrait être généré par le biais d'un algorithme avec un caractère aléatoire avéré.	ST-D-8
DS-1-1	Sécurité des données	Les données transmises doivent être chiffrées.	ST-D-11
DS-1-2	Sécurité des données	Un mode sécurisé devrait être appliqué lorsqu'un canal de données ou de commande est créé.	ST-D-11
DS-1-3	Sécurité des données	Les données stockées dans le dispositif doivent être chiffrées.	ST-D-11
DS-1-4	Sécurité des données	Les données supprimées ne doivent pas être restaurées.	ST-D-17
DS-2-1	Sécurité des données	Le trafic réseau non autorisé ne devrait pas être permis.	ST-G-1
DS-3-1	Sécurité des données	La session devrait être terminée après un temps d'inactivité.	ST-D-12
DS-3-2	Sécurité des données	L'identifiant de la session devrait être une valeur non prévisible.	ST-D-12
DS-4-1	Sécurité des données	Les informations d'identification personnelle devraient être gérées en toute sécurité dans le cycle de vie des clés.	ST-D-11
PL-1-1	Sécurité de la plate-forme du dispositif	Un codage sécurisé devrait être appliqué.	ST-D-10 ST-D-20 ST-D-23 ST-D-24
PL-1-2	Sécurité de la plate-forme du dispositif	Les vulnérabilités connues sur le plan de la sécurité devraient être analysées et éliminées.	ST-D-16 ST-D-21
PL-1-3	Sécurité de la plate-forme du dispositif	L'obfuscation devrait être appliquée.	ST-D-16
PL-1-4	Sécurité de la plate-forme du dispositif	Une fonction de vérification de l'intégrité pour les paramètres de configuration et les codes exécutables devrait être prise en charge.	ST-D-15
PL-2-1	Sécurité de la plate-forme du dispositif	Une mise à jour doit être effectuée par un utilisateur autorisé.	ST-D-13

Tableau A.1 – Liste de correspondance entre les exigences de sécurité pour l'IoT et les menaces/vulnérabilités pour la sécurité

Numéro de l'exigence	Dimension de l'exigence	Description de l'exigence	Menaces/vulnérabilités pour la sécurité
PL-2-2	Sécurité de la plate-forme du dispositif	Une fonction de retour en arrière devrait être prise en charge au cas d'échec de la mise à jour.	ST-D-14
PL-2-3	Sécurité de la plate-forme du dispositif	Une vérification de l'intégrité et de l'authentification devraient être effectuées avant la mise à jour.	ST-D-15
PL-3-1	Sécurité de la plate-forme du dispositif	Les dispositifs superflus devraient être désactivés.	ST-D-16
PL-3-2	Sécurité de la plate-forme du dispositif	La gestion à distance devrait s'effectuer dans un environnement fiable.	ST-D-18
PL-3-3	Sécurité de la plate-forme du dispositif	Une bibliothèque tierce sécurisée devrait être appliquée.	ST-D-22
PL-3-4	Sécurité de la plate-forme du dispositif	Un autotest devrait être fourni.	ST-D-19
PL-4-1	Sécurité de la plate-forme du dispositif	Un journal devrait être généré pour les évènements liés à la sécurité.	ST-D-23
PL-4-2	Sécurité de la plate-forme du dispositif	Un mécanisme de journalisation sécurisé devrait être fourni.	ST-D-23
PL-5-1	Sécurité de la plate-forme du dispositif	Un horodatage fiable devrait être fourni.	ST-D-18
PH-1-1	Sécurité physique	Toute interface externe superflue devrait être désactivée.	ST-D-24 ST-D-25
PH-1-2	Sécurité physique	Il convient d'empêcher l'accès non autorisé à l'interface interne.	ST-D-24 ST-D-25
PH-2-1	Sécurité physique	Une fonction de détection des manipulations physiques non autorisées et de réponse à ces manipulations devrait être prise en charge (par exemple des sceaux à l'épreuve de l'altération, des verrous, des mesures visant à prévenir l'altération, des interrupteurs de remise à zéro et des alarmes).	ST-D-24 ST-D-25

Appendice I

Capacités de sécurité pour l'Internet des objets

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

I.1 Présentation générale

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 [UIT-T X.1361]. L'architecture IoT devrait comprendre les capacités générales dont la liste est reproduite dans le Tableau I.1.

Tableau I.1 – Tableau de correspondance entre les exigences de sécurité et les capacités de sécurité

Capacités	Exigences apparentées
Capacité de communication sécurisée pour la prise en charge des communications de manière sécurisée et fiable avec protection de la vie privée	DP-1-1, DS-1-2
Capacité de gestion sécurisée des clés pour la prise en charge de communications sécurisées	CR-2-1
Capacité de gestion sécurisée des données pour assurer la gestion des données de manière sécurisée et fiable avec protection de la vie privée	DS-2-1, DS-1-4
Capacité d'authentification pour authentifier les dispositifs	AU-1-1, AU-1-2, AU-1-3, AU-1-4, AU-1-8
Capacité d'autorisation (contrôle d'accès) pour autoriser les dispositifs	AU-3-1, AU-3-2
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	PL-4-1, PL-4-2
Capacité de fourniture sécurisée de services pour fournir des services de manière sécurisée et fiable avec protection de la vie privée	DS-4-1, DS-3-2
Capacité d'intégration sécurisée pour intégrer les différentes politiques et techniques de sécurité se rapportant aux différents composants fonctionnels IoT	–
Capacité pour mettre en œuvre des protocoles sécurisés utilisant des algorithmes de chiffrement grand public et normalisés	CR-1-1
Capacité de mise en œuvre de protocoles sécurisés fondés sur une cryptographie pour environnements contraints	CR-1-1
Capacité de mise à jour logicielle sécurisée et solide pour mettre à jour les modules ou applications logiciels	PL-2-1, PL-2-2, PL-2-3
Capacité de gestion des identités pour les dispositifs/capteurs IoT, les passerelles et les plates-formes/services	AU-2-1, AU-2-2, AU-2-3, DS-3-2, DS-4-1
Capacité d'analyse des vulnérabilités	–
Capacité de surveillance de l'accès aux données ou des tentatives d'accès aux applications IoT de manière parfaitement transparente, traçable et reproductible	PL-4-1, PL-4-2
Capacité de sécurité installée sur le matériel (par exemple module de plate-forme fiable) pour empêcher les risques liés à la sécurité physique associés à la virtualisation des réseaux et des passerelles	PH-1-1, PH-1-2, PH-2-1
Capacité de routage par trajets multiples pour empêcher les attaques par retransmission sélective	–

Tableau I.1 – Tableau de correspondance entre les exigences de sécurité et les capacités de sécurité

Capacités	Exigences apparentées
Capacité de protection des informations d'identification personnelle contre les atteintes tout au long de leur cycle de vie	DS-4-1
Capacité de configuration sécurisée	–
Capacité utilisant une cryptographie pour environnements contraints	CR-1-1
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	–

L'architecture IoT devrait comprendre les capacités liées à l'algorithme cryptographique dont la liste est reproduite dans le Tableau I.2.

Tableau I.2 – Tableau de correspondance entre les exigences de sécurité et les capacités de sécurité pour l'algorithme cryptographique

Capacités	Exigences apparentées
Capacité de production d'un nombre aléatoire de qualité cryptographique pour la prise en charge de la gestion des clés [b-IETF RFC 4086]	CR-3-1
Capacité de mise à jour périodique des clés de chiffrement nécessaires pour les flux de radiodiffusion	–
Capacité utilisant des algorithmes de chiffrement normalisés	CR-1-1

L'architecture IoT devrait comprendre les capacités liées au contexte dont la liste est reproduite dans le Tableau I.3.

Tableau I.3 – Tableau de correspondance entre les exigences de sécurité et les capacités de sécurité concernant le contexte

Capacités	Exigences apparentées
Capacité de résistance aux attaques par voie latérale	–
Capacité de prise en charge de pratiques de codage sécurisé 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	PL-1-1, PL-1-3, PL-1-4
Capacité de réalisation d'une évaluation des risques planifiée afin de déterminer les risques dans différents contextes opérationnels	PL-1-4

I.2 Capacités de sécurité pour les capteurs/dispositifs

Les capteurs/dispositifs IoT devraient comprendre les capacités de sécurité dont la liste est reproduite dans le Tableau I.4.

Tableau I.4 – Tableau de correspondance entre les exigences de sécurité et les capacités de sécurité pour les capteurs/dispositifs IoT

Capacités	Exigences apparentées
Capacité de gestion des clés	CR-2-1
Capacité de négociation de l'algorithme de chiffrement	CR-1-1
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	CR-1-1, DS-1-1, DS-1-2
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 garantissent que les données d'utilisateurs ou les données de signalisation, de commande ou de gestion n'ont pas été modifiées ou altérées	CR-1-1, DS-1-1, DS-1-2, PL-2-3
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	AU-1-2, AU-1-6, PL-2-1
Capacité de gestion des correctifs, y compris pour la mise à jour ou de mise à niveau des modules logiciels sécurisés	PL-2-1, PL-2-2, PL-2-3
Capacité de mise en œuvre de protocoles sécurisés fondés sur une cryptographie pour environnements contraints	CR-1-1
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	AU-1-2, AU-3-1, AU-3-2
Capacité de détection ou de prévention des altérations	PH-2-1
Capacité de production de nombres aléatoires de qualité cryptographique pour la prise en charge de la gestion des clés	CR-3-1
Capacité de résistance aux attaques par voie latérale	–
Capacité de détection des logiciels malveillants et de protection contre ces logiciels	–
Capacité de protection des informations d'identification personnelle contre la fuite de ces informations	DS-4-1

Les dispositifs IoT devraient comprendre les capacités de sécurité dont la liste est reproduite dans le Tableau I.5.

Tableau I.5 – Tableau de correspondance entre les exigences de sécurité et les capacités de sécurité pour les dispositifs IoT

Capacités	Exigences apparentées
Capacité de vérification de l'authenticité et de l'intégrité des logiciels sur un dispositif utilisant des signatures numériques générées de manière cryptographique [b-ISO/CEI 9796-3]	PL-1-4
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	DS-2-1
Capacité de mise en place de configurations sécurisées	PL-1-4

I.3 Capacités de sécurité pour les passerelles

Les plates-formes/services devraient comprendre les capacités de sécurité dont la liste est reproduite dans le Tableau I.6.

Tableau I.6 – Tableau de correspondance entre les exigences de sécurité et les capacités de sécurité concernant les passerelles

Capacités	Exigences apparentées
Capacité de système de détection des intrusions (IDS)/système de prévention des intrusions (IPS)	DS-2-1
Capacité de gestion des clés	CR-2-1
Capacité de mise en place de configurations sécurisées	PL-1-4
Capacité de négociation de l'algorithme de chiffrement	CR1-1
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 potentiels problèmes de sécurité liés à la confidentialité des données transmises par l'intermédiaire de réseaux hertziens	CR-1-1, DS-1-1, DS-1-2
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 garantissent que les données d'utilisateurs ou les données de signalisation, de commande ou de gestion n'ont pas été modifiées ou altérées	CR-1-1, DS-1-1, DS-1-2, PL-2-3
Capacité disponible pour faire face aux attaques par déni de service, allant de l'utilisation de techniques de codage source sécurisé à des tests de l'analyse du code source et des vulnérabilités, en passant par l'utilisation d'un système IDS/IPS installé sur un réseau ou un serveur	PL-1-1
Capacité d'authentification de l'origine des données ou de l'identité du capteur/dispositif IoT ainsi que de l'administrateur et du personnel de maintenance du réseau de capteur	AU-1-2, AU-1-6, PL-2-1
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	AU-1-2, AU-3-1, AU-3-2
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	PL-4-1
Capacité de mise à jour des modules logiciels sécurisés	PL-2-1, PL-2-2, PL-2-3

I.4 Capacités de sécurité du réseau

Conformément à [b-UIT-T X.805], le réseau devrait comprendre les capacités de sécurité dont la liste est reproduite dans le Tableau I.7.

Tableau I.7 – Tableau de correspondance entre les exigences de sécurité et les capacités de sécurité du réseau

Éléments	Capacités	Exigences apparentées
C_NT.1 [b-UIT-T X.805]	La dimension de sécurité des communications garantit que les informations ne sont acheminées qu'entre les points d'extrémité autorisés (les informations ne sont ni déviées ni interceptées au cours de leur acheminement entre ces points).	PL-3-1

I.5 Capacités de sécurité de la plate-forme/du service

La plate-forme/le service devrait comprendre les capacités de sécurité dont la liste est reproduite dans le Tableau I.8.

Tableau I.8 – Tableau de correspondance entre les exigences de sécurité et les capacités de sécurité concernant la plate-forme/le service

Capacités	Exigences apparentées
Capacité de protection d'un justificatif pour les opérations de chiffrement, c'est-à-dire un ensemble de données présentées pour prouver une identité ou des privilèges revendiqués	DS-2-1
Capacité de modification des noms d'utilisateur et des mots de passe par défaut lors de l'établissement d'une connexion initiale	AU-1-1, AU-1-2
Capacité de mise en œuvre de mots de passe forts et d'une politique de contrôle d'accès granulaire	AU-1-4, AU-1-6
Capacité consistant à rendre les ports inutiles non disponibles	PL-3-1, PH-1-1, PH-1-2
Capacité de prise en charge d'une configuration sécurisée, par exemple pour supprimer les services et les logiciels inutiles	AU-1-5, PL-3-1
Capacité de protection contre les infections par des logiciels malveillants grâce à l'utilisation de logiciels de protection contre les logiciels malveillants	PL-3-4
Capacité de mise en œuvre de politiques de gestion des correctifs	PL-2-1, PL-2-2, PL-2-3
Capacité de gestion des vulnérabilités	PL-1-1, PL-1-2
Capacité de mise à jour des modules et applications logiciels sécurisés	PL-2-1, PL-2-3
Capacité de gestion des clés pour le transfert sécurisé de messages entre une passerelle et une plate-forme/un service	CR-1-2
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; capacité disponible pour faire face aux attaques par déni de service	AU-1-5, DS-1-1, DS-1-2
Capacité de surveillance du réseau	–
Capacité de protection des informations d'identification personnelle hors transmission	DS-4-1
Capacité de sécurité au niveau des applications pour prévenir les menaces et attaques au niveau des applications décrites au paragraphe 8.4 de [UIT-T X.1361]	–
Capacité permettant d'atténuer les attaques par inférence	–

Appendice II

Cas d'utilisation de l'application des exigences de sécurité pour les dispositifs et les passerelles de l'Internet des objets

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

De nombreux dispositifs IoT présentent des vulnérabilités et des faiblesses de sécurité concernant l'authentification, la cryptographie et la protection des données. De plus, la plupart de ces dispositifs sont vulnérables par rapport aux interfaces physiques et au plates-formes de développement des dispositifs. Le présent Appendice décrit des cas de développement sécurisé par rapport aux exigences proposées.

II.1 Cas d'utilisation de l'authentification – Vulnérabilité face aux attaques par intercepteur

Il existe une vulnérabilité au niveau de la procédure d'authentification entre le serveur et la caméra-réseau. La caméra-réseau ne refuse pas les certificats invalides lors de la prise de contact au niveau de la sécurité dans la couche transport (TLS). L'auteur d'une attaque vole une clé importante. Voir la Figure II.1.

Les contre-mesures sont notamment les suivantes:

– Déni de certificat invalide sur la couche de connexion sécurisée.

– Utilisation d'un épinglage de clé publique fondé sur le protocole de transfert hypertexte.

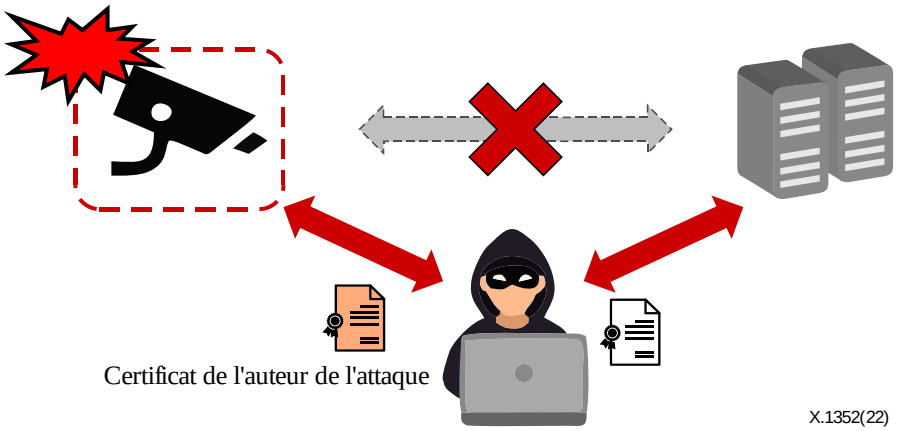

Figure II.1 – Cas d'utilisation de l'authentification

II.2 Cas d'utilisation du domaine cryptographique – Algorithme de chiffrement faible

Voir la Figure II.2.

Les vulnérabilités sont notamment les suivantes:

– Algorithme de chiffrement faible: Base64.

– Méthode de vérification des données: algorithme de hachage sécurisé 1 (SHA1).

Les contre-mesures sont notamment les suivantes:

– Force de sécurité supérieure à celle d'un algorithme de chiffrement à 128 bits (voir [b-ISO/IEC 19790]).

– Méthode de vérification des données: SHA256 [b-ISO/IEC 10118-3].

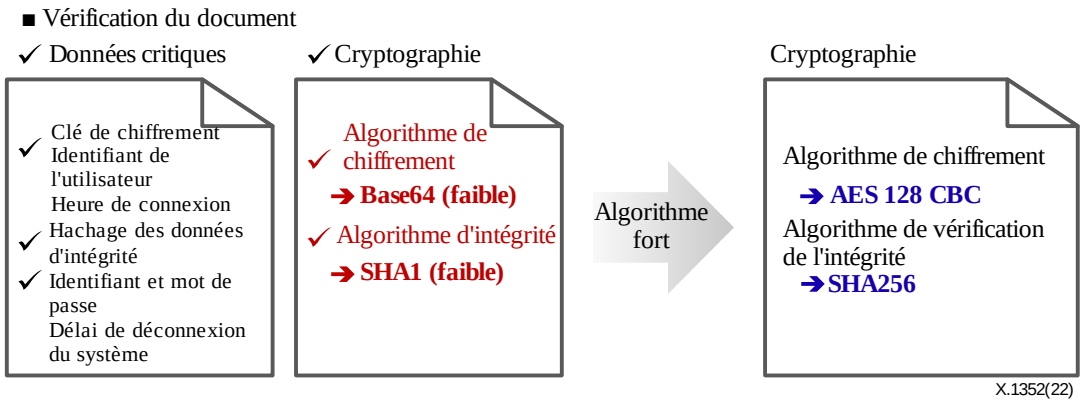

Figure II.2 – Cas d'utilisation du domaine cryptographique

II.3 Cas d'utilisation de la sécurité des données et du domaine cryptographique – Vérification faible de l'intégrité lors de l'envoi des données

Voir la Figure II.3.

La vulnérabilité est la suivante:

– Vérification faible de l'intégrité lors de l'envoi des données (méthode de vérification de l'intégrité des données: contrôle de redondance cyclique).

Les contre-mesures sont notamment les suivantes:

– Méthode de vérification des données: données de hachage SHA256 [b-ISO/IEC 10118-3].

– Total des données divisées et trame réassemblée.

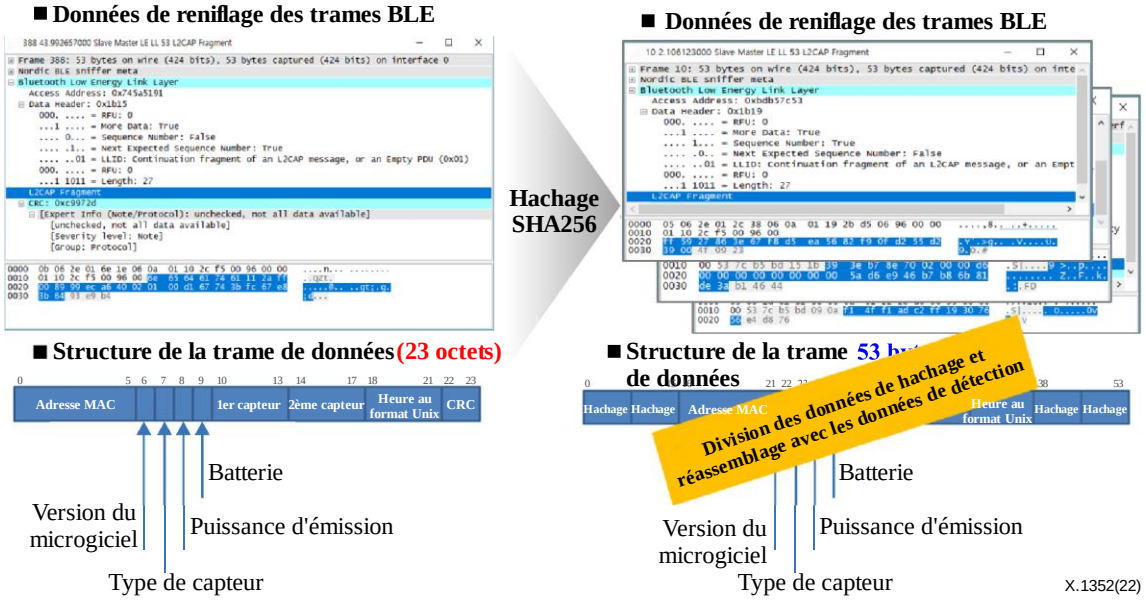

Figure II.3 – Cas d'utilisation de la sécurité des données et du domaine cryptographique

II.4 Cas d'utilisation du domaine lié à la sécurité des plates-formes de dispositif – Codage faible contre l'exploitation

Voir la Figure II.4.

La vulnérabilité est la suivante:

– Dépassement de la mémoire tampon et interface API faible.

La contre-mesure est la suivante:

– Vérification du codage sécurisé et proposition d'élimination des codes faibles grâce à des outils d'analyse statique.

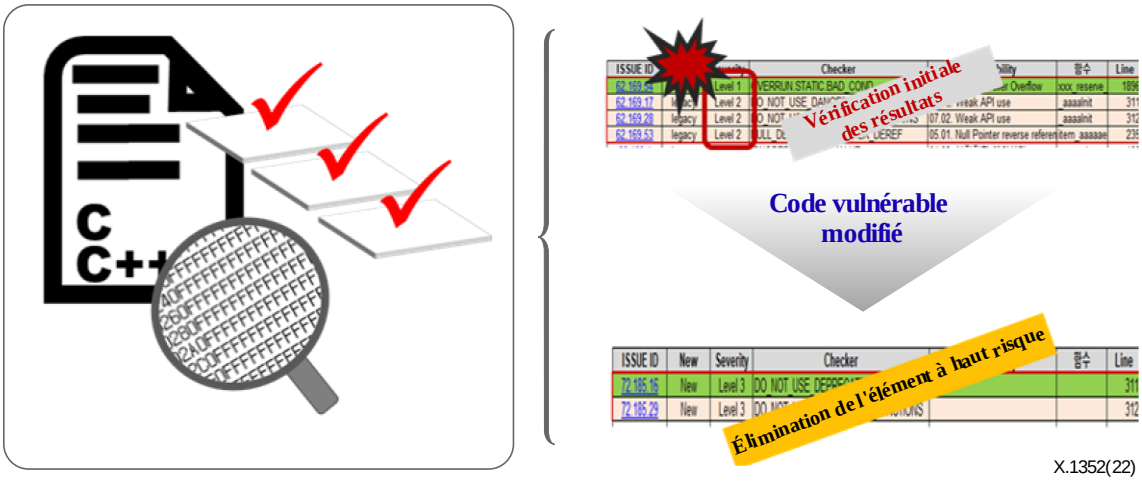

Figure II.4 – Cas d'utilisation du domaine lié à la sécurité des plates-formes de dispositif

II.5 Cas d'utilisation du domaine lié à la sécurité physique – Vulnérabilité de l'interface interne sur un circuit imprimé

Voir la Figure II.5.

La vulnérabilité est la suivante:

– Port JTAG disponible sur les produits de masse.

La contre-mesure est la suivante:

– Protection de l'accès mémoire mise en place dans le microcontrôleur.

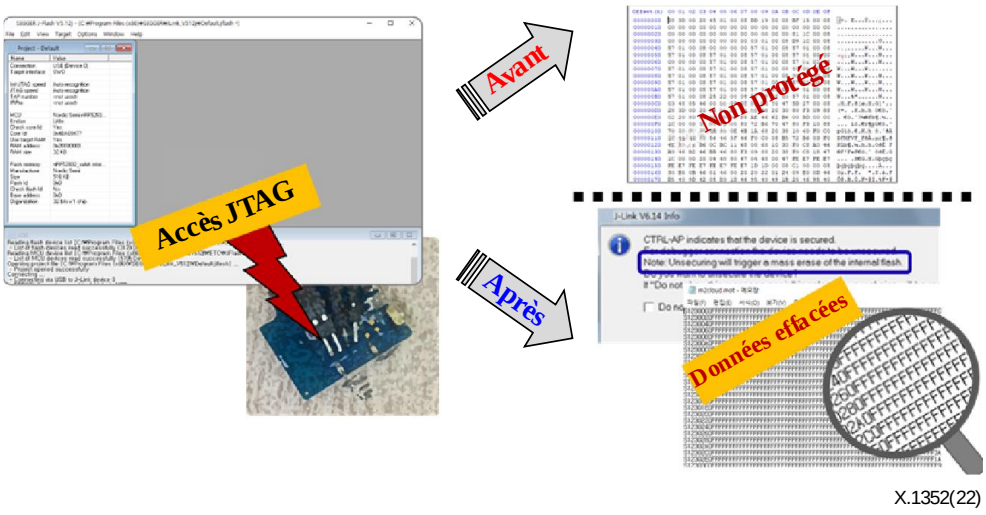

Figure II.5 – Cas d'utilisation du domaine lié à la sécurité physique

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.1252] Recommandation UIT-T X.1252 (2021), *Termes et définitions de base relatifs à la gestion d'identité*.

[b-UIT-T X.1254] Recommandation UIT-T X.1254 (2020), *Cadre de garantie d'authentification d'entité*.

[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-ISO 16100-1] ISO 16100-1:2009, *Systèmes d'automatisation industrielle et intégration – Profil d'aptitude du logiciel de fabrication pour interopérabilité – Partie 1: Cadre*.

[b-ISO/IEC 10118-3] ISO/IEC 10118-3 (2018), *Technologies de l'information – Techniques de sécurité – Fonctions de brouillage – Partie 3: Fonctions de brouillage dédiées*.

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

[b-ISO/IEC 27000] ISO/IEC 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/IEC 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/IEC 29100] ISO/IEC 29100: 2011, *Technologies de l'information – Techniques de sécurité – Cadre privé*.

[b-ISO/IEC 9796-3] ISO/IEC 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-IETF RFC 4086] IETF RFC 4086 (2005), *Randomness requirements for security (Exigences de sécurité pour les éléments aléatoires)*.

[b-CVE] Mitre Corporation (Internet). *Vulnérabilités et expositions courantes*. Bedford, MA: Mitre Corporation. Disponible à l'adresse: https://cve.mitre.org/ [consultée le 29/10/2022]

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, 2023