Circuit d'une transaction bancaire par carte à puce et sécurité

Nicola Spanti

2016-2017

Les transactions monétaires sont dans une proportion non négligeable faite via des banques, en particulier dans les zones usuellement dites développées. Or au début du 21^{e} siècle, une économie basée sur la monnaie est un élément central dans de nombreuses sociétés humaines. Dans celles-ci, il est donc impératif que les transactions monétaires soient surs à un degré élevé.

Une carte bancaire permet au porteur de s'authentifier sur le système bancaire pour faire une ou des opérations. Le paiement par carte bancaire se faisait historiquement via l'embossage, puis par piste magnétique, or il était facile dans les 2 cas de copier les informations permettant de réaliser une transaction. Cela a poussé à passer à la carte à puce qui permet plus de sécurité.

Nous allons dans cet article expliquer des éléments de sécurité pour les transactions monétaires par carte bancaire à puce.

Table des matières

1 Carte à puce **1**

2 Terminal de Paiement Électronique **2**

3 Serveur acquéreur **2**

4 Serveur émetteur **2**

5 Contrôles bancaires **3**

6 Demande d'autorisation **3**

7 Fin de l'opération **3**

1 Carte à puce

Il n'est pas possible de lire les informations d'une carte à puce, il y a une interface de communication qui permet de faire tampon et de gérer les accès : c'est le système d'exploitation (appelé masque) et les applications qui tournent dessus (en communiquant avec le protocole défini par la norme ISO 7816).

Le code PIN n'est pas enregistré sur la carte, mais un programme sur la carte permet de vérifier si le code est correct. La vérification met théoriquement le même temps peu importe le code correct et le code saisi, ce qui rend beaucoup plus dur les attaques par analyse électromagnétique. Au bout de 3 mauvais codes PIN, une diode de la carte à puce est brûlée, ensuite uniquement la banque émettrice peut réactiver la carte, cela permet d'empêcher les attaques par recherche exhaustive (dite de "force brute") puisqu'il n'y a que 3 diodes, donc au maximum 9 essais. Pour réduire encore la possibilité de trouver le code, une liste de codes triviaux (dont "0000") est interdit. Le code PIN est obligatoire pour les retraits et les paiements directement avec la puce, cependant il ne l'est pas pour les paiements sans contact (pour des raisons de confort), pour limiter les risques seulement des petites transactions sont réalisables avec ce moyen, et il faut généralement retaper son PIN après un nombre (dépendant de l'émetteur) de transactions uniquement sans contact. Le code PIN a été transmis via du papier imprimé par l'arrière, dans le but d'éviter qu'il soit lisible sans l'ouvrir.

Pour vérifier les données, il faut qu'elles soient signées. Cela passe par le mécanisme CDA (*Combined Data Authentication*). Cela permet d'éviter les *yes-card*, des cartes qui acceptent toujours les transactions. Pour plus de sécurité,

les données peuvent aussi être chiffrées. Cela passe historiquement le 3DES (3 DES successifs), et de plus en plus par l'AES.

Les cartes à puce doivent être certifiées "critères communs" (ISO 15408), un ensemble de normes pour vérifier la sécurité informatique. Les cartes doivent également agrémentées, ce qui comprend des tests de sécurité. Parmi les nombreux tests qu'elles doivent passer, il y a les tests du PCI Security Standard Council, notamment PCI-PA-DSS (*Payment Card Industry - Payment Application - Data Security Standard*), et potentiellement PCI-P2PE (chiffrement de bout en bout du point d'interaction jusqu'au tiers fournissant le service). De plus, elles doivent respecter les spécifications GlobalPlatform.

Une carte bancaire a une date d'expiration, généralement 2 à 3 ans après l'émission. Cela permet de renouveller régulièrement le parc de cartes, et donc qu'elles utilisent des technologies encore réputées sécurisées. Cela a par exemple permis de passer de DDA à CDA en environ 2 ans, ce qui était crucial pour limiter la fraude (du système bancaire et pas celle qu'il réalise lui-même ou en tant que complice comme l'évasion fiscale). La carte est désactivée à expiration, mais elle peut l'être pour d'autres raisons, par exemple par opposition du porteur à cause d'un vol.

Pour les cartes sans contact, il peut y avoir un isolement plus ou moins grand entre le paiement avec contact et sans. Par exemple, il peut y avoir 2 PAN, des applications différentes, voire 2 puces indépendantes (mais cela empêche de vérifier au niveau de la carte le nombre de transactions sans code, ce qui peut néanmoins être réalisé au niveau de la banque émettrice).

2 Terminal de Paiement Électronique

Les TPE intéragissent avec la carte et le serveur acquéreur. C'est via son intermédiaire que le code PIN est potentiellement tapé, mais il ne le traite pas, il se contente de le donner à la carte et l'oublier (en théorie en tout cas).

Un TPE n'affiche pas le code, il le masque (généralement en remplaçant les chiffres par des étoiles). De plus, le code est chiffré avec une clé de la banque acquéreur (une KT, une clé de transport).

Il s'occupe de vérifier que celui qui veut réaliser la transaction est bien le porteur et que la carte est valide. Il indique les étapes réalisées (*Transaction Status Information*) et les résultats (*Terminal Verification Results*).

Les messages aux serveurs pourraient être modifiés (par une attaque dite de l'humain du milieu). Chaque message est donc signé (par une clé de scellement, KSC), ce qui permet de détecter qu'un message n'a pas été modifié. Pour éviter d'autres types d'attaques venant du réseau, un pare-feu est configuré, et parfois également un VPN (un tunnel chiffré).

Pour des opérations cryptographiques, une SAM (*Secure Access Module*) peut être utilisée. C'est une carte à puce, mais pas ISO 7816 pour le format.

La sécurité d'un TPE n'est pas que technique et cryptographique, elle est aussi organisationnelle. Une pratique de sécurité organisationnelle triviale, mais nécessaire, est de changer le mot de passe par défaut.

3 Serveur acquéreur

Un serveur acquéreur n'a des données des porteurs de carte que pour les cas de nécessité professionnelle absolue. Il doit néanmoins surveiller les activités, notamment pour tenter de détecter la fraude (contre le système bancaire).

En mesure de sécurité organisationnelle, il faut limiter l'accès physique, car un serveur acquéreur traite beaucoup de données et a des clés secrètes. De plus, celles et ceux qui ont un accès physique à un serveur acquéreur ne doivent pas avoir accès à un serveur émetteur, et inversement.

4 Serveur émetteur

Un serveur émetteur peut envoyer des scripts aux cartes (avec contrôle d'intégrité). Pour la sécurité, cela peut par exemple permettre de révoquer une ou des clés compromises.

Un serveur émetteur s'occupe de la génération des codes confidentiels (c'est un HSM, *High Security Module*, dans ce cas). Les codes doivent être aléatoires, c'est essentiel, sinon ils sont prévisibles, or ils sont un des fondements de la sécurité de la carte. De plus, des éléments pour faire le même code PIN pour une potentielle prochaine carte doivent être conservés.

5 Contrôles bancaires

Un serveur émetteur garde une table des PAN émis. Si un PAN qui n'est pas dedans, mais avec le préfixe de la banque (le BIN, *Bank Identification Number*), cela permet de détecter une fraude.

Les réseaux interbancaires doivent vérifier que la carte à accès au dit réseau. Cela se fait notamment par signature. Pour que le routage soit fait vers le bon réseau, le IIN (*Issuer Identification Number*), les 6 premiers numéros du PAN (*Primary Account Number*), est utilisé. Par exemple, les cartes VISA doivent commencer par 4.

6 Demande d'autorisation

Une demande d'autorisation permet de vérifier que la demande est valide, et donc que le commerçant sera crédité. Dans ce cadre, une demande de capture de carte peut être émise par la banque émettrice en cas de carte volé.

7 Fin de l'opération

À la fin d'une transaction, un ticket est donné à l'acheteur ou l'acheteuse. Cela lui permet d'avoir une preuve papier de l'opération, ainsi que de vérifier le montant de son ou ses achats. De plus, le ticket comprend des informations techniques sur l'opération (type de logiciel carte, Application IDentification de la carte, numéro de siret, condensat de la transaction, etc.). Ces informations pourraient par exemple être utiles en cas de litige.

Dans le cas d'une transaction sans contact, la carte incrémente son compteur du nombre de transactions sans code PIN.

Licence