WARNING ! Ceux qui ont tenté par le passé de démontrer les failles des cartes bleues ont rapidement rencontré de gros problèmes. Le GIE Cartes Bancaires ne plaisante pas avec la question, même quand la sécurité de ses installations est clairement mise en défaut ; Serge Humpich s'en souvient encore. Dans ces pages, nous avons donc souhaité rester dans un cadre purement légal. C'est pourquoi nous ne pouvons vous donner le détail exact du matériel et du logiciel utilisés pour cette opération. De même, aucune donnée nominative ni bancaire n'a été récupérée lors des essais, à l'exception de celles du journaliste.

RFID/NFC : une sécurité douteuse ?

La preuve par le métro

Aussi aberrant que cela puisse paraître, la plupart des puces RFID qui sont en ce moment déployées à grande échelle ne disposent que d'une sécurité minimale voire inexistante. Ainsi, les passeports RFID n'exigent qu'un mot de passe assez simple et les cartes bancaires ne contiennent tout simplement aucune protection ! Nous avons donc cherché à savoir si cela représentait un réel problème dans la réalité ou s'il ne s'agissait que de paranoïa. *Canard PC Hardware* est donc allé bourlinguer dans le métro aux heures de pointe, équipé d'une besace de H4cKZ0r spécialement conçue pour aspirer les tags RFID et NFC. Et les résultats sont effrayants...

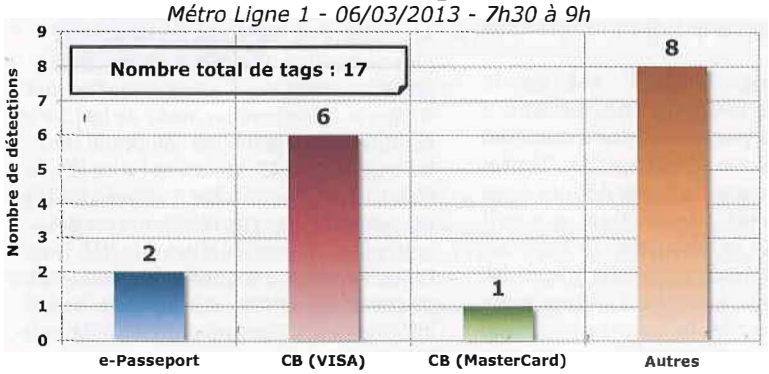
Avec un smartphone ou une tablette équipée d'une puce NFC comme le Nexus 7, il est possible d'accéder sans problème à toutes l es informations d'une CB. La portée est toutefois d'à peine 2 à 3 cm.

Le thème de la sécurité est venu sur le devant de la scène depuis que des données sensibles ont été rendues accessibles à distance. C'est le cas par exemple sur les cartes bleues RFID et les passeports biométriques. La problématique concerne deux points importants : la distance à laquelle les informations peuvent être récupérées et la nature de ces informations. Sur les cartes bleues NFC (VISA PayWave et MasterCard PayPass), ni les informations ni les communications ne sont cryptées. Il est ainsi possible d'accéder au nom de l'usager, au numéro de compte, à la date d'expiration, aux données de la bande magnétique mais aussi à l'historique des transactions. Seule la CVV (*Card Verification Value* – le code à trois chiffres qui se trouve au dos de votre CB) est absente de cette longue liste. La seule protection se résume à la liaison qui n'est possible qu'à très courte portée. Selon le GIE Cartes Bancaires, cela serait suffisant. Nous avons toutefois de sérieux doutes sur le sujet. Pour les passeports, les choses sont différentes : les données y sont encryptées et seule une clé permet d'y accéder. Problème : comme le précisent les spécifications techniques publiques du passeport biométrique, cette clé est dérivée d'informations (numéro du passeport et/ou de sa date de délivrance et/ou de la date de naissance du propriétaire) accessibles en clair à l'intérieur du passeport. Une attaque en "brute force" n'est pas inenvisageable vu le nombre limité de combinaisons possibles. Pire encore, comme pour tout cryptage, il est possible que celui-ci soit cassé dans les années à venir ; après tout, il fut un temps pas si lointain où le WEP était considéré comme parfaitement sûr. Le vol d'identité ou la création de faux passeport serait alors possible très facilement.

CPC H4cKz0R. Restait tout de même une inconnue de taille : est-il vraiment possible de lire ces puces à l'insu de leurs propriétaires ? Peut-on aspirer le contenu d'une CB à travers un sac à main, un portefeuille ou une poche de pantalon dans des conditions réelles ? C'est ce que nous avons voulu savoir. Pour cela, nous avons adapté et développé un système hardware et software pour nous livrer à l'expérience. Côté hardware, il a fallu dégainer le fer à souder même si nous avons opté pour une approche *Quick & Dirty*. L'objectif n'était bien évidemment pas de détrousser les gens à grande échelle mais juste de tester le concept. Nous utilisons donc une simple plateforme Arduino Uno R3 sur laquelle nous greffons un *shield* (carte fille) RFID/NFC d'Adafruit.com **(1)**. Nous avions toutefois besoin d'une plus grande portée que les 5 cm de l'antenne intégrée pour mener à bien notre expérience. Pour cela, nous

Détection de tags RFID

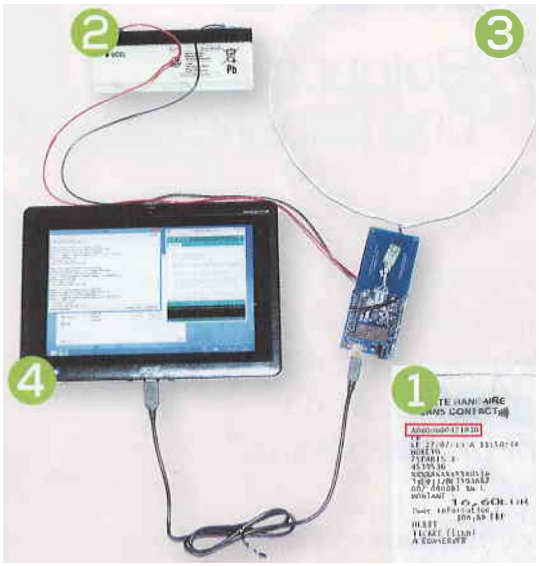
Métro Ligne 1 - 06/03/2013 - 7h30 à 9h



avons modifié ce shield afin de lui adapter un amplificateur RF pour augmenter la capacité de réception à distance. Ce petit ampli est alimenté par une batterie externe au plomb (12V/2.1Ah) **(2)**. Nous avons ensuite conçu une antenne "boucle" adaptée aux fréquences RFID (13.56 MHz) **(3)**. Grâce à elle, nous avons pu obtenir une portée jusqu'à 15-17 cm. Certes, ce n'est pas énorme dans l'absolu, mais avec plus de temps et de moyens, il est sans conteste possible de faire mieux. Les informations lues par le système sont récupérées par le microcontrôleur de l'Arduino, puis renvoyées via une connectique USB sur une tablette Windows de première génération, l'Acer W500 **(4)**.

Il nous a fallu ensuite créer la partie "software". Nous détectons 3 types de cartes : les passeports, les cartes bancaires et les autres (cartes de parking, de station-service, de déchetterie, de café, etc.). Les passeports et les cartes "autres" sont détectés directement à partir de leur "ID". Pour les cartes bancaires, c'est plus compliqué : on y accède via un système de fichier simplifié avec des fichiers et des répertoires. Grâce à la librairie libnfc, nous avons codé un firmware minimaliste uniquement capable de déterminer les types de tags RFID à proximité. Sans rentrer dans les détails pour des raisons légales, comme le précise le standard EMV, il suffit d'envoyer 3 commandes : l'une pour "réveiller" la carte qui ne comporte que des "0", la seconde pour accéder aux données de la carte bancaire avec un code unique et la troisième pour lire l'un des fichiers ou répertoires. Le second code n'a pas été compliqué à trouver puisqu'il figure en clair sur toutes les facturettes CB ! Si vous vous demandiez à quoi correspond le code "A0000000421010" que l'on trouve en haut de celles-ci (voir ci-dessus), vous voilà renseigné ! Afin de rester dans la légalité, nous nous contentons de déterminer le type de carte bancaire (VISA, MasterCard ou Amex) mais rien de plus : aucune autre donnée n'est lue mais un firmware plus sophistiqué et conçu dans ce but aurait pu extraire d'autres informations.

Les données personnelles des cartes bancaires RFID/NFC ne sont protégées par aucun cryptage



Depuis environ un an, la plupart des cartes bancaires disposent de la technologie NFC activée par défaut. Pour les reconnaître, elles disposent de ce programme.

Grand Theft Metro. Restait à sortir du labo pour aller tester tout cela en pratique. Nous avons d'abord embarqué tout le matériel dans un sac en bandoulière de manière à ce qu'il soit totalement invisible de l'extérieur. L'antenne se trouvait dans la poche avant (dans le rabat) avec le microcontrôleur, la tablette et la batterie au plomb) à l'intérieur. La hauteur de la sangle était réglée pour que l'ensemble se retrouve opportunément au niveau des sacs à main des dames et des poches de pantalon des messieurs. Restait à trouver une foule compacte et debout. Pour cela, rien ne vaut le métro aux heures de pointe ! Nous avons donc effectué le trajet Vincennes - La Défense (aller et retour) sur la ligne 1 du métro parisien (bondé) un mercredi matin vers 8 h. Nous changions de wagon à chacune des 25 stations pour maximiser le nombre d'interactions. Le test total a duré 1 h 30. Toutefois, nous avons constaté qu'une soudure de l'antenne avait lâché peu après le début du trajet retour selon les logs. La durée réelle du test est donc d'environ 45-50 minutes.

10 CB à l'heure ! Après analyse, voici les résultats que nous avons obtenus avec notre système bricolé en une après-midi pour moins de 100 euros tout compris : 2 passeports et 7 cartes bancaires ainsi que 8 cartes non-identifiées ! Encore une fois, si nous avions été malintentionnés, avec un firmware nettement plus évolué, nous aurions pu récupérer le numéro de la carte et sa date d'expiration, le nom, l'historique des achats des propriétaires et d'autres informations sensibles. De quoi réencoder sans problème la bande magnétique d'une carte vierge et aller faire des achats à l'étranger où la puce n'est pas toujours utilisée. Avec l'aide d'un commerçant malhonnête, nous aurions pu également leur prélever 20 euros chacun (montant maximum prélevable sans que l'utilisateur doive taper son code) grâce à un terminal de paiement NFC. La CNIL, qui est censée enquêter depuis plusieurs mois sur le sujet, reste totalement muette pour le moment. Quant au groupement des cartes bancaires, il indiquait à nos confrères de 01Net en septembre dernier que cela ne posait pas de problème puisque ces données sont *"de toute façon visibles à l'œil nu"*. À condition de disposer d'une vision capable de lire à travers les portefeuilles, peut-être. Et jusqu'à preuve du contraire, l'historique des achats n'est pas inscrit sur la carte ! Le consortium annonce toutefois l'air de rien – sans faire de rapport avec la sécurité inexistante des modèles actuels – qu'une nouvelle génération de carte NFC mieux protégée est prévue pour 2014 ou 2015. En attendant…