Activation des cartes à puce sans contact à l'insu du porteur

Carine Boursier, Pierre Girard, and Christophe Mourtel

Gemalto
prenom.nom@gemalto.com

1 Introduction

Depuis de nombreuses années, la technologie des produits sans contact est embarquée dans des applications propriétaires diverses. Avec l'élaboration de standards comme ISO 14443 et ISO 15693, la mise en place d'initiatives internationales comme les spécifications ICAO ou le succès commercial de programmes comme PayPass, cette technologie fait son entrée dans des marchés où les volumes de cartes sont beaucoup plus importants. Ce déploiement à grande échelle va s'accompagner de problématiques nouvelles en particulier concernant la sécurité : confidentialité des données, écoutes illégales, traçage des personnes, vie privée, déni de service...

Un enjeu sécuritaire fondamental dans la technologie sans contact est d'empêcher l'activation de la carte à l'insu du porteur. La communication entre une carte à contact et un lecteur n'est possible qu'à partir du moment où la carte est introduite dans celui-ci. Cet acte traduit en quelque sorte le consentement du porteur de la carte. Dans le cas d'une carte sans contact, une communication peut s'établir dès lors que la carte est présente dans une sphère d'environ 10 cm de rayon autour de l'antenne du lecteur. Le volume autour de l'antenne peut paraître suffisamment faible pour qu'une communication ne soit pas possible sans l'accord du porteur, mais en réalité un lecteur ou une antenne n'ayant pas des caractéristiques ISO pourrait avoir des performances bien plus élevées. Ce risque est donc bien réel.

Après un rappel des principes de fonctionnement et des différentes normes disponibles pour les produits sans contact, on fera dans cet article un tour d'horizon des applications le plus couramment associées à ce type de technologie comme le contrôle d'accès, le transport, le paiement ou l'identité en mettant l'accent sur des exemples concrets de déploiement à travers le monde. Puis, partant de ces cas d'utilisation, nous évoquerons les attaques et les menaces spécifiques à ces produits et nous dresserons un état de l'art des différentes solutions pour parer au problème d'activation à l'insu du porteur, en soulignant leurs contraintes et leurs limitations. Nous présenterons ensuite trois nouvelles solutions introduisant une notion de consentement du porteur tout en maintenant un bon niveau d'ergonomie pour l'application.

2 Principes des cartes sans contact

2.1 Énergie de fonctionnement de la carte

Il faut distinguer deux catégories de produits, ceux qui comportent une batterie embarquée et ceux qui reçoivent leur énergie du champ électromagnétique dans lequel ils sont placés. Les premiers sont dits auto-alimentés ou actifs, les seconds téléalimentés ou passifs. Les cartes à puce sans contact auxquelles nous nous intéressons font partie de la deuxième catégorie de produit. Elles reçoivent leur énergie du champ électromagnétique alternatif émis par l'antenne du lecteur devant lequel elles

sont placées pour fonctionner. Ce champ électromagnétique rayonne à partir de l'antenne du lecteur dans une sphère (ou demi-sphère) autour de celle-ci. La carte à puce, accordée sur la fréquence du champ électromagnétique, va ainsi récupérer au mieux, grâce à sa propre antenne de communication, l'énergie du champ électromagnétique et la transformer en tension pour son propre fonctionnement. Ainsi, quel que soit l'endroit où la carte va être positionnée dans le volume entourant l'antenne du lecteur, si l'énergie reçue est suffisante, la carte va être en mesure de fonctionner.

2.2 Transmission de données

La transmission de données dans le cas des produits qui nous intéressent, se fait par la modulation du champ électromagnétique servant à alimenter le produit. La modulation du champ électromagnétique sert de principe de transmission des données du lecteur vers la carte et réciproquement. Pour des questions de robustesse de la communication, le schéma de modulation peut prendre différentes formes (modulation d'amplitude, de fréquence, saut de phase, modulation avec sous-porteuse...).

La fréquence de l'onde du champ électromagnétique sert aussi d'horloge à la carte à puce afin de cadencer ses opérations.

Si ces principes généraux sont communs à l'ensemble des produits téléalimentés, nous allons préciser dans la section suivante les différentes normes de fonctionnement applicables.

2.3 Fréquences de fonctionnement

Plusieurs fréquences de fonctionnement (fréquence du champ électromagnétique) existent ; certaines sont plus utilisées que d'autres et les principales normalisations ont choisi le 13,56 MHz comme fréquence de référence.

125KHz Les plus anciennes fréquences de fonctionnement utilisent la gamme des 100 kHz (le plus souvent 125 ou 131 kHz). Cette gamme de fréquences est aujourd'hui principalement utilisée dans des applications industrielles car son immunité au bruit environnemental est très forte, ou dans des applications d'immobiliseurs de véhicule. Toutefois, les applications sur cette gamme de fréquences ne sont pas très largement déployées car elle n'a pas fait l'objet de normalisation.

Un autre facteur limitatif de cette fréquence de fonctionnement est la taille des éléments externes à ajouter à la puce afin de réaliser l'accord en fréquence. Typiquement les antennes doivent avoir une inductance de l'ordre du milli Henry (mH) ce qui nécessite quelques centaines de tours de bobinage. La capacité d'accord nécessaire est si volumineuse (de l'ordre du nano Farad, nF) qu'elle ne peut être intégrée dans le silicium de la puce. Ces impératifs se traduisent par un volume incompatible avec un format de carte ISO.

13,56 MHz C'est la fréquence qui a fait l'objet de deux normalisations (ISO 14443 et ISO 15693). Cette fréquence a été retenue pour plusieurs raisons ; la première est que cette gamme de fréquences permet de réduire la taille (et la valeur) des éléments nécessaires à l'accord en fréquence. L'antenne doit avoir une inductance de l'ordre du μH qui se réalise facilement avec quelques tours (trois à cinq) de bobinage de fils, et la capacité d'accord peut être intégrée dans le silicium de la puce puisque sa valeur est de l'ordre de la dizaine de pF. Ces aspects technologiques ont un fort impact sur les coûts de réalisation des produits et permettent de les réaliser au format ISO de la carte à puce.

Une autre raison est que l'augmentation de la fréquence du champ électromagnétique autorise l'augmentation du débit d'information entre la carte et le lecteur permettant d'atteindre facilement un débit de l'ordre du mégabits par seconde (à comparer à la dizaine de kilobits par seconde dans le cas du 125 KHz). La contre partie de cette gamme de fréquences est la sensibilité aux conditions environnementales. La présence de métal aux environs de l'antenne du lecteur ou de la carte modifie fortement les performances de l'ensemble.

Les normalisations autour de cette valeur de fréquence ont créé une dynamique qui a contribuée à l'imposer à la majorité des applications sans contact développées aujourd'hui. On la retrouve dans des applications de transport, d'identité, de contrôle d'accès, de paiement...

Les Gammes UHF et hyperfréquences D'autres fréquences de fonctionnement servent également de support à des applications sans contact. On peut citer les fréquences de 443 MHz, la gamme des 900 MHz, et plus haut on retrouve les fréquences de 2,45 et 5,8 GHz. Ces hyperfréquences sont utilisées dans des applications où la distance de fonctionnement doit être importante. Pour ces raisons, les produits de ces applications sont le plus souvent actifs, le champ électromagnétique servant seulement à transporter les informations et perdant son rôle de téléalimentation. Les applications typiques de ces fréquences sont les ouvre-portes à distance, les télépéages et des applications industrielles nécessitant l'identification à très longue distance.

Il n'existe pas encore de norme dans ces gammes de fréquences (une est en cours de définition, l'ISO 18000-x, sans qu'une fréquence unique ne semble s'imposer) et l'on retrouve une très grande hétérogénéité dans les produits et les applications.

2.4 Les normes du Sans Contact autour de la valeur 13,56 MHz

S'il existe plusieurs normes autour des produits sans contact, la plupart d'entre elles ne sont pas utilisées dans des applications de grand volume. On peut citer l'ISO 10536 relative au *close coupling* pour laquelle la distance de fonctionnement est inférieure au cm ou les ISO 11785 et 14 223 relatives à l'identification animale. Nous ne détaillerons pas ces normes et allons nous intéresser aux normes ISO 14443 et ISO 15693 relatives respectivement aux produits de proximité - fonctionnement jusqu'à 10 cm - et de voisinage - fonctionnement jusqu'à 70 cm.

Le but de ce document n'est pas de retranscrire la norme ISO 14443 dans son intégralité, mais plutôt d'en présenter la structure. Pour le détail complet de ces normes, il est conseillé de se reporter aux documents de l'ISO.

La norme ISO 14443 se décompose en quatre parties :

- Partie 1 : définit les caractéristiques physiques et mécaniques des produits.
- Partie 2 : décrit la manière dont la carte sans contact est téléalimentée, ainsi que la fréquence de fonctionnement et les signaux de communication entre la carte et le lecteur. Cette partie de la norme ainsi que la partie 3 sont découpées en deux sections définissant chacune un schéma de communication différent, que l'on nommera type A et type B.
- Partie 3 : définit les phases d'initialisation entre les parties et le traitement de l'anticollision pour le type A et B.
- Partie 4 : décrit la couche applicative des produits ISO. Cette couche est identique quel que soit le type (A ou B) du produit. Elle définit les règles d'échanges des blocs ou le chaînage des commandes.

3 Cas d'utilisation

La technologie sans contact a d'abord été perçue comme une technologie intéressante pour les transports, l'étiquetage, et d'aspect ludique à l'utilisation. Ont ainsi émergé des applications phares, entièrement dédiées et adaptées au sans contact comme le contrôle d'accès, le transport...

Le développement de produits autour de la norme ISO 14443, a permis d'envisager son utilisation dans des applications à forte valeur ajoutée comme les applications bancaires ou l'identité et plus récemment dans des produits multi applicatifs où des applications contact cohabitent avec des applications sans contact en partageant les mêmes ressources.

3.1 Contrôle d'accès

Les cartes sans contact sont des candidates idéales pour les applications de contrôle d'accès. La technologie sans contact propose en particulier un accès main-libre et permet une protection des cartes et des lecteurs contre la poussière, l'eau, le froid et autres conditions environnementales...

Trois technologies différentes peuvent supporter les applications de contrôle d'accès, 125 kHz, ISO/IEC 14443, ISO/IEC 15693, mais seules les deux dernières ont une intelligence et sont capables de réaliser des opérations de lecture/écriture ou des calculs. Grâce à ces technologies, on peut authentifier l'identité d'une personne et en déduire un niveau d'accès approprié. Certaines cartes peuvent aussi embarquer des facteurs d'authentification supplémentaires comme des PINs ou de la biométrie.

Dans la plupart des applications de contrôle d'accès, le lecteur lit une donnée dans la carte, la traite et l'envoie au panneau de contrôle. Le panneau de contrôle, après avoir éventuellement interrogé un ordinateur ou une base de données, détermine les droits de l'utilisateur et donne ou non l'autorisation finale. Cet accès peut dépendre aussi de la date, de l'heure...

3.2 Transport

Dans le domaine des transports, les contraintes de temps peuvent être très fortes (par exemple une transaction de six APDUs en moins de 140 ms et chaque APDU en moins de 20 ms pour certains produits). Des protocoles et des applications tiennent compte de ces contraintes comme Octopus, MiFare ou Calypso.

Octopus ce projet lancé en 1997 à Hong-Kong associe un schéma de porte-monnaie électronique et de transport public. Initié pour le paiement des transports, ce sont aujourd'hui plus de cent fournisseurs qui adhèrent à l'application (bus, taxi, tramway, train, mais aussi téléphone public, supermarchés, points de vente alimentaires, parking...). Le succès d'Octopus tient à sa très forte acceptation par le public, à l'omniprésence de points de chargement du porte-monnaie électronique mais aussi à la rentabilité du système. La technologie quasi exclusivement utilisée en Asie est la technologie Felica développée par Sony. Le succès d'Octopus à Hong-Kong a fait des émules en Asie. On peut citer Kansai Thru Pass au Japon, le métro de Washington qui a repris le schéma de l'application mais sur un autre standard que Felica...

Applications autour du produit Mifare Si Octopus est une des applications les plus développées en Asie, il existe un grand nombre d'autres applications de transport utilisant le produit Mifare de Philips à travers le monde. Le premier pilote a débuté à Séoul en 1995, et représente aujourd'hui plus de quinze millions de produits sur le terrain. Depuis, d'autres grandes agglomérations ont choisi ce principe notamment Moscou, Varsovie, Pékin, Ankara, Bombay, Sao Paulo... Le produit Mifare, qui a été un des premiers produits sans contact, bénéficie d'une technologie simple qui a été parfaitement éprouvée. Ce produit est une mémoire au format propriétaire, et peut être partagé entre plusieurs applications, chacune ayant des conditions d'accès particulières à sa propre zone. Cette mémoire peut également être configurée en fonction porte-monnaie, et c'est ainsi qu'elle est utilisée dans les applications transport. Sa compatibilité avec l'ISO 14443 est partielle (jusqu'à la partie 3 de la norme 14443 type A).

Calypso C'est le schéma défini en type B par le consortium Calypso. Ce consortium regroupe des acteurs européens du transport qui ont spécifié des règles communes pour les applications transports. Tout comme les fournisseurs, les utilisateurs doivent être licenciés pour pouvoir utiliser ce schéma de transport. Plusieurs villes européennes ont choisi de développer leur application autour de ce «standard» ; citons Paris (RATP et SNCF avec Navigo), Lisbonne, Venise, Bruxelles...

3.3 Paiement sans contact

Les applications de paiement dont nous allons parler ici sont les versions sans contact de cartes de paiement à contact ou à piste magnétique, pour lesquelles on recherche une facilité d'utilisation et pour lesquelles les montants de transaction restent de petits montants.

Speedpass Speedpass a été introduit par ExxonMobil en 1997. C'est un des premiers schémas de paiement à avoir adopté la technologie sans contact. A la différence des applications actuelles qui utilisent des produits ISO 14443, à l'époque du lancement de l'application les normes n'existaient pas et les produits choisis étaient des produits de Texas Instruments ayant une fréquence de fonctionnement dans la gamme des 100 kHz. Malgré un schéma propriétaire, près de six millions de personnes utilisent aujourd'hui ce principe de paiement dans les stations Exxon et Mobil à travers le monde. Le schéma de paiement retenu est le suivant : la pompe à essence initie un dialogue avec le produit sans contact afin d'autoriser la délivrance de l'essence après une reconnaissance du client au travers du numéro d'identification. Texas Instrument a développé un schéma de sécurité avec reconnaissance mutuelle par challenge/réponse entre le lecteur et le transpondeur ainsi qu'un chiffrement des échanges. On peut noter que le succès de Speedpass a suscité le lancement sous forme de pilote d'autres projets similaires, citons Shell qui a lancé EasyPay, un pilote à base de produit ISO 15693...

Paypass Afin de pousser le déploiement de la norme EMV, Mastercard a défini un produit à base de carte sans contact ISO 14443 capable de fonctionner en type A et B. Le schéma adopté est fondé sur le principe de la piste magnétique (qui sera d'ailleurs conservée sur la carte comme solution de secours). La carte à puce sans contact contiendra l'image de la piste magnétique (track 1 et track 2) qui sera échangée lors de la communication avec le lecteur. Ainsi l'application du terminal de paiement ne subira pas de changement. Le but de ce passage au sans contact est dans un premier temps de familiariser l'utilisateur avec les cartes à puces au travers d'une technologie très ludique.

Une fois l'adoption de cette technologie acquise, Mastercard prévoit de faire évoluer son schéma de paiement.

Visa Contactless Payment Depuis 1998, plus de sept millions de cartes sans contact ont été délivrées sous l'estampille Visa en Corée du Sud. Ces cartes utilisent une puce sans contact pour le paiement des transports et une piste magnétique pour les autres types de paiement. Le succès du paiement sans contact a fait que les nouveaux produits permettront à terme le paiement traditionnel par l'interface sans contact. En 2002 Visa a considéré cette technologie comme stratégique et introduit une carte GlobalPlatform dual-interface supportant VSDC. Le produit dual-interface ISO 14443 A et B, qui supporte aussi MIFARE pour les applications de transport, fait l'objet de nombreux pilotes pour développer le paiement sans contact. Un de ces pilotes associe la téléphonie et le paiement. Ce pilote lancé par SK Telecom et nommé Moneta a été lancé en 2002.

3.4 Passeport/identité

Les passeports doivent être interopérables et doivent fonctionner de la même manière à la frontière de tous les pays. Dans ce but, ICAO, une entité chapeautée par les Nations Unies, a rédigé un ensemble de directives pour les passeports électroniques qui transportent de l'information biométrique (reconnaissance faciale, empreintes digitales, reconnaissance de l'iris). Plusieurs gouvernements nationaux ont pour ambition de déployer les passeports électroniques en utilisant la biométrie et la technologie sans contact. Depuis 1998, les passeports malaisiens incluent une puce contenant une image du possesseur du passeport et depuis 2003 son empreinte digitale.

Dans les recommandations ICAO, le contrôle des passeports se passe de la façon suivante : le voyageur présente son passeport au douanier qui est capable de lire les données stockées dans la puce. La puce contient des données signées électroniquement par l'état qui a délivré le passeport et les données biométriques. Le MRZ (*Machine Readable Zone*) représente deux lignes sur le passeport incluant le nom, la date de naissance, le sexe, un identifiant du passeport et sa date de validité.

Le douanier :

1. déverrouille la carte grâce à la lecture du MRZ (BAC - *Basic Access Control*) et met au point un canal de communication sécurisé entre le lecteur et la puce du passeport : cette étape est une étape optionnelle ;
2. test si le possesseur présumé du passeport correspond bien à la biométrie qui est stockée sur la puce (*passive authentication*) : cette étape est obligatoire ;
3. vérifie l'intégrité du passeport (*active authentication*) en vérifiant que la carte contient bien le clef secrète certifiée par le pays d'origine : cette étape est optionnelle ;
4. une étape supplémentaire peut être rajoutée pour assurer de la confidentialité (EAC - *Extended Access Control*) lors de la lecture des données biométriques.

4 Etat de l'art des attaques

Les attaques des produits sans contact peuvent être rangées dans deux catégories. La première concerne les attaques dites passives, la seconde les attaques dites actives.

Dans la première catégorie, nous allons retrouver l'ensemble des attaques qui exploitent des informations recueillies sans intervention directe de l'attaquant sur le produit à attaquer. L'attaquant

se contente de collecter des informations liées au produit et/ou à l'application durant un échange autorisé entre le produit et un lecteur.

Les attaques dites actives, à l'inverse, reposent sur la sollicitation du produit à l'aide d'équipements appartenant à l'attaquant. Par exemple un lecteur illicite fabriqué par l'attaquant disposant de fonctions et de caractéristiques fonctionnelles non standard est utilisé pour initier une communication avec un produit dans le but de faire fonctionner le produit dans un environnement particulier et de récolter ainsi de l'information non standard.

Nous allons évoquer ci-après les menaces les plus couramment évoquées.

4.1 Ecoute illégale [1,3]

C'est la menace la plus souvent citée concernant les produits sans contact. Elle consiste à disposer un équipement dans l'entourage d'une communication sans contact et de capter à l'aide de celui-ci un signal contenant des informations permettant la compréhension des données échangées entre le produit et le lecteur.

Plusieurs publications démontrent qu'une écoute, permettant la compréhension des données échangées, est possible à plusieurs mètres de la communication légale. Rappelons que cette communication se fait avec un maximum de 10 cm entre le produit et le lecteur. Au-dela les conditions d'un échange ne sont plus réunies.

La prévention de cette menace impose la mise en place un canal de communication chiffré de manière à rendre inexploitable les informations tirées des signaux captés.

4.2 Scanning Actif [5,6]

A l'inverse de la précédente, la mise en œuvre de cette menace nécessite de la part de l'attaquant de développer un équipement lui permettant de communiquer avec des produits sans contact à l'insu de son porteur. Pour cela l'attaquant va doter son équipement de fonctionnalités hors normes afin d'augmenter la distance de communication entre le produit et son équipement. Pour ce faire il va devoir augmenter la puissance émise par le lecteur et la taille de l'antenne d'émission côté lecteur. Les résultats d'essais menés par des universitaires montrent que lorsque la puissance du lecteur passe de 0,6 W à 4 W et que la taille de l'antenne lecteur a une taille équivalente à une feuille A3, alors la distance de communication peut être augmentée à 50 cm. Ces résultats montrent également que l'augmentation de la puissance ou de la taille de l'antenne, au delà de ces valeurs, ne permet plus une augmentation de la distance de communication significative. Une fois cet équipement réalisé, l'attaquant dispose alors d'un outil lui permettant d'alimenter et de dialoguer avec un produit sans contact. Cela lui offre alors la possibilité d'envoyer au produit des commandes lui permettant de récupérer des informations auxquelles il n'aurait pas pu accéder, de positionner le produit dans des modes de fonctionnement non autorisés voire de le bloquer.

4.3 Attaque en relais [2,3]

L'objectif de cette attaque est de faire en sorte qu'un lecteur et qu'un produit très éloigné l'un de l'autre puissent communiquer entre eux. Pour cela leurs signaux respectifs (commandes et réponses) doivent être relayés sur la distance qui les sépare. Pour ce faire, l'attaquant doit disposer de deux équipements dont l'un va être présenté face au lecteur et un autre à proximité du produit dont on souhaite relayer les réponses au lecteur. Entre ces deux équipements un moyen de communication

de type radio fréquence doit être mis en place de manière à ce que l'équipement se trouvant devant le lecteur puisse communiquer avec celui à proximité du produit. Réciproquement l'équipement à proximité du produit doit pouvoir récupérer et comprendre la réponse de ce dernier afin de les relayer à l'équipement qui se trouve en face du lecteur afin que cet équipement puisse fournir au lecteur les réponses données par le produit.

Une variante de cette menace ne nécessite qu'un seul équipement doté des deux « interfaces ». En effet imaginons une file de paiement devant une caisse. Une personne munie d'un équipement dissimulé dans son sac à dos, présente face au lecteur une fausse carte de paiement qui est en fait reliée (par fil ou non) à l'équipement présent dans le sac à dos. Cet équipement dispose d'une antenne suffisamment importante pour dialoguer avec la carte de paiement de la personne suivante dans la file. L'attaquant peut alors utiliser la carte d'une victime pour payer ses achats.

Dans un tel scénario la puissance de l'attaque vient du fait que c'est un vrai produit qui répond à un vrai lecteur. Tous les mécanismes de sécurité reposant sur une communication sécurisée (*secure channel*, *secure messaging*...) sont inefficaces contre une telle attaque. Pour s'en prémunir, il faut empêcher une transaction à l'insu du porteur. En effet ce scénario ne nécessite pas d'action de la part du porteur et peut donc être réalisé sans son assentiment. Pour limiter toutes les communications indues sur un produit, l'application doit donc introduire un mécanisme impliquant soit une action de la part du porteur soit la présentation d'un élément connu de lui seul tel qu'un code secret.

5 État de l'art des solutions

Tous les problèmes cités précédemment sont difficiles à résoudre, car une carte sans contact est conçue pour répondre automatiquement à toute sollicitation d'un lecteur sans contact, a priori sans action particulière du porteur.

Le PIN code ou les authentifications par biométrie, en plus d'authentifier le porteur de la carte, sont des moyens classiques pour matérialiser la volonté de l'utilisateur de déverrouiller sa carte et d'effectuer une transaction. Mais, comme on l'a vu plus haut, cette solution est très sensible aux attaques par déni de service et à de nouvelles formes d'attaques exhaustives, et doit donc être combinée avec d'autres solutions d'actes volontaires.

De telles solutions existent mais elles imposent certaines contraintes ergonomiques :

- Étui de blindage ou cage de Faraday : pour éviter qu'une carte réponde à une sollicitation il est possible d'utiliser un portefeuille en métal pour créer une cage de Faraday autour de la carte. Mais l'utilisateur devra alors sortir la carte de son portefeuille et perdra ainsi les avantages du sans contact.
- Bouton poussoir : la carte peut être munie d'un bouton poussoir ou être équipée d'un capteur biométrique qui permettrait en plus d'identifier l'utilisateur. Pour des problèmes de coûts de revient de la carte, ces solutions ne sont pas idéales.
- Solution retenue pour le passeport électronique (ICAO) : la solution BAC (*Basic Access Control*) consiste à lire une donnée écrite physiquement sur la carte dans une zone prédéfinie (MRZ - *Machine Readable Zone*) qui sert ensuite de code d'accès aux données sensibles de la carte. Cette méthode présente l'inconvénient de devoir présenter sa carte à un système de lecture avant de pouvoir s'en servir mais réintroduit en revanche la notion d'acte volontaire de la part du porteur, tout en protégeant son intimité.

Ces systèmes présentent l'avantage de bloquer toute communication avec la carte sans action du porteur sur celle-ci, l'inconvénient étant que le porteur doit prendre la carte à la main pour initier toute communication, annulant ainsi la convivialité liée à l'utilisation du sans contact.

6 Nouvelles solutions

Devant les menaces importantes des attaques citées à la section 4, et les limitations importantes des solutions actuellement disponibles nous avons envisagé trois solutions nouvelles.

6.1 Capteur d'environnement

Cette solution s'appuie sur l'observation du fait qu'une carte utilisée de manière licite est normalement située à proximité du lecteur avec lequel elle doit dialoguer.

Cette condition d'utilisation implique que le lecteur et la carte soient dans le même environnement, et notamment dans le même environnement naturel.

Or, cet environnement peut être décrit par des paramètres physiques tels que la lumière, la température, l'humidité, etc. Il peut également être défini par un paramètre tel que le mouvement des objets qui sont mis en présence l'un de l'autre.

Un ou plusieurs capteurs d'environnement de même type peuvent ainsi être prévus sur la carte et le lecteur pour mesurer de manière simultanée ces paramètres. Avant tout échange de données sensibles entre la carte et le lecteur, les deux parties vérifient que les valeurs des paramètres mesurés sont identiques du coté de la carte et du côté du lecteur.

Afin de ne pas pouvoir être falsifiées, ces valeurs seront échangées et comparées après la mise en place d'un schéma de communication sécurisé.

Du côté du lecteur, il est très facile d'utiliser des capteurs existants. Du coté de la carte, pour respecter les contraintes de formes et de coût la sélection de capteurs pourra être un peu plus délicate. Cependant la progression des micro et nanocapteurs fait que des solutions économiquement viables seront disponibles rapidement.

Il est possible par ailleurs d'adapter les capteurs utilisés à l'application. Par exemple une application où le maintien physique de la carte par le porteur est requis pour plus de sécurité pourra utiliser un capteur de lumière, un capteur de température, ou les deux en combinaison.

En revanche si l'application permet que la carte reste dans un portefeuille, alors un capteur de mouvement sera plus adapté, le lecteur mesurant le mouvement de l'objet qui lui est présenté (par exemple avec une caméra) et la carte mesurant son mouvement propre (par exemple avec un accéléromètre). Si les deux sont en face l'un de l'autre, alors les mesures devraient donner la même valeur. Des combinaisons plus complexes entre les valeurs des capteurs sont tout à fait envisageables.

Dans un mode de réalisation plus élaboré, offrant une sécurisation supérieure, on peut prévoir que le lecteur puisse influencer son environnement immédiat et, en l'occurrence, pour reprendre un exemple précédent la température et la lumière dans cet environnement. On peut ainsi créer artificiellement une différence d'environnement même entre des points très proches. On peut ainsi éviter les attaques dans une file d'attente décrit plus haut qu'une mesure simple ne pourait éviter car il est probable que les contions environnementales seront stable dans une file d'attente.

Même si un attaquant peut mesurer et transmettre les paramètres d'environnement modifiés ou non par le lecteur, il lui sera très difficile d'influer sur l'environnement immédiat de la carte sans que cela soit remarqué par son porteur. Si ma carte est dans ma poche, comment l'éclairer, la chauffer ou la faire vibrer sans que je ne m'en rende compte ?

En résumé, une transaction entre une carte et un lecteur peut se dérouler selon le schéma suivant :

- émission d'un champ électromagnétique par le lecteur ;
- interrogation pour détecter la présence d'une carte ;

- détection de la présence d'une carte et sélection de la carte ;
- mesure d'un ou plusieurs paramètres physiques par les capteurs de la carte et du lecteur ;
- mise en place d'un canal de communication sécurisé entre le lecteur et la carte ;
- échange des signaux de mesure issus des capteurs à travers le canal sécurisé ;
- comparaison des valeurs de ces signaux ;
- poursuite de la communication entre le lecteur et la carte si la comparaison conduit à conclure que le lecteur et la carte sont dans le même environnement et interruption de la communication dans le cas contraire.

La variété des capteurs susceptibles d'être développés sur silicium est telle que le choix de ces capteurs pourra être établi en prenant en compte l'application envisagée et non l'inverse. En d'autres termes, le gain de sécurité apporté par l'invention sera dépourvu de tout effet négatif sur l'ergonomie, et cette sécurité supplémentaire pourra être facilement apportée à toute application existante.

De plus, la gamme des capteurs utilisables est suffisamment vaste pour qu'il soit possible, dans chaque cas, de trouver des capteurs permettant d'éviter à l'utilisateur de manipuler sa carte pour la rendre opérationnelle ou pour interdire son utilisation.

Bien sûr, de par l'imperfection des mesures, des seuils devront être calibrés pour prendre la décision de poursuivre ou non une transaction avec un compromis à trouver entre le taux de faux positifs et celui de faux négatifs.

L'inconvénient principal de cette solution est qu'elle amène à renouveler à la fois le parc des cartes et celui des lecteurs et surtout les protocoles de communication. Dans les solutions suivantes nous nous sommes attachés à trouver des solutions transparentes du point de vue des lecteurs et du protocole.

6.2 Déblocage de la carte par l'utilisateur

Le problème qui nous préoccupe est de s'assurer que le propriétaire de la carte a la volonté d'effectuer une transaction et que la carte n'est pas activée à son insu. Une autre solution est donc que la carte ne communique avec l'extérieur que si elle est débloquée par son propriétaire. Au lieu de la débloquer en l'extrayant d'un étui métallique ou en présentant un code personnel, l'idée est ici de faire varier l'état d'un ou plusieurs capteurs embarqués sur la carte sans contact d'une manière convenue, et dans des proportions convenues.

Le capteur de la carte sans contact est capable de mesurer une variation de l'état de celle-ci. Lors d'une éventuelle sollicitation de la carte, celle-ci n'acceptera d'établir une connexion, que si le processeur considère que la valeur relevée par le capteur, et la valeur de référence stockée dans la mémoire sont suffisamment similaire.

L'implémentation la plus naturelle semble être un accéléromètre permettant de détecter un mouvement et de le comparer à un mouvement de référence choisi par l'utilisateur et stocké à bord de la carte (par exemple un déplacement horizontal de la carte de gauche à droite, suivi immédiatement d'un déplacement horizontal de la carte de droite à gauche). Ainsi, si la carte est sollicitée par un lecteur à l'insu de son propriétaire (dans les transports en commun par exemple), il est particulièrement improbable que la carte réalise naturellement, et à ce moment-là, le mouvement de référence.

Le comportement attendu par la carte peut être secret. Dans ce cas là, on apporte, en plus de la preuve de l'intention de la transaction, une authentification du porteur. En effet, selon la complexité retenue du comportement, cette solution permet de recréer, en mode sans contact, un système proche de celui du code d'identification (dit PIN code) couramment utilisé en mode contact.

D'autres capteurs peuvent également être imaginés comme des capteurs de torsion.

Encore une fois, de par l'imprécision des mesures, le résultat de la comparaison des mesures et des valeurs de référence ne sera pas binaire mais sera un indice de similitude. On pourra calibrer un seuil d'acceptation résultant d'un compromis entre sécurité et confort d'utilisation. Ce seuil peut également être variable, par exemple, en tenant compte de l'intensité du signal électromagnétique, de son amplitude, etc. Ainsi, pour une tentative de connexion avec un signal particulièrement faible ou très fluctuant, ce qui peut faire penser à des conditions d'une tentative de fraude, le seuil pourra être très élevé, alors que lors d'une tentative de connexion avec un signal fort et stable le seuil d'acceptation pourrait être plus faible.

Cette solution, plus simple, a l'avantage de ne demander aucune modification des protocoles applicatifs ou des lecteurs. L'inconvénient est d'impliquer l'utilisateur qui devra être formé à l'utilisation de sa carte.

Pour éviter ce dernier inconvénient sans se priver de ses avantages, la solution suivante a été imaginée. Elle consiste à remplacer l'action de l'homme par celui d'un objet.

6.3 Déblocage de la carte par un autre objet sans contact

Pour éviter à l'utilisateur de mémoriser et reproduire un geste, une torsion de la carte ou autre, on peut déléguer l'activation de la carte sans contact à un autre objet que l'utilisateur porte en permanence et qui se trouvera très proche de la carte lors de son utilisation. On peut penser naturellement à une montre ou une bague. Une deuxième communication sans contact sera alors établie entre la carte et l'objet (avec authentification). En son absence la carte restera bloquée.

La portée des communications sans contact entre la carte et l'objet d'activation devra être réglée précisément de telle sorte que la carte soit active dans la main de l'utilisateur et bloquée, même portée sur lui.

Autre problème, une double attaque en relais reste possible quoique plus complexe. L'attaquant devra alors monter un relais entre l'objet d'activation et la carte ainsi qu'un deuxième entre la carte et le lecteur.

7 Conclusion

On l'a vu, l'activation de la carte à l'insu du porteur est une condition nécessaire pour un grand nombre d'attaques : effectuer des transactions frauduleuses avec une attaque en relais, suivre les déplacements d'une personnse, faire du déni de service... Le fait d'empêcher cette activation si le porteur n'est pas consentant protège contre la plupart des attaques spécifiques au sans contact.

Les différents types de protection peuvent avoir des impacts plus ou moins importants sur l'application et sur son déploiement : impact sur les équipements (les lecteurs par exemple), impact sur l'ergonomie d'utilisation (taper un code PIN ou non, sortir la carte du portefeuille ou non, réaliser un geste complexe), impact sur le temps de transaction (ce temps étant particulièrement critique pour certaines applications comme le transport par exemple).

Pour une application donnée, il faut mettre en perspective l'ensemble des contraintes et voir si elles sont acceptables. Par exemple, dans une application le passeport électronique pour laquelle le niveau de sécurité requis est important vis-à-vis du *tracking* ou de l'attaque en relais, on pourra accepter de modifier les lecteurs et de sortir son passeport du portefeuille pour mettre en place la solution BAC (il y a de toute façon une obligation de présenter le passeport au douanier). Ces contraintes ne vont pas être acceptables en revanche pour d'autres applications où les lecteurs

doivent pouvoir dialoguer avec la carte alors qu'elle est encore dans le portefeuille. Pour une application donnée, il sera donc nécessaire de faire une analyse de risques et de choisir le meilleur compromis par rapport au niveau de sécurité visé.

Références

1. Stephen C. Bono, Matthew Green, Adam Stubblefield, Ari Juels, Aviel D. Rubin, and Michael Szydlo. Security analysis of a cryptographically-enabled rfid device. In *SSYM'05 : Proceedings of the 14th conference on USENIX Security Symposium*, pages 1–1, Berkeley, CA, USA, 2005. USENIX Association.
2. Gerhard Hancke. A practical relay attack on iso 14443 proximity cards. `http://www.cl.cam.ac.uk/~gh275/relay.pdf`, February 2005.
3. Gerhard P. Hancke. Practical attacks on proximity identification systems (short paper). *sp*, 0 :328–333, 2006.
4. Ari Juels, David Molnar, and David Wagner. Security and privacy issues in e-passports. *securecomm*, 0 :74–88, 2005.
5. Ziv Kfir and Avishai Wool. Picking virtual pockets using relay attacks on contactless smartcard. *securecomm*, 0 :47–58, 2005.
6. Ilan Kirschenbaum and Avishai Wool. How to build a low-cost, extended-range rfid skimmer. In *USENIX-SS'06 : Proceedings of the 15th conference on USENIX Security Symposium*, pages 4–4, Berkeley, CA, USA, 2006. USENIX Association.