Le passeport biométrique attaqué

Les passeports biométriques français contiennent des puces dites RFID capables de communiquer sans fils. Les données personnelles du voyageur qu'elles contiennent ne deviennent accessibles qu'après que le lecteur de passeport a prouvé son droit de les recevoir en lisant, puis en transmettant à la puce, la clef chiffrée encodée en bas de la première page du passeport. Une fois cette formalité accomplie, le lecteur et le passeport créent une nouvelle clef temporaire pour chiffrer le numéro de passeport, le nom, la date de naissance, la nationalité et la photographie du propriétaire du document.

Toutefois, ce système de sécurité s'est révélé vulnérable. En 2005, il est apparu qu'il était facile de « casser » la clef de sécurité en employant la méthode dite de la force brute. Des failles logiques ont aussi été découvertes dans la conception du système. La première permettait de reconnaître le voyageur en exploitant un message d'erreur envoyé au cours de l'authentification.

En 2010, elle a été corrigée, mais on s'est alors aperçu que la durée exacte du temps de réponse livrait aussi l'identité du voyageur… Plus récemment encore, nous avons montré que la taille et le format des données chiffrées suffisent pour différencier de nombreux passeports, et donc pour les reconnaître dans un contexte particulier. Toutes ces attaques exigent toutefois de savantes mises en œuvre : le contenu des puces RFID de nos passeports est bien mieux protégé que celui de la plupart des puces RFID utilisées au quotidien…

Véronique Cortier,
CNRS-LORIA, Nancy

© Cyril Houshuterstock.com

par les bandits (par les pirates informatiques) ; il nous reste à passer à la pratique (à implémenter le système). Dans cette étape aussi, des failles de sécurité peuvent passer inaperçues. Les spécifications des protocoles n'étant jamais assez exhaustives, il est fréquent que les interprétations qu'en font ceux qui les implémentent confèrent au système certaines particularités, des incompatibilités avec d'autres systèmes, voire des failles de sécurité…

En 2008, on a ainsi découvert une faille dans la version de la suite logicielle *Open*SSH utilisée sur les serveurs *Linux* tournant avec le système d'exploitation *Debian*. Cette suite a été développée par l'équipe du projet *Open*BSD (un projet d'environnement UNIX libre) pour faciliter aux programmeurs l'établissement de connexions sécurisées à partir du protocole SSH (*Secure Shell* en anglais, ou ligne de commande sécurisée). Or il s'est avéré que les paires de clefs RSA de 2048 bits engendrées à l'aide de la version *Debian* de la bibliothèque d'outils de chiffrement *Open*SSL (utilisée par la suite logicielle *Open*SSH) entre 2006 et 2008 avaient en réalité une robustesse équivalente à celle d'une clef de… 16 bits. De fait, 20 minutes suffisaient pour casser les cryptages SSH pour serveurs *Debian*, et prendre ainsi le contrôle de la machine… Compromises, toutes ces clefs ont dû être changées.

Un autre exemple est celui du passeport électronique français introduit en 2006. Ce passeport incorpore une puce de radio-identification (ou RFID, pour *radio frequency identification*) qui, dans la version biométrique en circulation depuis 2008, contient les photos du détenteur et de deux de ses empreintes digitales. Si les spécifications de l'un des protocoles de communication entre la puce RFID du passeport et la borne de lecture étaient initialement correctes, l'implémentation choisie pour la version française du passeport introduisait une faille. Ses concepteurs avaient prévu qu'en cas d'incident d'authentication du passeport auprès d'une borne, un message d'erreur serait émis pour en préciser la cause.

L'intention était bonne, mais cette circulation supplémentaire d'information s'est révélée suffisante pour qu'un attaquant interceptant les communications puisse identifier le passeport français en voie d'authentification, et ainsi le suivre à la trace à travers le monde *(voir l'encadré ci-contre)*.

Ce type d'attaque ne remet pas en cause la spécification du système et ne concerne que certaines implémentations. Il est donc généralement plus aisé de les bloquer. Bien entendu, le mieux est toujours de les éviter en amont de l'implémentation. Il s'agit, là encore, de tester le système de sécurité en le simulant par un modèle théorique le plus réaliste possible. Malheureusement, tout modèle reste… un modèle, c'est-à-dire un jeu permettant de découvrir des attaques possibles dans un cadre restreint, parce que théorique…

Les failles non encore rendues publiques se monnayent

Notons que les failles dont l'existence n'a pas encore été rendue publique se vendent à prix d'or. Il existe en effet un marché de ce que l'on nomme des vulnérabilités « jour zéro » (le jour 1 étant celui de la publication). Ces attaques restées secrètes sont vendues au plus offrant, le plus souvent à des entreprises ou à des États concernés.

Quand la sécurisation des données repose sur une primitive inviolable, qu'elle a été conçue sans aucune faute logique et implé-

BIBLIOGRAPHIE

T. Chothia et V. Smirnov, **A traceability attack against e-passports**, dans *Financial Cryptography*, Springer, vol. 6052, pp. 20-34, 2010.

A. Armando *et al.*, **Formal analysis of SAML 2.0 web browser single sign on : Breaking the SAML-based single sign-on for Google apps.**, 6th ACM Workshop on Formal Methods in Security Engineering (FMSE 2008).

A. K. Lenstra, **Key Lengths, Contribution to the Handbook of Information Security**, Université d'Eindhoven, 2004.

SUR LE WEB

Page Internet du LORIA sur le passeport électronique : www.loria.fr/~glondu/epassport/attaque-tailles.html

Cours et séminaires du Collège de France sur la sécurité informatique : www.college-de-france.fr/site/martin-abadi/