

France :

2000, route des Lucioles - BP 29 - 06901 Sophia-Antipolis
Tél. : +33 493 330 666 - Fax. : +33 492 944 894

United Kingdom:

200 Brook Drive - Green Park - Reading RG2 6UB
Tel: +44 118 949 7506 - Fax: +44 118 949 7507

La norme 3-D Secure : la sécurité de demain pour le e-commerce ?

AVIS D'EXPERT par Michel Frenkiel

En 2007, les transactions en ligne représentent 5% du nombre total de transactions « scripturales » mais contribuent à hauteur de 32% de la fraude totale à la carte bancaire. Avec un montant de fraude de 33M€ pour la France en 2007 et un accroissement annuel des e-transactions supérieur à 40% par an, il est temps de réagir.

Alors que les organismes spécialisés (CNIL en France, APACS au Royaume Uni, FFIEC aux Etats-Unis) encouragent l'utilisation de l'authentification forte pour sécuriser les transactions, VISA et Mastercard ont développé le protocole 3-D Secure entre les banques et les marchands pour lutter contre la fraude sur les achats en ligne.

La fonction de 3-D Secure est d'authentifier le porteur lors d'un paiement en vérifiant un « secret » partagé entre le porteur et sa banque. Le protocole comporte donc deux étapes :

1. une étape d'enrôlement, où la carte est associée au « secret », par exemple un mot de passe ou une courte liste de questions/réponses liées à l'identité du porteur : couleur des yeux, prénom de la mère, etc.
2. puis des opérations de paiement, au cours desquelles le secret est contrôlé.

En général, l'implémentation du protocole 3-D Secure associe donc un mot de passe à une carte bancaire. Lors d'une transaction, les références de la carte et le mot de passe sont saisis sur le même clavier à quelques secondes d'intervalle, voire dans la même fenêtre. La même technique permet donc de les obtenir à l'insu du porteur (observation, key logger), puis de les réutiliser frauduleusement.

De plus, l'authentification du client peut être effectuée par sa banque ou confiée à un tiers. Le porteur est alors amené à fournir une information sensible (information bancaire et mot de passe) à un site web vers lequel il a été redirigé automatiquement et dont il ne peut pas vérifier qu'il n'est pas un site de phishing. Un tel site de phishing pourrait en effet intercepter les données fournies par le porteur. Ces données pourraient ensuite être utilisées frauduleusement pour effectuer des achats que le porteur aura plus de mal qu'aujourd'hui à répudier.

En effet, contrairement à la solution en place aujourd'hui, dans laquelle l'acheteur en ligne ne court aucun risque, puisqu'il peut annuler une transaction en déclarant qu'il n'en est pas l'auteur, 3-D Secure engage sa responsabilité mais transmet des informations sensibles (références de sa carte et mot de passe) sans lui apporter toutes les garanties souhaitables. En cas de doute ou de question à laquelle il ne souhaite pas répondre, le porteur renonce facilement à son achat, au détriment de tous : lui-même, le commerçant, la banque.

Le problème n'est pas lié au protocole 3-D Secure, mais à son implémentation lorsqu'elle est liée à une authentification par mot de passe ou question/réponse. Compte tenu du besoin croissant de sécurité, il semble souhaitable de remplacer le mot de passe par la reconnaissance d'un élément matériel, réalisant ainsi une authentification forte tout en restant conforme au protocole 3-D Secure.

Une authentification forte est en effet une procédure d'identification qui requiert le contrôle positif de deux éléments ou « facteurs » indépendants d'authentification parmi :

- Ce que l'entité connaît (ici le nom du porteur, numéro et la date d'expiration de sa carte),
- Ce que l'entité détient (un ordinateur ou un token, clé USB, carte à puce..., connecté à son ordinateur).

C'est vers cette solution que des groupements de banques se sont dirigés dès 2004, sans succès. En effet, il n'a pas été possible alors de développer un token (par exemple, un lecteur de carte bancaire) capable de fonctionner sur n'importe quel ordinateur. La situation est bien différente aujourd'hui : non seulement la portabilité des composants s'est améliorée, mais encore il existe des solutions d'authentification forte qui ne font pas appel à des tokens dédiés (Mobilegov SAWS par exemple). Il devient alors possible que le client lui-même choisisse son token

parmi son propre équipement, ce qui lui permet d'utiliser le même token pour plusieurs applications, lui évitant ainsi de se transformer en porte-clé.

Les avantages sont multiples.

Comme avec toute solution faisant intervenir un token connecté à l'ordinateur, l'utilisateur est à l'abri des *key loggers* ou *screen loggers*.

Le contrôle de la présence du token se fait sans intervention du porteur. Le porteur n'est même pas informé que ce contrôle a lieu : avant le contrôle, le site marchand peut lui rappeler de connecter le composant utilisé pour son authentification. Seul le numéro de carte (ou une partie de ce numéro) doit être communiqué au serveur de contrôle d'authentification (car un même porteur peut utiliser le même token pour s'authentifier avec plusieurs cartes).

Un site de phishing qui s'intercalerait dans la procédure ne pourrait au plus récupérer qu'un numéro de carte, ou une partie de ce numéro, inutilisable pour effectuer une transaction même sur un site marchand non sécurisé par 3-D Secure.

La mise en œuvre n'oblige pas le porteur à s'équiper d'un lecteur de carte et ne nécessite aucune installation logicielle sur son poste de travail. Côté serveur, elle n'est pas plus lourde que la solution mot de passe et moins chère qu'une solution de mot de passe à usage unique.