Enquête : Le paiement mobile NFC sécurisé, vraiment ?

Apple Pay marquera-t-il le vrai décollage du paiement mobile sans contact dans le monde et plus particulièrement en France ? S'il est encore trop tôt pour le dire, malgré les premiers chiffres encourageants avancés par le constructeur (qui a revendiqué million d'activations en trois jours), l'adoption de **la technologie NFC** pour effectuer ses paiements avec son smartphone dépendra notamment de la perception des utilisateurs à bénéficier de transactions sécurisées.

Rappelons que le *Near Field Communication* (ou communication en champ proche) est une technologie qui permet l'échange de données entre deux appareils proches de quelques centimètres (moins de 10) selon trois modes opérationnels : de pair-à-pair (pour transférer des fichiers entre deux smartphones par exemple), en lecture-écriture (le smartphone se transforme en lecteur NFC pour lire des étiquettes électroniques ou « tags » diffusant des informations), et en émulation (ou dématérialisation) de carte, que ce soit une carte de transport, de billettique, de gestion de couponing ou de paiement. C'est donc ce dernier mode qui nous préoccupe dans le cadre du paiement sans contact depuis un smartphone.

A en croire les industriels du secteur, **le paiement par NFC est absolument fiable** que ce soit avec le modèle SIM centric (l'application de paiement est stockée sur la carte SIM de l'opérateur, solution plutôt prisée des principales banques françaises aujourd'hui) ou avec la puce NFC embarquée sur le téléphone (le modèle adopté par Apple et Google notamment). *« Les solutions de paiement sur mobile sont validées par les banques (en France) et répondent aux recommandations EAL4+ »*, soutient Thibault de Dreuille, délégué général de l'AFSCM (Association française du sans contact mobile). L'EAL4+ indique un niveau d'assurance de certification d'un système d'information. Il est notamment adopté pour certaines puces de chiffrement comme celle qui équipe le Hoox m2, le smartphone ultra sécurisé de Bull.

Un coffre fort numérique embarqué

D'autre part, que ce soit sur SIM ou sur composant intégré au terminal, la puce NFC fournit un élément de sécurité (*secure element*), **sorte de coffre fort numérique** propre à chaque service et isolé des uns des autres, qui vise à protéger des attaques potentielles les données sensibles stockées sur le téléphone comme le code PIN d'une carte de crédit. Confié par le constructeur du smartphone, l'opérateur ou tout autre fournisseur de services (banques, distributeurs, transporteurs, au besoin par l'intermédiaire d'un prestataire), le secure element NFC répond ainsi à **l'exigence du protocole EMV** (Europay Mastercard Visa) propres aux transactions des cartes bancaires.

« Les données de transaction sont chiffrées. En hardware SIM ou secure element, on ne peut rien en faire, elles ne sont pas réexploitables », assure Christophe Zehnaecker, product manager emerging payments pour MasterCard. Qui ajoute que *« nous n'avons constaté aucun cas de fraude aujourd'hui sur les technologies sans contact. Les pirates vont se porter sur d'autres systèmes. »*

S'il ne peut y avoir de faiblesse du côté de la puce NFC (sur téléphone ou carte bancaire sans contact), qu'en est-il du côté des terminaux de paiement électroniques (TPE)? *« Sur la partie lecture, que l'information vienne du téléphone ou d'une carte bancaire, sans contact ou pas, les informations transmises sont les mêmes et de la même façon*, explique Michel Leger, EVP marketing et ventes chez le constructeur de solutions de paiement intégrées Ingenico Group. *Globalement, on sécurise les données transmises par un mécanisme de chiffrement point à point du terminal aux infrastructures de traitement de la banque. »* A la différence qu'un téléphone peut avoir un moyen d'identification propre. Apple Pay s'appuie sur la biométrie quand le groupement des cartes bancaires fait le choix du code PIN. *« C'est le terminal qui gère la demande d'authentification selon la règle des émetteurs »*, indique le porte-parole d'Ingenico.

Les faiblesses du protocole EMV

Ce qui nous ramène au smartphone et ses éventuelles faiblesses. Notamment l'aspiration à distance des informations contenues en clair sur la carte de paiement. *« Par définition, les communications sans fil sont facilement interceptables »*, avance Loïc Guézo. L'évangéliste Sécurité de l'Information pour l'Europe du Sud chez Trend Micro évoque les travaux de Renaud Lifchitz, ingénieur en sécurité chez BT, qui en 2012 avait mis en évidence **la possibilité de «sniffer» les cartes bancaires sans contact NFC** à l'aide d'une simple clé USB NFC. Il avait récupéré certaines informations non chiffrées: les nom et prénom du porteur, le numéro de la carte et la date d'échéance ainsi que les dernières transactions effectuée.

« Le problème vient de la transposition du mode contact du protocole EMV au mode sans contact », explique Bruno Salinier, directeur technique de projet NFC chez Orange Business Services. Autrement dit, l'application d'un protocole propre à un usage ancien sur une utilisation plus récente. Faut-il y voir une faille pour autant? Plusieurs interlocuteurs nous ont fait remarquer que ces informations étaient lisibles à l'œil nu sur la carte et qu'une bonne photo (ou une bonne mémoire) suffit à les capturer sans matériel sophistiqué. A condition néanmoins que la victime sorte sa carte de son portefeuille, une contrainte dont s'affranchit le NFC.

Depuis, et sous pression de la Cnil notamment, le groupement des cartes bancaires a corrigé le tir. Depuis 2014, **les nouvelles cartes NFC n'émettent plus les noms du porteur et l'historique des transactions**. Il n'en reste pas moins qu'un numéro de carte et sa date d'expiration pourront être exploitables sur un site de e-commerce pour peu qu'il ne fasse pas appel au cryptogramme visuel (les 3 chiffres inscrits au dos de la carte) ni à un deuxième niveau d'authentification comme le 3DSecure (confirmation de la transaction à partir d'un code reçu par SMS). Ce qui est possible dans nombre de pays étrangers. D'autre part, quel est le taux de cartes en service effectivement mises à jour avec la nouvelle version du protocole qui ne laisse pas fuiter le nom du porteur?

Un risque qui pourrait être résolu avec **le modèle Host Card Emulation**. Proposé depuis un an environ par Google, le HCE s'appuie sur le Cloud pour émuler des numéros virtuels et uniques de carte bancaire sur la base de jetons (tokens) à usage limité préchargés sur le téléphone et dont la politique de sécurité est définie par la banque. Une solution récemment adoptée par Visa, notamment, mais qui contourne les opérateurs et leur service de distribution et support, des applications NFC. Il restera donc à vérifier l'attrait des banques pour cette nouvelle solution.

Une transaction NFC à 1 million de dollars

Pour autant, les experts en sécurité ne se montrent pas aussi enthousiastes face au NFC que les industriels de la chaîne du paiement électronique. Pour Gaël Barrez, directeur des opérations France de Forescout, *« le risque pour un porteur de carte est plus grand encore en NFC [par le simple fait] de se faire voler son téléphone »*. En effet, **les paiements NFC n'imposent pas de saisie du code PIN sous 20 euros d'achat**. Le voleur du smartphone pourra donc effectuer un certain nombre de petites transactions avant d'être bloqué. Mais, *« si ce plafond est limité à 20 euros en France, il est accepté sans plafond dans une devise étrangère »*, avance Loïc Guézo. Du coup, même si les systèmes de surveillance des fournisseurs de cartes peuvent détecter les mouvements douteux et alerter la banque, *« qu'est-ce qui empêche néanmoins d'effectuer une ou deux transaction à 500 dollars sans être inquiété ? »*, s'interroge l'évangéliste de Trend Micro.

Plus grave, des chercheurs de l'université britannique de New Castle ont mis en évidence la capacité d'effectuer **une transaction jusqu'à 999 999 dollars en NFC sans avoir à saisir de code PIN**. Rien qu'en approchant un smartphone transformé en terminal de paiement (via une application développée à cet effet) de cartes bancaires sans contact. Qui plus est, la transaction est effectuée mais pas envoyée à la banque dans l'immédiat. Elle est stockée sur le smartphone-TPE. Le pirate devra alors trouver un commerçant complice, qui effectuera la transaction de paiement en ligne avec la banque, pour récupérer son pactole. *« Si on peut générer une transaction crédible par le biais du NFC en injectant de fausses données, on peut réaliser un paiement frauduleux »*, confirme Loïc Guézo. Pas à la portée du premier pirate venu mais possible techniquement, donc.

Pour éviter ce genre de désagrément, surtout pour les consommateurs qui voyagent hors de la zone euros, Gaël Barrez recommande d'isoler sa carte bancaire dans un étui qui fera office de cage de Faraday (on en trouve à foison sur le Net) et de désactiver la fonction NFC de son téléphone. Tout simplement.

Perte du contrôle du smartphone

Mais la perte totale de contrôle du smartphone n'est pas impossible. *« On peut aussi bien pirater un téléphone qu'un ordinateur, les mouchards de la NSA sont là pour nous le rappeler »*, estime l'expert de Forescout. Si tous les pirates ne disposent pas nécessairement des moyens de l'agence américaine pour s'introduire dans nos smartphones à distance, le nombre de malwares en circulation, particulièrement sur la plate-forme Android, accentue le risque de se faire voler ses données sur son smartphone. *« Qui dit malware dit objectif de s'attaquer au système de paiement »*, avance Loïc Guézo. Il nous remet en mémoire **la faille Android Fake ID** repérée par Bluebox Lab en juillet dernier, et qui aurait permis à un logiciel malveillant d'accéder aux données de paiement en se faisant passer pour Google Wallet, le système de paiement mobile de Google.

Si la faille était en fait corrigée par Mountain View lors de la publication de Bluebox, qui nous dit que ce sera toujours le cas à l'avenir ? Avec 8 millions de malwares Android en vue en 2015 selon les estimations de Trend Micro (12 à 15 chez McAfee), les risques ne sont pas négligeables. *« La problématique d'une plateforme ouverte qui attire l'intérêt des cybercriminels couplé à la volonté d'un Apple Pay de sortir du système bancaire ne peut que faire peser de nouvelles menaces à court terme »*, avance Loïc

Guézo. S'il reconnaît que la lecture de l'empreinte digitale de l'iPhone 6 pour valider un paiement NFC *« est une approche innovante »*, l'expert rappelle que **le fonctionnement du paiement de l'iPhone n'est pas normalisé chez Apple**. On ignore donc tout, ou presque, de son fonctionnement. *« Si Visa est partenaire, on peut penser qu'Apple Pay est suffisamment sécurisé. Mais si demain Apple peut se passer de Visa comme partenaire, quelle confiance pourra-t-on lui accorder ? »*

Pour Gaël Barrez, *« l'empreinte digitale n'offre pas une sécurité absolue, elle est contournable en trompant l'appareil avec une copie de l'empreinte »*. Un brun parano comme tout bon expert en sécurité, le responsable de Forescout reste très méfiant vis-à-vis du NFC. *« Le support n'est pas sûr, le réseau non plus. »* Pour autant, *« ces problèmes de sécurité ne sont pas un frein [à l'adoption]*, avance Gaël Barrez, *si l'outil permet de payer en trois secondes au lieu de 25, le marché va l'adopter. D'autant qu'il y a plus de porteurs de smartphones que de cartes bancaires. Et il y a un côté écolo avec moins de plastique à produire et un coût moindre de gestion pour les banques »*.

Des usages freinés par le manque de TPE

En attendant, ce n'est pas la sécurité, ou son absence de garantie totale, qui freine l'adoption mais le manque de terminaux de paiement électroniques en France. Si 6,6 millions d'utilisateurs sont aujourd'hui équipés d'un smartphone compatibles NFC et plus de 29 millions d'une carte bancaire sans contact, **seuls 233 000 TPE compatibles NFC ont été déployés** (en septembre 2014) selon l'Observatoire du sans contact. A peine 18% du parc installé. Or, *« c'est la phase d'équipement des commerçants qui va permettre le décollage des usages NFC »*, estime Thibault de Dreuille. Certes, la mise à niveau est rapide. Les professionnels espèrent que 30% du parc sera équipé à la fin de l'année. Attendu en 2015 en Europe, l'Apple Pay fera-t-il office de locomotive ?

Lire également
Visa veut accélérer les paiements NFC sur mobile
La RATP démocratise les services NFC pour les bus et les trams
La SNCF initie le NFC dans ses TER avec Orange

crédit photo © LDprod – shutterstock