LES DÉFIS DE SÉCURITÉ DE L'INTERNET DES OBJETS POUR LE B2B ET B2C

Sandoche Balakrichenan – sandoche2k@gmail.com

mots-clés : ?????????????????????

Même si le concept d'IdO (Internet des Objets) existe depuis environ 15 ans, ce n'est que depuis les quelques dernières années qu'il captive l'attention du grand public. Selon Gartner, il y aura dans le monde en 2020, environ 26 milliards d'appareils connectés qui mesureront et contrôleront tout ce qui aurait de l'intérêt pour l'humanité.

Les IdO vont grandement améliorer les processus des entreprises dans leurs activités commerciales et la manière dont le service sera proposé aux consommateurs. En contrepartie, les frontières aujourd'hui sécurisées entre entreprises (intranet) vont s'effondrer et les données vont transiter sur internet (ce dernier n'ayant pas été conçu dans un esprit de sécurité).

Dans cet article, nous allons tenter de donner une vue d'ensemble sur la façon dont les activités commerciales des entreprises et les consommateurs vont bénéficier des IdO, les défis que l'on peut déjà distinguer et les solutions possibles.

1 Introduction

IdO regroupe les *objets* du quotidien que l'on peut lire, reconnaître, localiser, adresser et contrôler via Internet. Les appareils que nous appelons communément *terminaux* (c'est-à-dire les appareils permettant aux utilisateurs d'accéder à des réseaux tels que les téléphones mobiles, les ordinateurs personnels, etc.), les produits de consommation du quotidien et même les éléments d'information (tels que les fichiers audio, vidéos, documents, pages web, etc.) sont des objets dans IdO. En bref, quoique ce soit qui ait un « intérêt » peut être classifié en tant qu'objet dans IdO.

Afin que ces objets puissent communiquer entre eux ou communiquer avec un réseau, il est nécessaire d'avoir un support pour les données. Ce support peut être embarqué ou fixé aux entités elles-mêmes. Tags RFID (*Radio Frequency Identifiers*), codes à barres, capteurs, etc., sont des exemples caractéristiques de supports de données, permettant d'accéder à des informations liées aux objets eux-mêmes (telles que leur identité, leur température, etc.).

La section suivante explique comment l'identifiant (ou identifiant d'objet) transporté par le support de données doit avoir une structure, afin de permettre sa résolution de façon globale.

IdO représente un vaste domaine et a de multiples applications telles que les villes intelligentes, les compteurs intelligents, les bâtiments intelligents, la santé, l'industrie de la consommation et les chaînes d'approvisionnement. Les aspects de sécurité des IdO, sur respectivement chacune de ces applications ne sont pas l'objet de cet article. Nous allons restreindre la portée de cet article sur les aspects de sécurité dans le B2C (section 3) et le B2B (section 4).

2 Propriétés des identifiants

Comme discuté dans l'introduction, l'identification des objets joue un rôle crucial pour les IdO. Les identifiants que nous avons l'habitude de manipuler (comme les

numéros de téléphone, les adresses IP, les noms de domaines, etc.) sont globalement uniques. De la même façon, l'identifiant d'un objet doit être nécessairement *unique*.

Ainsi, la définition et l'allocation des identifiants doivent suivre certaines règles pour préserver leur unicité. Dans un premier temps, il est nécessaire d'établir un « schéma d'identification ». Si nous prenons le cas des numéros de téléphone, *l'allocation* de ces identifiants suit le « Plan de numérotation E.164 » comme schéma d'identification. Ainsi défini, chaque numéro de téléphone est limité à 15 chiffres et comporte :

- un indicatif de pays [*Country Code* (CC)] ;
- un indicatif national de destination [*National Destination Code* (NDC)] ;
- un numéro d'abonné [*Subscriber Number* (SN)].

Par exemple en France, un numéro de téléphone en accord avec le plan de numérotation E.164 s'écrit : 33-1-60760000, où '33' est le CC, '1' est le NDC pour la région parisienne, et '60760000' est le SN.

Une fois ce schéma d'identification établi, il faut dans un deuxième temps définir la manière d'allouer les identifiants de façon à ce qu'il n'y ait pas deux identifiants attribués à la même entité. Dans le schéma d'identification E.164, les CC sont attribués selon les recommandations ITU-T (Secteur de la normalisation des télécommunications). Les NDC et les SN sont contrôlés directement par les gouvernements de chaque nation ou l'organisation nationale dédiée. Ce même schéma *hiérarchique d'allocation* est aussi utilisé dans d'autres schémas d'identifications tels que pour les noms de domaine, les adresses IP, etc.

Et dans un dernier temps, la gestion des identifiants doit être faite d'une manière *distribuée*, comme pour ceux que nous avons l'habitude d'utiliser aujourd'hui (tels que les noms de domaines, les adresses IP, etc.).

Dans le cas de l'identification des objets, il existe différents schémas d'identifications **[1] [2]**. Dans cet article, nous allons nous concentrer sur le schéma d'identification GTIN (*Global Trade Identification Number)*, qui est utilisé dans l'industrie des biens de consommation. Le GTIN, l'identifiant unique, d'après le schéma d'identification GTIN, peut être utilisé pour identifier l'objet de façon globale.

Fig. 1 : Exemple d'un code-barres GTIN.

Les GTIN sont alloués hiérarchiquement. Ainsi, chaque GTIN est composé de deux parties (cf. figure 1) :

- Le premier le '*code entreprise*' permet d'identifier l'entreprise (ayant fabriqué ou produit l'objet) de façon unique (« 3112345 » en Fig. 1). Les trois premiers chiffres du code d'entreprise indiquent à quel pays appartient le constructeur. Par exemple, si les trois premiers chiffres sont compris entre 300 et 379, cela indique que l'entreprise est basée en France.
- Et le deuxième est le 'code produit' («67890» en Fig. 1), qui permet de différencier les produits provenant d'une même entreprise (pour différencier deux vins produits par le même vigneron, par exemple).

Les GTIN sont gérés de manière distribuée. Les codes d'entreprise sont administrés au niveau des pays et les codes produits localement au niveau de l'entreprise directement.

L'observation que l'on peut avoir ici est que de la même façon que pour les identifiants que nous utilisons (les numéros de téléphone, les noms de domaine, etc.), une identification efficace d'objets doit suivre certaines règles :

- Elle doit être basée sur un schéma d'identification. Ainsi chaque identifiant répond à la même structure. Cela permet l'implémentation et l'utilisation d'un mécanisme commun pour la résolution des identifiants.
- Elle doit être allouée hiérarchiquement. Ainsi on préserve l'unicité des identifiants.
- Elle doit être gérée de manière distribuée pour des raisons d'évolutivité et de simplicité d'administration.

3 Emballage étendu (B2C)

Si, dans un supermarché nous scannons le code-barres d'un produit (à l'aide du lecteur de code-barres disponible dans les rayons), les informations présentées sont uniquement son nom et son prix.

Les IdO offrent la possibilité pour les marques et producteurs de présenter davantage d'informations aux consommateurs à partir de leur code-barre, que celles imprimées sur l'emballage. Ces informations supplémentaires sont ce que l'on appelle les « emballages étendus ».

Ces données sont présentes sur des serveurs accessibles via internet. Ainsi, en utilisant une application mobile permettant de scanner le code-barres et connectée à internet, il est possible pour le consommateur d'accéder à toutes les informations relatives au produit qui l'intéresse. Plusieurs études **[3]** ont montré l'importance de l'accès aux informations étendues d'un produit en utilisant un smartphone, aussi bien du point de vue des consommateurs que des marques.

Fig. 2 : Proxi-Produit – Un exemple réel d'emballage étendu.

Le schéma (Fig. 2) illustre un tel service (Proxi-Produit) **[4]** mis à disposition des citoyens par le gouvernement français.

3.1 Résolution d'un objet sur internet

Actuellement pour la résolution des informations étendues à partir de l'identifiant d'un objet sur Internet, c'est la norme ONS (*Object Naming Service*) **[5]** qui est utilisée. Il se trouve que la norme ONS utilise l'infrastructure DNS (*Domain Name System*) pour la récupération des informations des objets sur Internet. Ainsi les formats des requêtes et des réponses doivent être compatibles avec DNS. En d'autres termes cela revient à ce que les identifiants des objets soient convertis en noms de domaine et que les résultats correspondent à des enregistrements DNS.

L'application mobile scanne l'identificateur du produit (par exemple son code-barre), et convertit son identifiant en nom de domaine correspondant. Voici ci-dessous le résultat de cette conversion (cf. **[5]** pour la procédure de conversion) selon la norme ONS :

```
0.9.8.7.6.5.4.3.2.1.1.3.gtin.gs1.
id.onsepc.fr
```

Et en utilisant le résolveur DNS, l'application mobile récupère les informations relatives au nom de domaine correspondant (cf. Fig. 2). Ces informations sont stockées dans le serveur DNS sous forme d'enregistrement DNS. Voici ci-dessous l'enregistrement DNS (fictif) :

```
0.9.8.7.6.5.4.3.2.1.1.3.gtin.gs1.id.onspec.fr. IN NAPTR  0 0 "u"
EPC+http

"!^*$!http://example.com/!" .
```

Note
Cf. [5] pour plus de détails sur l'enregistrement DNS ci-dessus.

De cette réponse, l'application (dans le mobile) extrait l'URL http://example.com/ et requête le serveur web (cf. Fig. 3) approprié pour avoir l'emballage étendu de notre bouteille de vin.

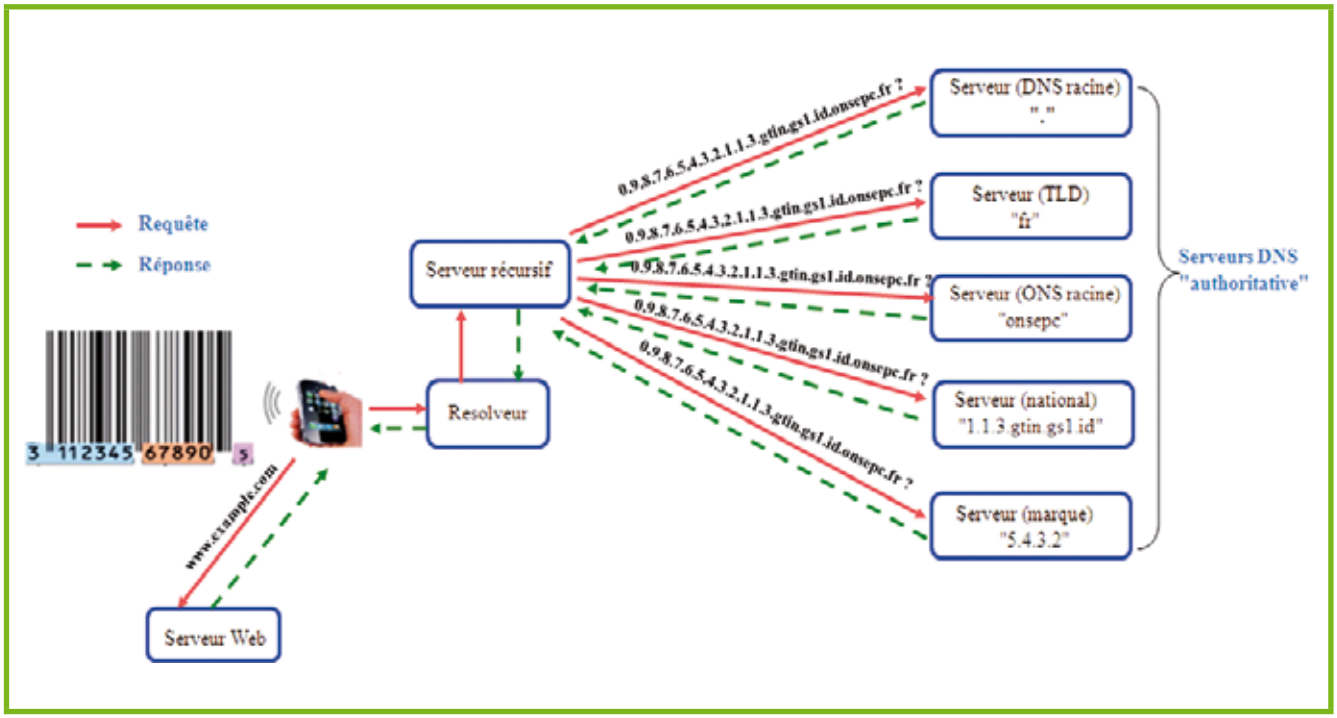

Fig. 3 : Le processus de résolution des informations étendues d'un objet.

3.2 Analyse de la sécurité des emballages étendus

Comme ONS réutilise les procédures et l'infrastructure DNS existantes (pour trouver sur internet les informations correspondant à l'identifiant d'objet), il est victime des mêmes problèmes de sécurité. Le RFC **[6]** contient un excellent résumé des vulnérabilités de DNS qui (parmi d'autres) sont :

- La modification des paquets IP relatifs aux informations DNS durant la transmission et la réception ;
- Un acteur malveillant peut récupérer l'identifiant de la requête DNS, son type et ainsi renvoyer une fausse réponse au client avant que celui-ci ne reçoive celle qui est correcte ;
- « L'empoisonnement du cache » DNS : il est aujourd'hui possible par différents moyens d'injecter des informations manipulées dans le cache DNS ;
- Il est également possible pour un acteur malveillant de compromettre les serveurs DNS qui contiennent les informations.

Imaginons qu'un patient scanne un médicament pour connaître ses contre-indications. Si un attaquant est capable de détourner la requête DNS et de lui renvoyer des informations erronées, cela peut rapidement conduire à un risque important mettant en cause la santé, voire la vie du patient.

Même si le service DNS est par définition un service hautement exposé, la raison sous-jacente à la plupart des vulnérabilités réside dans le fait qu'il n'était pas prévu (à la conception de DNS) de garantir l'intégrité des informations qui sont renvoyées en tant que réponse à une requête DNS.

3.3 Possibilités de remédiation

La principale approche pour répondre à ces failles de sécurité liées à DNS (souligné dans la section 3.2) est appelée DNSSEC (*Domain Name Security Extensions*) **[7]**.

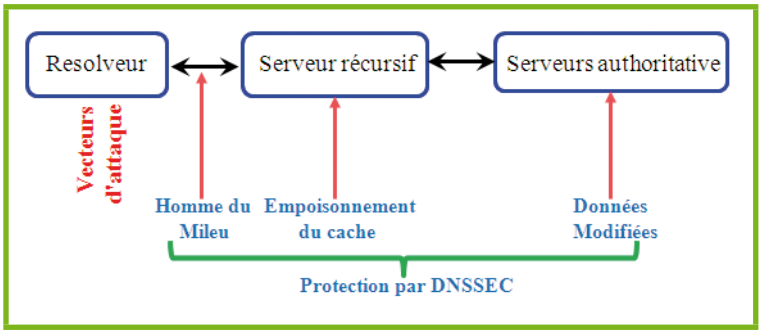

Fig. 4: Sections protégées par DNSSEC.

DNSSEC comprend un ensemble d'extensions du protocole DNS permettant de garantir l'intégrité et l'origine des données DNS, principalement à travers l'utilisation de clés cryptographiques publiques.

L'administrateur de la zone (qui stocke les informations étendues de produit) DNS, appose une signature numérique sur chaque ensemble d'enregistrement DNS RRset (*Resource Record set*). Ensuite, il publie l'ensemble de ces signatures numériques (RRSIG **[8]**) avec sa clé publique (DNSKEY **[8]**) dans le fichier de zone du serveur DNS lui-même. L'exemple ci-dessous montre le contenu du type d'enregistrement « A », pour une zone fictive « example.com » signée avec DNSSEC et la clé publique.

```
[...]
; Clé publique
example.com. IN   DNSKEY 256 3 5
AwEAAda013Wp4CQaUBrExCIRZCYpT5K93FIPvOXfTkgsrgfsgfdgfdgfddfdfg
; L'enregistrement du type "A"
example.com. 1   A   192.0.2.1
; RRSIG de l'enregistrement "A"
example.com. 1 RRSIG A 5 5 1  (20130930064057 20130403064057 3960
example.com.
                                s8dMOWQjoTKEo1bsK+EYUY+32dsqdsfdsfdsf
sdfdssssdfsfsfdsssdfshqt0AaiD= )
[...]
```

Pour la vérification d'une réponse DNS, pour un RRset donné, un client compatible DNSSEC, récupère les signatures numériques. Il effectue ensuite la vérification de la signature en utilisant la clé publique publiée de l'administrateur de zone, en la comparant à la valeur du hash du RRset qu'il calcule localement.

Le client valide ensuite la clé publique de l'administrateur de zone en utilisant le chemin hiérarchique, lié à la signature, qui conduit à un point fiable. Si le résultat de toutes ces vérifications est satisfaisant, alors le client peut avoir une certaine confiance sur l'authenticité de la réponse et sur le fait qu'elle soit complète.

4 Chaîne d'approvisionnement (B2B)

La section 3, à travers un exemple, présentait comment les IdO pouvaient aider les utilisateurs, c'est-à-dire les consommateurs. Cette section tente de montrer comment les IdO peuvent bénéficier aux activités commerciales inter-entreprises.

La chaîne d'approvisionnement est un enjeu important pour les activités commerciales. Du producteur au détaillant en passant par le distributeur, chaque acteur est dépendant d'une chaîne d'approvisionnement. Afin de garantir sa meilleure efficacité (qui se définit par un meilleur niveau de satisfaction du consommateur au coût le plus bas), les entreprises ont adopté des processus de gestion de la chaîne d'approvisionnement, et les technologies associées.

Le RFID intervient dans la chaîne d'approvisionnement en facilitant l'identification et le tracking d'un produit. Depuis 2005, de grands détaillants tels que Wal-Mart, Tesco, Target, etc., ont demandé à leurs fournisseurs de coller des étiquettes RFID sur les palettes (étiquetage au niveau des boites d'emballages et au niveau des palettes). Comme les étiquettes RFID deviennent moins coûteuses (5 à 10 centimes US$), il est envisagé d'étiqueter individuellement les produits et d'ailleurs certaines marchandises le sont déjà.

Les avantages des étiquettes par rapport aux codes-barres sont nombreux. En particulier, il n'y a pas de champ de vision pour leur lecteur. Ainsi les étapes intermédiaires pour orienter le lecteur correctement sont éliminées. Un autre avantage important du RFID est une capacité de stockage de données supérieure à celle du code-barres.

4.1 Le réseau EPC

La plupart des applications des RFID, pour les cas d'usage en chaînes d'approvisionnement, sont restées cloîtrées dans les réseaux internes des acteurs impliqués. Internet peut offrir aux chaînes d'approvisionnements des optimisations significatives telles que la réduction des coûts et l'amélioration du service. Ainsi, dans le but de profiter de ces améliorations, il est nécessaire de croiser les frontières actuelles.

Ainsi pour décloisonner le RFID, et créer de la valeur pour la chaîne d'approvisionnement, encore quelques éléments sont manquants. Premièrement, il faut que tous les acteurs s'accordent sur les moyens d'identification des items, afin qu'elle soit la même dans toute la chaîne d'approvisionnement. Deuxièmement, il est nécessaire d'avoir un moyen standard pour la découverte et le partage des données qui décrivent chaque item identifié.

La première condition peut être remplie en faisant évoluer le schéma GTIN. Comme nous l'avons vu précédemment, le GTIN permet d'identifier un fournisseur et une gamme de produits. Par exemple, l'entreprise Gillette et sa gamme de rasoirs MACH3. Ainsi, tous les MACH3 de Gillette portent un GTIN identique. Mais dans les chaînes d'approvisionnement, il y a besoin d'identifier différemment deux produits différents dans la même gamme et provenant de la même entreprise. C'est-à-dire avoir des identifiants différents pour deux MACH3 fabriqués par Gillette.

Pour réaliser cela, un numéro de série est ajouté. Ce numéro est unique et en accord avec la norme GTIN. C'est-à-dire qu'il n'y pas d'autre item du même GTIN ayant ce même numéro de série. Ainsi à chaque item est affecté un identifiant unique. Le constructeur ou le producteur alloue ce numéro de série au produit.

Le GTIN avec le numéro de série est appelé le SGTIN (Serialized GTIN) ou EPC (pour Code Produit Électronique) **[9]**. Ainsi en utilisant les EPC, les membres de la chaîne d'approvisionnement peuvent identifier et localiser les informations sur le producteur, la classe du produit et l'instance d'un produit particulier.

La deuxième condition est d'avoir des méthodes standards, entre les différents acteurs pour la découverte et le partage des données de ces EPC. Ceci est le rôle du réseau EPC **[10]**.

À partir de l'infrastructure d'internet, le réseau EPC crée un ensemble de services pour la découverte des informations associées à chaque EPC. Il est composé principalement de 3 éléments :

-un service de nommage d'objet (ONS) ;

-un service d'information EPC (EPC IS) ;

-et un service de découverte des EPC (EPC DS).

Chaque élément joue un rôle unique et important pour permettre ensemble la découverte sécurisée et le partage des informations liées aux produits, de manière détaillée et en temps réel.

Une fois fabriqué, un produit est associé à une étiquette RFID qui contient un numéro EPC. L'EPC et l'URL contenant les informations étendues de produits sont enregistrés sur un ONS (flèche 1 de la Fig. 5).

Les détails liés à un produit spécifique, du type : sa date de fabrication chez le fabricant, sa date d'entrée chez le distributeur, la date à laquelle il a été vendu chez le détaillant, etc., sont tous stockés au niveau de l'EPCIS (flèche 2 de la Fig. 5). Toutes les instances liées à un produit sont stockées au niveau de l'EPCDS (flèche 3 de la Fig. 5). Les pointeurs vers les EPCDS

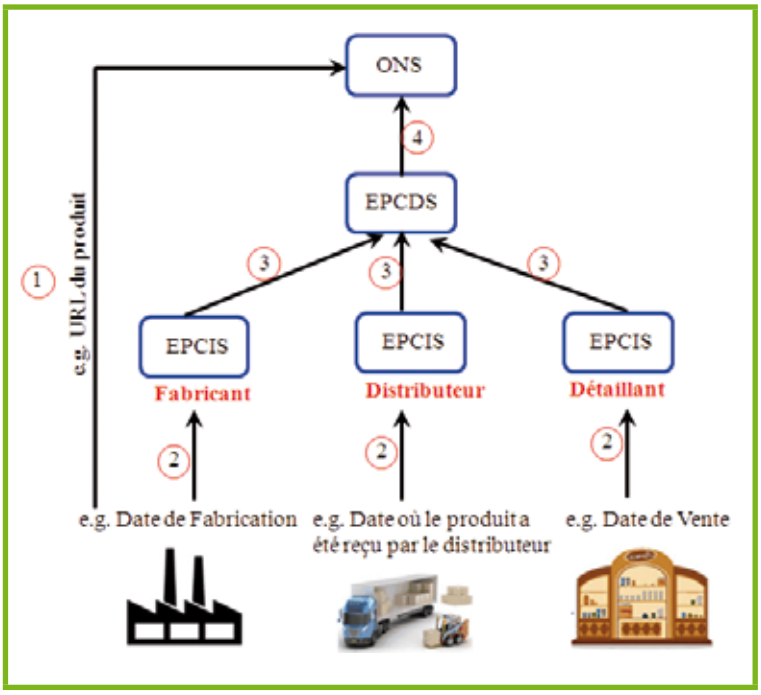

Fig. 5: Comment une information de produit est enregistrée dans le réseau EPC.

sont eux, stockés sur l'ONS (cf. la flèche 4 de la Fig. 5), c'est-à-dire dans la zone DNS comme suit :

```
0.9.8.7.6.5.4.3.2.1.1.3.gtin.gs1.id.onspec.fr. IN NAPTR  1 0 "u" EPC+DS
                                                    "!^*$!http://
example.com/discoveryservice!" .
```

Les EPCDS sont comparables aux moteurs de recherches sur internet. Pour la recherche d'un produit sur un de ces moteurs, on peut trouver différents liens vers le produit. De même, l'EPCDS dispose d'informations sur la façon d'accéder aux différents EPCIS pour le produit. L'EPCIS est le répertoire de données qui stocke l'information concernant les items uniques de la chaîne d'approvisionnement.

Il est important de noter que les différents composants du réseau EPC sont basés sur des standards ouverts (open), des plateformes indépendantes et peuvent être implémentés par quiconque pour sa propre utilisation.

4.2 Analyse de la sécurité dans les réseaux EPC

Dans cette section, nous allons aborder les différentes vulnérabilités dans le réseau EPC et évoquer brièvement les solutions possibles.

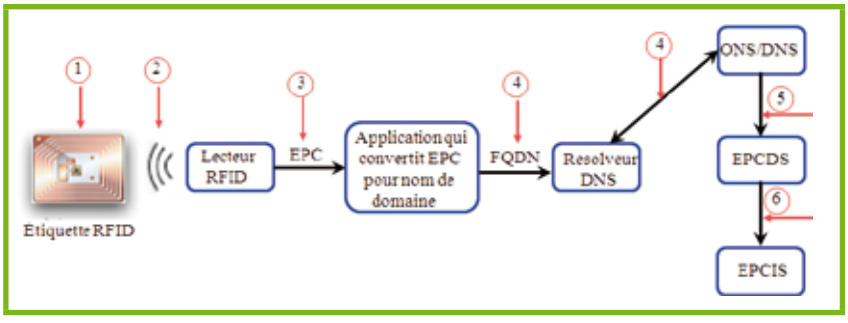

Fig. 6 : Des vulnérabilités dans le réseau EPC.

4.2.1 Au niveau de l'étiquette (flèche 1 de la Fig. 6)

L'information contenue dans une étiquette RFID est le numéro d'identifiant (c'est-à-dire l'EPC) pour un objet spécifique en mouvement dans la chaîne d'approvisionnement. Aucune autre information supplémentaire au-delà de ce numéro n'est transportée dans l'EPC au niveau de l'étiquette.

Même si l'EPC stocké dans l'étiquette RFID, est seulement un numéro et est sans signification, un intrus avec un lecteur RFID non autorisé peut lire le contenu de l'étiquette, et ensuite déterminer l'entreprise de provenance et le code produit, car le processus de génération des numéros EPC est standard.

En utilisant cette information, un intrus pourrait réussir à déterminer les types et quantités des items dans la chaîne d'approvisionnement, et revendre ces informations à des concurrents par exemple. Cette information pourrait être utilisée à des fins d'espionnage d'entreprise par des concurrents.

On pourrait avoir une solution simple en appliquant de la cryptographie sur les étiquettes pour empêcher des activités telles que les inventaires illicites. Mais cette solution implique d'avoir du matériel additionnel. Les coûts supplémentaires que représente donc cette solution dissuadent fortement aujourd'hui les acteurs. L'utilisation des techniques cryptographiques **[11] [12]** peut augmenter le coût de l'étiquette et rendre le modèle intenable économiquement, en particulier pour les items de bas coûts. Par exemple, ajouter une étiquette coûtant un euro sur une bouteille de lait valant deux euros, génère donc une augmentation de 50% des coûts.

4.2.2 Au niveau du lecteur

Le lecteur RFID consiste en 2 types d'interfaces :

- l'interface radio (flèche 2 de la Fig. 6) qui permet la lecture des données de l'étiquette RFID ;
- l'interface réseau (flèche 3 de la Fig. 6) qui permet la communication avec le système réseau.

Les communications sans-fil sur l'interface radio, c'est-à-dire entre l'étiquette RFID passive (les étiquettes passives sont moins onéreuses (de 5 US$ pièce pour un volume de 100 millions) et le type le plus répandu dans les chaînes d'approvisionnement) et le lecteur, peuvent être non sécurisées. De là, ces échanges sont susceptibles d'espionnage par un tiers ou être l'objet d'attaques de HDM (l'Homme du Milieu).

Il est plus facile de collecter les informations d'une étiquette RFID lorsqu'il est lu par un lecteur, plutôt qu'à partir de l'étiquette passive elle-même. Afin de collecter des informations à partir d'une étiquette passive par un lecteur non autorisé, l'intrus devra se placer avec son lecteur assez près des étiquettes (leur puissance d'émission étant limitée). Ainsi, ces étiquettes sont moins susceptibles d'espionnage.

Mais, les lecteurs RFID ont une plage de transmission bien plus élevée que celle des étiquettes passives. Ainsi, même si l'espion est en dehors de la plage du signal de l'étiquette, il peut toujours être capable d'intercepter les messages sortant du lecteur.

L'attaque type HDM est possible lorsque les données transitent d'un composant à un autre (entre l'étiquette et le lecteur). Un attaquant peut interrompre l'échange entre les deux composants et manipuler les informations **[13]**.

Les contre-mesures contre l'espionnage et les attaques HDM nécessitent d'établir des communications sécurisées et/ou le chiffrement des données transmises entre l'étiquette et le lecteur et d'avoir un protocole d'authentification. Mais toutes ces mesures doivent être implémentées sans faire augmenter les coûts.

Au niveau de l'interface réseau, l'architecture globale EPC définit le protocole de lecture RP (*Reader Protocol*).

Pour sécuriser l'interface de communication entre le lecteur et le serveur de back-end, le RP peut utiliser TLS (*Transport Layer Security*).

4.2.3 Au niveau du réseau

Au niveau du réseau, c'est-à-dire des communications entre EPCIS, ONS et EPCDS. Les aspects de sécurité et les contre-mesures liées à l'ONS (flèche 4 de la Fig. 6) ont déjà été discutés dans les sections 3.2 et 3.3.

Comme expliqué en section 4.1, l'EPCIS est utilisé pour collecter les informations des événements liés à un produit, et les mettre à disposition des utilisateurs autorisés. Dans les documents de la norme décrivant l'EPCIS **[14]**, les aspects de sécurité (flèche 6 de la Fig. 6) tels que les recommandations pour l'authentification et l'autorisation ne sont pas totalement renseignés (même s'il précise que les mécanismes d'authentification et d'autorisation doivent être implémentés dans l'EPCIS).

L'infrastructure du PKI X.509 **[15]** existante peut être utilisée pour l'authentification et l'autorisation dans l'EPCIS. Les AC (Autorité de Certification) autorisées peuvent générer des certificats X.509 pour des clients de confiance, et maintenir les CRL (*Certificate Revocation Lists*) lorsque la clé privée d'un certificat a été compromise. Un certificat valide est nécessaire pour l'enregistrement et la récupération d'informations à partir des EPCIS. L'authenticité du client pourra être vérifiée en contactant l'AC.

Dans le réseau EPC, l'EPCDS peut être comparé à un annuaire de téléphone, où toutes les adresses des entités en relation avec la chaîne d'approvisionnement sont renseignées. Mais, contrairement à un annuaire téléphonique, l'EPCDS ne doit pas être accessible au public (flèche 5 du schéma Fig. 6) puisqu'il contient des informations commerciales critiques.

Dans l'EPCIS, l'authentification des entités, pour l'accès à l'EPCDS peut être effectuée par des certificats X.509. Mais la procédure d'autorisation est plus compliquée. Un événement EPC peut être enregistré avec 3 niveaux différents d'autorisation. Soit : public, limité ou caché.

Récemment, un modèle sécurisé a été proposé **[16]** pour l'EPCDS, où les niveaux de contrôle d'accès ont été renforcés. Dans le modèle EPCDS sécurisé, quand l'information de l'événement est publiée dans l'EPCDS, les niveaux d'autorisations sont également publiés.

Conclusion

Il est très peu probable qu'il y aura un schéma d'identification global unique (tel que les adresses IP pour internet) pour les objets dans le monde, puisque la plupart des industriels ont leur propre schéma d'identification. Afin de permettre la résolution des identifiants d'objets appartenant à un schéma d'identification différent, de façon transparente, comme il est décrit dans le début de l'article, il est important qu'il réponde à certaines règles (un schéma d'identification, une allocation hiérarchique et administrée d'une manière distribuée).

Le terme IdO fut inventé par Kevin Ashton dans les années 1990 et il ciblait initialement l'industrie des chaînes d'approvisionnement. Même si actuellement, IdO est appliqué à des domaines variés, l'impact majeur d'IdO serait dans l'industrie B2B et B2C. Cet article donne une vue d'ensemble sur la façon dont IdO peut apporter un plus à ces industries, mais aussi sur les aspects de sécurité. Comme il y a été expliqué, il existe différentes solutions pour remédier aux problèmes de sécurité, mais le souci est que leurs implémentations génèrent des coûts non négligeables. De là, l'enjeu est que l'implémentation de ces solutions soit économiquement tenable. ■

Références

[1] http://en.wikipedia.org/wiki/Electronic_Product_Code

[2] http://en.wikipedia.org/wiki/Ucode_system

[3] http://www.worldpackagingnews.com/2012/08/boost-for-consumer-product-data-access/

[4] http://www.publications.gs1.fr/Publications/Proxi-Produit

[5] http://www.gs1.org/gsmp/kc/epcglobal/ons/ons_2_0_1-standard-20130131.pdf

[6] D.Atkins and R.Austein, « Threat analysis of the Domain Name System (DNS) », RFC 3833, Aug. 2004.

[7] Roy Arends, Rob Austein, Matt Larson, Dan Massey, and Scott Rose, « DNS Security Introduction and Requirements », RFC 4033, March 2005.

[8] Roy Arends, Rob Austein, Matt Larson, Dan Massey, and Scott Rose, « Resource Records for DNS Security extensions », RFC 4034, March 2005.

[9] http://fr.wikipedia.org/wiki/Code_produit_lectronique

[10] http://www.im.ethz.ch/education/HS08/Thiesse_Overview_EPC.pdf

[11] S.Vaudenay « RFID privacy based on Public-Key Cryptography », In Information Security and Cryptology, ICISC, 2006.

[12] A.Juels, « Minimalist Cryptography for Low-Cost RFID tags », In Security in Communication networks, 2005.

[13] Welch, D. & Lathrop, S. (2003). Wireless security threat taxonomy, Proc. of the 2003 Workshop on Information Assurance, pp. 76 – 83, ISBN: 0-7803-7808-3, 18-20 June 2003, West Point, NY.

[14] http://www.gs1.org/gsmp/kc/epcglobal/epcis/epcis_1_1-standard-20140520.pdf

[15] David Cooper, Stefan Santesson, Stephen Farrell, Sharon Boeyen, Russell Housley, and Tim Polk, « Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile », RFC 5280, May 2008.

[16] Jie Shi, Darren Sim, Yingjiu Li, Robert Deng, « SecDS : A Secure EPC Discovery Service System in. EPCglobal Network », IN CODASPY'12, 2012.