Les cartes de paiement interactives – La technologie HCE

APAPOULLE Théodore – BOUABID Mohammed – CHATIRON Thibault – JEMBA KOUM Adrien

***Abstract*— Ce projet de recherche est consacré aux cartes de paiements interactives. Il explique son mode de fonctionnement, la technologie utilisée ainsi que des failles de sécurité. Pour se protéger et se prémunir des attaques, plusieurs parades ont été proposés. Plusieurs entreprises ont proposés des solutions innovantes pour répondre aux attentes de sécurité de NFC qui sont abordés dans le rapport.**

I- Introduction

La cybercriminalité devient une activité de plus en plus professionnelle et commerciale, avec des groupes criminels organisés à travers le monde qui s'attachent à déployer des attaques en ligne ciblées, élaborées et rentables. Et l'intention n'est plus simplement de nuire à une image de marque, mais de réellement gagner de l'argent. Les cartes de paiement sont l'un des business des cybers délinquants.
Tout au long de ce rapport, nous allons nous concentrer sur les cartes de paiements interactives à travers ses principes de fonctionnement, la technologie utilisée en l'occurrence le NFC ainsi que les vulnérabilités, les attaques et les parades concernant cette technologie. Ensuite, nous étudierons une alternative à la technologie NFC : la technologie HCE.

II- Les cartes de paiement interactives

a- Notion de carte de paiement

Une carte de paiement est un objet plastique rectangulaire permettant d'effectuer des transactions financières. Elle fait partie de la famille des cartes à puce car elle est équipée d'un circuit intégré, la puce, permettant de stocker des informations et dans certains cas d'effectuer des opérations. Les cartes à puce sont principalement utilisées comme moyen d'identification personnelle (carte d'identité, badge d'accès aux bâtiments, carte d'assurance maladie, carte SIM) ou preuve d'abonnement à des services prépayés (carte de téléphone, titre de transport) ou dans notre cas, comme moyen de paiement (carte bancaire). Une carte de paiement est donc une carte à puce permettant d'effectuer des achats chez des commerçants en utilisant un code PIN ou encore d'acheter ses produits sur internet en renseignant le numéro de la carte et son cryptogramme.

b- Notion de carte de paiement interactive

Une carte de paiement interactive (aussi appelée carte de paiement sans contact) a les mêmes possibilités qu'une carte de paiement. Elle permet, en plus, d'utiliser la méthode de paiement sans contact. Le caractère interactif de la carte réside dans le fait que les deux objets, le terminal et la carte, dialoguent ensemble sans l'intervention d'une personne tierce pour effectuer la transaction. Cette carte peut être à la fois une carte plastique (carte bancaire) ou par abus de langage un Smartphone. Une carte de paiement sans contact est reconnaissable par la présence du sigle  sur le recto de la carte et un commerçant qui accepte les cartes bancaires sans contact dispose généralement du sigle  . En ce qui concerne les Smartphones, il faut que celui-ci ainsi que leur carte SIM soient compatibles avec la technologie NFC (Near Field Communication).

Pour que la communication puisse s'établir, la carte de paiement interactive doit être à une distance maximale de 10 cm du terminal. En effet ces derniers utilisent la technologie NFC qui fait partie de la famille des RFID *(Radio Frequency Identification)*. Le fonctionnement de cette technologie sera expliqué par la suite.

Figure 1 : Carte sans contact en utilisant la carte ou le smartphone

Dans une carte de paiement sous format plastique, interactive ou non, c'est la puce qui contient les informations bancaires. Avant l'arrivée des technologies de paiement sans fil, l'accès aux informations de cette puce par le lecteur du vendeur se faisait uniquement par contact direct. Les contacts de la puce sont reliés à ce qu'on appelle le micromodule. Le micromodule est le circuit imprimé que l'on voit à la surface de la carte et que l'on considère généralement à tord comme étant la puce elle même. Lors de l'insertion de la carte dans le lecteur, les contacts du lecteur viennent s'apposer sur le micromodule.
Avec l'arrivée du paiement sans contact, les cartes bancaires offrant ce service sont munies d'une antenne qui est directement reliée à la puce. En ce qui concerne les Smartphones, ils intègrent en plus de leur antenne de communication, une nouvelle antenne dédiée aux communications NFC qui est reliée à la carte SIM qui à la même fonction que la puce dans une carte bancaire. La communication entre le terminal et la carte ou le Smartphone se fait alors en onde radio. Le lecteur est l'initiateur de la communication et l'onde émise permet d'une part

d'interroger la carte et d'autre part de lui fournir l'énergie nécessaire pour pouvoir répondre.

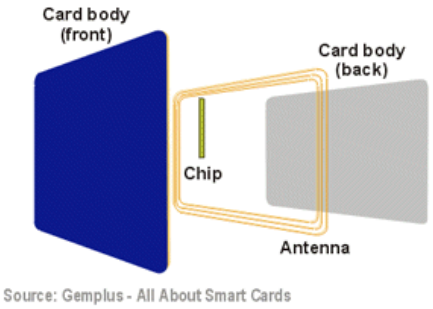
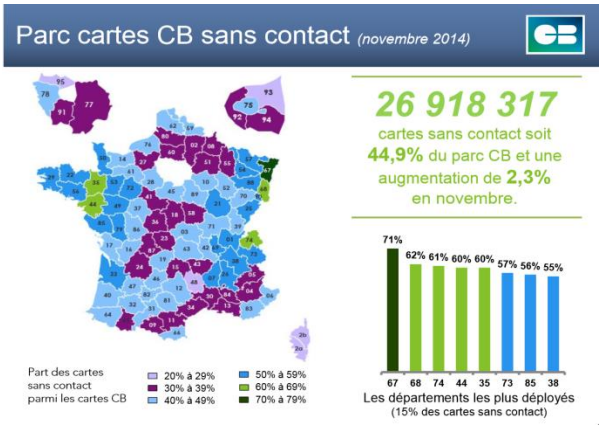


Figure 2 : La composition d'une carte de paiement interactive

c. Déploiement de la carte sans contact

En 2013 en France, les Membres CB qui sont des établissements autorisés à fournir des services de paiement conformément aux textes en vigueur, ont entrepris une campagne collective pour promouvoir le paiement sans contact. Ils ont d'abord entrepris en octobre 2013 la sensibilisation des professionnelles au paiement sans contact pour ensuite en février 2014 commencer la publicité au près du grand publique à travers la presse, internet et la télévision. En novembre 2014, la barre des 8 millions de transactions sans contact a été dépassée pour un montant de 94.2 millions d'euros. Voici ci-dessous deux cartes représentant le déploiement du paiement sans contact en France



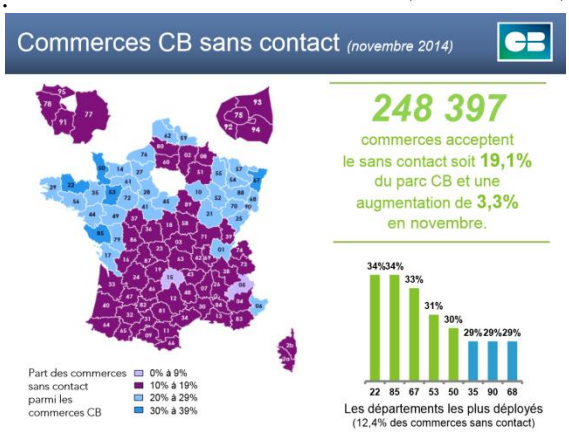


Figure 3 : Déploiement de la carte sans contact en France

III- La technologie RFID

a. Principe

RFID est une technologie d'identification automatique permettant de mémoriser et récupérer des données des objets à distance, en utilisant des tags radiofréquence appelés « radio-étiquettes ». Radio-étiquettes ou tag RFID sont des dispositifs récepteurs placés sur l'élément à identifier (objets, animal, carte…). Ils sont composés d'une puce reliée à une antenne (voir la figure 4).

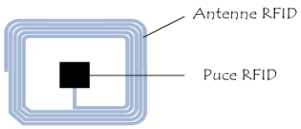


Figure 4 : La composition d'une radio- étiquettes

Cette technologie est basée sur les échanges de l'énergie électromagnétique afin de créer un système RFID composé en deux entités :

- Transpondeurs (radio-étiquettes, tag, identifiant) : son rôle est d'envoyer des informations aux coupleurs
- Coupleurs (interrogateurs, base station) : son rôle est de recevoir les informations émis par les transpondeurs.

Par exemple, quand on essaie de valider nos tickets lors de la monté au bus, le ticket contient un tag RFID qui se comporte comme un **Transpondeur,** et l'appareil de la validation est considéré comme un **Coupleur**

b. Types d'étiquettes

Pour exploiter les informations enregistrées dans une étiquette, il faut avoir un lecteur dédié qui permet d'alimenter l'étiquette en envoyant des ondes radio. Autrement dit activer la puce de l'étiquette, pour extraire les données enregistrées sur celle-ci. On peut distinguer différents types d'étiquettes :

- **Etiquettes passives (sans batterie) :** Elles ne contiennent aucune alimentation externe, elles dépendent de l'effet du signal électromagnétique émis par le lecteur afin d'alimenter leurs microcircuits. La distance de transmission est inférieure à mètre.

- **Etiquettes semi-passive :** Elles ressemblent aux cartes d'identification passive. Elles disposent d'une petite batterie pour des utilisations permanente pour que l'antenne puisse s'occuper d'autres taches, la réception des signaux par exemple.

- **Etiquettes active:** Elles permettent par rapport aux autres étiquettes d'effectuer la transmission et réception des signaux, notamment des fonctions de captage, de traitement des informations captées. Pour assurer tous ces fonctions, il faut une alimentation embarquée. Elles peuvent transmettre des signaux radio fréquences à centaines de mètres.

IV- La technologie NFC

a. Principe

La technologie NFC se popularise sur les Smartphones et les tablettes. Très proche du RFID dont elle tire une partie de ses spécifications, la technologie NFC permet pour le grand public toute une collection d'applications rendant l'expérience plus intéressante. Techniquement parlant, RFID et NFC sont deux domaines très riches que l'on peut adapter à des besoins spécifiques.
Le NFC se différencie du *Bluetooth* ou du WiFi par sa distance de fonctionnement limitée à quelques centimètres et son débit (106 à 424 Kbps). Elle est donc intrinsèquement adaptée aux transactions électroniques de proximité, par exemple, entre une carte et un lecteur.

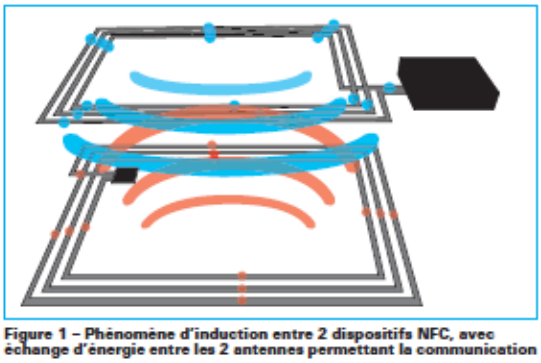


Figure 1 – Phénomène d'induction entre 2 dispositifs NFC, avec échange d'énergie entre les 2 antennes permettant la communication

Figure 1 : Phénomène d'induction entre 2 dispositifs NFC

RFID et NFC sont deux technologies très proches et similaires sur bien des points. NFC pour *Near Field Communication* est une norme définissant le même type de fonctionnalités et de technologies que RFID. Ces deux technologies ont des spécifications communes.

Dans le cas du NFC, on notera l'utilisation uniquement de tags passifs HF, à ceci s'ajoutent la communication peer-to-peer et l'émulation de tags qui permettra le partage de contenus via Android Beam et le paiement par smartphone. La différenciation entre RFID et NFC tient également dans le format des données stockées sur un tag : le NDEF (NFC Data Exchange Format) qui est un format binaire de messages permettant d'encapsuler des données pour une application.

Un tag NFC est un tag répondant aux standards ISO/IEC 14443 :
- ISO/IEC 14443-1 : caractéristiques physiques
- ISO/IEC 14443-2 : interface d'alimentation et de gestion de signaux par fréquence radio
- ISO/IEC 14443-3 : initialisation et anticollision
- ISO/IEC 14443-4 : protocole de transmission

Les trois modes de communication NFC :

- **Lecteur** : C'est une communication entre un dispositif NFC qui agit comme un lecteur et un transpondeur standard. Ce mode permet au lecteur d'échanger des informations avec le transpondeur.
- **Emulation** : C'est une communication entre un lecteur standard et un dispositif NFC vu par le lecteur comme un simple transpondeur. Ce mode peut être utilisé sur un téléphone portable pour intégrer des fonctions de paiement ou d'accès sécurisés.
- **Peer-to-Peer** : Il permet l'échange de données entre deux dispositifs NFC. Il peut être utilisé pour échanger des données entre plusieurs machines intelligentes dotées de la technologie NFC.

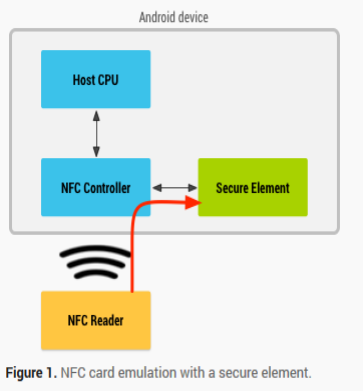


Figure 1. NFC card emulation with a secure element.

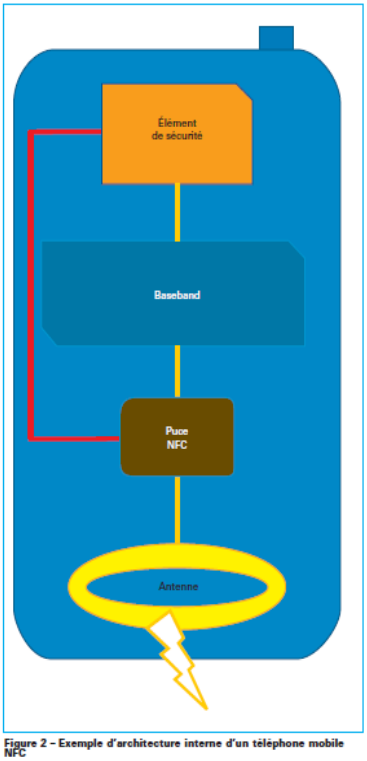


Figure 2 – Exemple d'architecture interne d'un téléphone mobile NFC

Figure 5: Architecture d'une carte NFC

On peut noter la possibilité d'émuler sa carte de paiement sur son Smartphone ou tablette. Mais comment cela fonctionne-t-il ? L'émulation de carte NFC est faite en utilisant un élément sécurisé (Carte SIM, micro-SD…), cette carte émulée est stockée dans l'élément sécurisé de l'appareil grâce à une application Android. Lorsque la carte émulée doit être lue, le contrôleur NFCdirige toutes les données du lecteur vers l'élément sécurisé (**cf Figure 5**).
L'élément sécurisé communique directement avec le terminal NFC (aucune application Android n'est impliquée dans la transaction). Une fois la transaction terminée, une application Android peut interroger l'élément sécurisé directement pour connaitre le statut de la transaction. A noter que l'élément de sécurité doit répondre à la certification EAL4+.

Dans l'application de paiement stockée dans une SIM, on retrouve :
- PAN (numéro de la carte à 16 chiffres), nom du porteur et date d'expiration ;
- code personnel ;
- clé secrète de la banque du client ;
- historique des transactions ;

- les compteurs cumulés de transaction, la limite à partir de laquelle la saisie du code personnel devient obligatoire (20 € en France).

Pour mettre en place le paiement en utilisant la technologie NFC, il faut mettre en place des éléments sur les différents acteurs :

- **L'émetteur :** La responsabilité principale est celle des émetteurs du moyen de paiement. Il existe plusieurs standards aux moyens de paiement :
  - EMV pour Europay Mastercard Visa
  - Nationaux (CB)
  - Paiement privatif (Accor, cofinoga…)

  L'application bancaire doit régulièrement procéder à une demande d'autorisation au serveur central, afin de remettre son compteur à zéro. Il est possible d'utiliser la connectivité du mobile NFC afin de gérer ce compteur de manière automatique à la seule condition que le mobile soit sous couverture réseau (car cette remise à zéro ne peut se faire au moment du paiement mobile NFC).

- **L'accepteur** :
  Pour le commerçant, les bénéfices sont :
  - la fluidité ;
  - moins de monnaie fiduciaire à gérer ;
  - la diminution de la fraude ;
  - l'image de marque de modernité.

  À savoir que le circuit de la transaction (échanges entre l'accepteuret l'acquéreur) reste exactement identique à celui actuellement en place pour les cartes.

- **L'acquéreur** : Il s'agit de l'organisme bancaire qui gère la transaction pour l'accepteur. Généralement, la banque du commerçant propose un TPE avec interface NFC. Ce TPE enregistre le montant et l'identification de la « carte bancaire virtuelle » stockée dans le mobile. Ce TPE transmet par télécollecte à la banque du commerçant tous les paiements enregistrés, CB et paiements mobiles. Les transactions de paiement mobile sont identiques aux transactions actuelles du point de vue serveurs bancaires. La demande d'autorisation de l'acquéreur auprès de l'émetteur n'est pas systématique, elle est gérée suivant le niveau de risque de la banque émettrice. Par exemple, l'émetteur peut laisser la possibilité à l'utilisateur de réaliser trois transactions en dessous de 20 € sans demande d'autorisation.

- **L'utilisateur** : L'utilisateur est client d'un émetteur/distributeur de moyens de paiement. Il peut avoir plusieurs moyens de paiement dans son mobile. L'utilisateur tire ainsi des bénéfices à travers le paiement mobile mais qu'en est-il de la vulnérabilité / sécurité du système ? Il faudra également être vigilant au respect de la vie privée, le mobile et le moyen de paiement étant deux objets personnels et sensibles.

b. Attaques & Bonnes pratiques

Nous remarquons que la plupart des systèmes ont montrés leurs limites tant au niveau technique qu'au niveau des protocoles de gestion utilisés. La sécurité des MifareClassic par exemple, a fait l'objet de travaux de recherche en sécurité et d'analyses qui ont conduit à la divulgation de certains problèmes de sécurité ainsi que la diffusion d'outils de tests. On notera par exemple, MFOC pour MifareClassic Offline Cracker qui permettra de découvrir l'ensemble des clés si une seule d'entre elles est connue.

Mais plus grave encore, c'est l'utilisation qui est faite de ces technologies qui reste le maillon faible car, la plupart du temps, les mécanismes de sécurité ne sont même pas utilisés.
En effet, reprenons l'exemple des MifareClassic qui ne respectent que partiellement le standard ISO 14443, puisqu'elles utilisent un protocole de sécurité propriétaire NXP (*CRYPTO1*) à la place du protocole de haut-niveau ISO 14443-4, et ne respectent pas le format de trames ISO 14443-3 dans les communications chiffrées. On notera que le protocole NXP utilisé pour l'authentification et le chiffrement a été cassé en 2008.

Tout système n'est pas sur à 100% et peut comporter des vulnérabilités que l'attaquant peut exploiter. La technologie NFC possède plusieurs vulnérabilités qui peuvent avoir un impact pour l'utilisateur lors du paiement d'une transaction.

i. Ecoute à distance

Cette attaque active consiste à venir activer et lire une carte sans le consentement de son propriétaire. Les difficultés rencontrées sont la téléalimentation de la carte et la récupération des données de la carte. Le principal objectif de cette attaque est la récupération des données contenues sur la carte, mais ses applications sont multiples (attaque replay, clonage, déni de service,...).
De plus, il est possible à l'aide d'une simple application disponible sur le Store telle que PayCardReader de :

- Collecter le numéro de la carte bancaire
- Collecter le nom du propriétaire de la carte
- Obtenir la date de fin de validité
- Connaitre les dernières transactions

-

Figure 2 : Collecte des informations via l'application NFC Credit Card Tool

On notera également que le code-source pour lire les données est accessible à l'adresse suivante : https://code.google.com/p/readnfccc/source/browse/trunk/readnfccc.c

Ainsi, tout le monde peut accéder aux données de votre carte bancaire s'il est équipé d'un smartphone avec technologie NFC ou même d'une clé USB NFC.

➢ ***Limite:***

En pratique, la lecture NFC peut se faire seulement sur 3 à 5 centimètres. Cependant, la distance peut être de 1,50 mètre si la lecture se fait avec un amplificateur et une antenne.

➢ ***Risques encourus :***

- Lire les données de la carte de la victime et l'utiliser sur des sites de commerce en ligne : CVV (Cryptogramme) pas toujours obligatoire et peut être forcée (seulement 1000 possibilités...)
- Attaque DoS (ex : envoyer 3 fois un mauvais code PIN)
- Créer une bande magnétique à distance (carte clone sera utile lorsque la carte à puce ou le code PIN n'est pas obligatoire : la plupart des pays de l'UE,USA,...)
- Identification de l'utilisateur et suivi

➢ ***Améliorations à apporter***

- Accès sans contact doit être authentifié pour éviter les fraudes
- Protocole sans contact doit être chiffré pour éviter les écoutes
- Intégrité de la session doit être protégée (par exemple HMAC) pour éviter une infiltration

On notera que ces améliorations existent déjà, notamment avec les cartes de transport « Navigo ». Donc, EMV est mal conçu pour la technologie NFC et a besoin d'une réécriture complète pour une meilleure sécurité.

➢ ***Conformités réglementaires***

- Le programme PCI DSS :

Les données de la carte bancaire (numéro de carte, date de fin de validité et les trois chiffres au dos de la carte) sont devenues sensibles car elles permettent de faire un paiement sur internet sans présence physique de la carte. Les fraudeurs cherchent à capturer ces numéros en attaquant les systèmes d'information des acteurs qui stockent ces données. Le programme PCI DSS vise à améliorer la sécurité physique et logique des systèmes d'information en demandant aux acteurs de respecter des bonnes pratiques de sécurité.

- Protection des données personnelles (CNIL)

➢ ***Protection :***

Il est possible de demander à sa banque de désactiver le service. Il existe des étuis en résine faisant office de cage de Faraday afin d'éviter la propagation et la détection des ondes.

ii. Attaque relais

Le principe de l'attaque relais est d'établir une communication non sollicitée entre un lecteur et une carte interactive. En effet, la plupart du temps la distance entre la carte sans contact et le lecteur est supérieure à la distance maximale de fonctionnement. La figure suivante montre le schéma d'attaque relais.

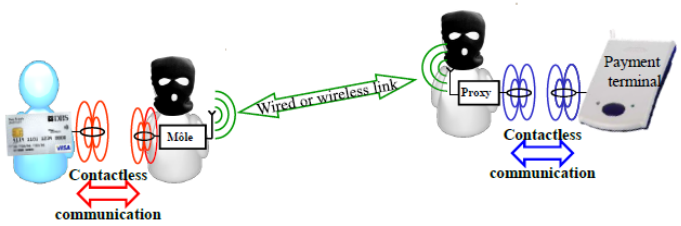


Figure 6 : Déroulement d'une attaque relais

Comme est indiqué sur la figure ci-dessus, le « môle » est placé près de la carte sans contact, il permet principalement de :

- Se comporter comme un véritable lecteur, afin de transmettre les signaux émis par le proxy à la carte
- Alimenter la carte
- Envoyer les réponses de la carte au proxy

Par ailleurs, le « proxy » est placé à proximité du lecteur, il assure deux fonctions :

- Envoie les requêtes du lecteur au « môle »
- L'envoie les réponses transmises via le « môle » d'une manière transparente au lecteur.

Pour augmenter la performance de l'attaque relais il faut améliorer la distance entre les éléments de l'attaque. En théorie, d'après un modèle de systèmes sans contact, la distance entre le proxy et le lecteur est de l'ordre de 50 m et de 50 cm entre la carte et le môle.

La figure suivante montre la première réalisation de l'attaque relais d'une distance de 50 m entre le lecteur et la carte sans contact.

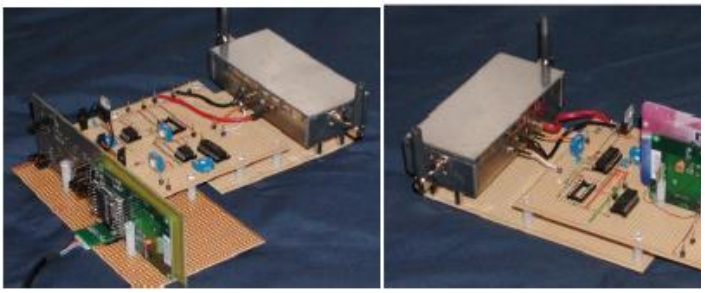


Figure 7 : Réalisation de l'attaque relais

Cette architecture d'attaque relais contient quelques faiblesses : La carte est placée sur le môle, ce qui ne sera pas possible lors d'une attaque réelle
Le retard engendré par le relais est supérieur à 15 microsecondes. Cette valeur peut être facilement mesurée par un système sans contact.

Scénario d'une attaque relais : Par le biais de l'attaque relais, l'attaquant peut payer ses achats en utilisant la carte sans contact d'une victime qui se trouve dans le périmètre de l'attaque relais, en effet l'attaquant place le proxy près du terminal de paiement. Quant à son complice, il dirige le môle à coté de la victime. Dans ce cas le vrai terminal communique avec la carte sans contact sans le consentement de la victime.

iii. Effectuer des transactions sans le code PIN

Les banques pour soi disant sécuriser le paiement sans contact, ont mis au point un plafond imposée pour les transactions : 20 € et une limite du nombre de paiements sans contact réalisables à la suite.
Une fois la limite dépassée, le porteur doit s'authentifier de manière traditionnelle avant de pouvoir effecteur des paiements sans contact. Récemment, des chercheurs britanniques ont démontré qu'il est possible de se faire prendre de l'argent avec les cartes bancaires NFC via une vulnérabilité qui serait présente au sein du protocole NFC. Les chercheurs ont détournées la limite. Le pirate passe simplement à cote de la cible, sans aucun contact et sans connaitre le code pour ainsi prendre de l'argent voire même vider le compte bancaire de la cible, des paiements pouvant atteindre la somme de 999 999,99 dollars.

Voici sur la figure ci-dessous, les différentes étapes de l'attaque :

Figure 8 : Implémentation de l'attaque via une application Android

- Le pirate utilisant son mobile utilisant la technologie NFC effectue toutes les transactions frauduleuses d'une cible. Cela peut être effectué sans aucun contact, simplement en passant à coté de la cible. Quand le Smartphone arrive à proximité de la carte bancaire sans contact, le pirate peut générer une transaction sans que le porteur ne s'en rende compte. En effet, les transactions sans contact ne nécessitent pas de code PIN pour être validées.
  Cette transaction est certes créée, mais pas encore envoyée à la banque. Elle est d'abord stockée dans le terminal. C'est possible car le standard EMV autorise les transactions en mode *offline*. Le pirate peut effectuer tranquillement des transactions auprès de ses victimes.
  (Voir Figure Etape 1 à 3).

  Le pirate va se concentrer sur la récupération des fonds. Il va décharger ces transactions sur n'importe quel système de paiement d'un marchand complice (**Rogue Merchant's Bank**) affilié au réseau EMV, pour les envoyer ensuite aux banques des victimes (**Victim's Bank**). Il suffit pour cela d'ajouter aux transactions stockées les données relatives à ce marchand. Cela est possible car, dans le standard EMV, les données du marchand ne font pas partie du sceau de validation cryptographique créée par la carte bancaire. (Voir Figure Etape 4 à 10).

En résumé, le pirate peut donc générer des transactions puis, dans un second temps, choisir le marchand auprès de qui il souhaite encaisser le pactole.

Pour implémenter l'attaque, les chercheurs ont développé une application qui simule un terminal de paiement et l'ont installée sur un Google Nexus 5. Cette application permet d'effectuer les transactions d'une carte. Ensuite il récupère les transactions effectuées. Les transactions sont stockées dans le téléphone avec l'OS Android pour être transmis au marchant complice appartenant au réseau EMV utilisant l'application.

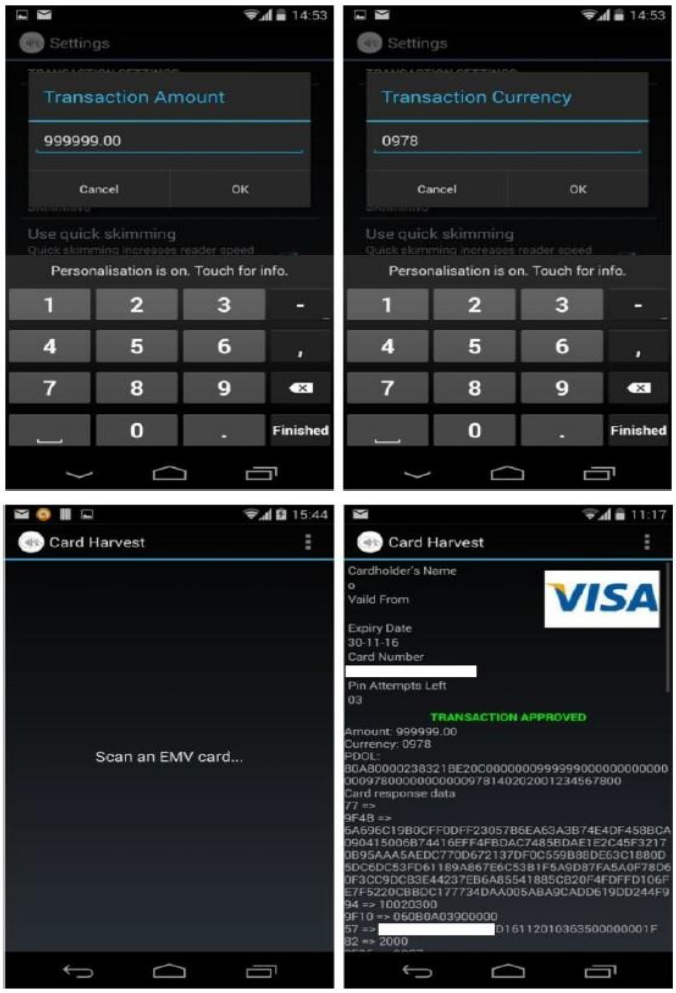


Figure 9 : Implémentation de l'attaque via une application Android

Contre-mesures

Utiliser des porte-cartes permet de protéger votre carte bancaire NFC contre toute tentative d'intrusion selon la même technique que la cage de Faraday protège les véhicules de la foudre.

c. Bonnes pratiques en général

Il existe trois solutions pour l'utilisateur concernant la sécurité des cartes de paiement NFC:

- Insister auprès de la banque pour obtenir une carte sans puce NFC.

D'après la CNIL, « les porteurs de carte doivent être clairement informés de la fonctionnalité sans contact et doivent pouvoir la refuser, soit en obtenant une carte ne disposant pas de cette fonctionnalité, soit en obtenant sa désactivation par leur banque. » [Source : CNIL]

- Ranger la carte dans un étui qui bloque l'émission des ondes.
- Neutraliser la puce NFC intégrée. C'est une méthode qui comporte des risques.

Méthode : « Pour cela, mettez-vous dans le noir, et plaquez une lampe torche sur votre carte afin de localiser l'emplacement de la bobine NFC. Marquez alors un point au crayon sur cette bande, en prenant soin de ne pas tomber sur la bande magnétique.

Coincez la carte pour qu'elle ne bouge pas et avec un cutter, un petit foret, ou un petit tournevis, commencez à percer un trou de 1 mm de diamètre environ. En y allant doucement, vous ne serez pas obligé de transpercer la carte. Si c'est le cas, ce n'est pas grave, mais vous pouvez juste creuser assez pour voir alors les connecteurs NFC et couper la boucle afin de rendre la puce inactive. Après vous pouvez reboucher le trou avec ce que vous avez découpé et passer un coup de feutre de couleur pour cacher la misère. Vous ne bénéficiez plus du paiement sans contact !» [Source : site Korben]

V- La technologie HCE

Le déploiement de solutions de paiement mobile NFC soulève des interrogations, en particulier concernant la sécurité des données et transactions. La technologie HCE va permettre de répondre aux critères de sécurité.

a. Principe

Le HCE nommée Host Card Emulation (HCE) est une technologie d'émulation de carte par une application mobile dans un smartphone NFC. Cette technologie a été développée par Google pour Android 4.4 (KitKat) et ultérieur.

A l'inverse de NFC utilisant le modèle « SIM-centric », HCE ne nécessite pas l'utilisation dans le mobile d'un Secure Element (SE) pour héberger les données sensibles de l'application de paiement.
La technologie HCE va router une communication NFC comme par exemple une transaction de paiement sans contact, directement du composant NFC vers une application installée dans le mobile et supportant les commandes applicatives échangées (ex. une application bancaire) (Figure 2)

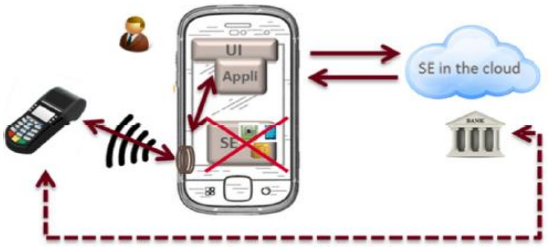


Figure 2 : Exemple – Cas d'application de la technologie HCE sans Secure Element

Le service HCE offre plus de flexibilité pour l'hébergement des données sensibles associées à l'application bancaire :
1. Dans l'application bancaire elle-même,
2. Dans un Secure Element,
3. Dans un environnement sécurisé du mobile,
4. Dans le Cloud (solution appelée « SE in the Cloud »

i. Scénario d'un paiement utilisant la solution « SE in the Cloud »

En février 2014, Visa a publié une implémentation de solutions de paiement mobile NFC n'utilisant pas de SE embarqué dans le mobile. Cette implémentation utilisant le HCE avec le « SE in the Cloud ».

Dans le cas d'une solution HCE « SE in the Cloud », le paiement tient compte de la couverture réseau selon l'environnement : soit en mode connecté, soit en mode non-connecté.
En mode connecté, la transaction s'exécute de façon synchronisée avec le serveur « SE in the Cloud ». Les données nécessaires pour réaliser une transaction EMV sont récupérées en temps réel depuis le serveur Cloud.
En mode non connecté, on récupère les données transactionnelles EMV (réalisée en mode connecté, Figure 6). Ces données sont chargées sur le mobile. Ensuite on réalise la transaction en utilisant ces données préalablement récupérées (réalisée en mode non-connecté, Figure 7). Ainsi, au moment de réaliser la transaction, les données transactionnelles (EMV) précédemment chargées sur le mobile sont utilisées, la couverture réseau n'est plus un prérequis

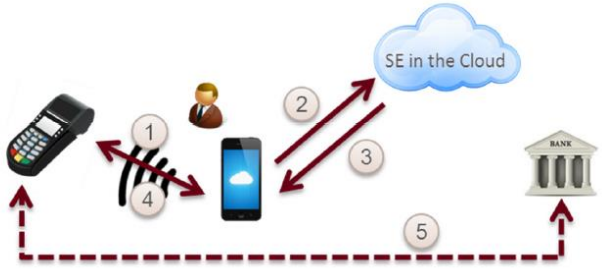


Figure 5 : Cinématique HCE « SE in the Cloud » - Paiement en mode connecté

Figure 6 : Cinématique HCE « SE in the Cloud » - Récupération des données de paiement

Figure 7 : Cinématique HCE « SE in the Cloud » - Paiement en mode non-connecté

ii. Scénario de paiement d'une solution « SE-based»

Pour implémenter une architecture HCE, il existe plusieurs solutions cités à la section précédente dont en particulier celle qui consiste à utiliser un SE pour stocker les données sensibles de l'application de paiement NFC.
Ce scénario permet de conserver un scénario de paiement plus « classique » sans avoir à considérer un fonctionnement en mode connecté ou non-connecté puisque le mobile dispose en local de tous les objets nécessaires pour réaliser une transaction (application, données, clés cryptographiques).

Le service Apple Pay du système iOS permet de réaliser une transaction de paiement NFC « SE-based » c'est-à-dire qu'il s'appuie sur les données de l'application de paiement NFC et les fonctions cryptographiques hébergés dans le SE pour dérouler la transaction. Les échanges NFC sont routés directement vers le « host » qui pilote la transaction. Le service Apple Pay ressemble à une architecture de type HCE « SE-based » cloisonnée.

iii. Processus de tokenisation

La mise en oeuvre d'un mécanisme de tokenisation est envisagée pour des questions de sécurité dans la mise en oeuvre de la technologie HCE.

Figure 8 : Processus de tokenisation et de dé-tokenisation par un TSP

La carte bancaire se caractérise par un PAN (Primary Account Number). Le tokenisation remplace le PAN par un Payment Token (rôle du Token Service Provider - TSP, qui garde le même format et les mêmes propriétés qu'un PAN classique.
Ceci permet de réaliser des paiements sans contact sans avoir à utiliser directement les données de la carte elle-même lors de la transaction sans contact et de protéger les données sensibles nécessaires au paiement contre les fraudes. La tokenisation est la pièce centrale de l'architecture de sécurité de paiement mobile de proximité.

Etudions le cas d'une transaction sans token afin de comprendre son importance dans le paiement.

Cas d'une transaction utilisant la technologie HCE « SE in the cloud » sans token :

1. Le consommateur s'enregistre et acquière les données de la carte soit à travers l'application bancaire ou utilisant le site Internet de la banque.
2. Au moment du paiement, le consommateur s'authentifie par le cloud (Utilisant les données de l'application bancaire). Le consommateur sélectionne la carte à utiliser pour payer à partir de son application mobile
3. Le données de la carte sont envoyées au mobile du consommateur pour initier la transaction. L'appareil transmet les données de paiement au marchand utilisant NFC.

Cette solution n'est pas très sécurisée. Les données de la carte peuvent être exposées à une attaque comme par exemple un malware résidant dans l'appareil qui collecte les données.

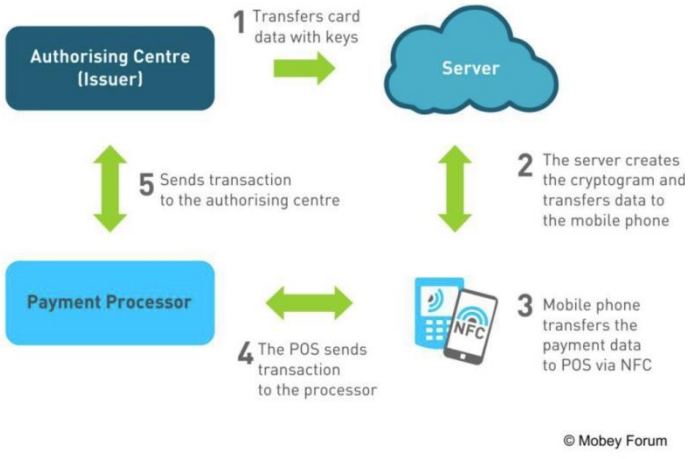


Figure 3: Transaction Flow in a Full Cloud Based HCE Solution

Cas d'une transaction utilisant la technologie HCE « SE in the Cloud » avec token :

1. L'émetteur offrant l'application mobile de paiement guide le consommateur à travers un processus d'inscription avec de fortes méthodes d'authentification. Puis le consommateur télécharger l'application de paiement. Donc L'authentification de l'utilisateur s'effectue en amont lorsqu'il télécharge et installe l'application fournie par sa banque qui lui envoie alors, en parallèle (par SMS par exemple), un code d'activation du service.

2. Les jetons sont pré chargés sur le téléphone, ainsi l'utilisateur n'a pas besoin de connexion data pour effectuer un achat. Les tokens peuvent être limités Cela dépend des règles définis par l'émetteur. Un token peut servir à une transaction ou à plusieurs, avec une durée de vie de quelques secondes à plusieurs jours.
   Par exemple, les tokens peuvent être :
   - Valide seulement pour les transactions ne dépassant pas un plafond
   - Limité l'utilisation : une seule utilisation (après un nouveau token doit être provisionné au mobile)
   - Valide seulement dans un temps limité
   - Valide seulement pour les transactions de paiements sans contacts
   - Valide seulement pour un certain commerçant.

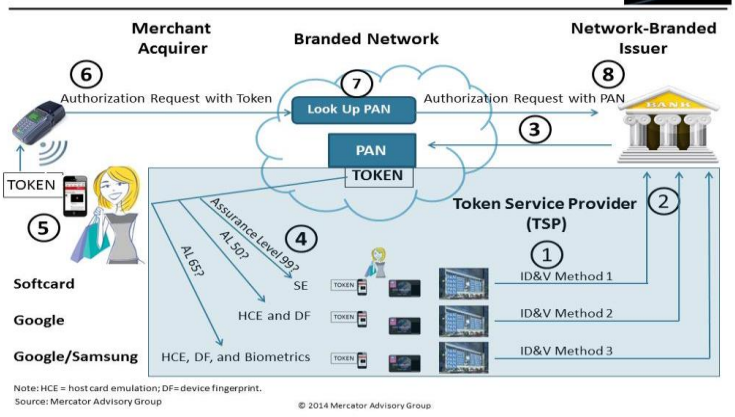
   La provision de tokens de paiement est livrée en avance, avant les transactions de paiement afin d'éviter les temps de latences. De plus, la provision de paiement demande au mobile d'être connecté. Donc pour recharger le lot de jetons, il faut que le mobile soit connecté au réseau mobile de son opérateur ou en Wi-Fi.

3. Au moment du paiement, l'application mobile de paiement du consommateur fournit le token de paiement au POS du marchant en utilisant la technologie NFC. Le consommateur peut probablement entrer un code PIN

4. Le commerçant route la transaction à l'acheteur et la transaction est reçu par la banque pour l'autorisation. La banque autorise la transaction après avoir vérifié, comparer le token avec le PAN de l'acheteur. La banque pour valider, ou non, la transaction. La banque aura la possibilité de tuer les token en temps réel alors qu'il faut une semaine en général à l'utilisateur pour s'opposer à l'usage de sa carte physique. On peut mettre en place un système de signatures pour la vérification de l'acheteur. Par exemple, la carte de paiement émulée dans le téléphone peut émettre une signature chiffrée qui valide la transaction à caractère unique.

Notons que cette solution a besoin de savoir comment sécuriser la livraison de provision de tokens de paiement au mobile. La communication doit être chiffrée entre le téléphone et la plate-forme.

Figure 4: A Network-Branded HCE Implementation of the EMVCo Tokenisation Standard



La solution ne réduit pas l'exposition des données sensibles à un malware dans l'appareil mais réduit l'impact d'éventuelles expositions en remplacement le PAN par un token. Dans le cas

ou les données sont stockées dans le cloud, les données sont transformées en token par le TSP (Token Service Provider) pour valider les transactions sur le terminal mobile. Si le pirate avec une attaque Man in the Middle, arrive à prendre le token, il ne pourra pas faire la correspondance avec le PAN. Le risque de malware est haut si l'appareil est jailbreaké.

VI- Conclusion

Le paiement sans contact se répand déjà en France, utilisant la technologie NFC. Mais les français ne sont pas toujours rassurés. De nombreuses failles de sécurité concernant la technologie NFC font l'actualité tels que la collecte d'informations bancaire, les vols d'argents. Pour limiter les risques, plusieurs entreprises ont proposé des solutions innovantes. Visa et Atos ont mis au point un mode de paiement mobile sans contact reposant sur la technologie HCE. Cette technologie permet de conserver les données sensibles dans un endroit sécurisé évitant les fraudes bancaires. Le challenge principal de la technologie HCE est de répondre aux attentes de sécurité né des retours de la technologie NFC.

D'autres entreprises se sont concentrés dans la biométrique. Zwipe et MasterCard propose un paiement sans contact biométrique. Le paiement n'est plus possible sans le doigt du détenteur de la carte. Des solutions qui répondent aux exigences de sécurité mais dont le déploiement demande du temps. Cependant, le modèle « SE-based » est le modèle le plus pragmatique dans le contexte actuel.

VII- Bibliographie

1. Alzahrani, A., A. Alqhtani, H. Elmiligi, F. Gebali, et M.S. Yasein. « NFC security analysis and vulnerabilities in healthcare applications ». In *2013 IEEE Pacific Rim Conference on Communications, Computers and Signal Processing (PACRIM)*, 302‑5, 2013. doi:10.1109/PACRIM.2013.6625493.

2. Chattha, N.A. « NFC #x2014; Vulnerabilities and defense ». In *2014 Conference on Information Assurance and Cyber Security (CIACS)*, 35‑38, 2014. doi:10.1109/CIACS.2014.6861328.

3. « Google fait le pari de la NFC - Techniques de l'Ingénieur ». Consulté le 19 décembre 2014. http://www.techniques-ingenieur.fr.proxy.utt.fr/actualite/high-tech-thematique_193/google-fait-le-pari-de-la-nfc-article_62458/.

4. « La carte bleue, bientôt complètement obsolète - Techniques de l'Ingénieur ». Consulté le 19 décembre 2014. http://www.techniques-ingenieur.fr.proxy.utt.fr/actualite/high-tech-thematique_193/la-carte-bleue-bientot-completement-obsolete-article_61907/.

5. « La technologie NFC - Principes de fonctionnement et applications | Techniques de l'Ingénieur ». Consulté le 19 décembre 2014. http://www.techniques-ingenieur.fr.proxy.utt.fr/base-documentaire/technologies-de-l-information-th9/internet-des-objets-42612210/la-technologie-nfc-s8650/.

6. « Sécurité du paiement mobile NFC | Techniques de l'Ingénieur ». Consulté le 19 décembre 2014. http://www.techniques-ingenieur.fr.proxy.utt.fr/base-documentaire/technologies-de-l-information-th9/internet-des-objets-42612210/securite-du-paiement-mobile-nfc-h3580/.

7. Verdult, R., et F. Kooman. « Practical Attacks on NFC Enabled Cell Phones ». In *2011 3rd International Workshop on Near Field Communication (NFC)*, 77‑82, 2011. doi:10.1109/NFC.2011.16.

8. « Alliance Activites : Publications : Host Card Emulation 101 » Smart Card Alliance ». Consulté le 1 janvier 2015. http://www.smartcardalliance.org/publications-host-card-emulation-101/

9. Martin Emms, Budi Arief, Leo Freitas, Joseph Hannon, Aad van Moorsel - « Harvesting High Value Foreign Currency Transactions from EMV Contactless Credit Cards without the PIN » - School of Computing Science, Newcastle University