Ticket de métro électronique et vie privée.

François-Xavier Standaert, François Koeune
UCL Crypto Group, Université catholique de Louvain

En mai 2008, la Société des Transports Intercommunaux Bruxellois (STIB) introduisait ses premiers tickets de métro électroniques, suivant ainsi une tendance largement observée dans d'autres grandes villes européennes (Paris et Londres, par exemple). Cette mise en circulation a donné lieu à différentes réactions de chercheurs, juristes et associations de consommateurs, s'inquiétant des problèmes éthiques soulevés par ce type de technologie. Dans ce contexte, l'absence de spécifications publiques (que doit permettre le ticket de métro, à qui, dans quelles circonstances?) entretient le scepticisme d'un certain nombre d'utilisateurs. Et l'absence d'une volonté politique claire empêche de lever ces réticences. Un rapide coup d'oeil aux évolutions possibles des technologies sans fil suggère pourtant que le ticket de métro pourrait servir d'exemple pour la bonne gestion d'autres objets électroniques bien plus invasifs.

La RFID ou identification par radiofréquence permet d'identifier à distance des objets, animaux ou personnes, sans contact physique ni visuel[1]. On la retrouve aujourd'hui dans de nombreuses applications : badges ou cartes d'accès à des bâtiments, abonnements à divers services, clés de voitures, antivols, étiquettes de produits dans les supermarchés, … En forçant un peu le trait, on peut dire que l'utilisation de RFID s'accompagne de deux risques principaux. D'une part, il existe un problème de sécurité : il s'agit d'éviter l'usurpation d'identité dans un contrôle d'accès ou l'utilisation non autorisée d'un service. D'autre part, il existe un problème de respect de la vie privée : il s'agit d'éviter qu'une puce électronique ne révèle trop d'information sur ses utilisateurs, permette de suivre leurs déplacements, … Ce risque s'illustre facilement avec le compostage d'un titre de transport public : alors que cette opération est anonyme dans le cas d'un ticket en papier, elle ne l'est plus forcément lorsque le ticket est électronique. En effet, si chaque utilisateur conserve la même carte à puce pour valider tous ses déplacements, un numéro d'identification présent dans ces cartes peut permettre d'enregistrer les dates et lieux de compostages. Le contrôle d'un billet étant invisible pour l'utilisateur, cette identification n'est d'ailleurs pas obligatoirement limitée aux moments d'utilisation du métro. Un traceur malveillant pourrait être caché n'importe où. Il en résulte la crainte d'un contrôle accru des citoyens telle que régulièrement commentée dans la presse quotidienne et spécialisée.

En théorie, le développement de tickets de métro électroniques est pourtant encadré par deux principes juridiques rassurants[2]. D'une part, les lois sur la criminalité informatique sont applicables. A l'instar d'un ordinateur connecté à un réseau, une carte à puce sans contact est considérée comme faisant partie d'un système informatique auquel un accès intentionnel sans autorisation est punissable. D'autre part, les responsables d'une infrastructure (la STIB dans notre exemple) sont soumis à la législation européenne sur la protection des données à caractère privé. Celle-ci fait appel au principe délicat de proportionnalité : les données recueillies doivent être pertinentes et non excessives. En principe, le consentement préalable des individus est toujours nécessaire à la légitimité du traitement de ces données. En outre, les textes font régulièrement référence à la notion de « *privacy by design* ». L'idée est que les développeurs de technologies doivent permettre l'application de ces règles en rendant disponibles les outils adéquats.

Prenant l'exemple des tickets de métro bruxellois, il semble qu'aucune de ces recommandations n'ait été parfaitement respectée. A peine quelques mois après leur introduction, des chercheurs ont constaté que l'identité des propriétaires, leur date de naissance, leur code postal et les lieux et heures de leurs trois derniers compostages étaient facilement accessibles à tout possesseur d'un lecteur de cartes à puces[3]. Par rapport aux règles énoncées ci-dessus, cela implique (1) que n'importe quel « pirate » peut récupérer ces informations, (2) que l'application du principe de proportionnalité est discutable - on peut en effet se demander dans quelle mesure la STIB a réellement besoin de stocker sur une carte de métro des informations personnelles qui étaient

[1] La Recherche, *Dossier RFID, sécurité et vie privée*, Mai 2006.
[2] Y. Poullet, A. Rouvroy, D. Darquennes, *Le droit à la rencontre des technologies de l'information et de la communication : le cas du RFID*, dans *Droit et nanotechnologies*, collection Droit, sciences et technologies, vol.1, pages 117-134, 2008.
[3] M. De Muelenaere, *Mobib : la carte trop curieuse*, Le Soir, 9 janvier 2009.

absentes des tickets en papier - et (3) que la notion de « *privacy by design* » n'était pas suffisamment déployée pour assurer un haut niveau d'anonymat dans les transports publics. Ces observations sont aussi en contradiction évidente avec les propos de M. Pascal Smet, alors Ministre en charge de la Mobilité de la Région de Bruxelles Capitale, lorsqu'il déclarait : « *les trajets ne sont pas enregistrés au niveau de la carte Mobib, mais ils le sont au niveau du valideur* »[4].

Et pourtant, l'utilisation de puces RFID n'est pas obligatoirement synonyme de contrôle accru. Assurer l'anonymat de leurs utilisateurs par rapport à des tiers est possible. A titre d'exemple, une technique intéressante dans le contexte qui nous occupe est celle des preuves à divulgation nulle (ou *zero knowledge*)[5]. En deux mots, une preuve à divulgation nulle me permet de convaincre quelqu'un que je connais un secret, sans pour autant lui révéler la moindre information à propos de ce secret, hormis le fait que je le connais. A partir de cette technique, on peut concevoir des systèmes de tickets virtuels anonymes. L'utilisateur qui consomme un ticket n'en transmet alors qu'une version chiffrée au vérificateur. Ce dernier est incapable de le déchiffrer et ne peut donc pas identifier l'utilisateur par comparaison avec la liste des tickets émis. En revanche il peut, en interagissant avec l'utilisateur et en testant diverses caractéristiques du ticket, vérifier que ce qu'il a reçu est bien la version chiffrée d'un ticket valide et qu'il est donc face à un utilisateur, anonyme certes, mais légitime. Notons que le vérificateur et l'émetteur des tickets peuvent être une seule et même personne sans que cela n'affecte l'anonymat. Ceci signifie que cet anonymat peut aussi être garanti par rapport au gestionnaire du réseau de transports. Bien évidemment, de tels schémas empêchent également le voyageur d'utiliser plusieurs fois le même ticket, par exemple en permettant de détecter une telle double utilisation et, dans ce cas, de briser l'anonymat – et donc de poursuivre le fraudeur.

Ce type de procédé permet d'ailleurs de résoudre d'autres problèmes. Imaginons une personne devant prouver qu'elle a plus de 65 ans pour bénéficier d'un certain tarif. Dans bien des cas (même avec des tickets en papier), on lui demandera de révéler son âge. Et pourtant, prouver que l'on a plus de 65 ans n'est pas équivalent à révéler qu'on en a exactement 67. Des protocoles cryptographiques existent, permettant de convaincre un vérifieur qu'une valeur (ici, l'âge) est supérieure à un certain seuil, sans pour autant révéler la moindre information supplémentaire concernant cette valeur. Cet exemple illustre bien que des tickets de métro électroniques peuvent être aussi anonymes que leurs ancêtres de papier. Dans certains cas, ils peuvent même offrir de meilleures propriétés d'anonymat. Ce n'est donc pas tant le choix d'une technologie qui menace la vie privée de ses utilisateurs que la façon dont elle est déployée. Sur ce sujet, il est finalement intéressant de revenir sur les propos de M. Pascal Smet. Ainsi, lorsqu'il déclarait que l'enregistrement des trajets au niveau du valideur permet « *d'ajuster de manière optimale l'offre et la demande* » de transport, il faut remarquer que ce ne sont pas les identités des usagers qui sont nécessaires pour cet ajustement, mais uniquement leur nombre. A nouveau, des solutions cryptographiques pourraient permettre d'améliorer l'efficacité du service de transport sans pour autant récolter des informations personnelles inutiles dans ce contexte.

Des améliorations technologiques telles que décrites dans cet article ne peuvent évidemment résoudre à elles seules la problématique de la protection de la vie privée. D'abord parce qu'elles ont un coût de développement non négligeable. Il n'est donc pas évident que des entreprises prendront le risque de mettre en oeuvre ces propriétés d'anonymat sans volonté politique. Ensuite parce que la technologie ne fait que répondre à des objectifs qu'il faut bien définir par ailleurs. Enfin parce que la sécurité qu'elles procurent reste relative. Un circuit mettant en oeuvre de bonnes techniques de protection de la vie privée ne sera plus « cassable » en 5 minutes et quelques euros comme la première version de la carte Mobib[6]. Mais il reste une cible raisonnable pour un adversaire bien renseigné et équipé d'un matériel suffisant. Au final, la question qui se pose est celle des critères et mesures de sécurité. Dès le moment où des puces électroniques

---

[4] Parlement de la Région de la Région de Bruxelles Capitale, *Compte rendu intégral des interpellations et questions orales,* mercredi 8 octobre 2008, commission de l'infrastructure chargée des travaux publics et des communications.
[5] J.-J. Quisquater, L.C. Guillou, T.A. Berson, *How to explain zero-knowledge protocols to your children*, annales de la conférence Crypto 19*89*, pages 628-631, Santa Barbara, Californie, Août 1990.
[6] Le terme casser est ici excessif puisque la carte Mobib répond en fait aux spécifications du standard de tickets électroniques Calypso [C09]. C'est donc plutôt l'adéquation de ce standard avec les exigences européennes en matière de respect de la vie privée qui est mériterait d'être analysée plus en détail.

sont impliquées dans des actions qui touchent de près à des droits fondamentaux, comment convaincre les utilisateurs qu'ils peuvent effectivement leur faire confiance ?
A cet égard et bien que préoccupant, le ticket de métro ne contient finalement que peu d'information par rapport à d'autres applications potentiellement ciblées par les technologies sans fil (passeport biométrique et carte d'identité notamment). Une rapide description de quelques évolutions possibles de ces technologies souligne d'ailleurs combien il serait intéressant de s'attaquer à ce problème dès à présent, en profitant d'applications relativement simples et anodines pour mettre en place des outils de contrôle efficaces et fiables.

Une première tendance est celle de la connectivité globale. La réflexion actuellement engagée sur un protocole unique qui permettrait de connecter un nombre presque infini d'adresses[7] à un « Internet des objets » démontre à quel point l'anonymat dans cet énorme réseau sera difficile à respecter. Il faut noter à ce sujet que de nombreux sous réseaux permettent déjà ce type de connexion (GSM, Wifi, …). A nouveau, ce n'est pas tant l'existence de divers réseaux qui est en cause que l'ampleur de leur développement, leur caractère non régulé et la difficulté pour l'utilisateur peu (ou mal) informé d'en ressentir l'impact et de s'en déconnecter. Une seconde tendance est celle de la miniaturisation. Une carte à puce sans contact ou étiquette RFID sont actuellement de petits objets, mais ils sont néanmoins décelables par leur porteur. La diminution des tailles de circuits est une évolution observée de manière constante depuis l'apparition du transistor et rappelle que cette visibilité ne sera plus forcément évidente à l'avenir. A titre d'exemple, un millimètre carré d'un circuit peut aujourd'hui contenir plusieurs millions de transistors et est donc déjà capable de calculs et traitements d'information non négligeables. L'intégration est une autre tendance importante. Un téléphone, un ticket de métro, une carte d'identité ou une carte de banque sont encore des objets distincts. Mais la possibilité de combiner un nombre toujours plus grand de fonctionnalités dans un seul objet électronique implique une confiance toujours plus grande dans un unique système de protection. Enfin, il faut mentionner que si le traçage de personnes porteuses de puces se fait souvent via un numéro d'identification présent dans les circuits, l'anonymisation de ces numéros ne suffit pas toujours à garantir le respect de la vie privée. Dans certains cas, un profilage statistique permet de reconnaître un utilisateur sans avoir recours à aucun identifiant unique. Par exemple, un consommateur dans un supermarché sera rapidement identifiable grâce à ses achats. De la même manière, un utilisateur de Google pourrait être rapidement identifié par ses requêtes.

En conclusion, une combinaison de mécanismes juridiques et technologiques pourrait parfaitement répondre aux inquiétudes citoyennes quant à l'impact d'objets électroniques toujours plus nombreux. Mais sa mise en œuvre demande une volonté politique claire car le respect de la vie privée influence aussi le coût du service offert. Il s'agit donc de spécifier les fonctionnalités demandées, par exemple à un ticket de métro. En caricaturant, il faut choisir entre pas d'anonymat, l'anonymat par rapport aux autres usagers ou l'anonymat par rapport aux autres usagers et le gestionnaire du service (beaucoup d'intermédiaires sont évidemment possibles). Cette décision prise, il faut ensuite mettre en place des critères d'évaluation publics permettant de convaincre le non spécialiste que l'outil technologique qu'il utilise remplit effectivement les fonctions qui lui sont demandées (et aucune autre). Cette discussion pose la question de l'expertise scientifique[8]. Elle souligne l'importance d'une recherche libre de contraintes comme contrepoids aux développements industriels. Elle rappelle aussi la nécessité d'associer différentes disciplines à ces développements dans une perspective préventive. Au final, une politique plus restrictive en matière de gestion des informations à caractère personnel n'est pas toujours en contradiction avec les intérêts privés. Une fois établis, des critères de respect de l'anonymat permettent également aux entreprises de valoriser une expertise qu'elles possèdent pour la plupart déjà. Une régulation transparente résultant d'un compromis crédible entre les intérêts en jeu est donc non seulement possible mais souhaitable pour tous.

[7] Plus de 667 millions de milliards d'adresses IP par mm² carré de surface terrestre pour l'Internet version 6. L'adresse IP est pour un ordinateur connecté à Internet l'équivalent de l'adresse postale d'une maison.
[8] Voir par exemple U. Beck, *La société du risque*, Flammarion, 1986 et P. Kemp, *L'irremplaçable*, Cerf, 1991.