COMMENT BIG BROTHER S'EST MIS LE DOIGT DANS L'ŒIL
Tome 1
[RFID ; la fraude à l'identité facilitée]

« Plus la preuve d'inviolabilité d'une pièce d'identité semble vantée par les institutions, plus simple semble la fraude.
En d'autres termes, la simple possession d'un «passeport biométrique» endormira la confiance des personnes chargées de leur contrôle… c'est là une quasi certitude. »[1]

L'utilisation de l'identité numérique et de la biométrie nous promet un avenir sécuritaire radieux avec le passeport européen biométrique et la carte d'identité française biométrique… Ces cartes ont recours à la technologie des puces RFID (Radio Frequence Identification) pour stocker et récupérer les informations numérisées nous concernant, à l'instar des cartes de transport en commun électronique NAVIGO et TECELY.
C'est, nous dit on, pour rendre infaillible ces papiers d'identification que ce choix a été fait.

Mais la technologie RFID est tout sauf infaillible. Se découvre alors une réussite d'industriels qui surent tirer profit des rêves de pouvoir et de contrôle de nos dirigeants, pour leur refourguer la camelote apte à booster la croissance.
Du clonage de passeport en passant par le virus RFID, petit tour Internet d'articles techno-addict qui ne cessent de découvrir l'ampleur de la mascarade.

[Rappel : Le GIXEL, lobby qui a sut toucher le cœur des gouvernants]

Le Groupement des industries de l'interconnexion des composants et des sous-ensembles électroniques (GIXEL) est un lobby qui compte, entre autres comme adhérents ALCATEL, ALSTOM, EADS, RADIALL, RENAULT, SCHNEIDER electronic, STMicroelectronics…
« Pour sortir de la crise par le haut, il faut une relance de grands programmes dans des domaines d'excellence de la France et de l'Europe. La Filière Electronique et Numérique présente dans ce «Livre Bleu» sa contribution aux réflexions sur le choix et les conditions de réalisation de ces grands programmes.[…]
Intérêt pour la filière et impact économique et industriel : Les infrastructures techniques autorisant l'usage de l'identité numérique comportent de multiples composantes matérielles et logicielles et leur mise en œuvre constitue un atout industriel de premier plan pour la compétitivité économique des sociétés qui y participent. Parmi celles-ci, les industriels de la filière électronique et numérique représentent une part importante dans des domaines tels que: les circuits intégrés, les cartes à puce, les terminaux privés (fixe, portable) ou publics (bornes publiques), les lecteurs… »
Extrait du « Livre bleu ». Voir : http://1984.over-blog.com/article-1712577.html

Les programmes et investissements de l'Etat et du privé qui suivirent lancent pour de bon la mode des puces RFID comme celle de la biométrie. La relance économique est assurée. Mais…

[Premières failles de la technologie RFID]

« Lors du symposium SSTIC 2006, le chercheur Gildas Avoine rapporte qu'il suffirait toujours, pour provoquer un déni de service des émetteurs/récepteurs, de les exposer [les RFID] *à une forte"nuisance" sonore. Dans le cas par exemple, très caricatural, d'un troupeau de vaches balisées par RFID, dont l'éleveur perdrait toute trace à chaque train qui passe, on se dit que*

[1] Extrait de : *Passeport électronique, acte I, scène 1*
http://www.reseaux-telecoms.net/actualites/lire-passeport-electronique-acte-i-scene-1-12116.html

l'application n'est pas critique, que ce n'est pas bien grave. Mais si l'on considère qu'à terme, ces puces présideront aussi aux démarrages des voitures ou à la lecture des passeports électroniques, on peut se poser des questions.
Dès à présent, de tels dispositifs sont par exemple en œuvre sur des véhicules Renault et Ford. Ils en commandent l'ouverture des portes et parfois même le démarrage ; ainsi certaines voitures estampillées du losange ne nécessitent plus de clé physique.
Dans le cas de Ford et d'après une preuve de concept, réalisée par des chercheurs, à partir d'un compromis temps/mémoire, muni d'un PC standard, il suffirait d'une petite minute pour casser cette clé. Pour obtenir l'algorithme, ils indiquent avoir procédé par ingénierie inverse du firmware. »

Source : Nouveau point sur la sécurité, très relative, de la technologie RFID [08/06/2006]
http://www.weka.fr/informatique/securite/itsecurite/actu/failles/43272/

[Un virus RFID qui infecterait les puces par l'intermédiaire des lecteurs]

«Récemment, le fondateur de RSA Security a montré qu'il serait possible de casser la protection de ces puces muni d'un simple téléphone mobile, aujourd'hui on apprend que les étiquettes (tags) RFID pourraient aussi être la proie de codes malicieux.
Dans un article universitaire "Votre chat est-il infecté par un virus informatique", Melanie Rieback, Bruno Crispo et Andrew Tannenbaum, leur professeur, ont dévoilé comment de futurs virus pourraient se propager par ce biais.[...]
Le code, que ces chercheurs ont développé, constitue probablement le premier virus RFID. En infectant la base de données qu'il est censé alimenter, il est capable de se propager aux autres étiquettes radio mises en présence du système. »

Les cartes d'abonnements aux transports en commun comme NAVIGO ou TECELY, lisibles à distances (quelques centimètres) par les bornes de validation, sont équipées de puce RFID.
Imaginons: une fois ces bornes infectées par un virus RFID, elles infecteraient chaque carte qui leur serait présentée. Le même scénario peut très bien s'envisager pour les passeports biométriques et autres cartes d'identité utilisant la technologie RFID; à chaque lecture d'un papier d'identité par une borne contrôlant les frontières, le virus se propagerait.

Source : *Vers l'apparition de virus RFID ?* [17/03/2006]
http://www.weka.fr/informatique/securite/itsecurite/actu/failles/43152/

[Des puces qui n'émetteraient plus]
« Une mini-bombe à impulsion électromagnétique **[pour 7 à 8 euros]**

Faites le vous même!
Explications et recommandations du CCC:
https://events.ccc.de/congress/2005/wiki/RFID-Zapper(EN)
Et
https://23b.nadir.org/rfidzapper

En attendant la commercialisation de gadgets portatifs tels que TagZapper ou RFIDWasher, permettant de désactiver les puces RFID, ou encore l'installation de tels désactivateurs automatisés dans les téléphones portables ou à l'entrée des magasins, la seule méthode 100% efficace consiste aujourd'hui à couper le fil composant l'antenne des puces RFID, au risque d'abîmer les vêtements dans lesquelles elles sont insérées, par exemple.
Afin d'éviter ce type de désagrément, le RFID Zapper pésenté au 22C3 [congrès annuel du Chaos Computer Club (CCC), organisation de hackers allemand, ndr] *génère pour sa part un choc électrique permettant de "griller" la puce. Cette technique, semblable aux bombes à impulsion électromagnétique (EMP) utilisées par les militaires afin de brouiller ou détruire le matériel radio de leurs adversaires, a néanmoins l'inconvénient de pouvoir également nuire aux disquettes, disques durs, cartes à puce et autres pacemakers. Elle pourrait également être mal perçue, tant par les forces de l'ordre que par des vigiles privés, qui pourraient y voir un outil destiné à brouiller les communications radio des avions, hopitaux, etc., ou à voler des objets en magasin.*
Néanmoins, et de même que les couteaux ne servent que très rarement à détourner des avions, on ne peut rejeter d'emblée l'idée d'un tel gadget, ou l'assimiler à quelque chose d'illégal. Et l'on pourra d'autant moins en freiner la fabrication que certains de ces dispositifs sont à la portée de

tout un chacun. Le RFID Zapper, par exemple, est bricolé à partir d'un appareil photo jetable doté d'un flash, dont le film est remplacé par un fil de cuivre, relié à la batterie en lieu et place du flash.

Plus simple encore, Richard Stallman, l'inventeur du logiciel libre, a pour sa part recouvert d'une feuille d'aluminium (à la manière d'une cage de Faraday bloquant les ondes électromagnétiques) le badge confié aux participants du récent Sommet mondial sur la société de l'information, empêchant ainsi les capteurs de pouvoir communiquer avec la puce RFID qui y était incorporée. »

Source: La surveillance high tech est-elle soluble dans le low tech ?
http://www.internetactu.net/?p=6329

[La lecture et la modification possible du contenu des RFID]

« Autre piste explorée : modifier les données que contiennent les puces. En 2003, les artistes et hacktivistes de la Carbon Defense League avaient lancé re-code.com, parodie de boutique en ligne qui permettait de choisir le prix de certains produits, en en modifiant le code barre. Menacé de poursuites, le site a depuis fermé, mais dans la mesure où les RFID ont vocation à supplanter les codes barre, d'autres initiatives similaires surgissent. Pas tant afin de "pirater" les puces qu'afin de pouvoir lire les données qui y sont inscrites, ou transmises, et éventuellement de les corriger ou de les effacer. »

Source: La surveillance high tech est-elle soluble dans le low tech ?
http://www.internetactu.net/?p=6329

« Loïc Dachary *a développé* un logiciel libre *pour lire et modifier les "tags" RFID [...] Développeur au département de recherche sur les interfaces homme/machine à l'Institut national de recherche en informatique et en automatique (*Inria*), ce représentant français de la* Free Software Foundation *pense que le fait que son logiciel soit libre peut aider à combattre le potentiel de surveillance et de restriction de la vie privée que porte la technologie RFID.[...]"Le logiciel permet de savoir quand le tag rentre et sort du champ de l'appareil de lecture et de lire ou modifier les informations qui se trouvent sur le tag, qui est en fait une petite zone mémoire sans fil qui contient entre 32 octets et 8 kilo-octets d'information."[...]*
Publié en licence GPL (General Public License), ce petit "driver" peut être utilisé et modifié librement par toute personne, qui s'engage à reverser au projet les éventuelles améliorations qu'il aura apportées. "Ainsi, la technologie RFID est démocratisée. Chacun peut savoir ce qu'il y a sur les étiquettes et essayer de les modifier, ce qui est impossible avec les logiciels propriétaires", explique Dachary[...]. "C'est très important car aujourd'hui, seuls les grands groupes financent les recherches dans ce domaine. Et ils voient dans cette technologie un grand potentiel de surveillance et de traçage."

Source: Dossier "Les étiquettes intelligentes"
http://www.transfert.net/Les-etiquettes-intelligentes-ont

[Le clonage des RFID à l'encontre de leur infaillibilité]
[Clonage d'un passeport]

La carte d'identité biométrique française sera disponible dès 2008. Le passeport biométrique européen dans la même période. Ces deux papiers d'identité seront munis d'une puce RFID pour stocker notre photo vectorielle numérisée et nos empreintes digitales elles aussi numérisées. Ces deux projets sont présentés comme des outils infalsifiables permettant de lutter contre le terrorisme, l'usurpation d'identité et le vol de documents administratifs.

« Il serait ainsi ridiculement facile de copier le contenu - chiffré - de la puce RFID, de le transposer dans la puce d'un autre passeport, et donc de le cloner intégralement.
Le plus extraordinaire, selon Grunwald, c'est que l'appareillage nécessaire pour se confectionner une copie électronique d'un passeport existant est à la fois réduit et peu onéreux : vous aurez seulement besoin d'un PC doté d'un lecteur-enregistreur de cartes au format SmartCard (un portable dans le cas de la démonstration faite à Las Vegas) et d'un lecteur de puces RFID. Il vous en coûtera aux environs de 1.200 euros en tout et pour tout. Dans ce concert de mauvaises nouvelles, il subsiste un coin de ciel bleu, cependant : l'algorithme de chiffrement des données

stockées sur la puce RFID serait à la hauteur de sa tâche, et seule une copie "en l'état" serait possible. En gros, on pourrait faire un "copier-coller" de données chiffrées, mais on ne pourrait avoir accès aux données elles-mêmes. Ouf... »

Source : RFID : passeport s'il vous plaît (et même s'il ne vous plaît pas) [17/08/06]
http://www.filrfid.org/archive-08-17-2006.html

[Clonage d'une puce sous-cutanée]

Faites le vous même!
Cloner une puce sous-cutanée Verychip.
"Demo: Cloning a Verichip Yourself"
http://cq.cx/vchdiy.pl (page en anglais)

Cette puce, de la taille d'un grain de riz, est injectée sous la peau d'un patient humain et utilise la technologie RFID pour transmettre sans fil l'identifiant unique qu'elle contient. Le dispositif permet à une personne dûment accréditée d'accéder- en principe en toute confidentialité - au dossier médical du porteur de la puce; d'autres applications sont également envisagées, par exemple en matière d'accès sécurisé à des endroits physiques ou à des machines (garantissant qu'un engin donné ne peut être piloté que par des personnes habilitées). Applied Digital avait d'ailleurs annoncé en juillet dernier que des puces Verichip venaient d'être implantées sous la peau du ministre de la justice mexicain, et de plusieurs des membres de son équipe, dans le but d'augmenter leur sécurité.
« Un informaticien canadien vient quant à lui de cloner la célèbre puce Verichip, destinée à être implantée sous la peau, et censée garantir une identification absolue de ses porteurs. »

Source: La surveillance high tech est-elle soluble dans le low tech ?
http://www.internetactu.net/?p=6329

Conclusion

Comment le gouvernement facilite finalement la fraude à l'identité

« Plus la « preuve » d'inviolabilité d'une pièce d'identité semble vantée par les institutions, plus simple semble la fraude. En d'autres termes, la simple possession d'un « passeport biométrique » endormira la confiance des personnes chargées de leur contrôle... c'est là une quasi certitude.
Ce qui risque également de devenir une quasi-certitude, hélas, c'est l'utilisation de ces données numérisées comme « élément de preuve d'identité » à part entière. Sans même que la présence physique du possesseur soit nécessaire. »

Source: Passeport électronique, acte I, scène 1
http://www.reseaux-telecoms.net/actualites/lire-passeport-electronique-acte-i-scene-1-12116.html

« Si les douaniers, par exemple, sont formés pour détecter les faux papiers -ce qui ne signifie pas non plus qu'ils les détectent tous-, que fera-t-on le jour où de faux papiers avec identifiants biométriques et puce RFID, reconnus comme valides par les machines, commenceront à circuler ?

*Plus difficiles à créer, et plus chers que les faux papiers actuels, ils seront réservés à une certaine "*élite*" (mafieux, terroristes, espions, barbouzes). Si les douaniers pourront plus facilement intercepter immigrants illégaux et sans-papiers, nos futures pièces d'identité high tech ne pourront pas pour autant nous prémunir de la menace terroriste. Pire : les nouveaux faux papiers pourraient bien se fondre dans la masse des "faux positifs" et erreurs, imputables tant aux hommes qu'aux machines, qu'on recense d'ores et déjà dans les systèmes en place, et dont la biométrie offre une bonne illustration. »*

Source: La surveillance high tech est-elle soluble dans le low tech ?
http://www.internetactu.net/?p=6329

Aidons à rendre le RFID inutile pour l'Etat, propageons l'information de leurs failles !