Léonard Gross,
Étudiant en systèmes de communication,
Haute École d'Ingénierie et de Gestion du Canton de Vaud,
Route de Cheseaux 1, CH-1401 Yverdon-les-Bains, Suisse

Stephan Robert,
Professeur,
Haute École d'Ingénierie et de Gestion du Canton de Vaud,
Route de Cheseaux 1, CH-1401 Yverdon-les-Bains, Suisse

Gildas Avoine,
Professeur en cryptologie,
UCL, Louvain-la-Neuve, Belgique,
gildas.avoine@uclouvain.be

L'ennemie publique numéro un de la RFID, c'est l'attaque par relais !

« Bizarre, bizarre, comme c'est bizarre... Les malfaiteurs ont pénétré dans votre bureau sans laisser de traces d'effraction alors que vous aviez fermé la porte à clef... Quoi ? Ce n'est pas une clef, mais une carte RFID qui permet le verrouillage ? Mais bon sang, mais c'est bien sûr ! Ils ont utilisé une attaque par relais ! »

mots clés : *attaques par relais / contrôle d'accès / fraude / contre-mesures*

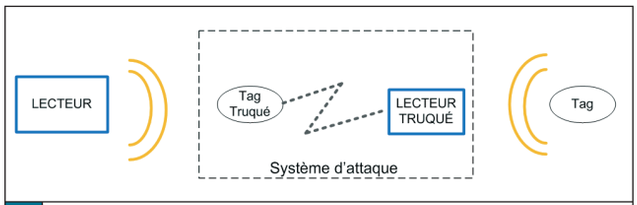
Accepteriez-vous qu'un inconnu vous aborde dans la rue pour vous demander la clef de votre bureau ou de votre appartement ? Pire, accepteriez-vous qu'il vous la subtilise, puis la replace délicatement dans votre poche après avoir commis son mauvais coup ? Certainement pas. Pourtant, un tel cas de figure peut très bien vous arriver, de manière virtuelle et à votre insu, si l'accès à votre bureau n'est protégé qu'avec de la RFID.

En effet, une belle blonde[1] vous frôle dans la rue, dans une file d'attente, dans la gare… Flatté, vous ne vous méfiez pas un seul instant. Mais sachez que la donzelle, en vous frôlant pendant une fraction de seconde, vient de permettre à son complice de pénétrer dans votre bureau, mais vous n'en savez rien. Elle ne vous a rien volé, elle vous a juste frôlé, mais elle vient de commettre un méfait, une attaque par relais, l'une des attaques les plus difficiles à contrer en RFID.

Attaque par relais

Les applications sensibles, comme le contrôle d'accès, reposent généralement sur le standard ISO 14443 qui offre une distance de communication relativement faible, de l'ordre de quelques centimètres. La distance de communication est en effet la pierre angulaire de la sécurité en RFID passive. Le tag répondant à toute sollicitation d'un lecteur sans demander l'accord de son porteur, le consentement implicite de celui-ci est sa présence dans le champ du lecteur. Cela implique une distance de communication courte, car il ne faudrait pas que la porte de votre bureau se déverrouille par inadvertance en recevant le signal de votre badge RFID, alors que vous être déjà sur le parking en partance pour votre domicile.

L'attaque par relais repose sur ce fait, c'est-à-dire que les tags passifs commercialisés peuvent être interrogés sans l'accord préalable de la personne qui les porte, a fortiori si celle-ci n'est pas consciente qu'elle en possède. Comme illustré sur la figure 1, **le système d'attaque consiste en deux entités reliées par un média de communication rapide** pour la transmission des données. Une entité (que nous appellerons « tag truqué ») simule un tag auprès du lecteur légitime et l'autre (que nous appellerons « lecteur truqué ») simule un lecteur auprès du tag légitime. Cette technique permet en quelque sorte de créer une « rallonge » entre le tag légitime et le lecteur légitime, laissant croire à celui-ci qu'il communique directement avec le tag légitime et vice-versa. Les informations circulent ainsi de manière transparente à travers le système d'attaque et **le point-clef est que ce dispositif ne modifie pas les données : il se contente de transmettre le signal dans les deux sens.**



I *Attaque par relais sur un système RFID*

Un point fondamental est que **cette attaque[2]** se situe au niveau physique (hardware). Le système d'attaque transmet le signal sans s'intéresser au contenu du message, ce qui rend cette attaque réalisable, même si des protocoles cryptographiques sûrs sont utilisés dans les niveaux supérieurs de la communication.

Dispositif et expérimentation

Afin d'illustrer les attaques par relais, nous avons réalisé un petit montage très facile à réaliser, sans casser sa tirelire. Tout lecteur de MISC, un tant soit peu débrouillard, sera en mesure de mettre en pratique notre séance de bricolage pour moins de cinq euros.

Notre système d'attaque très simple est entièrement passif : le tag truqué et le lecteur truqué sont des sondes (en fait des antennes « faites maison ») et le média entre ces deux sondes est un câble coaxial. La sonde (Figure 2) est constituée d'un circuit LC parallèle, paramétré de manière à ce que sa fréquence de résonance soit égale à la fréquence de fonctionnement du système, à savoir 13,56 Mhz dans le cas du standard ISO 14443. L'inductance est un fil de cuivre bobiné et la capacité un condensateur ajustable à l'aide d'une molette de manière à pouvoir calibrer précisément C tel que $1/(2\pi\sqrt{LC})=13{,}56$ MHz. Le tout est fixé sur une fiche mâle coaxiale qui permet de relier les deux sondes entre elles à l'aide d'un câble coaxial, comme représenté sur la figure 3, ou de relier une sonde à un oscilloscope.

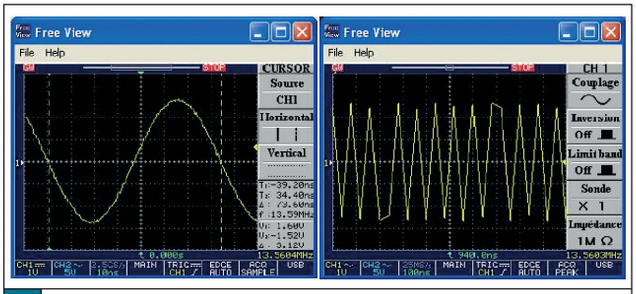
1 Remplacez par « un beau brun » selon vos préférences.
2 Cette attaque est parfois appelée « man-in-the-middle passif » ou « attaque de la mafia ».

2 *Sonde constituée d'un circuit LC*

3 *Sondes reliées entre elles par un câble coaxial, formant la « rallonge » pour l'attaque par relais*

Comme nous n'avions pas de système de contrôle d'accès à notre disposition, nous avons dû acheter un lecteur (EM Microelectronic EM4094) et un jeu de tags HF ISO 14443, car nous ne pouvions pas monter une attaque si nous n'avions rien à attaquer... Afin de « voir » ce qui se passe, nous avons également utilisé un oscilloscope. Celui-ci n'est évidemment pas utile pour réaliser l'attaque, mais il permet de l'illustrer agréablement.

Nous montrons sur la figure 4 deux expériences menées avec notre sonde. La première figure montre que le signal du lecteur sans tag est un signal sinusoïdal pur dont la fréquence est 13,56 MHz. La deuxième figure représente l'information codée dans le signal lors d'un échange entre un tag légitime et un lecteur légitime. On voit clairement les sauts de phase. Pour retrouver les bits, il serait nécessaire d'utiliser un détecteur d'enveloppe.



4 *Signal du lecteur sans tag, sinusoïdal, et information codée lors d'échanges entre le tag et le lecteur*

En utilisant la « rallonge » formée des deux sondes, nous avons pu faire croire au lecteur légitime que le tag légitime se trouvait dans son champ de lecture alors que ce n'était pas le cas. Notre dispositif à cinq euros nous a donc permis de réaliser une attaque par relais. Ce cas d'école, dont le but est purement illustratif, utilise un système d'attaque passif, qui ne permet donc pas une attaque sur une longue distance : notre « rallonge » mesurait environ 50 cm.

Distance limitée

Cinquante centimètres, c'est peu. Toutefois, des dispositifs actifs, donc plus onéreux, peuvent être réalisés. Par exemple, Hancke **[2,3]** a réalisé un système d'attaque performant, en utilisant une communication radio entre le tag truqué et le lecteur truqué. Son système est performant puisqu'il parvient à relayer le signal sur une distance de 50 m. Le coût du matériel ne dépasse cependant pas 200 €. Des expériences similaires ont été réalisées par Carluccio, Kasper et Paar **[4]** d'une part, et par Kfir et Wool **[1]** d'autre part.

Les attaques par relais n'en sont qu'à leurs premiers balbutiements et de nombreuses améliorations verront probablement le jour. Par exemple, on peut se demander s'il serait possible de réaliser une attaque par relais en utilisant une communication Bluethooth, GSM ou TCP/IP entre les deux entités truquées, permettant ainsi une communication bien supérieure à 50 m. Un *timer* nous complique toutefois la vie. En effet, il existe un timer tel que lorsqu'un délai donné s'est écoulé depuis l'envoi d'un signal sans obtention de réponse, le lecteur légitime considère que la communication a échoué. Ce timer dont le but premier n'est pas sécuritaire contrarie cependant un peu l'attaque par relais. Mais, il existe des cas de figure où le délai d'attente est important (de l'ordre de plusieurs secondes), ce qui laisse largement le temps de réaliser une attaque par relais sur une grande distance. Un tel délai est par exemple utilisé dans les passeports biométriques utilisant l'authentification active[3]. Ce problème a été très récemment soulevé par Hlaváč et Rosa dans **[8]**.

Notons enfin que, pour avoir lieu, l'attaque par relais nécessite que le lecteur truqué soit proche du tag légitime. La distance annoncée par les constructeurs de systèmes RFID et découlant du standard ISO 14443 est de l'ordre de 10 centimètres. Toutefois, des expériences ont montré que ces distances peuvent être augmentées en agissant sur les paramètres physiques du système. Par exemple, Sorrels dans **[5]** montre comment de manière relativement simple, en agissant sur le diamètre des antennes ou le facteur de qualité, la portée peut être accrue. Kfir et Wool **[1]** prétendent, quant à eux, être en mesure de lire un tag conforme au standard ISO 14443 à une distance de 50 cm. Déterminer la distance de lecture maximale entre un lecteur et un tag en utilisant des moyens éventuellement illégaux fait aujourd'hui l'objet de nombreuses études. Les prochains mois nous en diront certainement un peu plus sur le sujet.

Mais, ne négligeons pas le fait qu'un lecteur commercial avec une distance de communication de quelques centimètres peut être tout à fait suffisant pour réaliser une attaque par relais. Il suffit par exemple de dissimuler le lecteur truqué dans une mallette et de s'approcher suffisamment d'une victime (dans une file d'attente, magasin, banque, transport public, etc.) pour déclencher l'attaque. Avoine, Kalach et Quisquater ont, par exemple, caché un lecteur RFID dans une serviette pour interroger des passeports à l'insu de leurs porteurs[4].

Impact

Dans des cas concrets, cette attaque peut prendre une dimension dramatique et répréhensible pénalement. Nous avons vu le cas du contrôle d'accès, mais il existe de nombreuses autres applications sensibles à cette attaque.

Prenons le cas du passeport biométrique. L'Organisation de l'Aviation Civile Internationale (ICAO) requiert que les passeports[5] soient dorénavant munis d'un tag RFID afin de renforcer leur sécurité. Aujourd'hui, la présence d'un officier du contrôle de l'immigration est encore nécessaire, mais l'idée de bornes de

3 Voir article d'Avoine, Kalach et Quisquater dans ce dossier.
4 Voir http://www.dice.ucl.ac.be/crypto/passport/index.html.
5 Voir les articles sur le passeport biométrique dans ce dossier.

contrôle automatique est déjà dans les esprits. Lorsque tous les passeports seront munis de l'authentification active (système anti-clonage), l'utilisation de bornes de contrôle automatique pourrait bien émerger dans les aéroports. Dans un tel cas de figure, les attaques par relais accentueraient la psychose présente dans notre ère *post-9/11*.

Plus proche de nous, un autre exemple très illustratif concerne les paiements par carte. En effet, l'utilisation de la RFID pour les cartes de paiements (carte bancaire, porte-monnaie électronique, carte contenant des tickets d'entrée, etc.) se généralise, lentement, mais sûrement. Passer sa carte devant un lecteur est le seul geste requis pour effectuer le paiement. Ces applications sont naturellement très sujettes aux attaques par relais[6]. Il est possible avec ce type d'attaque de débiter le compte ou porte-monnaie d'une autre personne en plaçant le tag et lecteur truqués de manière judicieuse. Les problèmes de sécurité liés à la RFID sont actuellement sérieusement étudiés au sein du GIE Cartes Bancaires.

Les malfaiteurs sont généralement plus imaginatifs que ceux qui protègent les systèmes. Mais, il n'est pas difficile d'imaginer un scénario d'attaque en regardant nos propres habitudes. Par exemple, l'un des auteurs de cet article possède une carte d'abonnement à un cinéma. Cette carte rechargeable contient des tickets d'entrée, autrement dit de l'argent. Elle peut être présentée à la personne derrière le guichet ou « passée » devant une borne automatique située dans le hall du cinéma, qui délivre des tickets imprimés. Vous l'aurez compris, cette carte contient un tag RFID. Imaginons maintenant deux complices. Ils possèdent chacun un petit organiseur personnel (ex. Ipaq) munis d'une antenne RFID, qui font office de tag et lecteur truqués. L'un est devant la borne, alors que l'autre est dans la file d'attente. Est-il nécessaire de finir le scénario du film ? Non, vous aurez compris la suite… Doit-on préciser qu'il existe aujourd'hui des lecteurs RFID PCMCIA tout à fait adaptable à des Ipaq ? Doit-on préciser que des Ipaq peuvent communiquer entre eux par une connexion Bluetooth ?

Pour être très honnête, il n'existe pas aujourd'hui à notre connaissance d'attaques par relais qui utilisent des protocoles de communication complexes de type Bluetooth, GSM ou encore TCP/IP. C'est évidemment plus difficile de réaliser une attaque par relais à travers ce type de protocoles, car les délais engendrés par le traitement de l'information sont importants. On ne peut toutefois pas faire reposer la sécurité sur ce genre de considération, car il y a déjà plusieurs équipes de recherche qui travaillent à la réalisation d'attaques par relais à travers ce type de protocoles. Et puis, qu'à cela ne tienne, en attendant, nos deux complices peuvent utiliser une communication radio de bas niveau entre les deux Ipaq, à la « Hancke et Kuhn », qui permet une communication sur 50 m. C'est bien suffisant dans notre exemple, car si le premier complice doit remonter une file de 50 m pour atteindre la borne automatique, alors je me permettrais de lui suggérer de louer un DVD à la place…

Principe du distance bounding

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'attaques de très bas niveau. Rappelons-le, l'attaque consiste à relayer le signal sans se soucier de l'information contenue dans ce signal.

Des approches palliatives peuvent être imaginées pour se prémunir des attaques par relais, comme utiliser une cage de Faraday, un *blocker-tag* ou un *clipped-tag*[7]. Une autre manière d'aborder le problème consiste à utiliser entre le lecteur légitime et le tag légitime un protocole qui détermine une borne supérieure sur la réelle distance entre ces deux entités. Un tel protocole est dit de « *distance bounding* » et repose sur le fait qu'aucun signal ne peut se propager plus vite que la lumière : en envoyant une requête au tag et en calculant le temps de réponse, le lecteur peut déterminer si le tag est effectivement dans sa proximité.

En pratique, le procédé est un peu plus compliqué que cela. Le lecteur RFID doit pouvoir déterminer si le tag se trouve à une distance inférieure à une distance donnée. Nous parlerons par abus de langage dans ce dossier d'« évaluer la distance ». Cependant, la seule information de distance ne suffit pas pour authentifier un tag, car le lecteur ne sait pas en cas de test réussi si le tag qui a participé au protocole est bien le tag légitime ou bien un tag truqué. Un protocole de distance bounding doit donc à la fois évaluer la distance et authentifier le tag.

Évaluer la distance consiste à mesurer le temps écoulé entre l'envoi d'un message par le lecteur au tag et le retour de la réponse du tag au lecteur. Autrement dit, il s'agit d'un échange de type challenge/réponse[8] avec un timer qui est déclenché à l'envoi du challenge et arrêté à la réception de la réponse. Pour éviter que les délais de traitement ne « bruitent » les délais de propagation mesurés, il faut, d'une part, que cette procédure ait lieu à un très bas niveau (pour éviter synchronisations, évitement de collisions, détection d'erreurs, etc.) ; d'autre part, que la réponse soit rapide à calculer et à transmettre, donc courte. Toutefois, bien sûr, seul le tag légitime doit être capable de répondre correctement au challenge... Nous tombons donc sur un dilemme : nous voulons une réponse courte, mais telle que seul le tag légitime soit capable de la produire.

Les protocoles existants utilisent des messages extrêmement courts : challenge et réponse ne sont constitués que d'un seul bit chacun. Cela signifie qu'un tag truqué qui répondrait au hasard au lecteur aurait 50% de chance de le leurrer. Pour réduire les chances de succès d'un tag truqué, la procédure de challenge/réponse est répétée plusieurs fois, jusqu'à ce que le lecteur ait la conviction que le tag avec lequel il communique est réellement dans son champ de lecture.

Un protocole de distance bounding

Les pionniers dans le domaine des protocoles de distance bounding sont Stefan Brand et David Chaum qui publièrent **[7]** leurs premiers travaux en 1993. Ils y présentent le premier protocole de distance bounding. Leurs travaux n'étaient cependant pas destinés à la RFID, peu développée à cette époque. Il faut attendre 2005 pour voir le premier protocole de distance bounding spécialement conçu pour la RFID. Il s'agit du protocole de Hancke et Kuhn **[9]** que nous détaillons ici.

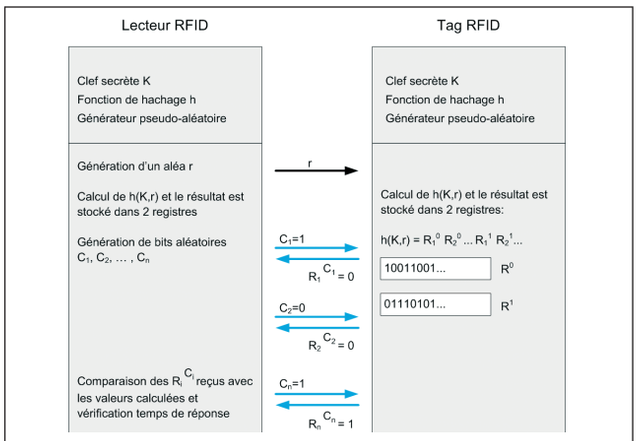
Le protocole cité requiert que le tag et le lecteur possèdent en commun une clef secrète *K*, une fonction de hachage *h*, et une fonction pseudo-aléatoire. Le déroulement du protocole est illustré

6 Les participants à SSTIC 2006 auront pu voir une vidéo sur l'attaque de la carte de paiement SpeedPass (www.speedpass.com). Il s'agissait alors d'une attaque par recherche exhaustive de la clef et non d'une attaque par relais.

7 Voir article introductif de Gildas Avoine dans ce dossier.

8 Voir article de Girault, Desmoulins et Juniot sur l'authentification dans ce dossier.

sur la figure 5. La première flèche, en rouge, symbolise une phase non critique au niveau du temps. Elle peut être effectuée avant la phase d'échange rapide de bits, symbolisée par des flèches bleues.



5 *Protocole de Hancke et Kuhn*

Étape 1 : La première étape consiste pour le lecteur à générer aléatoirement *n* bits C_i et à envoyer au tag une valeur aléatoire *r*. Lecteur et tag calculent *h(K,r)* au moyen de la fonction de hachage *h* (dont la taille de la sortie est au moins de longueur *2n*) et de la clef secrète partagée *K*. Le résultat de la fonction de hachage est stocké dans deux registres de *n* bits chacun, notés R^0 et R^1 (dans un tel protocole, *n* est petit, par exemple *n=8* ou *n=16*, pour apporter un niveau de sécurité raisonnable sans ralentir de manière inconsidérée l'authentification).

Étape 2 : La phase d'échange de bits rapide commence ensuite. Le lecteur envoie un par un les bits de challenge, C_i, auxquels le tag répond par R_i^{Ci}, où R_i^{Ci} est le *i*-ème bit du registre numéro C_i à savoir soit R_i^0, soit R_i^1. Le challenge définit donc le registre duquel le tag va extraire le bit de réponse.

Le protocole de Hancke et Kuhn souffre cependant de quelques inconvénients, que le lecteur intrigué pourra découvrir en parcourant **[6]**.

Difficultés pratiques

Pour implémenter un protocole de distance bounding, il faut être capable de mesurer le délai entre l'émission d'un signal et la réception du signal de réponse. La théorie est jolie, mais la mise en pratique est délicate. En effet, une légère imprécision sur la mesure du temps et la distance s'en trouve largement faussée. La lumière parcourt 30 cm en une nanoseconde : ce simple fait nous indique que l'implémentation physique n'est pas triviale

La résolution en distance d'un canal de communication est approximativement égale à c/B où c est la fréquence de la porteuse et B la largeur de bande. Les fréquences utilisées pour la RFID ne sont pas particulièrement appropriées pour faire de la localisation (c=13,56 MHz, B=300 kHz pour le standard ISO 14443). Il faut donc une autre technique de communication pour pouvoir estimer le temps d'aller-retour avec précision. L'idée de Hancke et Kuhn **[9]** est d'utiliser des signaux à très large bande (UWB : *Ultra Wide Band*, largeur de bande minimum : 500 MHz) qui sont constitués d'impulsions très brèves (flancs de 2 nsec ou moins).

Les C_i et R_i^{Ci} sont transmis sous forme d'impulsions à deux polarités selon que les valeurs des bits sont 1 ou 0 (Bi-Phase Modulation, BPM). Il est toutefois nécessaire de synchroniser l'émetteur et le récepteur pour récupérer les impulsions correctement. Les 13,56 MHz peuvent servir comme base de temps pour la synchronisation de la communication. Nous pouvons, par exemple, envoyer une impulsion t_t (petit) après le passage à zéro de la porteuse à 13,56 MHz. Le récepteur envoie une réponse t_d après avoir reçu l'impulsion de l'émetteur. La réponse est reçue par l'émetteur t_s après le passage à zéro de la porteuse. La distance estimée est simplement égale à $c(t_s - t_t - t_d)/2$.

Nous ne connaissons aujourd'hui aucune implémentation pratique de protocoles de distance bounding. Nous ne connaissons non plus personne qui ait essayé...

Conclusion

L'attaque par relais est relativement facile à mettre en œuvre, mais sa parade est en revanche nettement plus compliquée à implémenter. Notre opinion est que cette attaque pourrait être particulièrement nuisible au développement de la RFID dans les applications sensibles, et nuisible aux intérêts des utilisateurs. L'expérience que nous avons menée avec un simple câble coaxial n'est qu'un cas d'école, mais nous avons cité d'autres expériences qui ont déjà vu le jour et nous pourrions en citer bien d'autres qui sont encore en préparation. Pourtant, les fabricants ou revendeurs de solutions RFID ne semblent pas s'inquiéter de cette menace. Nous ne connaissons aucun fabricant qui se soit intéressé aux protocoles de distance bounding et la notion d'attaque par relais les laissent généralement indifférents. Difficulté technique ou enjeux économiques peu encourageants ? Certainement un peu des deux.

Références

[1] KFIR (Z.) et WOOL (A.), « *Picking virtual pockets using relay attacks on contactless smartcards systems* », Conférence SecureComm, septembre 2005.

[2] HANCKE (G.), « *A practival relay attack on ISO 14443 proximity cards* », Manuscript, février 2005.

[3] HANCKE (G.), « *Practical attacks on proximity identification systems (short paper)* », *IEEE Symposium on Security and Privacy*, mai 2006.

[4] CARLUCCIO (D.), KASPER (K.) et PAAR (C.), « *Implementation details of a multi-purpose ISO 14443 RFID-Tool* », *RFID Security*, juillet 2006.

[5] SORRELS (P.), « *Optimizing read range in RFID systems* », *EDNmag*, pages 173-184, décembre 2005.

[6] AVOINE (G.), « *Bibliography on Security and Privacy in RFID Systems* », bibliographie disponible en ligne sur Internet.

[7] BRANDS (S.) et CHAUM (D.), « *Distance bounding protocols (extended abstract)* », *Theory and Application of Cryptographic Techniques*, 1993.

[8] HLAVÁČ (M.) et ROSA (T.), « *A Note on the Relay Attacks on e-passports. The case of Czech e-passports* », *Eprint IACR,* numéro 244, juin 2007.

[9] HANCKE (G.) et KUHN (M.), « *An RFID distance bounding protocol* », Conférence SecureComm, septembre 2005.