Carte MoBIB

STANDAERT, François-Xavier; KOEUNE, François; Dumortier, Franck; Rouvroy, Antoinette

Published in:
Bruxelles en mouvements

Publication date:
2010

Document Version
le PDF de l'éditeur

III. Carte MoBIB
Un bon exemple de mauvaise mise en œuvre

Alors que la carte de métro bruxelloise MoBIB est en passe de remplacer définitivement les anciens titres de transport en papier de la STIB, de nombreux usagers continuent de s'interroger sur ses fonctionnalités. Ces questions donnent un cadre pratique à des réflexions générales sur l'utilisation de puces électroniques sans contact dans un nombre croissant d'applications.

ALMOS MIHALY

Précisons d'abord l'objet de la discussion qui suit. Elle concerne l'adéquation de la carte MoBIB avec les principes juridiques qui encadrent la sécurité des systèmes informatiques et l'état de l'art technologique de ces derniers. Pour rappel, le système MoBIB est basé sur la technologie RFID (ou identification par radiofréquence), qui permet le traitement automatisé et sans contact de données stockées sur une carte à puce. A ce titre, il est régi par la loi du 8 décembre 1992 sur la protection des données à caractère personnel. Les avis rendus par la Commission de la protection de la vie privée sur la problématique de la RFID sont également à prendre en compte. Dans la suite de ce texte, et pour faciliter sa lecture, les articles de la loi belge seront cités en caractères gras et les avis de la Commission en caractères italiques. A partir de ces bases juridiques, nous discuterons quelques principes importants dont il semble nécessaire d'exiger le respect par la STIB. Nous étudierons successivement la question de la légitimité du système MoBIB via le consentement de ses utilisateurs, les problèmes de sécurité informatique qu'il implique, la finalité des solutions mises en œuvre et les impératifs liés à la gestion des bases de données.

1. Le consentement

Selon la loi belge, l'utilisation de puces RFID traitant des données à caractère personnel doit être légitimée par **le consen-**

Le 17 novembre 2010, la Liga voor Mensenrechten remettra les Big Brother Awards distinguant les activités ou organisations qui ne respectent pas le droit à la vie privée. La carte MoBIB figure parmi les candidats.

tement libre, spécifique et informé de ses utilisateurs. La Commission précise à ce sujet : un consentement libre implique, entre autres, qu'un système alternatif soit proposé à la personne concernée, lequel doit être équivalent et ne peut impliquer aucune sanction. Ce principe étant rappelé, deux observations semblent importantes. Premièrement, le choix de la STIB s'est porté sur un standard (Calypso) dont une partie des spécifications (concernant la sécurité du système) n'est disponible ni directement, ni gratuitement, aux usagers. Le site *www.calypsotechnology.net* mentionne un paiement de 1000 euros et la signature d'un accord de confidentialité pour y accéder.

Cette opacité n'est pourtant pas une nécessité. En cryptographie (ou science de la sécurité de l'information), la protection des données ne se base jamais sur le secret des méthodes utilisées, mais bien sur celui d'une clé numérique. Deuxièmement, aucun système alternatif n'est actuellement prévu pour le voyageur en transport en commun qui serait réticent à utiliser une carte à puce sans contact. Le système MoBIB actuel est donc doublement incompatible avec les exigences légales dont l'interprétation a été précisée par la Commission de la protection de la vie privée.

2. La sécurité

En matière de sécurité informatique, il faut commencer par distinguer la sécurité dite «*en écriture*» sur une carte de celle dite «*en lecture*». En simplifiant, la sécurité en écriture protège principalement les intérêts de la STIB : elle permet par exemple d'éviter qu'un pirate puisse modifier le nombre de trajets disponibles sur son titre de transport. La sécurité en lecture protège plutôt la vie privée des utilisateurs du métro : elle permet d'éviter que les données stockées sur la carte soient lisibles par des tiers. Sur ce sujet, les choix effectués par la STIB sont pour le moins discutables. D'abord, il faut constater que si des mécanismes de sécurité sont mis en œuvre pour protéger l'écriture, rien n'est prévu pour protéger la lecture. A peine quelques mois après la mise en circulation de la carte MoBIB, des chercheurs ont constaté que l'identité de leurs détenteurs, leur date de naissance, leur code postal et les lieux et heures des trois derniers compostages étaient accessibles en clair (sans protection cryptographique), à tout possesseur d'un lecteur de cartes à puces sans fil (en vente libre). Pourtant, même en supposant que le stockage de ces données sur la carte soit justifié (ce que nous discuterons plus loin dans le texte), la loi belge est claire :

UCL

Les chercheurs de l'UCL ont constaté quelques mois après la mise en service de la carte MoBIB que les données étaient accessibles en clair.

DENIS DEVOS

Il suffit d'un simple lecteur de carte à puce pour avoir accès aux données stockées par MoBIB.

«***Afin de garantir la sécurité des données à caractère personnel, le responsable du traitement (...) doit prendre les mesures techniques et organisationnelles requises pour protéger ces données contre (...) la modification, l'accès et tout autre traitement non autorisé. Ces mesures doivent assurer un niveau de protection adéquat, compte tenu, d'une part, de l'état de la technique en la matière et des frais qu'entraîne l'application de ces mesures et, d'autre part, de la nature des données à protéger et des risques potentiels***». Notons que la protection de la lecture, et donc de l'anonymat des utilisateurs du métro, avec les mêmes techniques que celles choisies pour protéger l'écriture, n'aurait engendré aucun coût supplémentaire pour la STIB. L'absence de ce mécanisme minimum dans la carte MoBIB actuellement déployée relève donc de la négligence gratuite.

Les faiblesses de protection de la carte MoBIB

Pour la protection de la lecture et même pour la sécurité en écriture, les choix technologiques de la STIB sont loin d'être à la hauteur des standards techniques et de l'état de l'art. En effet, le seul mécanisme de protection prévu par le standard Calypso, utilisé pour la carte MoBIB, est basé sur la méthode de chiffrement DES (pour Data Encryption Standard), datant de 1977, et sur deux variantes de celle-ci : DES-X et Triple DES. La méthode de chiffrement DES est pourtant obsolète : un nouveau standard, AES (pour Advanced Encryption Standard) a été choisi par la communauté scientifique en octobre 2000. De plus, l'Institut National des Standards et Technologies (NIST) des USA a retiré le DES de la liste des méthodes recommandées en 2005, estimant sa sécurité insuffisante pour les applications actuelles.

La carte MoBIB étant une application nouvelle, pour laquelle aucune contrainte de compatibilité avec d'anciennes infrastructures ne se posait a priori, on peut s'interroger sur la pertinence de l'utilisation de technologies en fin de vie, voire périmées, comme base de la solution adoptée. Il faut aussi mentionner que le standard Calypso ne possède que des outils cryptographiques permettant le chiffrement des données. Les fonctionnalités avancées que l'on retrouve sur la plupart des cartes bancaires actuelles, permettant par exemple de mettre en œuvre de meilleures propriétés d'anonymat, sont absentes. Enfin, il faut noter qu'au-delà des techniques cryptographiques choisies pour la carte MoBIB, peu d'indications sont données quant à la sécurité «*physique*» du circuit électronique utilisé. On parle d'attaques physiques lorsqu'un pirate ne se contente pas d'espionner les entrées et sorties de la carte à puce, mais profite aussi d'autres canaux de communication. Par exemple, la consommation électrique d'un circuit peut être utilisée pour réaliser une sorte d'électro-encéphalogramme, qui donne à l'adversaire des informations supplémentaires pour retrouver les clés de protection. Précisons que ce contexte d'attaque est tout à fait réaliste dans le cas d'un ticket de transport. Il serait donc intéressant que la STIB informe également ses clients sur cette question, par exemple en publiant les résultats d'un rapport de certification, tel que communément requis dans l'industrie bancaire, pour les applications sécurisées.

Sur ces différents points, soulignons enfin que ce n'est pas seulement la vie privée des utilisateurs qui est menacée, mais aussi l'intégrité du système complet. Il n'est pas exclu qu'un pirate profite de la faiblesse des protections de la carte MoBIB, dans le cadre d'une fraude.

SEBASTIEN KENNES

Un membre d'un collectif citoyen interpelle un usager sur les implications du système MoBIB.

3. La finalité

Citons à nouveau la loi belge : «***Les données collectées doivent être adéquates, pertinentes, non excessives au regard des finalités pour lesquelles elles sont obtenues et pour lesquelles elles sont traitées ultérieurement***». La Commission de la protection de la vie privée explicite ce principe de «*minimisation des données*» et détaille : «*lorsque les données personnelles ne sont pas nécessaires, il ne faut pas les collecter. Lorsque leur collecte est indispensable pour répondre à des objectifs spécifiques, des technologies doivent être mises au point, afin que les individus puissent utiliser les services de manière totalement anonyme, ou en employant un pseudonyme*». Sur cette question essentielle, il faut d'abord rappeler que les finalités de la carte MoBIB sont «*la lutte contre la fraude*» et «*la gestion de la clientèle*». Concernant la lutte contre la fraude, il est évident que les données collectées par la STIB sont excessives. En effet, pour assurer cette fonctionnalité, il suffirait à la STIB de vérifier que chaque utilisateur soit en possession d'un ticket valide et, dans le cas contraire seulement, de procéder à un relevé d'identité. Il n'est donc pas nécessaire que le ticket (électronique ou en papier) révèle d'information à caractère personnel par défaut. Par ailleurs, concernant la gestion de la clientèle et du trafic, les tickets électroniques peuvent être un excellent outil pour optimiser le service de transport et obtenir des informations précises quant à la fréquentation des différentes lignes. Il n'est cependant pas nécessaire de stocker d'informations à caractère personnel pour ce faire. Des identifiants renouvelés aléatoirement à chaque compostage de ticket permettraient à la STIB de réaliser ces statistiques de fréquentation de façon parfaitement anonyme. En résumé, l'essentiel est de souligner que l'état de l'art permet d'apporter une solution technique aux impératifs juridiques. Malheureusement, le standard Calypso choisi par la STIB ne dispose pas d'une grande capacité d'adaptation, vu ses fonctionnalités limitées. A moyen terme, l'évolution du système vers des cartes à puces plus puissantes, et une infrastructure offrant de meilleures propriétés d'anonymat, semble donc souhaitable.

4. La gestion des bases de données

Ce point est presque accessoire au vu des arguments qui précèdent, car au final, les données stockées ne devraient pas être associables à un utilisateur de transports publics. Il faut néanmoins mentionner que, jusqu'à présent, les courriers envoyés par la STIB à ses clients ne contiennent pas de renseignements clairs au sujet de la durée de conservation des données relatives aux

trajets effectués par ceux-ci. A ce sujet, la loi belge est pourtant explicite : **Les données doivent être conservées (...) pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont obtenues.**

Pour conclure, soulignons que le cas du ticket de transport évoqué dans cet article n'est habituellement pas ressenti comme un danger grave par le citoyen. Il constitue pourtant un précédent préoccupant, dans la mesure où il illustre parfaitement le développement mal contrôlé de technologies potentiellement invasives. D'autres utilisations des puces électroniques sans contact, dans le domaine de la santé, de l'éducation, ou pour l'accès à un nombre croissant de services, ainsi que la possibilité éventuelle de combiner toutes les données recueillies par différentes sources, sont autant d'invitations à une réflexion en profondeur et à une application stricte de la loi. Par ailleurs, la situation actuelle est décevante, dans la mesure où l'expertise nécessaire à la conception de systèmes électroniques sécurisés existe, en Belgique et en Europe, dans les entreprises et les universités. Les textes juridiques sont également clairs quant à la volonté du législateur de protéger la vie privée des personnes.

L'évolution de la carte MoBIB vers une nouvelle version, offrant de meilleures propriétés de sécurité et se conformant à la loi belge sur la protection des données à caractère personnel, est donc nécessaire. Notons aussi que le maintien des tickets de transport en papier, en tant que système alternatif proposé aux utilisateurs du métro et du tram, est d'autant plus important que la carte MoBIB ne présente pas les mêmes propriétés d'anonymat. Mais le maintien des tickets doit aussi s'envisager pour des raisons budgétaires. Si le coût d'une infrastructure électronique anonyme (à évaluer) s'avère, dans un premier temps, trop élevé pour la STIB, cela signifie qu'un délai supplémentaire aurait dû (et doit encore) être envisagé, avant la généralisation des cartes MoBIB et sa substitution aux tickets en papier. Précisons que l'objectif de cet article est constructif. En réagissant positivement aux critiques formulées, la STIB pourrait se poser en exemple, favorisant l'évolution positive de systèmes de paiement électroniques anonymes. Enfin, les utilisateurs préoccupés par ces questions seront intéressés par l'action entreprise par la Ligue des Droits de l'Homme, qui vise à encourager une amélioration du respect de la vie privée des utilisateurs des transports publics bruxellois. Les détails de cette action (et la lettre à adresser à la STIB) sont disponibles à l'adresse suivante : *http://www.liguedh.be/*. Les suites de la campagne sont présentées en page 15.

François-Xavier Standaert et François Koeune (Crypto Group, UCL, Louvain-la-Neuve)
Franck Dumortier et Antoinette Rouvroy (Centre de Recherche Informatique et Droit, FUNDP, Namur)

JEROME MATAGNE

Pour laisser la liberté de choix entre l'abonnement MoBIB et la carte papier anonyme, les prix doivent rester équivalents.