UK : le passeport biométrique se fait hacker en beauté

Un chercheur en sécurité, annonce qu'il a réussi a cracker les nouveaux passeports biométriques britanniques. Un coup dur pour le gouvernement qui mise sur cette technologie pour renforcer la sécurité de ses frontières et mieux contrôler l'immigration.

Pour mener à bien son attaque, Adam Laurie, un consultant en sécurité qui a longtemps travaillé sur la RFID (Radio Fréquence Identification) et le Bluetooth, a simplement utilisé un lecteur RFID et un code personnalisé. D'après lui cette attaque reste totalement invisible. En effet, il a réussi a littéralement siphonner les données du chip RFID d'un passeport placé dans une enveloppe sous scellée.

Cependant cela n'a pas empêché Laurie d'accéder aux données stockées sur le chipset RFID et cela même en étant à plusieurs mètres de sa cible. Il a utilisé le passeport d'une femme affiliée à l'association No2ID, un groupe de protestation farouchement opposé au programme gouvernemental.

« *C'est franchement effrayant* » a déclaré Laurie dont l'expérience a été détaillée dans l'édition dominicale du « *Daily Mail.* »

Le gouvernement britannique qui a commencé a distribuer des passeports RFID il y a un an a l'intention d'y intégrer d'autres mesures de sécurité. Par exemple, des empreintes palmaires et d'autres données biométriques sur le chip. Forcément, de telles mesures ont le don d'agacer les activistes de la défense de la vie privée qui se demandent comment ces informations vont être protégées et gérées.

Pour l'instant, le chip RFID contient des données classiques, le nom, l'adresse, l'age, la photographie du détenteur…

Les données contenus sur le chipset sont bloquées, du moins jusqu'à ce qu'un utilisateur trouve la clé d'encryptage permettant d'y accéder. Cette série de chiffe est calculée en utilisant une combinaison des données personnelles de l'utilisateur, par exemple sa date de naissance, et elle est contenue dans ce que l'on nomme la MRZ « *machine-readable zone* », la chaîne de caractères et les chiffres au bas de la première page du passeport.

Lors du passage à la douane, le lecteur de caractères inscrits à l'encre optique scanne la MRZ et obtient la clé. Dés lors le chipset est débloqué et le contenu peut être lu.

Pourtant, Laurie a réussi à faire tout ce processus tranquillement installé chez lui. Pour cela il a soigneusement étudié le standard ICAO 9303 (International Civil Aviation Organization) qui a été adopté au niveau mondial.

Notons tout de même que Laurie connaissait certaines des données de sa cible comme sa date de naissance. Il a également utilisé le web pour cumuler les informations sur sa cible. Une fois cette étape terminée il a utilisé ce que les hackers appellent un programme de force brute qui répète

plusieurs combinaisons.

Après tout de même 40.000 tentatives, il a finalement trouvé la clé d'encryptage et cracké le passeport. Pour scanner le chip, il a utilisé un lecteur RFID classique de la marque ACG ID.

D'après Laurie, le risque associé a cette faille est énorme puisque une fois les données récupérées il est très facile de faire une copie d'un passeport et de berner les autorités.

Enfin, il a ironisé déclarant :*« Pour le moment, si vous voulez savoir ce qui est sur votre passeport, vous devez vous rendre au bureau des passeports et faire la queue. Avec mon code vous pouvez le faire de chez vous. »*