La sécurité des passeports électroniques prise en défaut

- Technologie -

Date de mise en ligne : jeudi 7 juin 2007

Des chercheurs ont montré que le contenu de la puce radio des passeports belges émis entre fin 2004 et juillet 2006 pouvait être lu sans difficulté.

Les passeports électroniques dotés d' une puce radio RFID n'ont pas le vent en poupe. Ces documents, que les pays européens comme la France ont été poussés à mettre en place après les attentats à New York le 11 septembre 2001, sont au coeur d'une polémique en matière de protection de la vie privée.

En effet, les informations personnelles inscrites sur la puce peuvent être lues et décryptées. C'est le cas pour les passeports électroniques belges et anglais, pourtant présentés par leurs gouvernements respectifs comme des documents sécurisés.

Fin 2006, le quotidien britannique The Guardian révélait que le contenu des puces des nouveaux passeports pouvait être décodé en deux jours à peine. Aujourd'hui, c'est la Belgique qui est secouée par des révélations de chercheurs de l'Université catholique de Louvain (UCL).

Ceux-ci ont découvert que les données personnelles inscrites sur la puce radio RFID des passeports émis entre fin 2004 et juillet 2006 pouvaient être lues sans aucun problème, en quelques secondes. De quoi inquiéter fortement les 720 000 détenteurs de ces documents, qui « ne possèdent aucun mécanisme de sécurité » selon le site de l'UCL.

Les trois spécialistes en cryptographie, Gildas Avoine, Kassem Kalach et Jean-Jacques Quisquater, ont démontré qu'il suffisait de passer le passeport à dix centimètres d'un lecteur RFID banal pour afficher le contenu de la puce : la photo d'identité, la signature manuscrite, le nom, les prénoms, le numéro de passeport, le sexe, la date et le lieu de naissance, le lieu d'émission du document, l'autorité ayant délivré le document, les dates d'émission et d'expiration. Une révélation inquiétante.

Un code d'accès parfois trop facile à deviner

« Le vol de cette information ouvre la voie à de nombreuses actions malveillantes », estiment les chercheurs sur leur site. Comme le vol de données personnelles pour réaliser de faux papiers par exemple ou la surveillance des personnes à leur insu. « Il devient en effet possible de "tracer" quelqu'un et de dire où il a été et à quelle heure », indique Jean-Jacques Quisquater, qui dirige l'unité de cryptographie de l'UCL.

« Il n'est pas rare aujourd'hui qu'une administration accepte un document signé reçu par fax. La qualité de la signature manuscrite numérisée dans le passeport est suffisante pour créer un faux fax signé par exemple », ajoute Gildas Avoine.

Les travaux des chercheurs de l'UCL ont aussi montré que les passeports fabriqués après juillet 2006 souffraient également de graves faiblesses, les mêmes que celles mises en évidence sur les passeports anglais, néerlandais, allemands et suisses. Logique, puisque ces différents modèles s'appuient sur le standard de l'Organisation de l'aviation civile internationale (OACI), qui établit des principes de sécurité.

Gildas Avoine explique ainsi que si l'on « passe le passeport [belge de deuxième génération, NDLR] près d'un lecteur, la lecture sera refusée. Pour accéder aux données, il faut indiquer à la puce trois éléments : date de

naissance du titulaire, date d'émission et numéro du passeport. Tant que le document est fermé, on ne connaît pas ces informations et il faut les deviner. » Ces trois éléments se trouvent dans les deux lignes en bas de la première page du passeport.

Il s'avère facile de contourner cette protection. La durée de validité des passeports belges est de cinq ans et leur numéro est attribué par ordre croissant au moment de leur fabrication. De fait, il suffit de tester avec un logiciel, qui s'appuie lui aussi sur les principes de l'OACI, les numéros les uns après les autres pour deviner la bonne combinaison. « Nous sommes capables de lire n'importe quel passeport de seconde génération en quelques heures, voire en quelques minutes si la date de naissance de la personne est connue », nous ont indiqué les chercheurs de Louvain. Dans le cas du passeport anglais, l'opération était plus longue, en raison d'un nombre de combinaisons à tester plus important (la durée de validité étant de dix ans, et non de cinq).

« Aucune fraude constatée »

Et en France ? Les passeports électroniques à puce RFID sont délivrés depuis l'été 2006. Plus de deux millions d'exemplaires ont déjà été écoulés selon un communiqué du ministère de l'Intérieur, daté de mars dernier (1). La puce, intégrée dans la couverture du document, renferme toutes les données de la deuxième page (nom, prénom, nationalité, autorité de délivrance, etc.).

Rien ne permet de dire, pour le moment, que les modèles français puissent être forcés, comme leurs homologues européens. Au moment des révélations britanniques, le ministère de l'Intérieur avait publié un communiqué pour indiquer « qu'aucune fraude ni aucune violation de la confidentialité des données numériques n'ont été constatées » depuis leur lancement. Et ajoutait que « l'accès aux données individuelles contenues dans la puce électronique est verrouillé par un code personnalisé ». Reste donc à savoir si ce code constituera une barrière réelle pour empêcher un accès à la puce ou s'il s'avèrera aussi facile à contourner que dans certains pays.

(1) Rappelons qu'après les passeports électroniques, les pays européens devront mettre en place le passeport dit « biométrique », d'ici à 2009 en principe. La puce du passeport français la puce RFID intégrera les empreintes digitales du demandeur.

Post-scriptum :

http://www.01net.com/article/350471.html