Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

X.1366

(09/2020)

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

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

Systèmes d'authentification de messages agrégés pour l'environnement de l'Internet des objets

Recommandation UIT-T X.1366

RECOMMANDATIONS UIT-T DE LA SÉRIE X

RÉSEAUX DE DONNÉES, COMMUNICATION ENTRE SYSTÈMES OUVERTS ET SÉCURITÉ

RÉSEAUX PUBLICS DE DONNÉES	X.1–X.199
INTERCONNEXION DES SYSTÈMES OUVERTS	X.200–X.299
INTERFONCTIONNEMENT DES RÉSEAUX	X.300–X.399
SYSTÈMES DE MESSAGERIE	X.400–X.499
ANNUAIRE	X.500–X.599
RÉSEAUTAGE OSI ET ASPECTS SYSTÈMES	X.600–X.699
GESTION OSI	X.700–X.799
SÉCURITÉ	X.800–X.849
APPLICATIONS OSI	X.850–X.899
TRAITEMENT RÉPARTI OUVERT	X.900–X.999
SÉCURITÉ DE L'INFORMATION ET DES RÉSEAUX	
Aspects généraux de la sécurité	X.1000–X.1029
Sécurité des réseaux	X.1030–X.1049
Gestion de la sécurité	X.1050–X.1069
Télébiométrie	X.1080–X.1099
APPLICATIONS ET SERVICES SÉCURISÉS (1)	
Sécurité en multidiffusion	X.1100–X.1109
Sécurité des réseaux domestiques	X.1110–X.1119
Sécurité des télécommunications mobiles	X.1120–X.1139
Sécurité de la toile	X.1140–X.1149
Protocoles de sécurité (1)	X.1150–X.1159
Sécurité d'homologue à homologue	X.1160–X.1169
Sécurité des identificateurs en réseau	X.1170–X.1179
Sécurité de la télévision par réseau IP	X.1180–X.1199
SÉCURITÉ DU CYBERESPACE	
Cybersécurité	X.1200–X.1229
Lutte contre le spam	X.1230–X.1249
Gestion des identités	X.1250–X.1279
APPLICATIONS ET SERVICES SÉCURISÉS (2)	
Communications d'urgence	X.1300–X.1309
Sécurité des réseaux de capteurs ubiquitaires	X.1310–X.1319
Sécurité des réseaux électriques intelligents	X.1330–X.1339
Courrier certifié	X.1340–X.1349
Sécurité de l'Internet des objets (IoT)	**X.1360–X.1369**
Sécurité des systèmes de transport intelligents	X.1370–X.1389
Sécurité de la technologie des registres distribués	X.1400–X.1449
Protocoles de sécurité (2)	X.1450–X.1459
ECHANGE D'INFORMATIONS SUR LA CYBERSÉCURITÉ	
Aperçu général de la cybersécurité	X.1500–X.1519
Échange concernant les vulnérabilités/les états	X.1520–X.1539
Échange concernant les événements/les incidents/l'heuristique	X.1540–X.1549
Échange de politiques	X.1550–X.1559
Heuristique et demande d'informations	X.1560–X.1569
Identification et découverte	X.1570–X.1579
Échange garanti	X.1580–X.1589
SÉCURITÉ DE L'INFORMATIQUE EN NUAGE	
Aperçu de la sécurité de l'informatique en nuage	X.1600–X.1601
Conception de la sécurité de l'informatique en nuage	X.1602–X.1639
Bonnes pratiques et lignes directrices concernant la sécurité de l'informatique en nuage	X.1640–X.1659
Mise en œuvre de la sécurité de l'informatique en nuage	X.1660–X.1679
Sécurité de l'informatique en nuage (autres)	X.1680–X.1699
COMMUNICATIONS QUANTIQUES	
Terminologie	X.1700–X.1701
Générateur quantique de nombres aléatoires	X.1702–X.1709
Cadre de sécurité pour les réseaux QKDN	X.1710–X.1711
Conception de la sécurité pour les réseaux QKDN	X.1712–X.1719
Techniques de sécurité pour les réseaux QKDN	X.1720–X.1729
SÉCURITÉ DES DONNÉES	
Sécurité des mégadonnées	X.1750–X.1759
SÉCURITÉ DE LA 5G	X.1800–X.1819

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

Recommandation UIT-T X.1366

Systèmes d'authentification de messages agrégés pour l'environnement de l'Internet des objets

Résumé

Le nombre de dispositifs de l'Internet des objets (IoT) est en constante augmentation et dans un avenir proche, un nombre considérable de dispositifs seront connectés au réseau IoT, y compris au réseau 5G. La Recommandation UIT-T X.1366 définit deux systèmes d'authentification de messages. Le premier est un système d'authentification de messages agrégés (AMA) pour l'IoT comme mécanisme de base. Le second est un système interactif d'authentification de messages agrégés (IAMA) doté d'un protocole interactif qui fonctionne de manière simple et sûre. Ces deux systèmes d'authentification de messages agrégés permettent d'assurer "l'authentification (de l'identité) des entités" ainsi que "l'authentification des messages". Il se peut que ces systèmes ne soient pas applicables à tous les cas d'utilisation des dispositifs IoT, mais ils sont relativement efficaces et adaptés dans les conditions d'utilisation suivantes:

- lorsqu'une authentification des messages est requise pour des dizaines à des dizaines de milliers de dispositifs IoT;
- lorsqu'on a recours de manière fréquente et intermittente à un processus d'authentification pour le traitement de données ou messages.

À titre d'exemple, les "applications de surveillance de l'utilisation de données d'image" et la "télémesure à distance", qui permettent notamment d'assurer la surveillance des activités des usines et le suivi médical, sont des exemples types de cas d'utilisation de ces systèmes.

Historique

Edition	Recommandation	Approbation	Commission d'études	Identifiant unique*
1.0	UIT-T X.1366	03-09-2020	17	11.1002/1000/14262

Mots clés

Authentification de messages agrégés, AMA, IoT.

* 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 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.1366

Systèmes d'authentification de messages agrégés pour l'environnement de l'Internet des objets

1 Domaine d'application

La présente Recommandation définit deux systèmes d'authentification de messages. Le premier est un système d'authentification de messages agrégés (AMA) pour l'IoT comme mécanisme de base. Le second est un système interactif d'authentification de messages agrégés (IAMA), doté d'un protocole interactif qui fonctionne de manière simple et sûre. Ces deux systèmes d'authentification de messages agrégés permettent d'assurer "l'authentification (de l'identité) des entités " ainsi que "l'authentification des messages".

Les modalités de mise en œuvre de ces systèmes dans un environnement IoT spécifique, ainsi que les techniques de signature agrégée, n'entrent pas dans le cadre de la présente Recommandation.

2 Références

Les Recommandations UIT-T et autres références suivantes contiennent des dispositions qui, par suite de la référence qui y est faite, constituent des dispositions de la présente Recommandation. Au moment de la publication, les éditions indiquées étaient en vigueur. Les Recommandations et autres références étant sujettes à révision, les utilisateurs de la présente Recommandation sont invités à rechercher la possibilité d'appliquer les éditions les plus récentes des Recommandations et autres références énumérées ci-dessous. Une liste des Recommandations UIT-T en vigueur est publiée périodiquement. La référence à un document figurant dans la présente Recommandation ne donne pas à ce document en tant que tel le statut de Recommandation.

Aucune.

3 Définitions

3.1 Termes définis ailleurs

La présente Recommandation utilise le terme suivant défini ailleurs:

3.1.1 code d'authentification de message (MAC, *message authentication code*) [b-UIT-T-X.813]: valeur de contrôle cryptographique utilisée pour assurer l'intégrité des données et l'authentification de leur origine.

3.2 Termes définis dans la présente Recommandation

La présente Recommandation définit les termes suivants:

3.2.1 authentification de messages: propriété qui garantit qu'un message n'a pas été modifié pendant le transit pour assurer l'intégrité des données, et qui permet au destinataire de vérifier l'origine du message.

3.2.2 authentification de messages agrégés (AMA): propriété qui permet d'agréger plusieurs codes d'authentification de messages, créés par plusieurs expéditeurs, dans un code d'authentification plus court qui peut toujours être vérifié par un destinataire possédant les clés secrètes des expéditeurs.

3.2.3 étiquettes d'authentification: élément de données à utiliser pour l'authentification de messages.

4 Abréviations et acronymes

La présente Recommandation utilise les abréviations et acronymes suivants:

AGT protocole de test de groupe adaptatif (*adaptive group testing protocol*)

AMA authentification de messages agrégés (*aggregate message authentication*)

AMAC code d'authentification de messages agrégés (*aggregate message authentication code*)

IAMA authentification interactive de messages agrégés (*interactive aggregate message authentication*)

IoT Internet des objets (*Internet of things*)

MAC code d'authentification de messages (*message authentication code*)

XOR opération OU exclusif (*exclusive OR operation*)

5 Conventions

Néant.

6 Vue d'ensemble et principe de base

6.1 Vue d'ensemble

Le nombre de dispositifs de l'Internet des objets (IoT) est en constante augmentation et dans un avenir proche, un nombre considérable de dispositifs seront connectés au réseau IoT, y compris au réseau 5G. La présente Recommandation définit un système d'authentification simple et sûr qui peut être utilisé en pareil cas.

Le code d'authentification de messages (MAC) constitue l'une des primitives de chiffrement les plus importantes, et le code MAC peut être utilisé en tant que primitive de chiffrement simple pour l'authentification des messages. Toutefois, il ressort de la Figure 1 que dans les systèmes IoT actuels, pour les messages envoyés depuis des dispositifs IoT, des étiquettes d'authentification (voir le § 3.2.3) sont créées de manière individuelle du côté du dispositif IoT, et que chaque message comportant une étiquette ainsi créée est en principe vérifié par un processus de vérification du côté du récepteur. Dans le scénario IoT actuel, il est admis que le principal problème est que la charge des processus existants d'authentification et de vérification augmente proportionnellement à l'accroissement du nombre de dispositifs IoT.

Le code d'authentification de messages agrégés (AMAC) est une technique existante qui permet de comprimer plusieurs étiquettes MAC sur plusieurs messages créés par différents dispositifs pour former une seule étiquette agrégée, sans compromettre la sécurité (voir l'Appendice II). L'avantage du code AMAC tient au fait que la taille d'une étiquette agrégée est beaucoup plus petite que la taille totale combinée des étiquettes MAC. Par conséquent, ce code sera utile dans les applications des réseaux mobiles ou des réseaux IoT, dans lesquels un grand nombre de dispositifs envoyant des messages sont connectés. Le code AMAC peut plus particulièrement être utilisé dans certaines applications pour accroître l'efficacité des réseaux utilisant des codes MAC. Toutefois, cette méthode ne permet pas d'identifier les messages non valables parmi les multiples messages, une fois que ceux-ci sont considérés en général comme non valables au moyen d'une étiquette agrégée dans le code AMAC. Dans la présente Recommandation, le système AMAC existant est élargi de façon à permettre la compression de plusieurs étiquettes MAC avec possibilité de détection pour indiquer les messages non valides.

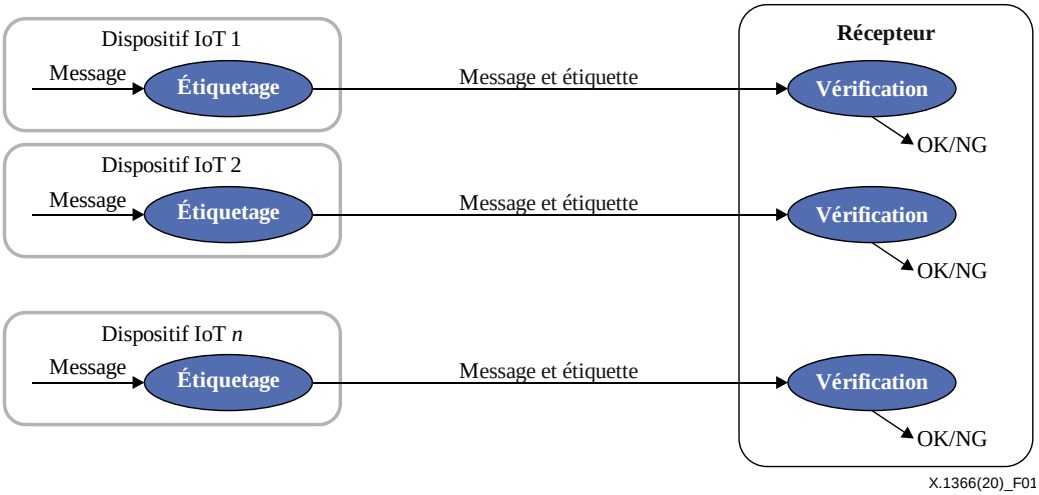

Figure 1 – Système d'authentification biunivoque (système classique)

6.2 Système d'authentification de messages agrégés: principe de base

6.2.1 Considérations générales

La Figure 2 illustre le système de base de l'authentification de messages agrégés (AMA) proposé dans la présente Recommandation. Un nœud d'agrégation est installé dans un système de réseau IoT pour agréger les étiquettes MAC/étiquettes d'authentification, sans modifier les formats d'entrée ou les structures des codes MAC existants dans le réseau. Le nœud d'agrégation comprime plusieurs étiquettes MAC jointes à plusieurs messages créés par différents dispositifs pour former une seule étiquette agrégée, sans compromettre la sécurité, et l'étiquette agrégée est transmise par un canal principal vers un récepteur pour mener à bien les processus de vérification concernant l'étiquette. Le récepteur vérifie la validité des messages multiples en utilisant l'étiquette agrégée et peut identifier les messages ou les données non valables à partir de cette étiquette. Cette technique est efficace pour réduire le volume de données transmises lorsque la taille de l'étiquette agrégée est beaucoup plus petite que la taille totale des multiples étiquettes MAC.

La présente Recommandation décrit un système AMA pour l'IoT en tant que mécanisme de base et système interactif AMA (IAMA), pour expliquer la façon dont les processus d'agrégation et de vérification sont mis en œuvre. Dans le système AMA, seul le canal principal entre le nœud d'agrégation et le récepteur est utilisé pour transmettre l'étiquette agrégée. Les algorithmes d'agrégation et de vérification du système AMA sont décrits au § 7. Dans le système IAMA, on utilise également, en plus du canal principal, un canal d'information de retour, qui est un canal authentifié avec une largeur de bande réduite entre le récepteur et le nœud d'agrégation En transmettant un résultat de vérification du récepteur vers le nœud d'agrégation par l'intermédiaire du canal information de retour, le nœud d'agrégation peut comprimer les étiquettes MAC de façon plus efficace que le système AMA décrit au § 7. Un protocole interactif entre le nœud d'agrégation et le récepteur est exécuté à des fins de vérification, comme décrit au § 8.

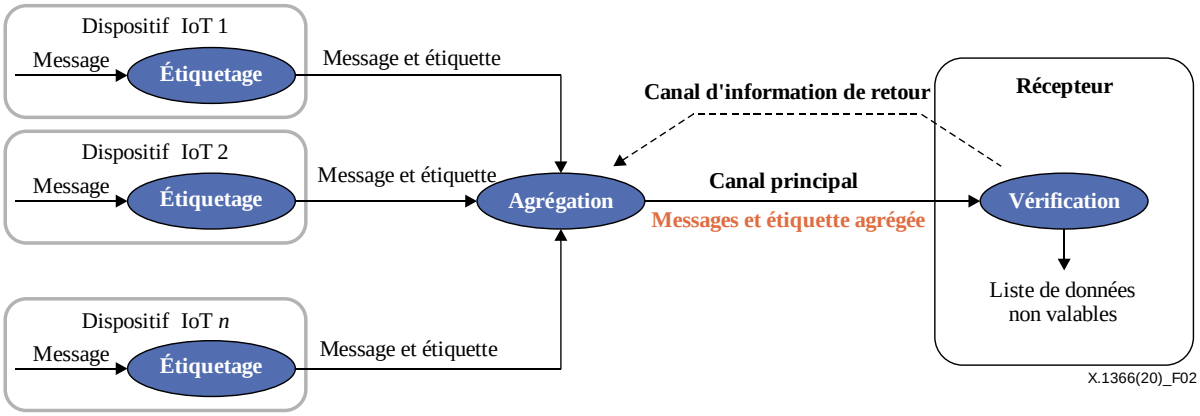

Figure 2 – Système d'authentification de messages agrégés: principe de base

NOTE – Dans le cas où plusieurs dispositifs envoient des données relatives à la vie privée au moyen de systèmes "chiffrement suivi du code MAC", la technique d'agrégation décrite dans la présente Recommandation peut être appliquée pour comprimer plusieurs étiquettes MAC.

Dans la présente Recommandation, quatre processus sont utilisés pour mettre en œuvre les systèmes AMA et IAMA: production de clés, étiquetage, agrégation et vérification, comme indiqué ci-après:

1) La production de clés prend en entrée un paramètre de sécurité et un identifiant, et produit une clé secrète pour l'identifiant.

2) L'étiquetage prend en entrée un message, un identifiant et une clé secrète correspondant à l'identifiant, et produit une étiquette en sortie.

3) L'agrégation prend en entrée plusieurs multiplets d'identifiants, de messages et d 'étiquettes provenant de plusieurs dispositifs et produit en sortie un multiplet d'étiquettes agrégées.

4) La vérification prend en entrée toutes les clés secrètes, plusieurs paires d'identifiants et les messages provenant de plusieurs dispositifs, ainsi qu'un multiplet d'étiquettes agrégées. Elle indique les messages non valables et produit en sortie une liste d'identifiants des dispositifs, dont les messages ne sont pas valables.

7 Authentification des messages agrégés

7.1 Considérations générales

Le système AMAC décrit dans la présente Recommandation permet à la fois d'agréger plusieurs étiquettes MAC pour former une étiquette plus courte et d'identifier les messages non valables qui en émanent. Le présent paragraphe fournit des précisions sur la manière dont les quatre algorithmes, à savoir la production de clés, l'étiquetage, l'agrégation et la vérification, sont construits pour créer un code AMAC.

7.2 Notation spécifique

Dans la présente Recommandation, les notations spécifiques ci-après sont utilisées:

n: nombre de dispositifs

d: nombre de messages non valables provenant des dispositifs

id: identifiant d'un dispositif. Soit $ID = \{id_1, id_2, \ldots, id_n\}$ l'ensemble de tous les identifiants

m: message

k_{id}: clé secrète de l'identifiant (id) d'un dispositif. Par souci de simplicité, k_i désigne la clé secrète correspondant à id_i au lieu de k_{id_i}

$F()$: fonction MAC qui prend une clé secrète et un message en entrée et produit une étiquette MAC en sortie

$G = (g_{i,j})$: matrice *d*-disjointe avec *u* lignes et *n* colonnes. La matrice *G* a des entrées dans {0,1}, et les colonnes sont indexées par identifiant, $id_1, id_2, \ldots, id_n$. On dit que G est *d*-disjoint, si les sommes booléennes de l'une quelconque des colonnes *d* de G ne contiennent aucune autre colonne, où $x = (x_1, x_2, \ldots, x_u)$ contient $y = (y_1, y_2, \ldots, y_u)$ si $x_i \geq y_i$ pour chaque $1 \leq i \leq u$

$I(G, i)$: l'ensemble de j ($1 \leq j \leq n$) de telle sorte que $g_{i,j} = 1$ pour chaque $i = 1,2, \ldots, u$

$\oplus$: opération XOR (OU exclusif) bit à bit

$H()$: fonction de hachage

7.3 Spécification des algorithmes

Pour couvrir des applications plus larges, deux types de codes MAC agrégés avec fonctionnalité de détection sont fournis. L'un est basé sur un OU exclusif (§ 7.3.1) et l'autre sur une fonction de hachage (§ 7.3.2).

7.3.1 Construction basée sur un OU exclusif

7.3.1.1 Production de clés

Pour chaque id, ce processus produit une clé aléatoire, représentée par k_{id}.

7.3.1.2 Étiquetage

L'étiquetage prend en entrée un message, un identifiant et une clé secrète correspondant à l'identifiant, représentés respectivement par id, m, k_{id}, et produit en sortie une étiquette MAC *t* qui est calculée par $F(k_{id}, m)$.

7.3.1.3 Agrégation

L'agrégation prend en entrée des identifiants, des messages et leurs étiquettes MAC à partir de *n* dispositifs, qui sont représentés par $(id_1, m_1, t_1), \ldots, (id_n, m_n, t_n)$. Pour chaque *i* ($1 \leq i \leq u$), prendre le OU exclusif bit à bit des étiquettes MAC dont les identifiants correspondants sont inclus dans $I(G, i)$ et les définir en tant que T_i, c'est-à-dire $T_i = \oplus_{j \in I(G,i)} t_j$. Puis, produire en sortie $(T_1, T_2, \ldots, T_u)$ en tant qu'étiquette agrégée.

7.3.1.4 Vérification

La vérification prend en entrée toutes les clés secrètes représentées par $(k_1, \ldots, k_n)$, plusieurs paires d'identifiants et de messages provenant de *n* dispositifs représentés par $(id_1, m_1), \ldots, (id_n, m_n)$, et une étiquette agrégée représentée par $(T_1, T_2, \ldots, T_u)$. Puis elle produit en sortie une liste *J* après avoir appliqué la procédure suivante:

Étape 1: $J \leftarrow \{id_1, id_2, \ldots, id_n\}$

Étape 2: Pour $i = 1,2, \ldots, u$, procéder comme suit:

Si $T_i = \oplus_{j \in I(G,i)} t_j$, alors $J \leftarrow J \setminus \{id_j\}$ pour chaque $j \in I(G, i)$.

7.3.2 Construction par hachage

7.3.2.1 Production de clés

Pour chaque id, ce processus produit une clé aléatoire, représentée par k_{id}.

7.3.2.2 Étiquetage

L'étiquetage prend en entrée un message, un identifiant et une clé secrète correspondant à l'identifiant, représentés respectivement par id, m, k_{id}, et produit en sortie une étiquette MAC *t*, qui est calculée par $F(k_{id}, m)$.

7.3.2.3 Agrégation

L'agrégation prend en entrée des identifiants, des messages et leurs étiquettes MAC à partir de *n* dispositifs, qui sont représentés par $(id_1, m_1, t_1), \ldots, (id_n, m_n, t_n)$. Pour chaque i $(1 \leq i \leq u)$, calculer une valeur de hachage des étiquettes MAC dont les identifiants correspondants sont inclus dans $I(G, i)$ et les définir en tant que T_i, c'est-à-dire $T_i = H(t_{j_1}, t_{j_2}, \ldots)$, où $I(G, i) = \{j_1, j_2, \ldots\}$ pour $1 \leq j_1 < j_2 < \cdots$.

Puis, elle produit en sortie $(T_1, T_2, \ldots, T_u)$ en tant qu'étiquette agrégée.

7.3.2.4 Vérification

La vérification prend en entrée toutes les clés secrètes représentées par $(k_1, \ldots, k_n)$, plusieurs paires d'identifiants et de messages provenant de *n* dispositifs représentés par $(id_1, m_1), \ldots, (id_n, m_n)$, et une étiquette agrégée représentée par $(T_1, T_2, \ldots, T_u)$. Puis, elle produit en sortie une liste J après avoir appliqué la procédure suivante:

Étape 1: $J \leftarrow \{id_1, id_2, \ldots, id_n\}$

Étape 2: Pour $i = 1,2, \ldots, u$, procéder comme suit:

Si $T_i = H(t_{j_1}, t_{j_2}, \ldots)$, où $I(G, i) = \{j_1, j_2, \ldots\}$ pour $1 \leq j_1 < j_2 < \cdots$,

alors $J \leftarrow J \setminus \{id_j\}$ pour chaque $j \in I(G, i)$.

8 Authentification interactive de messages agrégés

8.1 Considérations générales

Le système IAMA proposé dans la présente Recommandation offre une fonctionnalité qui permet à l'authentification IAMA d'identifier les messages non valables avec une taille d'étiquettes inférieure à celle du système AMA décrit au § 7. Un système IAMA se compose de deux algorithmes, à savoir la production de clés et l'étiquetage, et d'un protocole interactif entre l'agrégation et la vérification. Le présent paragraphe donne des précisions sur la façon dont ces algorithmes et le protocole sont construits.

8.2 Notation spécifique

Dans la présente Recommandation, les notations spécifiques ci-après sont utilisées:

n: nombre de dispositifs

d: nombre de messages non valables provenant des dispositifs

id: identifiant d'un dispositif. Soit $ID = \{id_1, id_2, \ldots, id_n\}$ l'ensemble de tous les identifiants

m: message

k_{id}: clé secrète de l'*id* d'un dispositif. Par souci de simplicité, k_i désigne la clé secrète correspondant à id_i au lieu de k_{id_i}.

F(): fonction MAC qui prend une clé secrète et un message en entrée et produit une étiquette MAC en sortie

AGT: protocole de test de groupe adaptatif

$\oplus$: opération XOR (OU exclusif) bit à bit

H(): fonction de hachage

8.3 Spécification du protocole interactif

Une authentification IAMA peut être construite à partir d'une fonction MAC *F*() et d'un protocole de test AGT, voir l'Appendice III pour les tests de groupe adaptatif. Ces constructions sont présentées ici en utilisant deux types d'opérations, un OU exclusif ou une fonction de hachage, telles que présentées dans les constructions de l'authentification AMA.

8.3.1 Construction basée sur un OU exclusif

8.3.1.1 Production de clés

Pour chaque *id,* ce processus produit une clé aléatoire, représentée par k_{id}.

8.3.1.2 Étiquetage

L'étiquetage prend en entrée un message, un identifiant et une clé secrète correspondant à l'identifiant, représentés respectivement par id, m, k_{id}, et produit en sortie une étiquette MAC *t*, qui est calculée par $F(k_{id}, m)$.

8.3.1.3 Agrégation et vérification

L'agrégation et la vérification sont construites sur la base d'un protocole AGT, comme indiqué sur la Figure 3. L'agrégation prend en entrée l'ensemble complet d'identifiants $ID = \{id_1, id_2, \dots, id_n\}$, les messages, et leurs étiquettes MAC à partir de n dispositifs, qui sont représentés par $(m_1, t_1), \dots, (m_n, t_n)$, où (m_i, t_i) $(1 \leq i \leq n)$ est une paire de message-étiquette correspondant à id_i. La vérification prend en entrée l'ensemble complet d'identifiants ID et toutes les clés secrètes k_i $(1 \leq i \leq n)$ correspondant à id_i. En premier lieu, l'agrégation choisit un sous-ensemble $S \subseteq ID$, produit une étiquette agrégée T_S en comprimant les étiquettes MAC de S: il est possible de générer T_S en prenant le OU exclusif des étiquettes MAC, $T_S = \bigoplus_{j \in S} t_j$. Puis, l'agrégation envoie T_S avec les messages $(m_1, \dots, m_n)$ à la vérification. Ensuite, la vérification définit $J = ID$, et vérifie la validité de T_S en utilisant les clés secrètes de S: T_S est considéré comme valable si $T_S = \bigoplus_{j \in S} t_j$, où $t_j = F(k_j, m_j)$; sinon, T_S est considéré comme non valable. Si T_S est valable, donner la valeur $J \leftarrow J \setminus S$. La vérification envoie le résultat du contrôle de T_S (c'est-à-dire une information d'un bit) à l'agrégation. Puis l'agrégation choisit un autre sous-ensemble $S' \subseteq ID$, produit une étiquette agrégée $T_{S'}$, en comprimant les étiquettes MAC de S', et envoie $T_{S'}$,à la vérification. La vérification vérifie la validité de T_S en utilisant les clés secrètes de S'; si $T_{S'}$, est valable, $J \leftarrow J \setminus S'$. La vérification envoie le résultat du contrôle de $T_{S'}$ à l'agrégation. Après avoir répété les procédures ci-dessus entre l'agrégation et la vérification, la vérification produit finalement en sortie une liste J qui comprend les identifiants des dispositifs dont les messages ne sont pas valables.

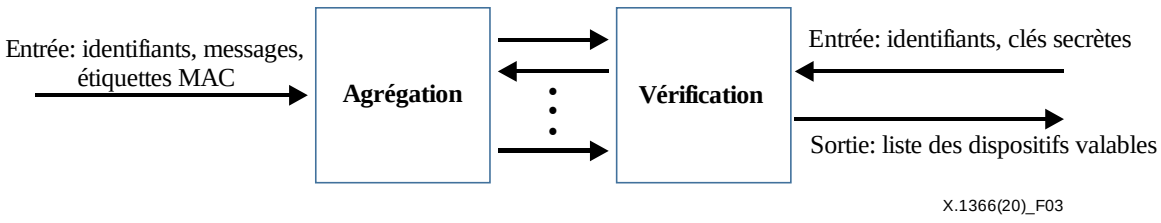

Figure 3 – Protocole interactif entre l'agrégation et la vérification

8.3.2 Construction par hachage

8.3.2.1 Production de clés

Pour chaque *id*, ce processus produit une clé aléatoire, représentée par k_{id}.

8.3.2.2 Étiquetage

L'étiquetage prend en entrée un message, un identifiant et une clé secrète correspondant à l'identifiant, représentés respectivement par id, m, k_{id}, et produit en sortie une étiquette MAC *t*, qui est calculée par $F(k_{id}, m)$.

8.3.2.3 Agrégation et vérification

L'agrégation et la vérification sont construites sur la base d'un protocole AGT, comme indiqué sur la Figure 3. L'agrégation prend en entrée l'ensemble complet d'identifiants $ID = \{id_1, id_2, \dots, id_n\}$, les messages, et leurs étiquettes MAC à partir de *n* dispositifs, qui sont représentés par $(m_1, t_1), \dots, (m_n, t_n)$, où (m_i, t_i) $(1 \leq i \leq n)$ est une paire de message–étiquette correspondant à id_i. La vérification prend en entrée l'ensemble complet d'identifiants ID et toutes les clés secrètes k_i $(1 \leq i \leq n)$ correspondant à id_i. En premier lieu, l'agrégation choisit un sous-ensemble $S \subseteq ID$, produit une étiquette agrégée T_S en calculant une valeur de hachage $T_S = H(t_{j_1}, t_{j_2}, \dots)$ où $S = \{id_{j_1}, id_{j_2}, \dots\}$ pour $1 \leq j_1 < j_2 < \cdots$. Puis, l'agrégation envoie T_S avec les messages $(m_1, \dots, m_n)$ à la vérification. Ensuite, la vérification définit $J = ID$, et vérifie la validité de T_S en utilisant les clés secrètes de S: T_S est considéré comme valable si $T_S = H(t_{j_1}, t_{j_2}, \dots)$, où $t_j = F(k_j, m_j)$; sinon, T_S est considéré comme non valable. Si T_S est valable, donner la valeur $J \leftarrow J \setminus S$. La vérification envoie le résultat du contrôle de T_S (c'est-à-dire une information d'un bit) à l'agrégation. Puis l'agrégation choisit un autre sous-ensemble $S' \subseteq ID$, produit une étiquette agrégée $T_{S'}$ en comprimant les étiquettes MAC de S', et envoie $T_{S'}$ à la vérification. La vérification vérifie la validité de T_S en utilisant les clés secrètes de S'; si $T_{S'}$ est valable, $J \leftarrow J \setminus S'$. La vérification envoie le résultat du contrôle de $T_{S'}$ à l'agrégation. Après avoir répété les procédures ci-dessus entre l'agrégation et la vérification, la vérification produit finalement en sortie une liste J qui comprend les identifiants des dispositifs dont les messages ne sont pas valables.

Annexe A

Conseils et limites

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

A.1 Conseils relatifs à l'utilisation de l'authentification de messages agrégés (AMA)

La présente Recommandation traite de la possibilité d'intégrer un nœud agrégé dans les protocoles de code d'authentification de messages (MAC) existants sans modifier les formats d'entrée ou les connexions réseau de codes MAC sous-jacents. En outre, l'agrégation est une procédure sans clé, et ne nécessite pas la conservation d'une clé secrète dans le nœud d'agrégation. En outre, l'agrégation n'est exécutée qu'en effectuant des calculs basés sur des opérations OU exclusif bit à bit ou des fonctions de hachage, de sorte que les systèmes AMA décrits dans la présente Recommandation peuvent être utilisés pour l'authentification simple.

Lors du traitement de l'agrégation décrit au § 7, une matrice *d*-disjointe doit être créée et stockée. Plusieurs méthodes telles que celles décrites dans la publication [b-TM05] pour créer des matrices *d*-disjointes sont connues, et il est également possible d'utiliser une forme comprimée d'une matrice *d*-disjointe comme indiqué dans la publication [b-MK19]. Dans la présente Recommandation, il est proposé d'utiliser ces techniques même dans les systèmes AMA. Pour une matrice d-disjointe avec des lignes u et des colonnes n, le système AMA est plus efficace que l'authentification biunivoque traditionnelle si $u < n$; et plus efficace si $d \ll \sqrt{n}$.

NOTE – Les niveaux de sécurité des systèmes AMA (ou IAMA) construits par un OU exclusif bit à bit ou des fonctions de hachage sont décrits ici conformément aux systèmes décrits dans les publications [b-HS18] et [b-SS19]. Il existe trois types de notions de sécurité: caractère non falsifiable, identifiabilité-exhaustivité, et identifiabilité-(faible)-solidité: le caractère non falsifiable garantit qu'aucun message ne peut être falsifié; l'identifiabilité-exhaustivité garantit qu'un message valable est considéré comme valable par le système; l'identifiabilité-solidité garantit qu'un message non valable est considéré comme non valable par le système, tandis que l'identifiabilité-faible-solidité est identique à l'identifiabilité-solidité, si ce n'est qu'un adversaire est censé n'obtenir aucune étiquette MAC valable et ne corrompre aucun dispositif avant de mener une attaque. La faible-solidité demeure utile dans les applications, dans la mesure où elle englobe l'altération volontaire des messages.

Les niveaux de sécurité des systèmes AMA (ou IAMA) dont il est question dans la présente Recommandation sont décrits comme suit. La construction basée sur un OU exclusif répond aux critères concernant le caractère non falsifiable, l'identifiabilité-exhaustivité et l'identifiabilité-faible-solidité, si le code MAC sous-jacent est conforme au critère concernant le caractère non falsifiable La construction basée sur la fonction de hachage répond aux critères d'infalsifiabilité, d'identifiabilité-exhaustivité et d'identifiabilité-solidité, si le code sous-jacent répond au critère relatif au caractère non falsifiable et si la fonction de hachage est considérée comme une fonction aléatoire.

A.2 Limites concernant l'utilisation de l'authentification AMA

Dans la présente Recommandation, on suppose que le nombre de messages non valables correspond au plus à *d* dans les systèmes AMA, et ce paramètre est défini en tant que paramètre système. Cela signifie qu'il est nécessaire d'estimer le nombre *d* au préalable.

Que se passe-t-il si le nombre de messages non valables dépasse la valeur prise pour hypothèse *d*? En pareil cas, la vérification produit finalement en sortie une liste *J* qui contient plus de *d* identifiants de dispositifs; les identifiants des dispositifs qui avaient envoyé des messages non valables sont inclus dans la liste *J*; toutefois, certains identifiants de dispositifs qui n'avaient pas envoyé de messages non valables peuvent également être inclus dans la liste *J*. En pareil cas, il est recommandé de définir à nouveau une valeur *d* plus grande pour le système AMA.

Annexe B

Utilisation en association avec des protocoles d'authentification biunivoque

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

Les systèmes AMA (ou IAMA) dont il est question dans la présente recommandation peuvent être utilisés en association avec l'authentification biunivoque classique. L'authentification biunivoque classique désigne le système AMA dans lequel la matrice disjointe sous-jacente est la matrice d'identité. Pour $n = n_1 + n_2$ dispositifs, s'il est préférable de n'agréger que n_1 étiquettes MAC parmi n étiquettes MAC, il convient de procéder comme suit: appliquer un système AMA (ou IAMA) pour les n_1 dispositifs, et appliquer l'authentification biunivoque pour les autres n_2 dispositifs, comme indiqué à la Figure B.1.

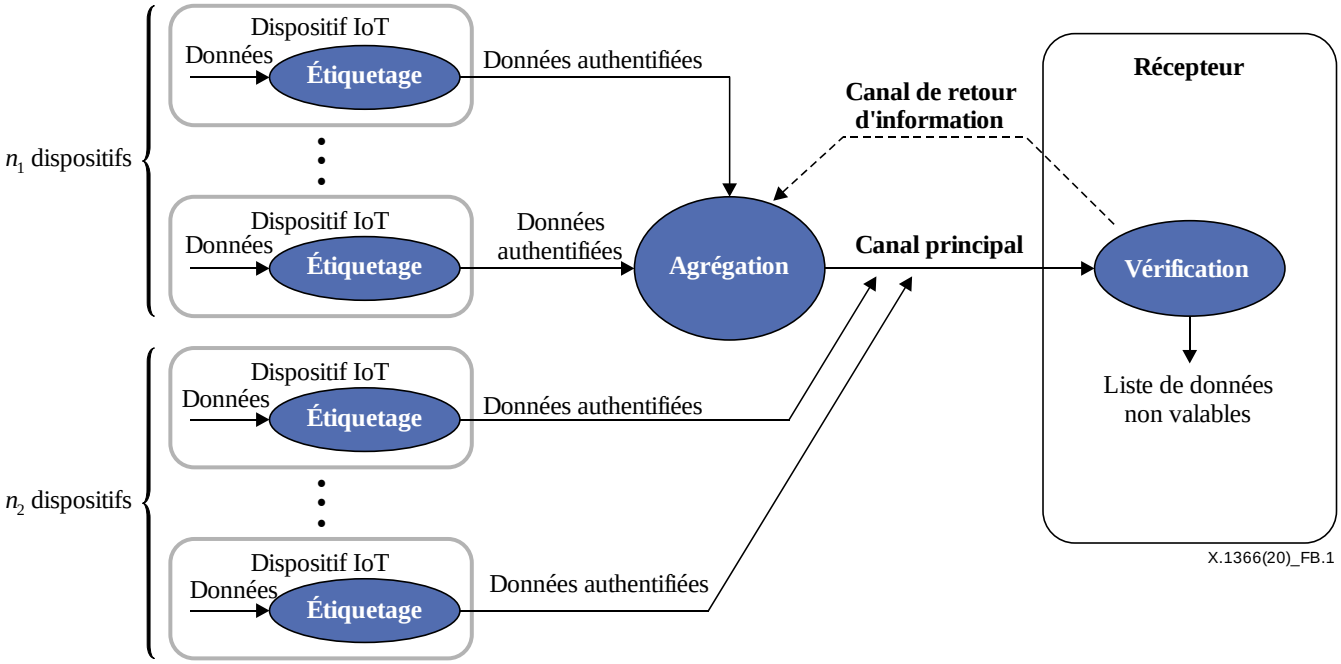

Figure B.1 – Utilisation en association avec des protocoles d'authentification biunivoque

Appendice I

Cas d'utilisation concernant l'authentification AMA

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

I.1 Introduction

Le système d'authentification de messages agrégés peut être appliqué pour assurer l'authentification (l'identité) de l'entité ainsi que l'authentification des messages. De plus, il se peut que ce système ne soit pas applicable dans tous les cas d'utilisation des dispositifs de l'Internet des objets (IoT). Toutefois, ce système est très efficace et adapté dans les conditions d'utilisation suivantes:

- lorsqu'une authentification des messages est requise pour des dizaines à des dizaines de milliers de dispositifs IoT;
- lorsqu'on a recours de manière fréquente et intermittente à un processus d'authentification pour le traitement de données/messages.

On trouvera ci-après des exemples d'applications dont on peut expressément supposer qu'elles utiliseront la technologie d'authentification agrégée:

a) Applications permettant d'envoyer fréquemment et de manière concise des données/messages telles que des données de semi-film (images fixes)
   - Applications de surveillance utilisant des données d'image

b) Applications pour la télémesure à distance
   - Applications permettant d'assurer la surveillance des activités des usines
   - Applications de sondage de la dynamique de l'audience
   - Applications de suivi médical, telles que le "Marathon citoyen"
   - Applications de gestion d'installations telles que l'éclairage public dans les zones urbaines
   - Applications de surveillance du trafic
   - Applications de surveillance du niveau des cours d'eau

L'application de cette technologie d'authentification agrégée dans les applications IoT ci-dessus permet d'améliorer considérablement l'efficacité du traitement de la transmission et de l'authentification de messages dans l'ensemble du système IoT.

Les cas d'utilisation suivants sont des exemples d'utilisation du système d'authentification agrégée décrit dans la présente Recommandation.

I.2 Cas d'utilisation 1: Parcs à thème et centres de loisirs

Dans le cas des parcs et des centres de loisirs, etc., on peut supposer qu'il y a entre 1 000 et 10 000 visiteurs simultanément. Autrement dit, des milliers de visiteurs disposent de privilèges appropriés pour l'utilisation des attractions du parc/centre, que l'on est parfois amené à vérifier simultanément. En pareil cas, un système d'authentification agrégée peut être parfaitement adapté pour assurer une gestion efficace des autorisations. Comme indiqué sur la Figure I.1, des serveurs agrégés peuvent se trouver dans chaque centre d'attraction pour recueillir et agréger les étiquettes d'authentification, afin de demander une vérification au serveur dorsal d'authentification.

Plus précisément, les visiteurs achètent à l'avance un billet d'entrée dans lequel des informations sur les événements, l'accès aux attractions et les services web à fournir sont intégrées dans des puces. Cette technologie est largement utilisée dans les marathons. Les bracelets avec puces intégrées peuvent également être considérés comme une solution de remplacement possible aux billets d'entrée.

À l'entrée principale du lieu de l'événement, ou aux différentes portes d'accès au site de chaque attraction, le contenu du billet d'entrée est lu, agrégé à l'aide d'une technologie d'authentification agrégée et envoyé au serveur d'authentification agrégée.

Le centre-serveur d'authentification agrégée analyse le contenu et les exigences des services fournis aux visiteurs, informe les différents sites d'attraction et les fournisseurs de services web et utilise ces informations pour l'analyse et la prévision des encombrements.

Après vérification, les visiteurs peuvent utiliser divers services web enregistrés en utilisant leurs propres smartphones ou des dispositifs à porter sur soi de type lunettes, par exemple.

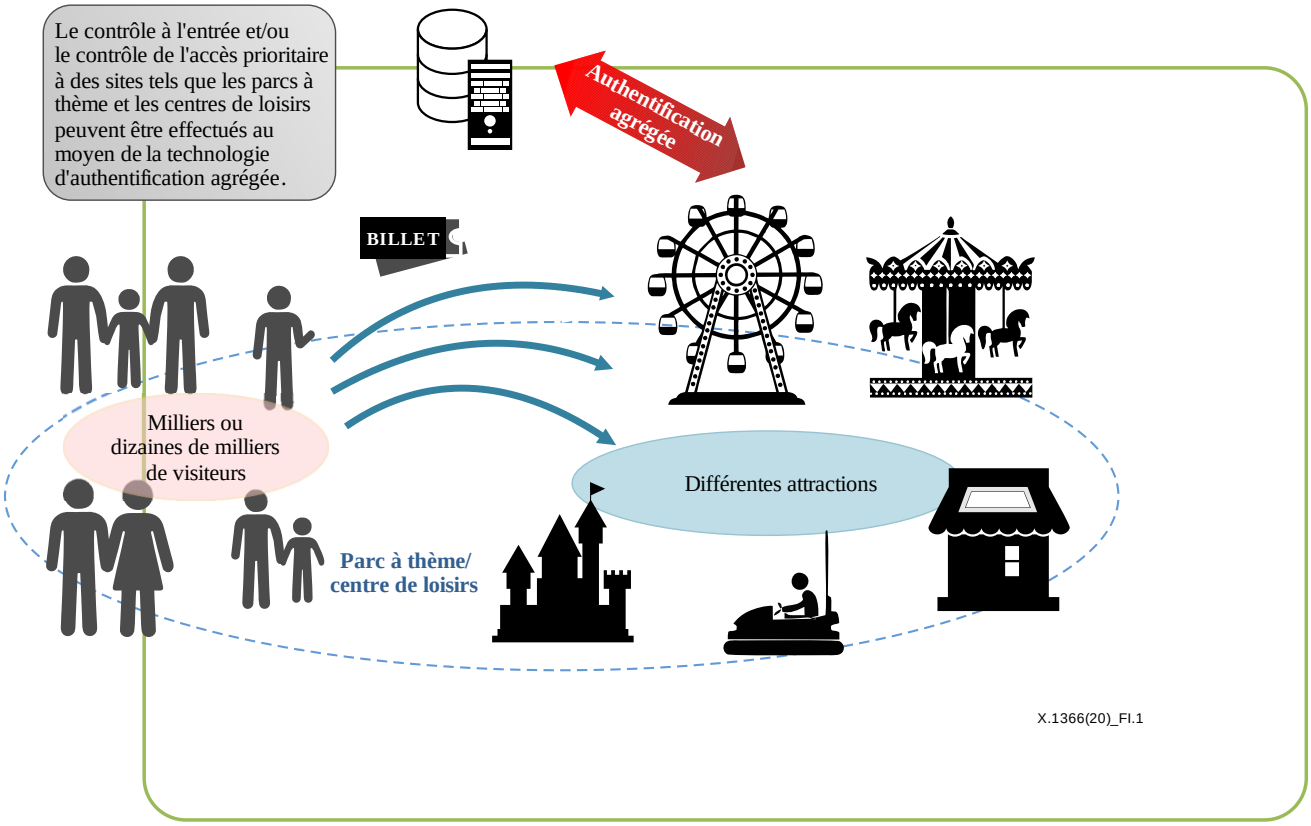

Figure I.1 – Système d'authentification agrégée dans les parcs à thème et les centres de loisirs

I.3 Cas d'utilisation 2: Capteurs de surveillance

I.3.1 Généralités

Afin d'être averti et d'intervenir à un stade précoce en cas de catastrophe naturelle et d'accident/incident, la surveillance des activités à l'aide de capteurs de surveillance, tels que des caméras pour les dispositifs IoT, peut être un cas d'utilisation des systèmes d'authentification agrégée décrits dans la présente Recommandation.

En pareil cas, les séquences quasi-vidéo ou les images fixes captées par plusieurs caméras de surveillance sont envoyées à un centre de surveillance en temps quasi réel (ou périodiquement), mais il est important de garantir la fiabilité et l'intégrité des données envoyées.

Cependant, lorsque le nombre de capteurs de surveillance augmente considérablement, il n'est plus efficace de vérifier un code d'authentification avec les données d'image provenant de chaque caméra en vérifiant le code d'authentification de chaque caméra une par une. Dans ce type d'environnement, le système d'authentification agrégée est efficace. Les codes d'authentification avec des données peuvent être agrégés dans les serveurs agrégés avant d'être envoyés au centre de surveillance, afin que l'ensemble du système IoT puisse assurer une authentification et des communications efficaces.

Le nombre de serveurs d'agrégation dépend du nombre de capteurs de surveillance. La Figure I.2 représente des capteurs de surveillance dans un système d'authentification agrégée.

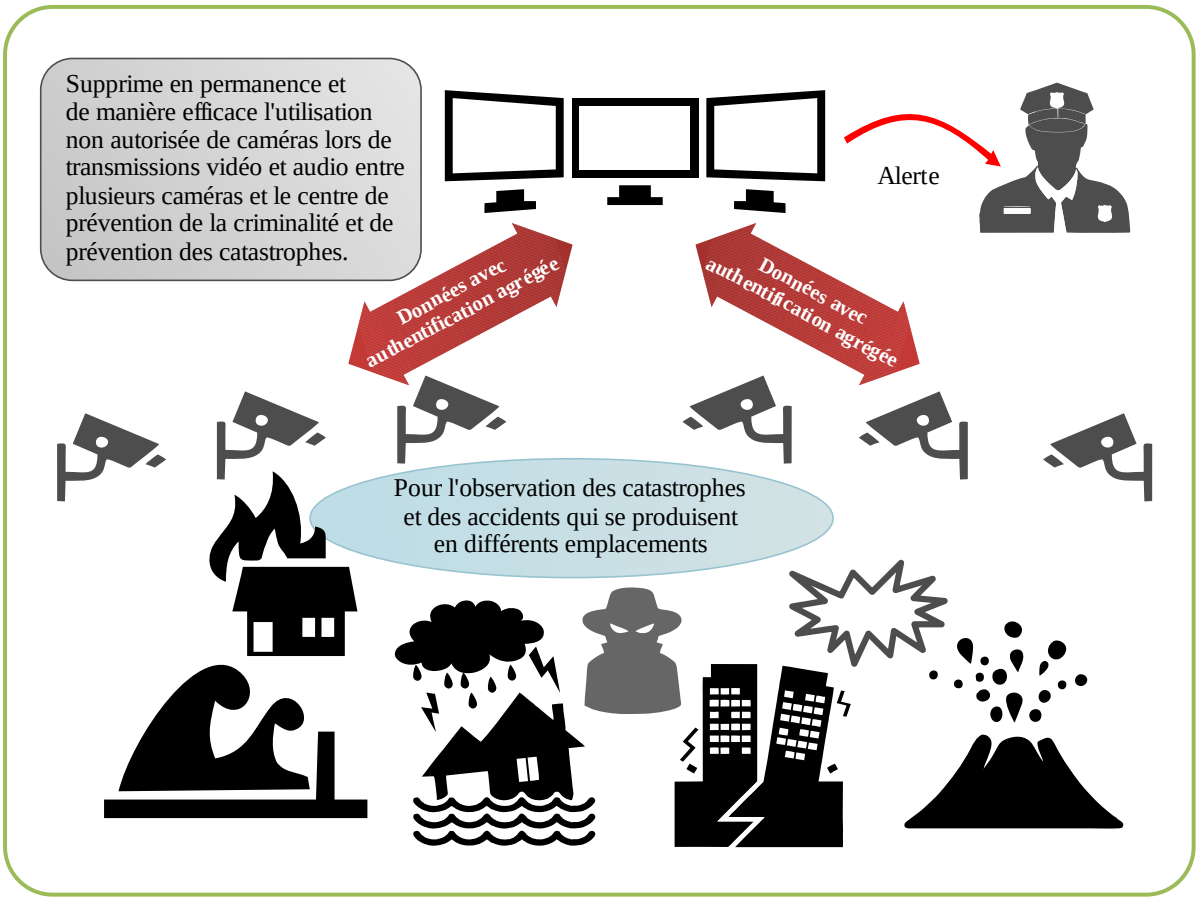

Figure I.2 – Capteurs de surveillance dans un système d'authentification agrégée

I.3.2 Cas d'utilisation particuliers

1) Surveillance de lieux de vie tels que les communautés et l'habitat

Les informations sur les lieux de vie provenant de divers capteurs, par exemple les caméras de surveillance fixées aux immeubles d'habitation, les communautés intelligentes, les habitations privées, etc. sont agrégées au niveau d'une passerelle (centre IoT) et transmises à un serveur central à l'aide d'une technologie d'authentification d'agrégation.

Le centre analysera les informations reçues et les utilisera pour faciliter la surveillance du lieu de vie, la prévision des anomalies et des défaillances et favoriser la rapidité des interventions et la prévision de la criminalité et des catastrophes.

Plus précisément, les données recueillies par divers capteurs environnementaux, capteurs pour appareils ménagers, caméras de surveillance, capteurs détectant l'état ouvert ou fermé des portes/fenêtres, capteurs pour détecter l'état de fonctionnement des infrastructures de gaz/eau/électricité, capteurs de surveillance des ascenseurs, etc. sont envoyées à des centres externes. Les systèmes d'authentification par agrégation utilisant à la fois l'authentification des terminaux et l'authentification des données sont efficaces en tant que moyen d'authentification pour recueillir de grandes quantités de données de nature très diverse et pour les transmettre de manière efficace.

2) Maintenance et surveillance des infrastructures sociales, interventions en cas de catastrophe

L'utilisation de l'IoT pour la maintenance et la gestion d'infrastructures sociales telles que les ponts, les tunnels et les routes commence à se généraliser dans divers domaines, et tout porte à croire que les services IoT vont jouer un rôle extrêmement important dans l'édification d'une société sûre et

sécurisée dans un avenir proche. Par exemple, dans le cas de ponts vieillissants et de routes surélevées, des données telles que les contraintes, les vibrations, le déplacement, l'inclinaison, etc. et des informations vidéo détaillées sont recueillies par divers capteurs. Le volume de données qui devra être envoyé au centre devient extrêmement important.

Actuellement, la méthode d'authentification agrégée se révèle très efficace pour améliorer l'efficacité de l'utilisation des circuits Internet sans fil et pour éviter les encombrements. Outre la maintenance et la gestion de ces infrastructures sociales, il est également possible d'appliquer la méthode d'authentification agrégée à la passerelle du système IoT pour l'utilisation de systèmes de surveillance constante des niveaux d'eau et des changements de débit des cours d'eau ainsi que des lacs en milieu agricole.

3) Systèmes de prévention des catastrophes utilisant des caméras de surveillance

Les caméras de surveillance sont installées et utilisées à des fins très diverses, notamment pour la prévention de la criminalité et des catastrophes en divers endroits du monde. En général, dans un réseau qui traite des informations image et audio, il est nécessaire de transmettre en permanence une grande quantité de données au centre, et il s'avère efficace de recourir à une technique d'authentification par agrégation pour assurer l'efficacité de la transmission. En d'autres termes, il est possible d'améliorer l'efficacité de la communication entre le dispositif IoT et la passerelle IoT, et entre la passerelle IoT et le centre, en appliquant la méthode d'authentification par agrégation.

4) Surveillance de la logistique, amélioration de l'efficacité des systèmes de transport

Dans les systèmes logistiques et de transport à vocation commerciale, les systèmes IoT sont de plus en plus utilisés pour améliorer l'efficacité et les nombreuses fonctionnalités de l'entreprise. Par exemple, une solution qui permet de gérer avec précision les informations sur l'état des marchandises et des colis, de l'expédition à la livraison, est mise en pratique dans divers domaines. Avec ce système, il est possible d'assurer une gestion plus stable et efficace de la logistique en appliquant une technologie d'authentification agrégée au système, qui envoie au centre diverses informations de capteurs sur tous les colis. Il est également envisageable de fournir une passerelle IoT pour des véhicules tels que les voitures équipées d'un très grand nombre de capteurs et de recourir à une technologie d'authentification agrégée au niveau de la passerelle du véhicule pour les systèmes de transport.

Appendice II

Activités connexes relatives aux systèmes AMA

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

Un système AMA différent du système décrit au § 7, proposé pour la première fois par Katz et Lindell dans la publication [b-KL08], permet l'agrégation de plusieurs étiquettes MAC de plusieurs messages pour former une étiquette plus courte. Katz et Lindell [b-KL08] ont plus particulièrement formalisé le modèle et la sécurité de l'authentification AMA et ont fourni la construction simple de l'authentification AMA en prenant le OU exclusif bit à bit de toutes les étiquettes MAC. Il est possible de vérifier la validité de plusieurs messages avec une seule étiquette plus courte, mais il est généralement impossible d'identifier les messages non valables dans leur système AMA une fois que plusieurs messages sont jugés non valables par rapport à l'étiquette unique. Les systèmes AMA décrits dans la présente Recommandation permettent à la fois d'agréger plusieurs étiquettes MAC pour former une étiquette plus courte et d'identifier les messages non valables issus de celle-ci. Le code AMA indiqué au § 7 de la présente Recommandation repose sur la publication [b-HS18], tandis que le protocole d'authentification interactif pour l'utilisation de l'authentification AMA dont il est question au § 8 repose sur la publication [b-SS19].

Appendice III

Protocole de test de groupe adaptatif

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

Les tests de groupe, tels que décrits dans la publication [b-DH00], constituent une méthode permettant de définir des éléments spéciaux, appelés éléments défectueux, parmi un grand nombre d'éléments entiers au moyen d'un petit nombre de tests, au lieu d'effectuer un test individuel pour chaque élément.

Dans l'exemple suivant de protocole de test de groupe présenté à la Figure III.1, on suppose qu'il y a un total de *n* éléments parmi lesquels figurent *d* éléments défectueux.

Dans les tests de groupe adaptatifs, les tests peuvent être effectués plusieurs fois, de manière à pouvoir sélectionner un sous-ensemble d'éléments à tester après avoir observé les résultats du test précédent. Un test de groupe compétitif est un test de groupe adaptatif qui n'a pas besoin de connaître au préalable le nombre *d* d'éléments défectueux.

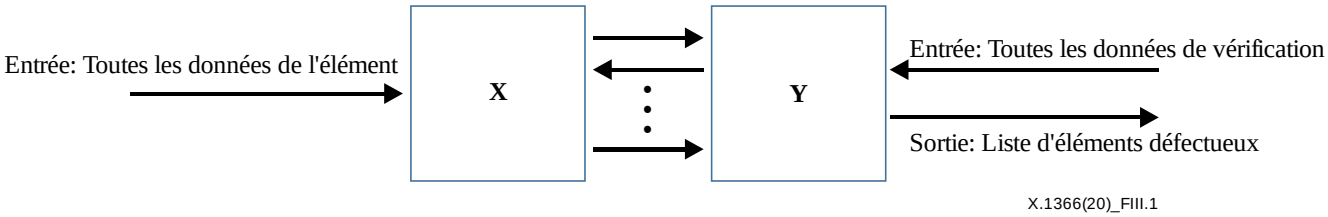

Figure III.1 – Protocole de test de groupe adaptatif

En théorie, un test de groupe adaptatif est un protocole interactif entre X et Y, comme indiqué sur la Figure III.1.

X prend l'ensemble des identifiants ID $ID = \{id_1, id_2, \ldots, id_n\}$ et toutes les données de l'élément $data_i$ ($1 \leq i \leq n$) correspondant à id_i. Y prend l'ensemble complet des identifiants *ID* et toutes les données de vérification ans_i ($1 \leq i \leq n$) correspondant à id_i. En premier lieu, *X* sélectionne un sous-ensemble $S \subseteq ID$, génère un $\_test_S$ en comprimant les données de l'élément de S, et envoie un $test_S$ à *Y*. Ensuite, *Y* définit $J = ID$, et vérifie la validité du $test_S$ en utilisant les données de vérification de *S*. Si le $test_S$ est valable, définir $J \leftarrow J \setminus S$. *Y* envoie le résultat de la vérification du $test_S$ (c'est-à-dire les informations sur un bit) à *X*. Ensuite, *X* sélectionne un autre sous-ensemble d'identifiants, et répète les procédures entre *X* et *Y*. Après avoir répété les procédures ci-dessus entre *X* et *Y*, *Y* produit finalement en sortie une liste *J* qui comprend les identifiants des éléments défectueux.

Ainsi, les protocoles de test de groupe adaptatif comprennent la recherche binaire, l'algorithme "rake-and-winnow" [b-EGH07], l'algorithme à plusieurs étapes de Li [b-Li62], et l'algorithme de recherche décrit au § 4.6 de la publication [b-DH00].

Bibliographie

[b-UIT-T X.813] Recommandation UIT-T X.813 (1996), *Technologies de l'information – Interconnexion des systèmes ouverts – Cadres de sécurité pour les systèmes ouverts: non-répudiation*.

[b-DH00] D. Z. Du et F. K. Hwang, *Combinatorial Group Testing and Its Applications*, Series on Applied Mathematics, vol. 12, 2nd edn. World Scientific, Singapore, 2000.

[b-EGH07] D. Eppstein, M. T. Goodrich, et D. S. Hirschberg, *Improved Combinatorial Group Testing Algorithms for Real-world Problem Sizes*, SIAM J. Comput. 36(5), pp. 1360-1375, 2007.

[b-HS18] S. Hirose et J. Shikata, *Non-adaptive Group-Testing Aggregate MAC Schemes*, The 14th International Conference on Information Security Practice and Experience (ISPEC 2018), LNCS 11125, pp. 357-372, Springer, 2018.

[b-KL08] J. Katz et A.Y. Lindell, *Aggregate message authentication codes*, CT-RSA 2008, LNCS 4964, pp. 155-169. Springer, 2008.

[b-Li62] C. H. Li, *A Sequential Method for Screening Experimental Variables*, J. Am. Stat. Assoc. 57 (298), pp. 455-477, 1962.

[b-MK19] K. Minematsu et N. Kamiya, *Symmetric-key Corruption Detection: When XOR-MACs meet combinatorial group testing*, ESORICS 2019, Part I, LNCS 11735, pp. 595-615, Springer, 2019.

[b-MOV96] A. J. Menezes, P. C. van Oorschot, et S. A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, octobre 1996, Fifth Printing (août 2001).

[b-SS19] S. Sato et J. Shikata, *Interactive Aggregate Message Authentication Scheme with Detecting Functionality*, The 33rd International Conference on Advanced Information Networking and Applications (AINA-2019), pp. 1316-1328, Springer, 2019.

[b-TM05] N. Thierry-Mieg, *A New Pooling Strategy for High-throughput Screening: the Shifted Transversal Design*, BMC Bioinformatics, vol. 7, no. 28, 2005.

SÉRIES DES RECOMMANDATIONS UIT-T

Série A	Organisation du travail de l'UIT-T
Série D	Principes de tarification et de comptabilité et questions de politique générale et d'économie relatives aux télécommunications internationales/TIC
Série E	Exploitation générale du réseau, service téléphonique, exploitation des services et facteurs humains
Série F	Services de télécommunication non téléphoniques
Série G	Systèmes et supports de transmission, systèmes et réseaux numériques
Série H	Systèmes audiovisuels et multimédias
Série I	Réseau numérique à intégration de services
Série J	Réseaux câblés et transmission des signaux radiophoniques, télévisuels et autres signaux multimédias
Série K	Protection contre les perturbations
Série L	Environnement et TIC, changement climatique, déchets d'équipements électriques et électroniques, efficacité énergétique; construction, installation et protection des câbles et autres éléments des installations extérieures
Série M	Gestion des télécommunications y compris le RGT et maintenance des réseaux
Série N	Maintenance: circuits internationaux de transmission radiophonique et télévisuelle
Série O	Spécifications des appareils de mesure
Série P	Qualité de transmission téléphonique, installations téléphoniques et réseaux locaux
Série Q	Commutation et signalisation et mesures et tests associés
Série R	Transmission télégraphique
Série S	Équipements terminaux de télégraphie
Série T	Terminaux des services télématiques
Série U	Commutation télégraphique
Série V	Communications de données sur le réseau téléphonique
Série X	**Réseaux de données, communication entre systèmes ouverts et sécurité**
Série Y	Infrastructure mondiale de l'information, protocole Internet, réseaux de prochaine génération, Internet des objets et villes intelligentes
Série Z	Langages et aspects généraux logiciels des systèmes de télécommunication

Imprimé en Suisse
Genève, 2021