Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

X.1332

(03/2020)

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

Sécurité des réseaux électriques intelligents

Lignes directrices relatives à la sécurité des services de compteurs intelligents dans les réseaux électriques intelligents

Recommandation UIT-T X.1332

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
Sécurité de la technologie des registres distribués	X.1430–X.1449
Protocoles de sécurité (2)	X.1450–X.1459
ECHANGE D'INFORMATIONS SUR LA CYBERSÉCURITÉ	
Aperçu général de la cybersécurité	X.1500–X.1519
Echange concernant les vulnérabilités/les états	X.1520–X.1539
Echange concernant les événements/les incidents/l'heuristique	X.1540–X.1549
Echange de politiques	X.1550–X.1559
Heuristique et demande d'informations	X.1560–X.1569
Identification et découverte	X.1570–X.1579
Echange garanti	X.1580–X.1589
SÉCURITÉ DE L'INFORMATIQUE EN NUAGE	
Aperçu de la sécurité de l'informatique en nuage	X.1600–X.1601
Conception de la sécurité de l'informatique en nuage	X.1602–X.1639
Bonnes pratiques et lignes directrices concernant la sécurité de l'informatique en nuage	X.1640–X.1659
Mise en oeuvre de la sécurité de l'informatique en nuage	X.1660–X.1679
Sécurité de l'informatique en nuage (autres)	X.1680–X.1699

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

Recommandation UIT-T X.1332

Lignes directrices relatives à la sécurité des services de compteurs intelligents dans les réseaux électriques intelligents

Résumé

Les services de compteurs intelligents ont été largement déployés à travers le monde afin de rendre les réseaux électriques plus efficaces et plus fiables, en réunissant/fournissant des informations sur la consommation électrique des/aux clients, respectivement. Ces informations peuvent être utilisées pour estimer les besoins d'électricité des clients et cette estimation peut servir à modifier la demande ou à changer le comportement des clients en matière de consommation électrique, en leur fournissant des informations sur la consommation électrique. Toutefois, les services de compteurs intelligents peuvent subir des dysfonctionnements découlant de diverses menaces. Par exemple, des informations de comptage inexactes peuvent conduire à des décisions erronées en matière de gestion de la demande et l'utilisation à mauvais escient des fonctions de commande de la charge peuvent causer des dégâts économiques et physiques aux clients. La Recommandation UIT-T X.1332 fournit des lignes directrices relatives à la sécurité des services de compteurs intelligents, afin de permettre aux fournisseurs de services de mettre en œuvre les mesures de sécurité appropriées pour garantir la sécurité de leurs services. Elle identifie les menaces de sécurité et les méthodes d'attaque contre les services de compteurs intelligents et définit les exigences de sécurité et les capacités permettant d'atténuer ces menaces et de faire face à ces attaques en conséquence.

Historique

Edition	Recommandation	Approbation	Commission d'études	ID unique*
1.0	ITU-T X.1332	2020-03-26	17	11.1002/1000/14086

Mots clés

Infrastructure de comptage évoluée, lignes directrices relatives à la sécurité, réseaux électriques intelligents, service de compteurs intelligents

* 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.1332

Lignes directrices relatives à la sécurité des services de compteurs intelligents dans les réseaux électriques intelligents

1 Domaine d'application

La présente Recommandation fournit des lignes directrices relatives à la sécurité des services de compteurs intelligents dans les réseaux électriques intelligents. Elle couvre les sujets suivants:

- identification des menaces de sécurité et des attaques contre les services de compteurs intelligents;
- exigences de sécurité pour les services de compteurs intelligents; et
- lignes directrices relatives à la sécurité des services de compteurs intelligents pour respecter les exigences de sécurité.

2 Références

Aucune.

3 Définitions

3.1 Termes définis ailleurs

La présente Recommandation utilise les termes suivants définis ailleurs:

3.1.1 gestion active de la demande (DR) [b-UIT-T Y.2071]: Fonctionnalité des réseaux électriques intelligents qui permet aux clients de réduire ou de modifier leurs schémas de consommation électrique aux heures de pointe, moyennant, en général, une incitation financière. Elle comprend des mécanismes et des incitations visant à ce que les clients (services publics, commerces, industries et particuliers) diminuent leur consommation électrique pendant les heures de pointe ou lorsque la fiabilité du réseau est menacée. La gestion active de la demande est nécessaire pour optimiser l'équilibre entre l'offre et la demande en matière d'alimentation électrique.

3.1.2 opérateur du système d'alimentation électrique [b-CEI 60050-617]: Entité responsable de l'exploitation sûre et fiable d'une partie du système d'alimentation électrique dans une zone donnée et de la connexion avec les autres parties du système d'alimentation électrique.

3.1.3 système de gestion de l'énergie (EMS) [b-UIT-T Y.2071]: Système informatique composé d'une plate-forme logicielle fournissant des services d'appui de base et d'un ensemble d'applications fournissant les fonctionnalités nécessaires au fonctionnement efficace des installations de production et de distribution d'électricité, afin d'assurer la sécurité adéquate de l'alimentation en énergie à un coût minimal.

3.1.4 compteur intelligent [b-UIT-T X.1331]: Dispositif installé dans les locaux pour suivre et maîtriser la consommation électrique des dispositifs domestiques intelligents sur la base des informations de gestion active de la demande qu'ils reçoivent.

3.2 Termes définis dans la présente Recommandation

La présente Recommandation définit les termes suivants:

3.2.1 concentrateur de données: Dispositif intermédiaire situé entre un compteur intelligent et les systèmes de la compagnie d'électricité ayant pour principal objectif de recueillir et de gérer les données provenant du compteur intelligent.

3.2.2 système de gestion des données de comptage (MDMS): Système qui regroupe et valide les données de comptage telles que la consommation et la production électriques ainsi que les journaux d'informations de comptage, et qui réalise des estimations sur la base de ces données et autorise leur modification. Un système MDMS stocke ces données pendant une durée limitée avant qu'elles ne soient transmises à un entrepôt de données et les met à la disposition des systèmes autorisés.

NOTE − D'après [b-UIT-T Y.2071].

3.2.3 service de compteurs intelligents: Service qui regroupe des données relatives à la consommation électrique au moyen de compteurs intelligents et qui fournit une analyse des informations aux clients et à la compagnie d'électricité; les fournisseurs de services tiers peuvent aussi prendre part à ce service en exploitant les données relatives à la consommation électrique en vue de fournir un service ou un ensemble de services au client.

4 Abréviations et acronymes

La présente Recommandation utilise les abréviations et acronymes suivants:

AMRC accès multiple par répartition en code

CPL courants porteurs en ligne

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

DoS déni de service (*denial of service*)

EMS système de gestion de l'énergie (*energy management system*)

EUIS système d'information sur la consommation d'énergie (*energy usage information system*)

HMAC code d'authentification de message par hachage (*hash-based message authentication code*)

IHD système d'affichage à domicile (*in-home display*)

LTE évolution à long terme (*long-term evolution*)

MDMS système de gestion des données de comptage (*meter data management system*)

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

QoS qualité de service (*quality of service*)

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

VPN réseau privé virtuel (*virtual private network*)

5 Conventions

Aucune.

6 Présentation générale

Les services de compteurs intelligents, qui constituent l'une des principales fonctionnalités d'un réseau électrique intelligent, ont été largement déployés à travers le monde, afin de rendre les réseaux électriques plus efficaces et plus fiables, en réunissant des informations émanant des clients ou en leur fournissant des informations, respectivement.

Un compteur intelligent mesure, enregistre et transmet la quantité d'électricité qu'un client a consommée. Les données de comptage sont transmises de façon périodique, par exemple toutes les 5 ou 15 minutes. Les fournisseurs de services de compteurs intelligents peuvent utiliser ces données pour réaliser une estimation des besoins d'électricité des clients. Cette estimation leur permet

d'améliorer la fiabilité du réseau électrique en modifiant la demande ou en changeant le comportement des clients en matière de consommation électrique.

Les fournisseurs de services de compteurs intelligents peuvent fournir aux clients des informations concernant leur consommation électrique ainsi que le prix de l'électricité en temps réel, une estimation de leurs factures, des données statistiques ou l'évolution de la demande. Les clients peuvent utiliser ces informations pour essayer de réduire volontairement leur consommation électrique. Par exemple, si un fournisseur applique une tarification dynamique et fait varier le prix en fonction des besoins d'électricité, les clients peuvent retarder ou anticiper leurs activités qui consomment de l'électricité.

Toutefois, il existe des menaces pouvant entraîner des dysfonctionnements des réseaux électriques intelligents. Par exemple, des informations de comptage inexactes peuvent conduire à des décisions erronées en matière de gestion de la demande et l'utilisation à mauvais escient des fonctions de commande de la charge peuvent causer des dégâts économiques et physiques aux clients. En outre, lorsque des fournisseurs de services tiers ont accès aux informations de comptage, il convient de tenir compte de la question de la protection des informations d'identification personnelle (PII).

De plus, les informations sur la consommation électrique, les statistiques et les informations concernant les coûts sont généralement transmises à des dispositifs des clients connectés à Internet, tels que des smartphones ou des ordinateurs de poche. Par conséquent, presque toutes les menaces pesant sur les dispositifs mobiles peuvent aussi affecter les services de compteurs intelligents.

La présente Recommandation examine les menaces de sécurité qui pèsent sur les services de compteurs intelligents et définit les exigences de sécurité et les capacités permettant de garantir la sécurité des services de compteurs intelligents.

7 Architecture des services de compteurs intelligents

Avant d'aborder la sécurité des services de compteurs intelligents, on définit une architecture pour ces services, afin d'identifier toutes les entités intervenant dans les services de compteurs intelligents et de clarifier les relations qu'elles entretiennent les unes avec les autres.

En vue de définir un modèle général pour les services de compteurs, on considère, dans le cadre de la présente Recommandation, les cas d'utilisation suivants:

- regrouper les données relatives à la consommation électrique fournies par les dispositifs de comptage;
- indiquer aux clients l'évolution de la consommation électrique;
- fournir des informations relatives à la consommation électrique à des fournisseurs de services tiers; et
- fournir des informations relatives à la consommation électrique aux opérateurs du système d'alimentation électrique.

La Figure 7-1 illustre l'architecture d'un service de compteurs intelligents pour ces cas d'utilisation. Ce modèle comprend six entités principales: le dispositif de comptage, l'opérateur du système d'alimentation électrique, le système de gestion des données de comptage (MDMS), la compagnie d'électricité (système), le fournisseur de services tiers et le client.

Un dispositif de comptage mesure la consommation électrique du client et envoie les données de comptage au système MDMS d'une compagnie d'électricité. Cette dernière dispose d'un système d'information sur la consommation d'énergie (EUIS) permettant de communiquer l'évolution de la consommation électrique aux clients. Pour établir des données statistiques, le système EUIS se procure les données de comptage auprès du système MDMS. Le système de facturation de la compagnie d'électricité utilise aussi les données de comptage. Dans cette architecture, le système EUIS et le système de facturation sont considérés comme des systèmes de la compagnie d'électricité.

Les opérateurs du système d'alimentation électrique utilisent les données de comptage afin de réaliser des estimations concernant l'état actuel et futur du système d'alimentation. Le système de gestion de l'énergie (EMS) de ces opérateurs reçoit les données de comptage provenant du système MDMS et les utilise pour analyser l'évolution de la demande d'électricité. L'estimation des besoins permet à l'opérateur d'ajuster la quantité d'électricité disponible, afin d'assurer l'équilibre entre l'offre et la demande dans le système d'alimentation.

Les clients disposent de systèmes intelligents d'affichage de l'énergie ou de dispositifs intelligents qui indiquent des statistiques relatives à la consommation d'énergie et surveillent les charges connectées à leur réseau local. Les clients peuvent disposer de plusieurs types de systèmes d'affichage pour accéder au système EUIS de la compagnie d'électricité, tels que des smartphones, des tablettes, des téléviseurs intelligents, des ordinateurs personnels ou des systèmes d'affichage à domicile (IHD) spécialisés.

Les fournisseurs de services tiers utilisent les données de comptage pour améliorer la qualité de leurs services. Par exemple, une société de télévision par câble peut diffuser une publicité pour une lessive à un client particulier, si elle sait que ce client est justement en train de laver son linge.

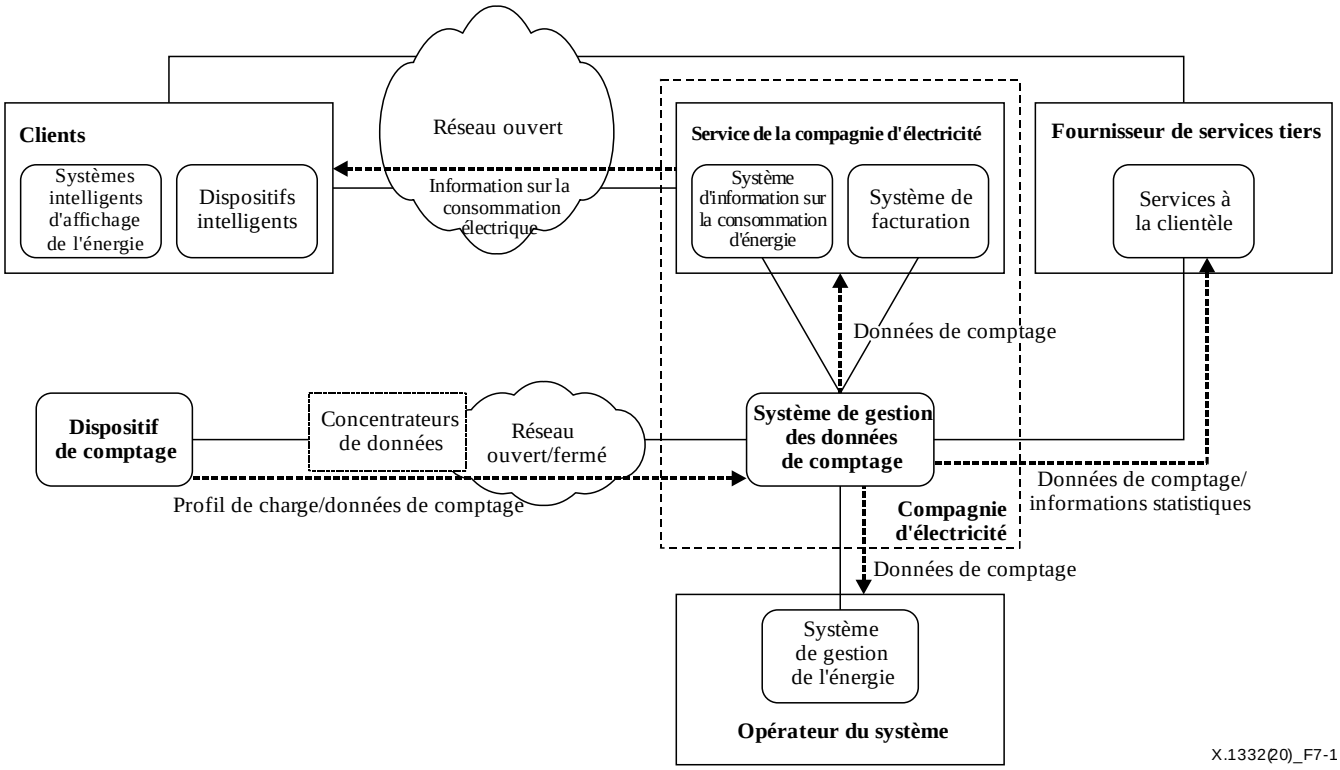

Figure 7-1 – Architecture d'un service de compteurs intelligents

Dans ce modèle d'architecture, les six relations suivantes entre les entités sont prises en compte: dispositif de comptage et système MDMS, système MDMS et système EMS, système MDMS et système de la compagnie d'électricité, système MDMS et fournisseur de services tiers, client et système de la compagnie d'électricité, client et fournisseur de services tiers.

Les dispositifs de comptage sont reliés au système MDMS par un réseau. Le réseau peut être ouvert, comme c'est le cas pour les réseaux LTE ou AMRC, ou fermé, comme c'est le cas pour les réseaux CPL ou les réseaux de lignes louées. Quel que soit le type de réseau, les concentrateurs de données regroupent les données de comptage en un emplacement et envoient les données agrégées au système MDMS.

Le système MDMS et le système EMS communiquent l'un avec l'autre par l'intermédiaire d'un réseau de télécommunication à qualité de service garantie.

Le système MDMS et le système de la compagnie d'électricité sont généralement situés sur le même réseau. Si ce n'est pas le cas, ils sont généralement reliés l'un à l'autre par un réseau de télécommunication à qualité de service garantie.

Le système MDMS peut être relié à des fournisseurs de services tiers par un réseau de télécommunication à qualité de service garantie.

Étant donné que les clients utilisent un réseau ouvert tel qu'Internet, le système de la compagnie d'électricité et le fournisseur de services tiers sont tous deux reliés aux clients par ce réseau ouvert. Les clients peuvent accéder aux réseaux au moyen des technologies WiFi, LTE ou encore Bluetooth.

8 Menaces de sécurité pesant sur les services de compteurs intelligents

8.1 Menaces pesant sur l'interface entre un dispositif de comptage et un système MDMS

L'interface entre le dispositif de comptage et le système MDMS est utilisée pour recueillir et traiter un grand nombre de données relatives à la consommation électrique des clients, y compris les données de comptage, le profil de charge et les mesures de la qualité de l'électricité. Les données transférées par cette interface constituent la cible principale des auteurs d'attaques. Ces derniers altèrent les services de compteurs intelligents par interception, falsification et répétition de ces données.

Les auteurs d'attaques visent aussi le déni des services de compteurs intelligents au moyen d'attaques par déni de service réparti (DDoS) contre le système MDMS.

L'interface entre un dispositif de comptage et un système MDMS est vulnérable face aux menaces suivantes:

- Fuite d'information: Les dispositifs de comptage intelligents (autrement dit, les compteurs intelligents) envoient régulièrement des données concernant la charge électrique (les données de comptage) au système MDMS par l'intermédiaire d'un concentrateur de données. Dans les réseaux électriques intelligents, cette opération est réalisée à des intervalles de temps très courts (par exemple cinq minutes ou moins). Par conséquent, les auteurs d'attaques peuvent observer les habitudes de vie des clients s'ils parviennent à renifler les données de comptage.
- Falsification des données de comptage: Les auteurs d'attaques peuvent bloquer les données de comptage réelles et en envoyer de fausses au système MDMS. Ces attaques peuvent entraîner des erreurs dans l'estimation de la demande en empêchant le système MDMS et le système EMS d'accéder aux données de comptage réelles recueillies. Ces erreurs peuvent aussi engendrer un déséquilibre entre l'offre et la demande, entraînant ainsi une coupure de courant.
- Falsification du profil de charge: Les auteurs d'attaques peuvent apporter des modifications non autorisées au profil de charge stocké dans les dispositifs de comptage. Étant donné que le système de facturation calcule les montants dus par les clients en fonction de leur profil de charge, cette menace peut engendrer des erreurs dans la facturation des clients.

- Déni de service (DoS): Les auteurs d'attaques peuvent perpétrer des attaques DoS afin d'exécuter un code malveillant sur un certain nombre de dispositifs de comptage ou de concentrateurs de données et d'inonder une cible (en général, le système MDMS) avec un grand nombre de données ou de demandes de service. Ce type d'attaque peut ralentir voire interrompre un service de compteurs intelligents.

8.2 Menaces pesant sur l'interface entre un système MDMS et un fournisseur de services tiers

L'interface entre un système MDMS et un fournisseur de services tiers est utilisée pour le partage des données de comptage, afin que le fournisseur tiers puisse fournir divers services personnalisés à chaque client. Étant donné que des informations PII peuvent être transférées par cette interface, les auteurs d'attaques ciblent principalement ces données et altèrent les services de compteurs intelligents en interceptant et en utilisant ces données.

L'interface entre un système MDMS et un fournisseur de services tiers est vulnérable face aux menaces suivantes:

- Atteintes aux informations PII: Les auteurs d'attaques peuvent intercepter les informations PII en lançant une attaque par reniflage des paquets ou en exécutant un code malveillant sur les systèmes du fournisseur de services tiers connectés à Internet.

8.3 Menaces pesant sur l'interface entre le système de la compagnie d'électricité et un client

L'interface entre le système de la compagnie d'électricité et les dispositifs locaux d'un client fournit différents types d'informations visant à encourager les clients à prendre part à la gestion active de la demande. Les informations pouvant être transmises comprennent l'évolution de la consommation électrique des clients, les prix de l'électricité en temps réel, l'évolution de la demande, les factures ainsi que des données statistiques. En falsifiant les informations transférées, les auteurs d'attaques peuvent inciter un client à consommer une quantité excessive d'électricité. Les attaques DoS constituent une autre menace éventuelle sérieuse pesant sur le système de la compagnie d'électricité connecté aux dispositifs locaux des clients.

Les interfaces entre le système de la compagnie d'électricité et les dispositifs du client sont vulnérables face aux menaces suivantes:

- Falsification du prix en temps réel: Les auteurs d'attaques peuvent falsifier le prix en temps réel communiqué par le système de la compagnie d'électricité aux clients afin d'induire ces derniers en erreur. Si le prix falsifié est inférieur au prix réel, les dispositifs des clients (par exemple un système intelligent d'affichage de l'énergie) peuvent conduire des dispositifs consommant de l'électricité (par exemple un véhicule électrique) à consommer davantage. À l'inverse, si le prix est rendu supérieur au prix réel, le client peut laisser passer la possibilité de stocker de l'électricité à faible coût.
- Déni de service: Les auteurs d'attaques peuvent perpétrer des attaques DoS afin d'exécuter un code malveillant sur un certain nombre de dispositifs de clients et d'inonder une cible (en général, un système EUIS) avec un grand nombre de demandes de service. Ce type d'attaque peut ralentir voire interrompre un service de compteurs intelligents.
- Atteinte aux informations PII: L'auteur d'une attaque peut intercepter les informations PII en lançant une attaque par reniflage des paquets ou en exécutant un code malveillant sur le dispositif d'un client connecté à Internet.

9 Exigences de sécurité pour les services de compteurs intelligents

9.1 Exigences de sécurité pour les relevés de consommation électrique

Les relevés de consommation électrique constituent la fonctionnalité la plus importante des services de compteurs intelligents. Lorsqu'il fonctionne correctement, un système MDMS peut recueillir les informations nécessaires pour calculer l'évolution de la consommation électrique, le profil de consommation de chaque client, les factures d'électricité, etc. En outre, d'autres entités impliquées dans les services de compteurs intelligents peuvent utiliser ces informations pour assurer leur rôle de manière appropriée. Par conséquent, l'intégrité, l'authenticité et la confidentialité des données de comptage sont les principales exigences de sécurité portant sur la procédure de recueil des informations.

Pour répondre de façon appropriée aux menaces pesant sur l'interface de communication entre les compteurs intelligents et un système MDMS, il conviendrait de tenir compte des exigences de sécurité suivantes:

- La confidentialité de bout en bout des données transférées par l'interface de communication entre un compteur intelligent et le système MDMS devrait être assurée.
- L'intégrité de bout en bout des messages de communication entre un compteur intelligent et le système MDMS devrait être assurée, afin d'empêcher la modification non autorisée des données.
- Les données de comptage et les informations d'authentification stockées dans des dispositifs tels que des compteurs intelligents, des concentrateurs de données et le système MDMS devraient être protégées contre les accès non autorisés.
- L'authenticité de l'émetteur devrait être vérifiée pour chaque communication.

9.2 Exigences de sécurité pour les informations utilisées par les clients

Étant donné que les dispositifs des clients peuvent accéder au système d'une compagnie d'électricité connecté au système d'extrémité de distribution électrique, ils constituent la principale cible des attaques visant les services de compteurs intelligents. Par conséquent, pour cette partie d'un service de compteurs intelligents, les données et applications contenues dans les dispositifs des clients devraient être protégées.

Pour atténuer les effets secondaires éventuels des menaces pesant sur l'interface de communication entre le système de la compagnie d'électricité et les clients, il conviendrait de tenir compte des exigences de sécurité suivantes:

- La confidentialité des données au niveau de l'interface de communication entre le client et le système de la compagnie d'électricité devrait être assurée.
- L'intégrité des données des messages de communication entre le client et le système de la compagnie d'électricité devrait être assurée, afin d'empêcher une modification non autorisée des données.
- L'authenticité de l'émetteur devrait être vérifiée pour chaque communication.
- Les informations stockées dans le dispositif d'un client et dans le système de la compagnie d'électricité devraient être protégées contre les accès non autorisés.
- L'intégrité des applications présentes dans les dispositifs des clients devrait être vérifiée.

9.3 Exigences de sécurité pour les informations utilisées par les fournisseurs de services tiers

Les principales préoccupations concernant ce point portent sur le traitement des données PII et sur les atteintes aux informations PII entre un fournisseur de services tiers et un système MDMS.

Pour traiter de façon appropriée les menaces pesant sur l'interface de communication entre un système MDMS et un fournisseur de services tiers, il conviendrait de tenir compte des exigences de sécurité suivantes:

- La confidentialité des données au niveau de l'interface de communication entre un système MDMS et un fournisseur de services tiers devrait être assurée.
- L'intégrité des données des messages de communication entre le système MDMS et un fournisseur de services tiers devrait être assurée, afin d'empêcher une modification non autorisée des données.
- L'authenticité de l'émetteur devrait être vérifiée pour chaque communication.
- Pour la fourniture de services personnalisés, les données PII devraient être traitées de manière adéquate, afin de n'être communiquées qu'avec l'accord du client.
- En ce qui concerne les services qui n'utilisent pas d'informations PII, les informations PII relatives au comptage ne devraient pas être fournies.

9.4 Exigences de sécurité pour les informations utilisées par l'opérateur du système d'alimentation électrique

Pour lutter de façon appropriée contre les menaces pesant sur les interfaces de communication entre un système MDMS et l'opérateur du système d'alimentation électrique, il conviendrait de tenir compte des exigences de sécurité suivantes:

- La confidentialité des données au niveau de l'interface de communication entre un système MDMS et l'opérateur du système d'alimentation électrique devrait être assurée.
- L'intégrité des données des messages de communication entre un système MDMS et l'opérateur du système d'alimentation électrique devrait être assurée, afin d'empêcher une modification non autorisée des données.
- Seules les entités autorisées devraient pouvoir accéder à l'interface de communication entre un système MDMS et l'opérateur du système d'alimentation électrique.
- Les informations PII relatives au comptage ne devraient pas être fournies.

10 Lignes directrices relatives à la sécurité des services de compteurs intelligents

10.1 Contrôles de sécurité pour les relevés de consommation électrique

Pour satisfaire les exigences de sécurité pour les relevés de consommation électrique, il conviendrait d'envisager la mise en œuvre des contrôles de sécurité suivants en tant que capacités dans chaque entité impliquée dans les relevés de consommation électrique.

- Le contrôle d'accès aux données de comptage devrait être appliqué aux dispositifs de comptage, aux concentrateurs de données et au système MDMS. Seules les entités autorisées devraient pouvoir accéder aux données de consommation électrique.
- Un mécanisme d'authentification mutuelle entre le dispositif de comptage et le système MDMS devrait être utilisé afin de garantir l'authenticité de l'émetteur.
- Des mesures d'authentification des messages devraient être prises pour protéger l'intégrité des données de consommation électrique transmises au système MDMS. Par exemple, des codes de chiffrement pour l'authentification des messages tels que les codes HMAC peuvent être utilisés à cet égard.

- Le chiffrement des données peut être considéré comme une mesure de sécurité visant à protéger les données relatives à la facturation.
- Une détection des erreurs dans l'intégrité des données et dans le déchiffrement de données chiffrées devrait être réalisée au niveau du système MDMS.
- Un mécanisme sécurisé de gestion des clés devrait être adopté au niveau des dispositifs de comptage, des concentrateurs de données et du système MDMS pour garantir la génération sécurisée, l'approbation, le stockage et le rafraîchissement des clés de chiffrement.
- Un mécanisme de protection des données devrait être utilisé pour garantir la confidentialité et l'intégrité des données de comptage stockées dans le système MDMS.
- Des mesures de sécurité visant à atténuer les effets des attaques DoS peuvent être adoptées au niveau du système MDMS.

10.2 Contrôles de sécurité pour les informations utilisées par les clients

Pour satisfaire les exigences de sécurité pour les informations utilisées par les clients, il conviendrait d'envisager la mise en œuvre des contrôles de sécurité suivants en tant que capacités dans chaque entité:

- Des mesures de sécurisation des communications, comme la sécurité TLS, devraient être appliquées aux communications entre les dispositifs des clients et le système de la compagnie d'électricité. Il conviendrait d'assurer les fonctions d'authentification mutuelle ainsi que d'authentification et de chiffrement des données de communication entre les dispositifs des clients et le système de la compagnie d'électricité.
- L'authentification et l'autorisation des utilisateurs pour l'accès aux informations de consommation électrique devraient être mises en œuvre dans les applications fournissant ces informations. Le système de la compagnie d'électricité devrait uniquement autoriser les utilisateurs à accéder à leurs propres données.
- Les données d'authentification des utilisateurs et les clés de chiffrement utilisées pour l'authentification des utilisateurs et la sécurisation des communications ainsi que les informations PII devraient être stockées de façon sécurisée dans les dispositifs des clients.
- Des mesures de vérification de l'intégrité devraient être prises pour détecter la falsification d'une application lorsqu'elle est exécutée sur le dispositif d'un client.

10.3 Contrôles de sécurité pour les informations utilisées par les fournisseurs de services tiers

Pour satisfaire les exigences de sécurité pour les informations utilisées par un fournisseur de services tiers, il conviendrait d'envisager la mise en œuvre des contrôles de sécurité suivants en tant que capacités dans chaque entité:

- Une ligne louée peut être utilisée pour empêcher des utilisateurs non autorisés d'accéder à la connexion entre un système MDMS et un fournisseur de services tiers.
- Des mesures de sécurisation des communications, comme un réseau privé virtuel (VPN), devraient être appliquées aux communications entre les dispositifs des clients et le système de la compagnie d'électricité. Il conviendrait d'assurer les fonctions d'authentification mutuelle ainsi que d'authentification et de chiffrement des données de communication entre les dispositifs des clients et le système de la compagnie d'électricité.

- Des processus de protection des informations PII devraient être appliqués tout au long du cycle de vie de ces informations, dans les cas où l'accès à ces données est demandé par des fournisseurs de services tiers [b-GAO-08-343]. Il est possible d'appliquer la désidentification si le fournisseur de services tiers n'a pas besoin des données d'identification.

10.4 Contrôles de sécurité pour les informations utilisées par l'opérateur du système d'alimentation électrique

Pour satisfaire les exigences de sécurité pour les informations utilisées par l'opérateur du système d'alimentation électrique, il conviendrait d'envisager la mise en œuvre des contrôles de sécurité suivants en tant que capacités dans chaque entité:

- Une ligne louée devrait être utilisée afin de réduire le risque d'accès non autorisé à la connexion entre un système MDMS et l'opérateur du système d'alimentation électrique.
- Des mesures de sécurisation des communications, comme un réseau VPN, devraient être appliquées aux communications entre un système MDMS et l'opérateur du système d'alimentation électrique. Il conviendrait d'assurer les fonctions d'authentification mutuelle ainsi que d'authentification et de chiffrement des données de communication entre un système MDMS et l'opérateur du système d'alimentation électrique.
- Il est possible d'appliquer la désidentification si l'opérateur du système d'alimentation électrique n'a pas besoin des données d'identification.

Bibliographie

[b-UIT-T X.1331] Recommandation UIT-T X.1331 (2018), *Lignes directrices relatives à la sécurité des dispositifs des réseaux domestiques (HAN) dans les réseaux électriques intelligents.*

[b-UIT-T Y.2071] Recommandation UIT-T Y.2071 (2015), *Cadre applicable aux micro-réseaux électriques.*

[b-GAO-08-343] *United States Government Accountability Office*, GAO-08-343:2008. *Information Security: Protecting Personally Identifiable Information.* https://www.gao.gov/new.items/d08343.pdf

[b-CEI 60050-617] CEI 60050-617:2009, *Vocabulaire électrotechnique international – Partie 617: Organisation/Marché de l'électricité*

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	Equipements terminaux de télégraphie
Série T	Terminaux des services télématiques
Série U	Commutation télégraphique
Série V	Communications de données sur le réseau téléphonique
Série X	**Réseaux de données, communication entre systèmes ouverts et sécurité**
Série Y	Infrastructure mondiale de l'information, protocole Internet, 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, 2020