Les composants RFID sont-ils vulnérables ? (2ème partie)

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

INTRODUCTION

Dans un précédent article [1], nous avons montré que même sans accès physique aux composants RFID de l'architecture EPCglobal, une attaque et un vol de données était tout à fait possible. Mais qu'en est-il de l'altération des données stockées par les radio-étiquettes de l'architecture, lorsqu'elles sont accessibles en mode écriture à partir d'un canal sans fil faiblement protégé ?

En effet, les radio-étiquettes EPC-Gen2 offrent l'option de réinscrire, dans leur mémoire interne, des informations transmises par les lecteurs RFID. Même si cette option d'écriture est peu exploitée dans les applications actuelles de la technologie EPC (probablement dû aux faibles mesures d'authenticité, discutées dans la première partie de cet article [1]), elle sera très utilisée dans les nouvelles applications EPC. La possibilité de pouvoir réinscrire la mémoire des étiquettes permettra en effet des extensions très utiles comme par exemple le stockage d'informations complémentaires sur les objets en temps réel (la localisation des objets, l'estampillage, la température des objets, etc.).

Il est donc important d'analyser le risque d'une attaque d'altération des données stockées par les étiquettes EPC-Gen2, lorsqu'elles sont accessibles en mode écriture à partir d'un canal sans fil faiblement protégé. C'est ce que nous nous proposons de faire en suivant la même méthodologie que dans la première partie de cette étude.

RISQUE ASSOCIÉ À UNE ATTAQUE D'ALTÉRATION DES DONNÉES

Pour évaluer la possibilité, pour un attaquant, de modifier les informations stockées dans une étiquette accessible en mode écriture, nous nous basons sur la situation suivante. Nous supposons que cette opération est accessible à partir d'un canal faiblement protégé. La motivation de l'attaquant est considérée comme étant modérée, car son service malveillant peut être vendu à des organisations intéressées à perturber les opérations d'approvisionnement du système ciblé. Pour mettre en place cette attaque, nous imaginons qu'il obtient le code PIN (Personal Identification Number) associé à la routine d'écriture (dans le cas où cette option n'a pas été bloquée par l'administrateur du système).

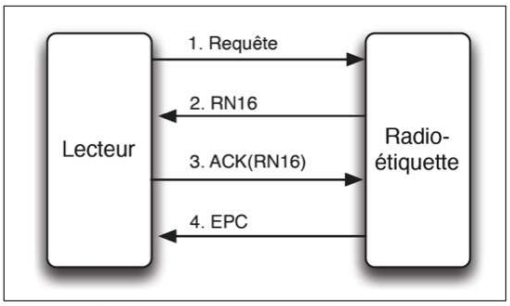

Figure 1. Interrogation entre lecteur et radio-étiquette EPC-Gen2

La figure 1 rappelle, de façon simplifiée, les étapes du protocole de communications pendant l'exécution d'un processus d'interrogation entre un lecteur et une étiquette. L'étape 1 représente la réalisation d'une requête de type select. Lorsque l'étiquette reçoit la requête, elle renvoie une chaîne aléatoire de 16 bits que l'on désigne par RN16. Cette chaîne aléatoire est stockée temporairement dans la mémoire de l'étiquette, et renvoyée plus tard par le lecteur dans un accusé de réception (voir étape 3). Elle sert à vérifier l'accusé de réception fourni par le lecteur. La chaîne de 16 bits de l'accusé de réception doit correspondre à celle stockée temporairement dans la mémoire. Si l'accusé de réception est correct, l'étiquette envoie finalement, à l'étape 4, son identifiant EPC et reste disponible pour exécuter d'autres actions.

La figure 2 représente les étapes suivantes du protocole pendant la demande et l'exécution de la routine d'accès pour écrire dans la mémoire de l'étiquette.

L'ATTAQUE ÉTAPE PAR ÉTAPE

En utilisant l'identifiant RN16 obtenu précédemment (étape 2, figure 2), le lecteur demande à l'étape 5 un descripteur d'opération (que l'on désigne comme Handle à l'étape 6). 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 de demande et d'exécution d'écriture. 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 l'étiquette au lecteur doivent être accompagnés de ce descripteur. Une fois que le lecteur a obtenu le descripteur à l'étape 6, il répond à l'étiquette avec une copie de cette séquence, comme accusé de réception.

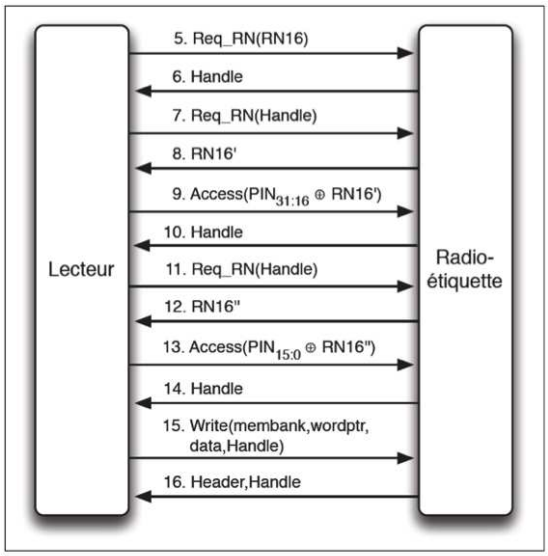

Figure 2. Demande et exécution d'écriture dans la mémoire d'une radio-étiquette EPC-Gen2.

Pour continuer l'exécution de la routine d'accès, 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 2 par PIN31:16 et PIN15:0. Afin de protéger la communication de ce mot de passe, le lecteur obtient aux étapes 8 et 12, deux séquences de 16 bits désignées dans la figure 2 par RN16' et RN16". Les séquences RN16' et RN16" sont utilisées par le lecteur pour cacher le mot de passe pendant l'envoi vers l'étiquette. À l'étape 9, le lecteur masque les premiers 16 bits du mot de passe en appliquant une opération XOR (désignée par le symbole + cerclé dans la figure 2) avec la séquence RN16'. Il envoie le résultat à l'étiquette, qui renvoie au lecteur un accusé de réception avec le descripteur Handle à l'étape 10. 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 l'étiquette. Finalement, l'étiquette renvoie au lecteur un accusé de réception avec le descripteur Handle à l'étape 14. Ce dernier confirme en plus l'exécution avec succès de l'opération d'accès et conduit à l'écriture de l'étiquette (étapes 15 et 16).

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'écriture, il est théoriquement possible de le faire. Il suffit d'intercepter les séquences RN16' et RN16", aux étapes 8 et 12, et de les appliquer avec l'opération XOR au contenu des étapes 9 et 13.

Les difficultés techniques pour mettre en œuvre cette attaque sont solubles. La probabilité de la menace, selon la méthodologie présentée plus haut, même sans accès physique aux composants RFID, doit être donc considérée comme étant possible. Concernant l'impact de cette menace, nous estimons qu'il est potentiellement élevé, en fonction de l'organisation visée. Par exemple, dans le contexte d'une chaîne d'approvisionnement des marchandises pharmaceutiques, l'altération des données dans la mémoire des étiquettes peut être très dangereuse. La perturbation temporaire du fonctionnement de la chaîne peut conduire à des erreurs dangereuses : la livraison des médicaments avec des données erronées, ou livrés à des patients non concernés, peut conduire à la prise par un patient d'une mauvaise médication. Dans ces conditions, et selon notre méthodologie, nous évaluons l'impact potentiel au niveau élevé.

Cette combinaison de probabilité de se produire et d'impact élevé nous conduit à conclure que le risque associé à cette menace est critique. La menace doit être traitée par des contre-mesures appropriées afin d'améliorer la sécurité de l'architecture EPCglobal.

CONCLUSIONS

Nous concluons, avec cet article, une évaluation des risques à l'authenticité et la intégrité 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 ces menaces, selon leur impact dans le système ou la victime ciblée, comme étant critiques. Elles doivent être traitées par des contre-mesures appropriées afin d'améliorer la sécurité de l'architecture EPCglobal.

RÉFÉRENCES

[1] Alfaro, J. G., Barbeau, M., and Kranakis, E. Les composants RFID sont-ils vulnérables ? La lettre des Éditions Techniques de l'Ingénieur, n.4, juillet 2009.

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