Les composants RFID sont-ils vulnérables ?

Par J.G. Alfaro, M. Barbeau, E. Kranakis
Carleton University, School of Computer Science

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. L'évaluation est en fonction d'une méthodologie proposée par l'European Telecommunications Standards Institute (ETSI).

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 dialoguent. 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 :

- nommer l'objet ;
- et 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).

Cette technologie recèle toutefois un problème majeur. 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. Mis à part 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 attaques, à l'endroit de l'architecture EPCglobal, essaieraient de cibler le niveau RFID (radio-étiquettes et lecteurs).

Dans ce contexte, quel est le risque associé à la menace à l'authenticité du service d'échange de données entre radio-étiquettes et lecteurs ? Tel est l'objet de notre analyse pour laquelle nous supposons que des attaquants potentiels n'ont pas d'accès physique aux composants et que d'autres mécanismes de sécurité existent dans l'organisation, tels qu'un contrôle d'accès physique ou la présence de caméras de surveillance. L'analyse est basée sur une étude antérieure présentée dans la référence [2].

MÉTHODOLOGIE

La méthodologie que nous utilisons repose sur l'identification des menaces en fonction de :

- la probabilité de se produire ;
- l'impact possible sur le système ciblé ;
- et le risque qu'elles peuvent représenter pour la victime potentielle de l'attaque.

Cette dernière est basée sur une proposition de l'European Telecommunications Standards Institute (ETSI) [3], mais légèrement modifiée afin de faire ressortir les menaces réelles envers les applications de réseaux sans fil [4].

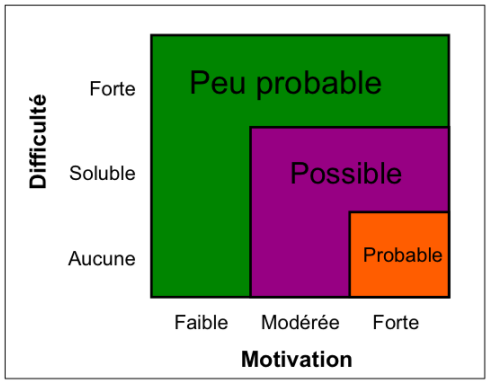

Figure 1. Fonction de probabilité

La probabilité poue que survienne une menace (voir figure 1) est déterminée par la motivation d'un attaquant et les difficultés techniques à surmonter pour la

mettre en œuvre. Par ailleurs, le risque associé à une menace (voir figure 2) est déterminé par la probabilité qu'elle survienne ainsi que par l'impact potentiel sur le système ciblé. Ce risque est classé comme mineur si la probabilité pour que survienne une menace est faible, ou si son impact sur le système est également faible. Par contre, le risque est classé comme majeur si la probabilité qu'elle survienne 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.

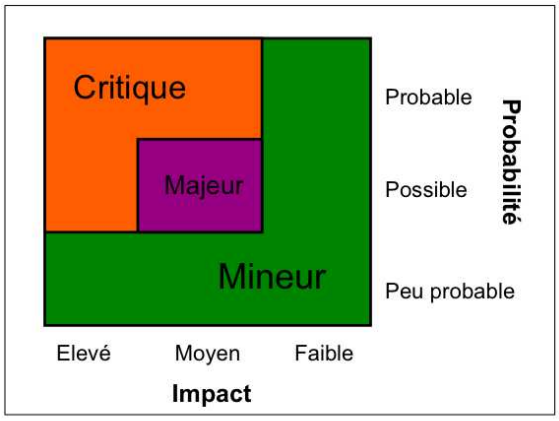

Figure 2. Fonction de risque

MENACE À L'AUTHENTICITÉ

Commençons par étudier la motivation et les difficultés techniques de la 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 que ce service soit vendu 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.

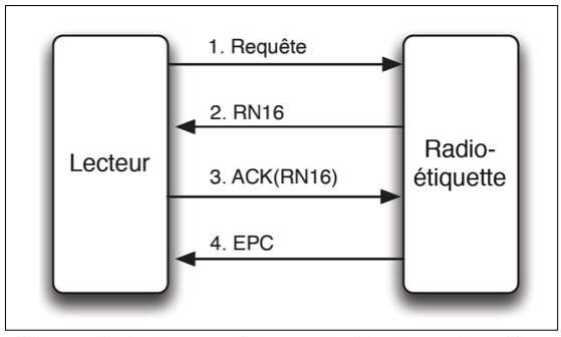

Figure 3. Interrogation entre lecteur et radio-étiquette EPC-Gen2

Les difficultés techniques quant à elles, sont solubles. La figure 3 représente les étapes du protocole l'EPC-Gen2 pendant l'exécution d'un processus d'interrogation entre un lecteur et une radio-étiquette. Au cours de l'étape 1, le lecteur envoie une requête à l'étiquette avec l'une des options suivantes : sélection, inventaire, ou accès. La figure 3 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 3 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, s'il est 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 lorganisation.

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 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. A partir d'un code EPC, l'attaquant peut aussi obtenir des informations tels que les fournisseurs et les types de produits. Autant d'éléments qui peuvent être utilisés pour l'espionnage industriel ou d'autres attaques contre l'organisation possédant la chaîne d'approvisionnement. Enfin, au delà, les attaquants peuvent cloner les étiquettes balayées pour mettre en place des attaques ultérieures d'usurpation d'identité, tout ça sans aucun accès physique à l'organisation.

La motivation des attaquants pour mettre en œuvre des attaques à l'authenticité des composants RFID de l'architecture EPCglobal est donc forte, d'autant que les difficultés techniques pour mener ces attaques sont solubles. Avec cette motivation et ce degré de difficulté, la probabilité pour que survienne une attaque est possible et 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.

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.

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 classé les menaces à l'authenticité et à la confidentialité du service comme menaces critiques. Ces deux 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), LNCS, Vol. 4104, 2006, pp. 266-279.