

Passeports biométriques Jeudi 14 mai 2009

«La sécurité n'est actuellement pas assurée»

Par Olivier Dessibourg

Nombre de questions se posent concernant la fiabilité technologique du document d'identité, au cœur des votations de ce dimanche. Les réponses, optimistes ou alarmistes, de Serge Vaudenay, spécialiste de l'EPF de Lausanne

Infailible, le passeport biométrique? Non, disent les spécialistes. L'objet est-il pour autant totalement non sécurisé? Non plus. Quelles sont les menaces qui planent sur ce document d'identité? Tout et son contraire a été dit et écrit. Le point avec Serge Vaudenay, professeur au Laboratoire de sécurité et cryptographie de l'EPFL.

Le Temps: Comment fonctionne ce passeport biométrique?

Serge Vaudenay : Une puce électronique ainsi qu'une antenne sont insérées dans l'une de ses pages. Cette puce est passive, sans batterie, mais est capable d'émettre des ondes de radiofréquences à 13.56 MHz (d'où le nom RFID, pour Radio Frequency Identification) lorsqu'elle est sollicitée par les ondes d'un lecteur placé dans son voisinage. Elle lui répond en lui envoyant un numéro qui lui sert à la repérer. Avec le passeport suisse, ce numéro change à chaque sollicitation du lecteur, soit plusieurs fois par seconde. Ce qui est une bonne chose, car cela évite le traçage de la puce. Par contre sur d'autres passeports, dont l'italien ou le néo-zélandais, ce numéro est fixe. Sur l'australien, il ne commence pas par le code 08, fixé par les standards internationaux. Un puissant détecteur peut donc identifier, dans son voisinage, la nationalité des détenteurs de ce type de passeports.

- Certains avancent que le déclenchement d'une bombe pourrait être associé à l'identification d'une nationalité précise (à travers la lecture d'une puce aux propriétés spécifiques). Est-ce réaliste?

- Oui. Et les critères de différenciation des puces entre elles sont nombreux. La vitesse de transmission des informations en est un: la puce des passeports suisses est ainsi aisément distinguable de celle des documents français.

- A quelle distance doit se trouver le détecteur pour lire la puce?

- Avec les lecteurs standards que l'on peut acquérir dans le commerce pour une centaine de francs, on lit la puce à une distance de trois centimètres. Mais selon un rapport de l'Office fédéral de la communication, il est possible de bricoler ces appareils et d'y rajouter une antenne plus puissante, ce qui permet une portée de trois mètres. Par extrapolation, les auteurs de ce rapport ont supposé qu'il serait possible de le faire sur 25 mètres. Ceci en respectant les puissances d'émissions de rayonnement autorisées. Il est donc vraisemblable que l'on puisse facilement lire la plupart des puces à plusieurs mètres.

- Serait-il possible de rendre ces puces moins bavardes?

- Oui. Le problème avec la puce RFID, c'est qu'elle répond à chaque fois qu'on la sollicite, que le passeport soit fermé ou ouvert. Une solution raisonnable pourrait être d'ajouter un système permettant de désactiver la puce lorsqu'elle n'est pas censée répondre, lorsque le passeport est fermé par exemple. Par ailleurs, aux Etats-Unis, une couverture métallique sur le passeport est supposée l'isoler. Mais cette protection est «poreuse», et un faible signal de la puce peut malgré tout être détecté. D'ailleurs, cette faible intensité devient une signature permettant d'identifier le passeport comme américain...

- Une fois la communication établie entre la puce et le lecteur...

-... le lecteur va chercher à prendre connaissance du contenu de la mémoire de la puce. Pour cela,

selon les standards de l'Organisation de l'aviation civile internationale (OACI), il doit passer un contrôle d'accès. Qui se résume à démontrer que l'on connaît quelques informations privées: la date de naissance de la personne, le numéro et la date d'expiration du passeport. Ces trois éléments figurent dans une suite de caractères inscrits dans le document qui peuvent être lus avec un simple scanner optique tel que ceux utilisés aux douanes. Et si une personne (plus ou moins malveillante) a obtenu ces informations par un quelconque moyen, elle obtient un droit d'accès illimité au passeport. Cette «clé d'accès» n'est donc pas très fiable.

- Ne peut-on pas mieux la sécuriser?

- Oui. Il existe un nouveau standard européen (dit EAC) qui offre une bien meilleure sécurité. L'idée: le lecteur doit «montrer» à la puce qu'il est habilité à lire le passeport. Or cette habilitation doit être fournie par l'autorité émettrice du passeport au lecteur (donc à son possesseur), sous forme aussi d'une clé électronique. De plus, cette autorisation est révoquée: si un lecteur vient à être volé, ou si la clé est perdue, il suffit d'attendre sa date d'expiration pour que cela ne compromette pas la sécurité intrinsèque des passeports. Dans le passeport suisse «version 2006», ce système n'est pas utilisé, car il a été finalisé l'an dernier. Il faudra attendre la «version 2010» pour en bénéficier.

- Ce contrôle d'accès passé, que lit le détecteur sur la puce?

- Une copie numérique des données imprimées sur le passeport: nom de la personne, sa nationalité, sa date de naissance, son sexe, ainsi qu'une photo numérisée du visage. Le détecteur lira aussi une signature électronique qui certifie que ces données sont approuvées par l'autorité émettrice. Cette signature est d'ailleurs une preuve irréfutable et transmissible de la validité des données, ce que n'est pas une photocopie: cette dernière peut en effet être le fruit d'une manipulation du document de base. Par contre, la signature électronique est infalsifiable: dans l'état actuel des connaissances, on ne sait pas forger une telle signature sur la base de données non approuvées par l'autorité compétente. En ce sens, il est impossible d'inventer une identité sur un passeport biométrique, mais uniquement possible de cloner un document existant. Ce qui encourage le vol d'identité.

- Dans quelle mesure est-ce possible?

- Imaginons le cas d'un hôtel. Le réceptionniste voit passer des centaines de passeports, qu'il pourrait lire électroniquement. Les photos numérisées ainsi récoltées pourraient être comparées avec celle d'une personne malveillante cherchant à s'approprier une autre identité. Or les algorithmes de reconnaissance faciale actuels ont un taux d'erreur de 1%. A terme, il y a des chances que l'une des photos collectées corresponde à la physionomie de la personne malveillante. Qui pourrait alors totalement s'approprier l'identité d'un client de l'hôtel.

- La reconnaissance faciale n'est donc pas gage de sécurité?

- En deux dimensions, à ce stade, non. Il existe déjà des méthodes en 3D, qui affichent de meilleures performances. Mais pour permettre une identification sûre des personnes, il faudra disposer d'une méthode multimodale, avec plusieurs types de biométrie: reconnaissances de la face et des empreintes digitales. Cela sera possible dans le «passeport 2010».

- Mais là aussi, selon plusieurs experts, il est possible, sur la base de données numériques décrivant une empreinte et à l'aide de quelques simples éléments de bricolage, de la «mouler», de la coller sur son doigt, et ainsi de s'approprier l'identité d'un autre.

- Oui. D'ailleurs mes étudiants l'ont fait avec de la glycérine de suppositoire. Ce sera alors aux officiers de sécurité de vérifier que la personne contrôlée n'a pas un «faux doigt». Mais si ces contrôles sont automatisés, cette remarque tombe...

- Qu'allez-vous voter dimanche?

- Je ne voterai pas, car je suis Français. Mais dans les passeports biométriques actuels, la sécurité n'est pas assurée. Elle pourra mieux l'être avec l'utilisation des standards européens. Cela dit, les bénéfices de ce passeport biométrique sont mis en balance avec les inconvénients. Sans même parler de la nécessité de centraliser les informations dans une base de données centrale. A mon avis, le passeport biométrique est indésirable, mais c'est un mal inévitable dans un avenir proche.