# Sécurité dans les systèmes RFID

Gildas Avoine

UCL Louvain-la-Neuve, Belgique
Information Security Group
http://sites.uclouvain.be/security/

**Résumé** Il est aujourd'hui difficile de parler d'identification par radiofréquence (RFID) sans que ne viennent à l'esprit les termes de « sécurité de l'information » et de « protection des données personnelles ». Nous présentons ici les grandes familles de menaces auxquelles doit faire face la RFID, ainsi que leur impact dans notre vie de tous les jours.

## 1 L'évolution de la technologie RFID

Contrairement à ce que l'on pourrait croire, l'identification par radiofréquence (RFID) n'est pas une révolution technologique du vingt-et-unième siècle, mais de la première moitié du vingtième. Elle a cependant beaucoup évolué depuis lors et celle qui nous entoure aujourd'hui n'a plus grand-chose à voir avec la RFID de nos aïeux. Bien sûr, les principes physiques sur lesquels elle repose restent les mêmes, mais les progrès réalisés en électronique ont radicalement changé la donne : le prix d'un tag peut atteindre une quinzaine de centimes d'euros et sa taille est parfois inférieure à un grain de riz. Ces valeurs extrêmes ne doivent cependant pas cacher la réalité, car à chaque application correspond un tag qui lui est adapté : il est inutile d'utiliser un tag minuscule (et donc coûteux) pour une application qui ne le nécessite pas, et il est impossible d'utiliser un tag à 15 centimes d'euros pour une application qui requiert de la sécurité. Il existe donc une large gamme de tags avec des caractéristiques très variées, allant de la simple mémoire sans capacité de calcul, à la carte à puce sans contact capable d'utiliser de la cryptographie à clef publique.

Les tags RFID les plus courants sont « passifs », c'est-à-dire qu'ils ne possèdent pas de source d'énergie embarquée: ils obtiennent leur énergie à partir du champ électromagnétique émis par le lecteur. Cela signifie que les tags doivent être présents dans le champ du lecteur pour communiquer et éventuellement effectuer des calculs. Ils répondent donc à la sollicitation d'un lecteur mais n'initient pas eux-mêmes de communication. Ils ont une distance de communication pouvant aller de quelques centimètres à quelques mètres selon la technologie utilisée, c'est-à-dire substantiellement plus faible que les tags avec batterie, dits « actifs ». Ce sont ces tags passifs qui sont aujourd'hui sur le devant de la scène et il est même devenu usuel d'utiliser simplement le terme « RFID » pour désigner la RFID passive et de dire explicitement « RFID active » dans le cas contraire.

Les tags passifs les moins chers ne sont dotés que d'une mémoire contenant un identifiant unique. La communication entre le lecteur et le tag est alors très simple : sur sollicitation du lecteur, le tag envoie son identifiant, comme le ferait tout simplement une personne à qui l'on demanderait son nom. La communication peut parfois bénéficier de mécanismes légèrement plus évolués : certains tags ne fourniront leur identifiant que si le lecteur envoie un mot de passe correct, convenu à l'avance, lors de la fabrication ou de l'initialisation du tag. Le déploiement des tags à très bas coût a été renforcé et même catapulté par la création d'un consortium aux États-Unis en 1999, l'Auto-ID Center [10], qui a pour but de standardiser et de promouvoir l'utilisation de la RFID dans les chaînes logistiques, en particulier dans la grande distribution.

Un autre exemple de tag, cette fois plus coûteux, est un tag qui possède des capacités de calcul importante, capable d'effectuer des opérations cryptographiques, qui permettent de sécuriser le système RFID considéré notamment en chiffrant la communication entre le lecteur et le tag. Ces tags possèdent également une mémoire pour stocker des données, généralement un ou deux kilo-octets, mais des valeurs bien supérieures peuvent être atteintes, comme c'est le cas avec les passeports biométriques. Ces derniers peuvent contenir plusieurs dizaines de kilo-octets de données. Un tag de ce type possède une distance de communication de l'ordre de quelques centimètres (ISO 14443) ou décimètres (ISO 15693).

## 2 Usurpation d'identité

S'il existe plusieurs types de tags, c'est bien parce qu'il existe aussi plusieurs types d'applications. Il faut principalement distinguer celles dont l'objectif est *l'identification* d'objets ou de sujets (remplacement des codes-barres, tatouage du bétail, etc.) de celles dont l'objectif est *l'authentification* de ces mêmes objets ou sujets (badge d'accès à un immeuble, clef de démarrage d'une voiture, abonnement aux transports publics, etc.).

L'identification n'a pas pour but de prouver l'identité d'une personne ou d'un objet, mais seulement d'annoncer une identité. Quiconque écoute la communication entre un lecteur et un tag est donc en mesure « d'entendre » cette identité mais il ne s'agit pas là d'un vol. En revanche, un protocole d'authentification doit assurer au lecteur qu'il communique réellement avec la personne ou l'objet prétendu.

Alors qu'il est possible de concevoir des protocoles d'authentification qui soient sûrs, il n'est pas rare de voir en pratique des attaques sur des systèmes d'authentification reposant sur la RFID, en particulier des systèmes de contrôle d'accès. Plusieurs raisons expliquent cela. Tout d'abord, de nombreuses firmes proposent des systèmes d'authentificaton qui cachent en fait seulement un protocole d'identification. Ensuite, les contraintes de la RFID, en particulier en termes de calcul, incite à utiliser des algorithmes cryptographiques "allégés" en termes de calcul, mais aussi malheureusement "allégés" en termes de sécurité. Deux exemples très médiatisés sont le module DST de Texas Instrument cassé en 2005 [1] et la puce NXP Mifare Classic vendue à plusieurs centaines de millions d'exemplaires – et toujours en vente – est totalement cassée depuis 2008 [3–7, 13].

Notons enfin qu'une attaque générique à prendre très au sérieux permet également de déjouer n'importe quel protocole d'authentification existant, aussi solide soit-il. Cette attaque, dite *par relais*, exploite le fait que les tags acceptent de répondre sans l'accord préalable de leur porteur. Elle implique deux complices reliés par un canal de communication suffisamment rapide (une communication radio par exemple) pour la transmission des données. L'un des complices est situé à proximité d'un lecteur RFID légitime – par exemple un distributeur de tickets de cinémas – alors que le second est situé à côté du tag RFID victime – par exemple un client qui attend patiemment son tour dans la file pour acheter un ticket. Cette technique permet en quelque sorte de créer une rallonge entre la victime et le distributeur : les deux attaquants relaient simplement les messages entre les deux parties, laissant croire à la victime qu'elle communique directement avec un distributeur légitime et vice-versa. Hancke [8] a réalisé un système d'attaque performant, en utilisant une communication radio entre les deux attaquants. Son système parvient à relayer le signal sur une distance de 50 mètres. Le coût du matériel ne dépasse cependant pas une centaine d'euros. Des expériences similaires ont été réalisées par Kasper, Carluccio et Paar [2] d'une part, et par Kfir et Wool [9] d'autre part. Se protéger des attaques par relais n'est pas une chose aisée car l'utilisation de la cryptographie seule ne permet pas de contrer ce type d'attaque de très bas niveau.

## 3 Fuite d'information

Alors que l'usurpation d'identité ne concerne que les tags qui ont pour objectif de réaliser de l'authentification, le problème de la fuite d'information concerne potentiellement tous les tags. Il se pose dès lors que les données envoyées par le tag révèlent de l'information sur l'objet ou la personne qui le porte.

Par exemple, un document d'identité ou une carte de paiement peut révéler des informations confidentielles. Une carte de transport public peut révéler les dates et lieux des derniers passages de son porteur. Plus préoccupant, les produits pharmaceutiques marqués électroniquement, comme préconisé par le Food & Drug Administration aux États-Unis, pourraient indirectement révéler les pathologies d'une personne, etc. Mais la fuite d'information n'est pas seulement le vol d'informations personnelles. Un problème rarement évoqué est l'espionnage industriel. Celui-ci peut prendre différentes formes. Au lieu de soulever la bâche d'un camion de la société concurrente, il est aujourd'hui plus facile de découvrir leur contenu en les scannant lorsqu'ils sortent de l'entrepôt ou lorsqu'ils sont stationnés sur les aires de repos. Nombre de cartons, palettes et containers sont en effet déjà marqués aujourd'hui avec des tags RFID.

La limite entre les attaques théoriques et les attaques pratiques est difficile à fixer car elle dépend principalement de la motivation de l'attaquant à réaliser son méfait. Prenons l'exemple d'une carte de transport public qui divulgue à qui le lui demande le nom de son porteur, ainsi que les trois derniers trajets de celui-ci. La probabilité que Monsieur Dupont, employé communale de Joinville-le-Pont, soit

scanné à distance dans la rue par un attaquant qui souhaite connaître son nom à des fins malicieuses est faible[1]. Le réel risque pour Monsieur Dupont vient plutôt de Madame Dupont elle-même. En effet, Madame Dupont n'a bien sûr aucun intérêt à lire l'identité de son mari sur la carte de transport, mais elle peut chercher à savoir si Monsieur Dupont est bien rentré directement de son travail sans faire un détour inexpliqué et inexplicable. La carte de Monsieur Dupont apportera cette réponse, que Monsieur Dupont ou non soit d'accord. Plutôt qu'il s'agisse de Madame Dupont, il peut s'agir de Monsieur Chef, supérieur hiérarchique de Monsieur Dupont, qui souhaite s'assurer que son subalterne dit la vérité lorsqu'il affirme qu'il est arrivé en retard en raison d'un problème sur la ligne 4 du métro.

## 4 Traçabilité malveillante

Le problème de la traçabilité malveillante est plus délicat à traiter. Quelle que soit l'information envoyée par le tag, elle peut potentiellement être utilisée pour le tracer dans l'espace ou dans le temps.

Pour ne pas permettre la traçabilité malveillante, le tag doit n'envoyer aux lecteurs que des réponses qui « semblent » être aléatoires sauf pour le lecteur autorisé. Cette technique n'est presque jamais employée car elle présente plusieurs inconvénients majeurs : (1) le tag doit avoir les capacités suffisantes pour utiliser de la cryptographie ; (2) pour pouvoir lire efficacement les données reçues, le lecteur doit connaître l'identité du tag (pour savoir quel secret utiliser), mais pour connaître l'identité du tag, il doit savoir lire les données reçues ; (3) pour pouvoir communiquer, le système RFID utilise un protocole d'évitement de collisions qui repose souvent sur le fait que chaque tag possède un identifiant d'évitement de collisions unique et fixe (UID) ; en conséquence, même si le prococole d'identification ou d'authentification évite la traçabilité malveillante, le protocole d'évitement de collisions peut permettre la traçabilité du tag et donc de son porteur. Le seul exemple que nous connaissons où le problème de la traçabilité malveillante est pris en compte de manière sécurisée est le passeport biométrique. En effet, dans le cas du passeport, le tag ne délivre des informations intelligibles qu'à partir du moment où le lecteur s'est correctement authentifié. En outre, l'identifiant d'évitement de collisions n'est pas fixe : il est généré aléatoirement chaque fois que le tag est sollicité par un lecteur.

## 5 Déni de service

Enfin, le piratage peut ne pas concerner un tag donné, mais un système donné en cherchant à déstabiliser son infrastructure. Cela peut être fait de manière inintéressée, au même titre qu'un pirate informatique déface un site web ou qu'un délinquant dessine des graffitis sur les murs, ou cela peut être le fruit d'un travail élaboré et prémédité. Ce dernier cas est tout à fait envisageable dans une situation de concurrence entre deux sociétés. Il pourrait être tentant de déstabiliser son concurrent en anéantissant le système RFID qui contrôle sa chaîne de production.

Les techniques qui permettent de faire cela sont diverses et variées et dépendent fortement de la technologie RFID utilisée. Cela peut aller du brouillage électromagnétique qui empêche la lecture des tags à leur destruction en utilisant des dispositifs extrêmement peu coûteux [11], en passant par l'exploitation de failles dans les lecteurs ou la diffusion de virus [12]. Alors que cette dernière menace semble peu réaliste à l'heure actuelle, l'exploitation de failles dans les lecteurs pour déstabiliser un système est quant à elle tout à fait réelle. Par exemple, une étude menée en 2006 sur la compatibilité des systèmes de vérification de passeports avec le document 9303 publié par l'Organisation de l'Aviation Civile Internationale, montre que les implémentations de ce standard souffrent généralement de nombreux problèmes, allant parfois jusqu'à la non-vérification des mesures de sécurité embarquées sur les passeports.

L'étude des dénis de service dans les systèmes RFID n'en est qu'à ses premiers balbutiements. Ce domaine profite d'une longue histoire et expérience dans le domaine plus général de l'informatique qui pourront être utilisées, à bon ou mauvais escient, dans le domaine plus restreint de la RFID.

1. Notons toutefois qu'un jour de manifestation où Monsieur Dupont brise des vitrines, les forces de l'ordre pourraient s'infiltrer dans la foule et scanner les identités des délinquants sans prendre le risque d'intervenir physiquement.

## 6 Conclusion

Cette succinte présentation de la sécurité de la RFID a pour but de présenter et de clarifier les menaces qui pèsent aujourd'hui sur cette technologie. Sans aborder les aspects purement techniques, elle permet de distinguer ce qui est réalisable de ce qui ne l'est pas. Usurpation d'identité, fuite d'informations, traçabilité malveillante et déni de service sont autant de menaces qu'il faut considérer sérieusement. Certaines d'entre elles trouvent incontestablement leur parade dans l'usage de la cryptographie. D'autres sont plus délicates à traiter. Mais il est un point important qu'il faut garder à l'esprit : les techniques mises en oeuvre pour sécuriser la RFID repose sur le postulat que les attaques proviendront d'un pirate extérieur au système. Une menace majeure, pourtant, concerne l'utilisation abusive voire frauduleuse des données par les personnes mêmes qui les recueillent licitement.

## Références


1. Steve Bono, Matthew Green, Adam Stubblefield, Ari Juels, Avi Rubin, and Michael Szydlo. Security Analysis of a Cryptographically-Enabled RFID Device. In *USENIX Security Symposium*, pages 1–16, Baltimore, Maryland, USA, July-August 2005. USENIX.
2. Dario Carluccio, Timo Kasper, and Christof Paar. Implementation Details of a Multi Purpose ISO 14443 RFID-Tool. In *Workshop on RFID Security – RFIDSec'06*, Graz, Austria, July 2006. Ecrypt.
3. Nicolas T. Courtois. The Dark Side of Security by Obscurity and Cloning MiFare Classic Rail and Building Passes, Anywhere, Anytime. In *Workshop on RFID Security – RFIDSec'09*, Leuven, Belgium, July 2009.
4. Gerhard de Koning Gans. Analysis of the Mifare Classic used in the OV-Chipkaart Project, 2008.
5. Gerhard de Koning Gans, Jaap-Henk Hoepman, and Flavio D. Garcia. A Practical Attack on the MIFARE Classic. In *Proceding of the 8th Smart Card Research and Advanced Applications – CARDIS 2008*, Lecture Notes in Computer Science, Royal Holloway University of London, UK, September 2008. Springer.
6. Flavio D. Garcia, Gerhard de Koning Gans, Ruben Muijrers, Peter van Rossum, Roel Verdult, and Ronny Wichers Schreur. Dismantling MIFARE Classic. In *Proceding of the 13th European Symposium on Research in Computer Security – ESORICS 2008*, volume 5283 of *Lecture Notes in Computer Science*, pages 97–114, Malaga, Spain, October 2008. Springer.
7. Flavio D. Garcia, Peter van Rossum, Roel Verdult, and Ronny Wichers Schreur. Wirelessly Pickpocketing a Mifare Classic Card. In *IEEE Symposium on Security and Privacy — S&P '09*, Oakland, California, USA, May 2009. IEEE.
8. Gerhard Hancke. Practical Attacks on Proximity Identification Systems (Short Paper). In *IEEE Symposium on Security and Privacy*, Oakland, California, USA, May 2006. IEEE, IEEE Computer Society Press.
9. Ziv Kfir and Avishai Wool. Picking Virtual Pockets Using Relay Attacks on Contactless Smartcard Systems. In *Conference on Security and Privacy for Emerging Areas in Communication Networks – SecureComm 2005*, Athens, Greece, September 2005. IEEE.
10. EPC Global Network. http://www.epcglobalinc.org/.
11. RFID Zapper. https://events.ccc.de/congress/2005/static/r/f/i/RFID-Zapper(EN)_77f3.html.
12. Melanie Rieback, Bruno Crispo, and Andrew Tanenbaum. Is Your Cat Infected with a Computer Virus? In *Pervasive Computing and Communications*, Pisa, Italy, March 2006. IEEE, IEEE Computer Society Press.
13. Wouter Teepe. Making the Best of Mifare Classic, October 2008. www.sos.cs.ru.nl/applications/rfid/2008-thebest.pdf.