Jeudi 25/02/2010
Rencontre-débat

Puces RFID, bluetooth : des mouchards dans la poche ?

Intervenants

- **Franck Dumortier**, chercheur au Centre de recherches informatique et droit – FUNDP à Namur
- **François Koeune**, chargé de recherches à l'Université catholique de Louvain
- **François-Xavier Standaert**, chercheur qualifié FNRS-F.R.S et professeur à l'Université catholique de Louvain

Remarque liminaire :
Le texte présenté ci-bas est issu d'une conférence organisée par la Ligue des droits de l'Homme durant sa semaine thématique consacrée aux nouvelles technologies en février 2010. Afin d'éviter les répétitions inhérentes à un débat faisant appel à plusieurs intervenants et de rendre la synthèse de la lecture plus fluide, les diverses interventions des orateurs ont été mélangées.

Lors de cette conférence, il ne sera pas question de savoir si la technologie et les RFID représentent un acquis ou une menace. Cette question n'a pour nous pas ou peu de sens. La technologie y est avant tout vue comme un outil et décrite comme telle.

Qu'est-ce que le RFID ?

Tout d'abord, il faut distinguer différentes technologies :

1. Les cartes à puces (comme celles qui se trouvent sur les cartes bancaires, les cartes d'identité, les cartes de crédit…) sont dotées de puces électroniques. Ces puces sont en quelque sorte des ordinateurs grâce auxquels un lecteur de puce peut afficher les réponses aux questions posées : la puce est capable de faire un calcul. L'ordinateur est protégé (on ne peut pas la parcourir ou la lire comme on le veut) et il est impossible de lire ce qu'elle a en mémoire.

2. Le RFID (Radio Frequency IDentification[1]) est une puce que l'on colle sur une surface (containers, palettes, vêtements, emballages…) et dont les informations peuvent être lues à distance. Cette technologie, efficace et au prix de revient relativement peu élevé, permet de localiser et d'identifier ces objets dans le but, entre autres, de gérer des stocks. On peut également utiliser cette technologie pour le traçage de bétail ou encore pour les ski-pass qui permettent de prendre la remontée mécanique à condition d'être en ordre de paiement et d'abonnement. Le passeport électronique contient aussi un RFID. Evidemment le RFID devient, dans ce cas, plus coûteux et plus complexe que pour une simple utilisation de gestion de stocks. En effet, il s'agit ici de sécuriser les données contenues dans la puce afin de ne pas en permettre la lecture à n'importe qui et d'en éviter la falsification.

Quelles sont les similitudes et les différences entre la puce et le RFID ?

Similitudes : la puce et le RFID sont des ordinateurs capables de faire un calcul, de fournir l'information demandée. Ces technologies ne demandent pas de pile, ni de batterie.

Différences : Outre l'usage, la puissance de calcul est différente. On se connecte au RFID grâce à un champ électromagnétique, tandis que pour lire une puce, il faut la brancher, établir un contact direct. De manière générale, le RFID est plus performante que la puce.

Le RFID s'inscrit dans une ligne directrice plus large. Le GSM et le Wifi s'inscrivent dans la même mouvance générale : on peut se connecter à un GSM ou à une borne à distance à partir d'un autre GSM.

Par exemple, un grille pain « hi-tech » peut se connecter à Internet par wifi pour donner la météo sur les toasts qu'il est en train de griller. Ou un frigo intelligent peut évaluer son stock et envoyer une liste de courses sur votre gsm, vous signaler les aliments périmés ou en passe de l'être.

Mais tout appareil qui se connecte au wifi transmet des informations qui sont stockées quelque part !

[1] La **radio-identification** plus souvent désignée par le sigle **RFID** (de l'anglais ***Radio Frequency IDentification***) est une méthode pour mémoriser et récupérer des données à distance en utilisant des marqueurs appelés « radio-étiquettes » (« *RFID tag* » ou « *RFID transponder* » en anglais)[1]. Les radio-étiquettes sont de petits objets, tels que des étiquettes autoadhésives, qui peuvent être collées ou incorporées dans des objets ou produits et même implantées dans des organismes vivants (animaux, corps humain[citation nécessaire]). Les radio-étiquettes comprennent une antenne associée à une puce électronique qui leur permet de recevoir et de répondre aux requêtes radio émises depuis l'émetteur-récepteur.

Ces puces électroniques contiennent un identifiant et éventuellement des données complémentaires.
Cette technologie d'identification peut être utilisée pour identifier :
- les objets, comme avec un code à barres (on parle alors d'étiquette électronique)
- les personnes, en étant intégrée dans les passeports, carte de transport, carte de paiement (on parle alors de carte sans contact).(Source : http://fr.wikipedia.org/

Quels sont les avantages du RFID ?

- Le RFID permet d'économiser du temps. Par exemple, dans les supermarchés, la possibilité de passer avec sa charrette sous un portique qui identifie tous vos produits via leur puce RFID sans que vous ayez à faire des manipulations telles sortir les produits, les emballer…
- Le RFID permet par exemple de signaler si la température des congélateurs des supermarchés a baissé, grâce à des capteurs installés sur l'emballage des produits, vérifier si la chaine du froid a été interrompue ...
- Le RFID installé dans un micro-onde permet, par exemple, de ne plus avoir à lire le modalités d'utilisation concernant le mode de cuisson en fonction du poids ou de la nature de l'aliment.
- Grâce aux possibilités de connexion à distance, le GSM peut se connecter aux sites de téléphonie par Internet. Cela peut avoir des avantages en matière de coût (via Skype par exemple, moins cher qu'un opérateur de téléphonie mobile).

Quels sont les dangers ?

- L'appareil est interrogeable à distance. Donc un supermarché pourrait, grâce au RFID de la carte de fidélité des clients, enregistrer les allées et venues de chaque client afin de connaître ses habitudes. Il faut se rappeler que les puces RFID ont une capacité de mémoire.
- Une personne mal intentionnée peut lire à distance ce que vos cartes contiennent.

Une technologie inviolable ?

La carte MOBIB, par exemple, est lue grâce aux bornes de la STIB placées à l'entrée de chaque station, mais une personne en dehors de la STIB peut très bien avoir l'information car il est très facile de craquer le système.

Des chercheurs de l'UCL ont prouvé qu'une carte équipée d'une puce RFID comme la carte MOBIB pouvait être très facilement « craquée » et qu'à une distance de 10 mètres, il était possible de lire ce que contient cette carte (sur la Carte MOBIB, voir plus loin). Le passeport, quant à lui, est lié à un système de base de données du VIS (une base de données conçue en 2004 à la suite des attentats du 11 septembre 2001 dans le but de lutter contre la fraude et la demande multiple de visas. Elle peut contenir les empreintes digitales de 70 millions de personnes). Europol, ainsi que la police, ont accès à ces bases de données, dans le cadre de leur mission de lutte contre le terrorisme.

D'ailleurs, à l'origine simple document d'identité, le passeport est devenu, grâce à la présence d'une puce RFID, un moyen d'investigation et d'accès à des lieux sécurisés. La finalité de l'outil a complètement changé !

Informations - plus aussi - personnelles

- La carte SIS contient des données médicales. Le pharmacien peut lire toutes les informations que contient cette carte SIS grâce au lecteur de carte. Sur base des informations concernant les médicaments achetés durant ces derniers mois, le pharmacien peut facilement déduire les problèmes de santé rencontrés dans le passé.

- Une firme de vêtements pourrait très bien poser des étiquettes RFID sur ses vêtements afin que le vendeur puisse constater s'il s'agit d'une contrefaçon ou pas. Mais en posant des étiquettes RFID sur plusieurs vêtements (par exemple, sur la cravate, les chaussettes et la chemise), on peut facilement obtenir des informations sur la personne qui porterait ces trois vêtements et ainsi suivre cette personne à la trace dans ses déplacements via des lecteurs RFID qui s'implantent petit à petit dans l'espace public.

- La borne wifi permet de se connecter à un réseau mais cependant rien ne garantit qu'un voisin n'a pas accès à mon réseau et qu'il n'est pas en train de lire et de voir tout ce que je fais à partir de mon portable. Une adresse IP et une connexion Internet personnelles peuvent être utilisées par quelqu'un d'autre et ce très facilement. En cas de méfait, l'usurpation de ces éléments a pour conséquence de me rendre suspect puisqu'il s'agit de mon adresse IP et qu'elle m'identifie au même titre, par exemple, que mon adresse postale..

- La même question se pose pour les bornes wifi tout public : à quoi l'utilisateur se connecte-t-il réellement lorsqu'il utilise un accès à Internet dans une gare ou dans un café ? L'accès à ces informations est-il protégé? Qu'est-ce qui est fait des données transmises ?

La cryptographie : une solution envisageable

La cryptographie est la science de la sécurité de l'information.

Son utilisation permet :

- de pouvoir échanger des messages en toute confidentialité. Le cryptage d'un message rend très difficile la lecture des données interceptées lors d'une connexion à une borne wifi par exemple
- de garantir l'authenticité de l'information dans le cadre d'une transaction bancaire par exemple : l'ordre qui a été donné vient-il de la bonne personne ? On parle ici de l'aspect de la signature électronique, telle qu'utilisée pour le service tax-on-web.

de rendre plus difficile le traçage : la cryptographie a développé un protocole qui permet à l'utilisateur de se connecter sur Internet via une borne wifi tout en lui offrant à chaque fois une série de chiffres d'identification différente. Ce qui permet de protéger la confidentialité des passages sur Internet.

La cryptographie a développé un protocole à « divulgation minimale » : quand une jeune personne entre dans un magasin pour acheter de l'alcool, le vendeur peut lui demander son âge afin de savoir si elle a plus de 18 ans. Il peut alors demander sa

carte d'identité. Ce faisant, il a accès à toutes les informations (nom, prénom, adresse, date de naissance…) ! Le protocole à divulgation minimale permet au vendeur de voir uniquement si la personne est en âge d'acheter de l'alcool, sans pour autant divulguer les autres informations contenues dans la carte. La machine répond uniquement à la question de l'âge par oui ou non.

Le principe de Kerckhoffs

Ce principe exprime que la sécurité d'un cryptosystème ne doit reposer que sur le secret de la clef. Autrement dit, tous les autres paramètres doivent être supposés publiquement connus.

La cryptographie travaille sur base d'algorithmes. On peut comparer son fonctionnement à celui de la méthodologie à appliquer, aux étapes à suivre pour passer un appel téléphonique. Par exemple, l'algorithme d'un appel, c'est décrocher le combiné, composer un numéro et enfin appeler. Ce principe se retrouve dans le cryptage comme une série de chiffrage. La clé est le secret que seul l'utilisateur connaît. La méthode – l'algorithme - est publique ; la clé seule est secrète. C'est pourquoi tout bon système de sécurité peut être dévoilé et expliqué, aussi complexe soit-il. Mais la clé demeure secrète.

Spécification vs Réglementation

Pour aborder les problématiques liées au RFID, il est important de comprendre la distinction entre la spécification - la manière dont les choses vont fonctionner - et la réglementation - le but auquel on veut arriver.

En effet, s'il existe déjà une série d'applications qui utilisent le RFID (comme la carte MOBIB), un élément crucial semble avoir été oublié : celui d'une réglementation qui précise l'objectif poursuivi, ce qui est fait de ces RFID, à quoi doivent-elles servir. Même si spécification il y a, comment savoir si le RFID remplit correctement son rôle ? Comment envisager si son usage n'est pas détourné, si son rôle n'est pas indubitablement détourné ? Il n'y a que très peu de réponses à ces questions.

Les concepteurs n'ont pas défini le but et ce qu'on peut faire (ou pas) avec ces cartes. La carte MOBIB constitue, à cet égard, un exemple édifiant.

Créée pour contrôler plus facilement les voyageurs, la carte, réputée inviolable, était sensée ne contenir que les nom et prénom du client. Le ministre des transports de l'époque avait affirmé que les trajets des voyageurs ne seraient pas enregistrés sur la carte.

En craquant la carte, des chercheurs de l'UCL ont néanmoins prouvé deux choses :

1. La carte MOBIB est facilement piratable en raison de l'absence de mécanisme de sécurité efficace (pas de cryptographie), ce qui constitue une atteinte à l'obligation de sécurité. Nos données sont transmises par wifi à la base de données de la STIB chaque jour et des personnes mal intentionnées pourraient, jusqu'à 10 mètres de distance des bornes, intercepter les données enregistrées sur la puce RFID.

.

2. La carte possédait bien plus d'informations qu'officiellement annoncé :
    - Le prénom et le nom du détenteur de la carte
    - La date de naissance du détenteur
    - Le code postal du détenteur
    - Les trois dernières validations du détenteur (date, heure, ligne de bus, arrêt de bus, station de métro…)
    - Les informations relatives aux abonnements du détenteur
    - Certaines autres données techniques (transit, nombre total de validation, date d'achat…)

Pourquoi la STIB détient-elle tant d'informations ?

La finalité de la carte est de contrôler plus facilement les voyageurs.

Pourtant, une série d'autres finalités semblent compléter ses potentialités. Il est notamment stipulé dans le contrat que toute personne achetant une carte MOBIB accepte que ses données soient utilisées à des fins de marketing direct. On y consent de manière automatique, il faut écrire à la STIB pour annuler cette approbation par défaut.

Pour assurer sa finalité de contrôle, la STIB n'a pas besoin de connaître notre trajet : seul importe de savoir si le voyageur est en ordre ou pas.

Autre problème que pose la présence de données surnuméraires : le contrôle d'identité. Un contrôleur de la STIB ne peut pas procéder à un contrôle d'identité. Seule la police est autorisée à le faire. Pourtant, grâce à la carte MOBIB, il n'y a plus besoin de se voir proposer ouvertement à un contrôle d'identité : toutes les informations dont les contrôleurs ont besoin sont dans la carte MOBIB (nom, prénom, adresse, date de naissance, informations quant au type d'abonnement ou de paiement). Cette technologique transfère donc, de facto, des compétences policières à la STIB, du public vers le privé.

La STIB commet également une autre infraction quant à la durée de conservation des données. A la STIB, cette durée est illimitée, alors que la loi impose que la durée soit spécifiée et qu'à aucun moment, elle ne peut être illimitée.

Inquiétantes finalités et effets collatéraux

La présence de données concernant les trois dernières validations du détenteur ne va pas sans poser de graves questions quant à certaines finalités poursuivies par cette carte.

Imaginons une manifestation se déroule à la gare du midi. Un individu prend son métro à la station Hankar, pour descendre à la gare du midi à l'heure où la manifestation commence. La STIB détient des données sensibles puisque grâce à ces données, elle peut déduire que cette personne soutient la cause pour laquelle la manifestation a été organisée. C'est une atteinte à la liberté de manifester, d'expression, de circulation et d'opinion, d'autant que la police peut également avoir accès à ces données par lecture de la carte RFID – à distance !

Enfin, de manière collatérale, la création de bornes et de portiques difficilement franchissables sans carte déresponsabilise le citoyen. Ce n'est en effet plus une personne qui va mettre « à la porte » le sans-abri qui squatte la station, mais bien … des portes qui, pour être franchies, nécessitent d'être en ordre de paiement. Cette carte MOBIB favorise donc l'exclusion sociale des transports publics (mendiants et démunis).

Piratage et sécurité

Lire une carte MOBIB avec un lecteur de carte au départ de chez soi est considéré comme étant du piratage. Une personne peut être poursuivie pour cela. Mais est-ce vraiment du piratage ? La carte a juste été lue, de la même manière que l'on se promène en rue que l'on voit la porte d'une maison ouverte. Il serait légitime d'y faire quelques pas jusqu'à ce que l'on y voie une personne pour lui signaler que sa porte est ouverte. Pirater une conversation privée ne peut pas être mis sur le même pied que lire une carte MOBIB. Pourtant, la loi ne distingue pas ces deux types de piratage informatiques. Le vrai hacker a un but mauvais caché derrière son acte.

Les questions liées à la sécurité et au respect de la vie privée doivent impérativement être prises en compte lors de la conception de ce genre de technologie. Des outils doivent être mis en place pour protéger la vie privée.

Et si la finalité de cette carte est bien le contrôle légitime du paiement par le voyageur, à bien y regarder, une carte anonyme avec une photo est largement suffisante. Il suffit que le contrôleur sache si on est en ordre de paiement et si on correspond à la photo. Cette carte anonyme avec photo uniquement est une idée à développer : il évite d'avoir à faire figurer des données telles les coordonnées postales, la date d'achat du titre de transport ou encore les derniers trajets validés.

Le futur avec MOBIB

D'autres utilisations sont prévues à partir de ce même système de carte :

- Paiement pour le système de partage de voitures Cambio
- Pour le Thalys
- Les locations de vélo
- Les parkings de dissuasion
- L'entrée des 25 musées bruxellois
- Batibouw, matchs de football, etc.
- Et une interopérabilité au niveau international : utilisation de la même carte à Bruxelles, Paris, Londres, Porto ou Funchal.

A l'image de la carte MOBIB, des tendances lourdes se dégagent dans la manière dont s'effectue le développement technologique :

- Connectivité globale : c'est une tendance à vouloir coller des RFID sur tous les objets. Mais en coller partout ne résout aucun problème. A nouveau, les finalités ne sont pas clairement établies.

- Miniaturisation : les ordinateurs sont plus puissants grâce à la multitude de collants transistors installés sur les puces. On réduit ainsi la taille de l'ordinateur et on cherche à tout miniaturiser quotidiennement.
- Intégration : volonté de combiner le téléphone, la carte d'identité, la carte bancaire, etc. en un seul objet. Cette tendance n'est pas forcément négative mais il est compliqué de déterminer les fonctionnalités propres à chacun de ces objets, ainsi que les spécificités en termes de vie privée propres à chacun.
- On parle aussi de capteurs de rythme cardiaque, de sudation… Ces applications révèlent des données délicates quant à chaque être humain, entre autres sur ses émotions.

Des recherches scientifiques sont à la base de toute création technologique. Les chercheurs ont besoin de financements et les détenteurs des finances ont besoin d'une valorisation claire (« si je mène mon projet, cela va créer une plus value »). Cette relation évacue une question primordiale : quel est le but de cette technologie ? Que veut-on précisément obtenir avec, par exemple, les potentialités d'applications offertes par une carte comme la MOBIB ?

Dans ce contexte, il est nécessaire qu'un dialogue interdisciplinaire soit mis en place réunissant les chercheurs en sciences humaines, les spécialistes de la technologie et les politiques pour envisager les règles en la matière. Malheureusement, ce dialogue prend beaucoup de temps.

Le RFID, dont la puce est lisible à distance, est une technologie, en soi, assez neutre. Les dangers résident dans la base de données et les systèmes technologiques complexes dans lesquels s'intègre le RFID. Mais est-ce grave ? A force de combiner trop de finalités, on ne sait plus ce qu'on fait. Le manque de sécurité, l'opacité des traitements, le manque d'informations et une érosion du principe de finalité comportent des risques d'atteintes à la vie privée, problématique par ailleurs complètement délaissée dans la réflexion, technique et juridique, concernant les RFID de façon générale.

Lier tout avec tout, relier ensemble toutes les finalitése risque de créer un moyen de répression.

Trop d'interconnexions créent des maillons de répressions.