Étude des passeports électroniques

Patrick Lacharme

GREYC (Ensicaen)
patrick.lacharme@ensicaen.fr

Journées C2 - Avril 2011

Plan

Description d'un passeport électronique

Protocoles de la première génération

Deuxième génération de protocoles

Un passeport électronique

FIGURE: Passeport électronique

Premiers passeports électroniques : Malaisie, 1998.

Première spécification de l'ICAO : 2004 [3].

Zone visible du passeport (MRZ)

La zone visible du passeport (MRZ, *Machine Readable Zone*) correspond aux deux lignes de texte en bas du passeport :

P < FRADALTON < < JOE < < < < < < < < < < < < <
'L898902C'3'FRA'700707'5'M'110623'1'< < < < < <

Les informations contenues dans ces deux lignes :

1. Le nom et prénom du porteur + 3 lettres du pays.
2. Le **numéro du passeport**.
3. La **date de naissance du porteur**.
4. La **date d'expiration du passeport**.
5. 3 digits de contrôle (checksum : $7x_1 + 3x_2 + x_3 \bmod 10$).

Cette zone est lue par un scanner optique (OCR) lors du contrôle du document.

Informations biométriques

Données biométriques encodées au format CBEFF (spécifié dans la norme ISO 19785).

Deux types de données biométriques pouvant être intégrées dans un passeport :

- Données *non sensibles* : **photographie faciale numérisée** en format jpeg.
- Données *sensibles* : emplacement pour les **empreintes digitales** ou l'iris.

L'Union Européenne rend obligatoire la présence des empreintes digitales à partir de 2009.

On parle aussi de passeport biométrique.

Données intégrées en mémoire

La mémoire contient 16 groupes de données, notés DG1,..., DG16 et une zone SOD (*Document Security Object*). Ces données sont protégées en écriture.

- DG1 contient les deux lignes du bas du passeport (MRZ).
- DG2 contient le fichier jpeg de la photo.
- DG3 contient les empreintes digitales et DG4 l'iris.
- DG14 et DG15 contiennent des clés publiques.

Ces données sont hachées, puis signées par le pays d'origine. Le résultat est stocké dans la zone SOD.

Il existe une section sécurisée utilisée pour stocker des clés secrètes qui ne peut être lue ou copiée de l'extérieur.

Technologie sans contact

Le passeport électronique doit contenir un circuit intégré (Doc. 9303 de l'ICAO, 2004, [3]).

La puce sans contact est conforme à la norme ISO 14443 (standard pour les puces RFID de proximité).

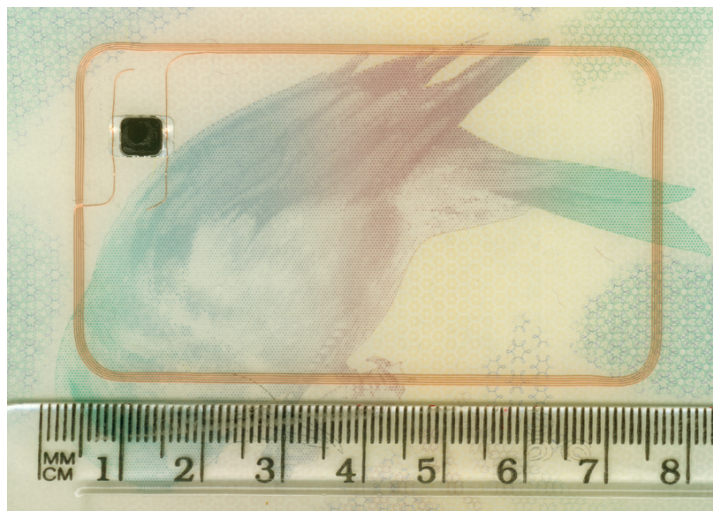

FIGURE: Puce RFID

Vulnérabilités de la technologie sans contact

Usurpation d'identité :
Le lecteur (ou le tag) essaie de se faire passer pour un vrai lecteur (ou un vrai tag).

Divulgation d'informations :
Les données contenues dans la puce (ou échangées lors d'une communication) peuvent être récupérées.

Déni de service :
Techniques extrèmement variées (destruction, brouillage électromagnétique, ...).

Traçabilité malveillante :
Récupérer des informations sur le porteur du passeport, ses déplacements (heure, lieu).

Mise en oeuvre des attaques

Attaque par interception :
Un attaquant intercepte une communication entre un lecteur et une puce. Nécessite la mise en place d'un canal de communication sécurisé entre la puce et le lecteur.

Attaque active :
Un attaquant communique avec la puce, sans le consentement du propriétaire, pour accéder aux informations. Nécessite d'être dans l'entourage de la puce.

Attaque en relais :
La puce qui s'authentifie fait croire au lecteur qu'elle est présente dans son champ d'interrogation (ou inversement), avec un complice. Variante de l'attaque *man in the middle*.

Plan

Description d'un passeport électronique

Protocoles de la première génération

Deuxième génération de protocoles

Protocoles de la première génération

La première spécification de l'ICAO (2004) présente un ensemble de trois protocoles :

1. **Contrôle d'accès** (**BAC**, *Basic Acces Control*)
2. **Authentification passive** (AP, *Passive Authentication*)
3. **Authentification active** (AA, *Active Authentication*)

Seul le protocole d'authentification passive était obligatoire dans la première spécification.

L'objectif du protocole d'authentification active est de vérifier l'authenticité du passeport.

Auhentification passive

Objectif : vérifier que le contenu de la mémoire de la puce n'a pas été modifié (intégrité des données).

Principe : contrôle de la signature des données.

Protocole :

1. Le lecteur retrouve la clé publique de la signature des données et vérifie qu'elle est correcte.
2. Le lecteur calcule le haché des données en mémoire et les compare avec les valeurs stockées.

Protocole d'accès aux données (BAC)

Objectifs :

Empécher toute communication avec la puce à l'insu du porteur

Établir une clé de session pour chiffrer les communications futures entre le lecteur et la puce (une nouvelle clé de session est établie à chaque contrôle).

Principe :

Le lecteur doit lire la zone MRZ afin de calculer les clés :

$$K = 128msb(\text{SHA-1}(\text{MRZ})),$$

$$K_{enc} = 128msb(\text{SHA-1}(K||1)),$$

$$K_{mac} = 128msb(\text{SHA-1}(K||2)).$$

Protocole challenge/réponse symétrique, utilisé avec un algorithme de chiffrement 3-DES et un MAC.

Description du protocole BAC

1. La puce génère et envoie un challenge C_p de 64 bits.
2. Le lecteur génère deux mots K_l et C_l de 64 bits et envoie à la puce $\text{MAC}(\text{ENC}(C_l||C_p||K_l))||\text{ENC}(C_l||C_p||K_l)$.
3. La puce déchiffre le challenge C_p et extrait la clé K_l.
4. La puce génère une clé K_p de 64 bits et envoie au lecteur $\text{MAC}(\text{ENC}(C_p||C_l||K_p))||\text{ENC}(C_p||C_l||K_p)$.
5. Le lecteur retrouve son challenge C_l et extrait la clé K_p.
6. Le lecteur et la puce calculent la clé $K = K_l \oplus K_p$, puis $K_{enc} = 128msb(\text{SHA-1}(K||1))$, et $K_{mac} = 128msb(\text{SHA-1}(K||2))$.

Vulnérabilités du protocole BAC

Accès à la zone MRZ :

Les données décrites sur la zone MRZ peuvent être lues directement sur le passeport (personnel d'un aéroport,..) ou connues partiellement (date de naissance).

Entropie de la clé BAC :

La clé de 128 bits, dérivée de la zone MRZ possède peu d'entropie. Possibilité de faire une recherche exhaustive.

Corrélation possible entre la date d'expiration et du numéro du passeport électronique.

Mise en oeuvre

Attaque active (on-line) :

Envoyer suffisament de requêtes au passeport pour déterminer la clé de session par force brute.

Difficile à mener à cause du temps de réponse de la puce.

Attaque par interception (off-line) :

Cette attaque requiert l'interception d'une communication normale entre un lecteur et un passeport.

Le signal du tag RFID est plus difficile à intercepter que celui du lecteur (en terme de distance).

Example : attaque sur le passeport belge (G. Avoine, K. Kalach et J.J. Quisquater, 2008 [1]).

Plan

Description d'un passeport électronique

Protocoles de la première génération

Deuxième génération de protocoles

Extended Access Control (EAC) v.1

Spécification proposée par D. Kügler (BSI, 2005 [2]) pour les passeports de l'Union Européenne.

Utilisation successive de trois protocoles :

1. Le lecteur et le passeport établissent une clé de session pour chiffrer les communications avec le **protocole BAC**.
2. **Authentification de la puce** (remplace le protocole d'authentification active).
3. **Authentification du lecteur** (utilise une PKI).

Sécurité : utilisation du protocole BAC (et ses vulnérabilités). La puce ne possède pas d'horloge interne pour s'assurer que le lecteur possède un certificat valide.

Extended Access Control, version 2

Nouvelles spécifications présentées par le BSI (2008, [2]) :

Accès aux données biométriques non sensibles :

1. Protocole BAC.
2. Authentification de la puce v1.
3. Authentification du lecteur v1.

Accès aux données biométriques sensibles :

1. Protocole PACE.
2. Authentification du lecteur v2.
3. Authentification de la puce v2.

Protocole d'accès PACE

Password **A**uthenticated **C**onnection **E**stablishment (PACE) :

Objectif : Remplacer le protocole BAC (et ses vulnérabilités).

Permettre à la puce de vérifier que l'accès aux données ne soit pas fait à son insu et établir une clé de session pour l'établissement d'un canal sécurisé entre les deux parties.

Password **A**uthenticated **K**ey **E**xchange (PAKE) :

Protocole d'échange de clés basé sur un mot de passe partagé entre deux entités.

Modèle de sécurité : Bellare, Pointcheval et Rogaway (2000).

PACE : contrôle d'accès

Utilisation d'un mot de passe π partagé par le lecteur et la puce avec une fonction de dérivation de clé :

1. La puce génère un challenge R_p.
2. La puce calcule $K_\pi = \text{SHA-1}(\pi||3)$, chiffre R_p avec la clé K_π et envoie le chiffré z au lecteur.
3. Le lecteur calcule de son coté $K_\pi = \text{SHA-1}(\pi||3)$, déchiffre z et retrouve le challenge R_p.
4. La puce envoie les paramètres du domaine D_p au lecteur.
5. La puce et le lecteur calculent les nouveaux paramètres provisoires de domaine D' avec R_p et D_p.

PACE : génération des clés de session

1. **Échange de clés :**
   La puce et le lecteur génèrent chacun un couple de clés provisoires (Pr_p, Pu_p) et (Pr_l, Pu_l) et dérivent une clé K à l'aide d'un protocole DH ou ECDH et des paramètres D'.

2. **Dérivation des clés :**
   La puce et le lecteur calculent les clés de session : $K_{enc} = \text{SHA-1}(K||1)$ et $K_{mac} = \text{SHA-1}(K||2)$.

3. **Confirmation :**
   Le lecteur envoie $T_l = MAC(K_{mac}, Pu_p)$ à la puce. La puce envoie $T_p = MAC(K_{mac}, Pu_l)$ au lecteur. Chaque partie vérifie en comparant le résultat avec sa clé publique.

Sécurité du protocole PACE

Entropie du mot de passe :

Le mot de passe π, supporte de multiples types de clés, sans relation entre ce mot de passe et le porteur du document. L'entropie de π doit éviter des attaques actives.

Attaque par interception :

L'interception des données échangées ne permet pas de retrouver le mot de passe par recherche exhaustive.

Les clés de session sont générées à partir de clés éphémères (et non du mot de passe).

Protocole SAC :

Protocole **S**upplemental **A**ccess **C**ontrol (PACE v.2) mis en oeuvre actuellement dans les passeports [4, 5].

Conclusion

Intégration des protocoles cryptographiques :

Les protocoles de la dernière spécification ont corrigé de nombreux problèmes de sécurité, mais ne sont pas forcément encore intégrés dans tous les passeports électroniques.

Intégration des données biométriques :

Avis très réservé de la CNIL et du G29 sur l'intégration de données biométriques dans les passeports.

Utilisation de la technologie sans contact :

Risque d'une collecte malveillante de données plus importante. Cette technologie, prévue pour rendre plus rapide le contrôle des usagers, est elle nécessaire ?

Bibliographie

- G. Avoine, K. Kalach et J.J. Quisquater : ePassport : Securing international contacts with contactless chips. Proc. of FC'08, LNCS 5143, p 141-155, 2008.
- BSI- TR-03110, v 2.02 : Advanced Security Mechanism for Machine Readable Travel Documents.
- ICAO- Doc 9303 : Machine Readable Travel Documents - Part 1, Volume 1 (2004) et 2 (2006).
- ISO/IEC JTC1 SC17 WG3/TF5 for ICAO. Supplemental Access Control for Machine Readable Travel Documents. Technical Report, November 11, 2010.
- J.S. Coron, A. Gouget, T. Icart et P. Paillier : Supplemental Access Control (PACE v2) : Security Analysis of PACE integrated Map. `eprint.iacr/org`