Menaces à la sécurité des composants RFID de l'architecture EPCglobal

J. G. Alfaro, M. Barbeau, E. Kranakis

Carleton University, School of Computer Science
5375 Herzberg Building, 1125 Colonel By Drive
Ottawa, Ontario, K1S 5B6, Canada

Résumé : Nous présentons une évaluation des risques d'attaques à la sécurité des composants RFID de l'architecture EPCglobal. Nous analysons les menaces à la sécurité des radio-étiquettes et des lecteurs RFID, en raison de l'utilisation d'un canal sans fil faiblement protégé. Nous analysons les menaces en fonction d'une méthodologie proposée par *l'European Telecommunications Standards Institute* (ETSI).

1. Introduction

L'architecture EPCglobal est une extension du système des codes barres. Il s'agit d'une adaptation des technologies Internet au secteur de la logistique et de l'approvisionnement. Au niveau inférieur de cette architecture, on trouve l'utilisation des radio-étiquettes (puces RFID) collées aux objets avec lesquels les autres composants de l'architecture vont dialoguer. Ces radio-étiquettes sont des dispositifs passifs qui obtiennent leur énergie à partir des interrogations effectuées par des lecteurs RFID. Chaque radio-étiquette contient un identifiant unique, l'*Electronic product code* (EPC), qui permet d'identifier l'objet auquel elle est associée dans la chaîne de production. Cet identifiant unique est utilisé par les composants de haut niveau de l'architecture pour : (1) identifier l'objet et (2) obtenir de plus amples informations à son sujet à partir de bases de données distribuées dans l'Internet (par exemple, en utilisant des services Web).

Les informations sur chaque objet ne sont pas donc stockées sur chaque étiquette RFID, mais distribuées et référencées par plusieurs services connectés à l'Internet. Pour cette architecture, un ensemble de nouveaux standards Internet ont été élaborés par le consortium international *EPCglobal Inc.*. On peut trouver, par exemple, les standards suivants dans la référence [1] : EPC-Gen2 (*EPC Class-1 Generation-2 UHF Air Interface*), EPC-IS (*EPC – Information Services*) et l'ONS (*Object Naming Service*). Chaque standard définit chacun des différents niveaux de l'architecture EPCglobal. Du point de vue sécurité, l'exploitation des vulnérabilités existantes au niveau RFID est la menace la plus importante envers l'architecture EPCglobal. En effet, les données échangées entre étiquettes et lecteurs RFID sont transportées par des connexions sans fil faiblement protégées (voir section 3). Cette situation permet à des attaquants d'abuser du service RFID de l'architecture EPCglobal et de perturber les informations échangées ; ou de suivre à la trace les positions géographiques des objets ou de leur détenteur. Nous présentons dans la suite de cet article une analyse des menaces qui ciblent les composants au niveau RFID de l'architecture EPCglobal. Notre analyse est basée sur une étude antérieure présentée dans la référence [2].

2. Méthodologie

La méthodologie utilisée pour notre évaluation repose sur l'identification des menaces en fonction de : (1) la probabilité de se produire ; (2) leur impact possible sur le système ciblé ; et (3) le risque qu'elles peuvent représenter à la victime potentielle de l'attaque. Notre méthodologie est basée sur une proposition de l'*European Telecommunications Standards Institute* (ETSI) présentée dans la référence [3]; mais légèrement modifiée afin de tenir compte des suggestions introduites dans la référence [4]. Ces modifications ont pour but de faire ressortir les menaces réelles envers les applications de réseaux sans fil.

La probabilité d'une menace (voir figure 1(a)) est déterminée par la motivation d'un attaquant à mettre en œuvre cette menace ; ainsi que les difficultés techniques à surmonter pour mettre en œuvre la menace. D'un autre côté, le risque associé à une menace (voir figure 1(b)) est déterminé par la probabilité de survenir ; ainsi que par l'impact potentiel sur le système ciblé. Ce risque est classé comme *mineur* si la probabilité de survenir est *faible*, ou si l'impact de la menace sur le système est également *faible*. Par contre, le risque est classé comme *majeur* si la probabilité de survenir est *possible* et l'impact potentiel sur le système est *moyen*. Finalement, une menace est considérée comme *critique* si elle est *probable* et son impact est *moyen* ou *élevé* ; ou bien si son risque est *possible* et son impact est *élevé*.

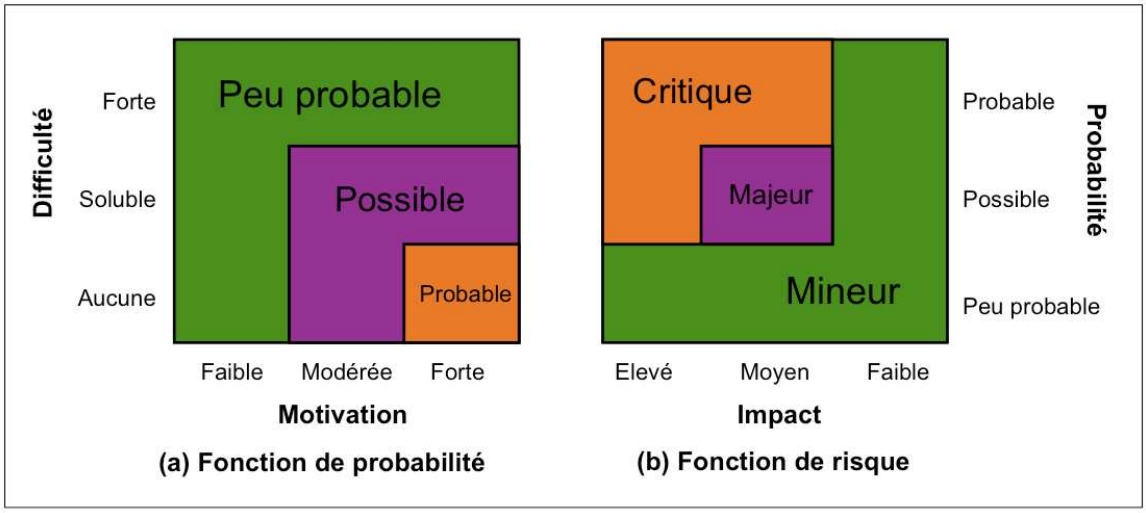

Figure 1. Fonctions de probabilité et de risque

3. Menaces à l'endroit des composants RFID de l'architecture EPCglobal

Le canal de communication sans fil utilisé entre les composants du niveau RFID (radio-étiquettes et lecteurs) de l'architecture EPCglobal, basée sur l'utilisation du standard EPC-Gen2 (*EPC Class-1 Generation-2 UHF Air Interface*) [1], est faiblement sécurisé. Au-delà de l'utilisation d'un *Contrôle de Redondance Cyclique* (CRC) sur les données envoyées et d'un blindage aléatoire faible de quelques données importantes (par exemple, mots de passe pour l'exécution d'opérations spéciales, comme l'écriture ou la désactivation des radio-étiquettes), aucune mesure forte de sécurité n'est mise en œuvre à ce niveau. Il est donc raisonnable de supposer que la plupart des menaces, à l'endroit de l'architecture EPCglobal, essaieraient de cibler le niveau RFID (radio-étiquettes et lecteurs). Nous analysons dans ce contexte quelques menaces, d'un point du vue sécurité, telles que menaces envers l'authenticité, l'intégrité, la confidentialité et la disponibilité du service pour l'échange de données entre radio-étiquettes et lecteurs. Nous supposons pour notre évaluation que des attaquants potentiels n'ont pas d'accès physique aux composants. Nous supposons toutefois la présence d'autres mécanismes de sécurité dans l'organisation, tels qu'un contrôle d'accès physique ou la présence de cameras de surveillance. Le tableau 1 montre les résultats de notre évaluation.

Objectif	Motivation	Difficulté	Probabilité	Impact	Risque
Authenticité	*Forte*	*Soluble*	*Possible*	*Elevé*	*Critique*
Confidentialité	*Forte*	*Soluble*	*Possible*	*Elevé*	*Critique*
Disponibilité	*Faible*	*Soluble*	*Peu probable*	*Moyen*	*Mineur*
Intégrité	*Modérée*	*Soluble*	*Possible*	*Moyen*	*Majeur*

Tableau 1. Évaluation des menaces

3.1 Menace à l'authenticité.

Nous allons commencer par étudier la motivation et les difficultés techniques d'une menace à l'authenticité fondée sur une attaque potentielle d'usurpation d'identité. Nous partons de l'hypothèse que l'utilisation d'un composant RFID non légitime, un lecteur par exemple, peut offrir à des attaquants des bénéfices potentiels s'ils arrivent à vendre leur service malveillant. On peut supposer la vente de ce service à une organisation concurrente ou à un voleur qui cherche à réaliser un inventaire non autorisé de la chaîne d'approvisionnement. La motivation d'un attaquant pour exécuter cette attaque est donc forte. Concernant les difficultés techniques, elles sont solubles. En effet, la figure 2 représente les étapes du protocole l'EPC-Gen2 pendant l'exécution d'un processus d'interrogation entre un lecteur et une radio-étiquette. Au

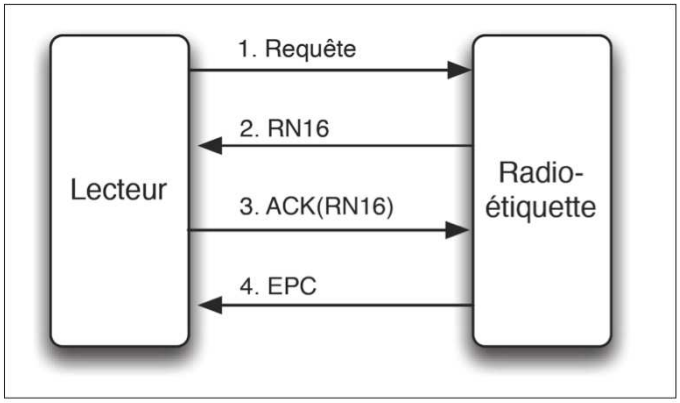

Figure 2. Interrogation entre lecteur et radio-étiquette EPC-Gen2

cours de l'étape 1, le lecteur envoie une requête à l'étiquette avec l'une des options suivantes : sélection, inventaire, ou accès [1]. La figure 2 représente la réalisation d'une requête de type *inventaire*. Lorsque l'étiquette reçoit la requête, elle renvoie une chaîne aléatoire de 16 bits que l'on désigne dans la figure 2 par RN16. Cette chaîne aléatoire est stockée temporairement dans la mémoire de l'étiquette. Le lecteur ré-envoie à l'étiquette un accusé de réception de la chaîne aléatoire à l'étape 3. Si la copie envoyée, comme accusé de réception, correspond à la chaîne RN16 stockée temporairement dans la mémoire de l'étiquette, elle envoie finalement à l'étape 4 son identifiant EPC.

Cet exemple nous permet de conclure que tout lecteur compatible avec le standard EPC-Gen2, si placé à proximité, peut accéder à l'identifiant EPC de chaque radio-étiquette sans difficulté. Cela est dû à l'absence d'un processus d'authentification entre lecteurs et radio-étiquettes EPC-Gen2. Des attaquants équipés avec des lecteurs compatibles avec le standard EPC-Gen2 peuvent donc balayer ces radio-étiquettes si elles sont placées à une distance appropriée, même sans accès physique aux objets de l'organisation. Selon *EPCglobal Inc.*, les informations stockées sur les radio-étiquettes ne fournissent pas de données supplémentaires au-delà du code EPC lui-même. Toute information supplémentaire associée à ce numéro doit être récupérée auprès d'un service EPC-IS (*EPC-Information Service*) [1]. Mais nous soulignons qu'avec ces données stockées dans les étiquettes, des attaquants peuvent déterminer et inférer avec succès les types et les quantités d'articles dans la chaîne d'approvisionnement balayée. Ils peuvent plus tard vendre cette information à des organisations concurrentes ou à des voleurs potentiels. Tout d'abord, l'attaquant peut obtenir des informations à partir d'un code EPC, tels que les fournisseurs et les types de produits. Ces informations peuvent être utilisées aussi pour l'espionnage industriel ou d'autres attaques contre l'organisation possédant la chaîne d'approvisionnement balayée. En plus de l'utilisation des codes EPC obtenus avec des lecteurs non autorisés, les attaquants peuvent plus tard cloner les étiquettes balayées pour mettre en place des attaques ultérieures d'usurpation d'identité avec les étiquettes clonées − et tout ça sans aucun accès physique à l'organisation.

Nous considérons donc que la motivation des attaquants pour mettre en œuvre des attaques à l'authenticité des composants RFID de l'architecture EPCglobal est *forte*. D'un autre côté, on a vu avec l'exemple précédent que les difficultés techniques pour mener ces attaques sont *solubles*. Avec cette motivation et degré de difficulté, on obtient une probabilité de se produire désignée, selon notre méthodologie (voir section 2), comme *possible*. Les conséquences pour l'organisation si l'attaquant arrive à offrir son service malveillant sont *graves*. L'impact associé à cette menace est donc *élevé*, ce qui nous conduit à conclure que cette menace doit être considérée comme *critique* pour l'organisation qui en fait l'objet.

3.2 Menace à la confidentialité.

Comme nous l'avons vu dans la section précédente, les interactions entre les lecteurs et les radio-étiquettes sont effectuées sans aucune procédure d'authentification. En effet, tout lecteur compatible avec le standard EPC-Gen2 peut potentiellement obtenir l'identifiant d'une radio-ettiquette. Toute radio-étiquette compatible avec le standard EPC-Gen2 peut répondre aux requêtes envoyées par les lecteurs de l'architecture EPCglobal. Même si des actions malveillantes peuvent être partiellement prévenues en

réduisant la distance d'émission de ces composants, il est théoriquement possible de mettre en place des écoutes passives pour violer la confidentialité des données échangées. Les données interceptées par ces écoutes passives peuvent être vendues à des fins d'espionnage industriel ou d'autres attaques contre l'organisation propriétaire de la chaîne d'approvisionnement balayée. Il est donc raisonnable d'assumer que la motivation d'un attaquant pour mettre en œuvre des attaques à la confidentialité du service est *forte*. En conséquence, la menace d'une attaque à la confidentialité des données échangées par les composants RFID de l'architecture EPCglobal doit être classée dans la catégorie *critique*.

3.3 Menace à la disponibilité.

On peut envisager différents types de mécanismes qui permettent de mettre en place une attaque à la disponibilité des composants RFID de l'architecture EPCglobal. Par exemple, un attaquant peut essayer d'envoyer avec un lecteur illégitime une commande de type *kill* pour commander l'autodestruction d'une radio-étiquette. En effet, le standard EPC-Gen2 exige que toute radio-étiquette possède, à des fins de confidentialité, une routine d'autodestruction des mécanismes d'émission et de stockage des données (principalement, l'identifiant EPC). Cette routine doit être protégée par un mot de passe (*Personal Identification Number* ou PIN) de 32 bits. La figure 3 représente les étapes du protocole EPC-Gen2 pendant la demande et l'exécution de cette routine de destruction. Elle suppose qu'une opération de type *select* ait déjà été exécutée antérieurement. On suppose que le lecteur dispose déjà d'un identificateur *RN16* pour communiquer et demander l'exécution des opérations à la radio-etiquette. En utilisant l'identifiant RN16, le lecteur demande à l'étape 1 un descripteur d'opération (que l'on désigne comme *Handle* à l'étape 2). Ce descripteur est une nouvelle séquence aléatoire de 16 bits qui sera utilisée par le lecteur et l'étiquette pendant toute la durée de l'opération. En effet, toute commande demandée par le lecteur à l'étiquette doit inclure ce descripteur, en tant que paramètre dans la commande. De la même manière, tous les accusés de réception envoyés par la radio-étiquette au lecteur doivent être accompagnés de ce descripteur. Une fois que le lecteur a obtenu le descripteur à l'étape 2, il répond à l'étiquette avec une copie de cette séquence, comme accusé de réception. Pour continuer l'exécution de la routine de destruction, le lecteur doit communiquer le mot de passe de 32 bits associé. Ce mot de passe est en fait composé de deux séquences de 16 bits, désignées dans la figure 3 par $PIN_{31:16}$ et

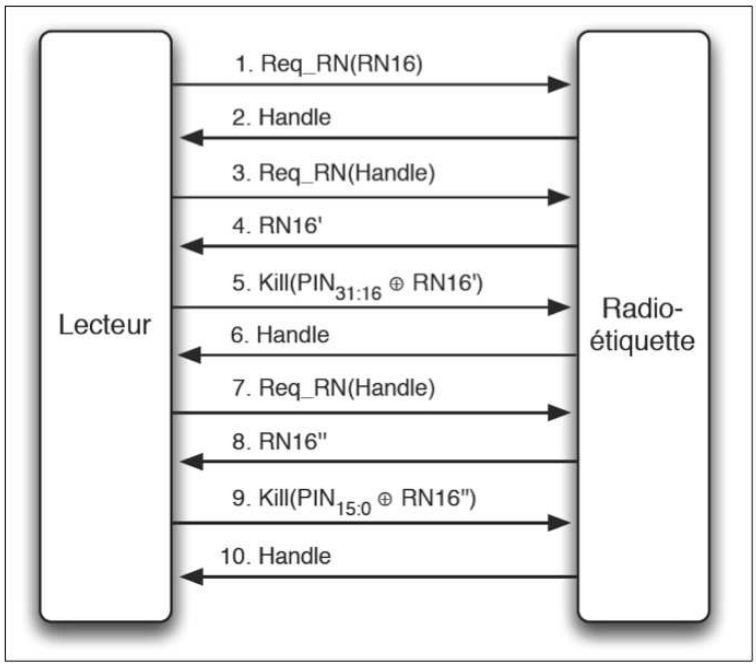

Figure 3. Désactivation d'une radio-étiquette EPC-Gen2

$PIN_{15:0}$. Afin de protéger la communication de ce mot de passe, le lecteur obtient aux étapes 4 et 8, deux séquences de 16 bits désignées dans la figure 3 par *RN16'* et *RN16''*. Les séquences *RN16'* et *RN16''* sont utilisées par le lecteur pour cacher le mot de passe pendant l'envoi vers la radio-étiquette. À l'étape 5, le lecteur masque les premiers 16 bits du mot de passe en appliquant une opération *XOR* (désignée par le symbole dans la figure 3) avec la séquence *RN16'*. Il envoie le résultat à la radio-étiquette, qui ré-envoie au lecteur un accusé de réception avec le descripteur *Handle* à l'étape 6. De la même façon, le lecteur masque les derniers 16 bits du mot de passe en appliquant un XOR avec la séquence *RN16''*, et envoie le résultat à la radio-étiquette. Finalement, la radio-étiquette ré-envoie au lecteur un accusé de réception avec le descripteur *Handle* à l'étape 10. Ce dernier confirme en plus l'exécution avec succès de l'opération d'autodestruction.

Nous pouvons observer, à partir de l'exemple précédent que, même s'il existe des difficultés pour retrouver le code PIN qui protège la routine d'autodestruction, c'est théoriquement possible. Il suffit d'intercepter les séquences *RN16'* et *RN16''* aux étapes 4 et 8 et de les appliquer avec l'opération XOR au contenu des étapes 5 et 9. Dans la référence [5], par exemple, les auteurs ont présenté une attaque pour récupérer les codes PIN de 8 bits qui protègent la même routine d'autodestruction des étiquettes EPC-Gen1. Bien que cette attaque fonctionne uniquement pour le standard EPC-Gen1, les auteurs affirment dans la référence [5] que le standard EPC-Gen2 est également vulnérable à leur attaque. Nous considérons donc que les difficultés techniques pour mettre en place ces attaques doivent être désignées comme *solubles*. Des attaquants potentiels peuvent aussi, en utilisant des émetteurs très puissants, générer du bruit sur la fréquence des lecteurs ciblés. Bien que ces attaques soient possibles et, bien sûr *solubles*, le signal généré pour l'attaque est illégal et il est très facile de découvrir l'emplacement des émetteurs de ce signal. Nous considérons que cela réduit très fortement la motivation vers *faible*. Dans les deux cas (récupération du mot de passe ou génération de bruit) nous considérons donc que la probabilité d'une menace à la disponibilité du service, sans accès physique aux composants RFID, doit être considérée comme *peu probable*. Concernant l'impact de cette menace, nous considérons qu'il doit être désigné comme *moyen*, car elle ne représente pas pour l'organisation des pertes financières. Elle représente plutôt une perturbation temporaire de ses activités. Cette combinaison de probabilité de se produire et d'impact nous conduit à classer le risque associé à cette menace comme *mineur*.

3.4 Menace à l'intégrité.

Nous considérons finalement la possibilité pour un attaquant d'ajouter ou de modifier les informations stockées dans une radio-étiquette ; ou de transmettre des informations altérées d'une radio-étiquette à un lecteur. La motivation des attaquants doit être considérée comme *modérée*, car leur service malveillant peur être vendu à des organisations concurrentes intéressées à perturber les opérations commerciales du système ciblé. Les difficultés pour la réalisation des attaques à l'intégrité du service doivent être désignées comme *solubles*. Une possibilité est l'obtention avec succès du code PIN de 32 bits pour réussir à accéder et modifier la mémoire interne d'une radio-étiquette (par exemple, en effectuant une analyse du signal comme celle présentée dans la référence [5]). Si l'attaquant réussi à obtenir ce mot de passe, il pourra altérer les données de l'étiquette (l'identifiant EPC, par exemple). L'attaquant peut aussi essayer de modifier l'information transmise à partir de la radio-étiquette au lecteur, en altérant les données au

moment précis où le lecteur en fait la demande. Même si nous considérons qu'il y a d'importantes difficultés techniques à surmonter pour mettre en place ces deux attaques, elles sont théoriquement *solubles*. La probabilité pour cette menace de se produire est donc désignée comme *possible*. D'un autre côté, cette menace peut en plus constituer quelques pertes financières à l'organisation ciblée (par exemple, si l'attaquant réussi à altérer l'identifiant EPC des radio-étiquettes). Nous estimons pourtant l'impact de cette menace comme *moyen*. Dans ces conditions, et selon notre méthodologie, le risque associé à cette menace doit être classé comme *majeur*.

4. Conclusions

Nous avons présenté dans cet article une évaluation des menaces à la sécurité des composants RFID de l'architecture EPCglobal. Nous supposons pour notre évaluation que des attaquants potentiels n'ont pas d'accès physique aux composants. Ils peuvent seulement attaquer le canal de communication sans fil entre lecteurs et radio-étiquettes. Avec ces hypothèses, nous avons identifié et classé quatre menaces que nous considérons pertinentes d'un point de vue sécurité : menaces à l'authenticité, à la confidentialité, à l'intégrité et à la disponibilité du service. Nous avons classé les menaces à l'authenticité et à la confidentialité du service comme menaces *critiques*. Et la menace à l'intégrité du service comme *majeure*. Ces trois menaces doivent être traitées par des contre-mesures appropriées afin d'améliorer la sécurité de l'architecture EPCglobal.

Références

[1] EPCglobal Inc. http://www.epcglobalinc.org/

[2] Alfaro, J. G., Barbeau, M., and Kranakis, E. Security Threats on EPC based RFID Systems. In: 5th International Conference on Information Technology: New Generations (ITNG 2008), IEEE Computer Society, Las Vegas, Nevada, USA, April 2008.

[3] ETSI, Methods and Protocols for Security; Part 1: Threat Analysis. ETSI TS 102 165-1 V4.1.1, 2003.

[4] Laurendeau, C. and Barbeau, M. Threats to Security in DSRC/WAVE. In: 5th International Conference on Ad-hoc Networks (ADHOC-NOW), Lecture Notes in Computer Science, Springer Berlin / Heidelberg, Volume 4104, 2006, pp. 266-279.

[5] Oren, Y. and Shamir, A. Power Analysis of RFID Tags. In: Rump session of Advances in Cryptology, CRYPTO 2006, 2006.