Paiement Electronique

Anthony Garcia Anthony.Garcia@e.ujf-grenoble.fr
Laurent Eyraud Laurent.Eyraud@e.ujf-grenoble.fr

23 décembre 2002

Résumé

Ce document traite du paiement électronique, c'est à dire tous les moyens mis en oeuvre pour effectuer des achats par correspondance sur internet. C'est un commerce en plein essor car le nombre d'utilisateurs potentiels est considérable et qu'il permet une réduction des coûts. Néanmoins, cette nouvelle forme de commerce introduit un certain nombre de problèmes : provenance de l'argent, sécurité des transactions, coût des micropaiements,... Nous allons développer ces problèmes et étudier les solutions existantes.

Mots clés :
Argent électronique, sécurité, micro-paiements, authentification, provenance de l'argent, commerce électronique.

Abstract

This paper is about electronic payment, i.e. all existing means to buy by internet. This business is in full expansion due to a huge potential of users, and also because of the diminution of costs compare to traditional trade. Nevertheless, this new business inputs several problems like money source, trades security, micro payments cost,... Here, we will talk about all these problems and we will examine the solutions.

Keywords:
Electronic money, security, micro payments, authentication, source of money, electronic trade.

Table des matières

1 Introduction

Le paiement électronique est actuellement une forme de commerce par correspondance relativement peu développée. Pourtant, le potentiel de croissance de ce moyen de consommation et l'évolution vers le "tout en ligne" de la société amène à penser que l'avenir de la vente par correspondance est sur le réseau.
Mais ce mode de paiement pose un certain nombre de problèmes liés d'une part au fait qu'on utilise un réseau informatique mais aussi que dans toute vente à distance la notion de contact est absente ce qui implique une nécessaire confiance réciproque entre le client et le commerçant.

2 La problématique du commerce électronique

Il existe un certain nombre de problèmes liés au commerce électronique. Tout d'abord il y a des problèmes d'ordre juridique :

- L'authentification de l'argent électronique
- L'authentification et l'intégrité des échanges client-fournisseur

- La non-répudiation c'est à dire la possibilité de prouver qu'on a émis ou reçu un message

Dans le commerce via internet, on est également confronté à des problèmes d'ordre économique :

- La divisibilité de l'argent c'est à dire la capacité à utiliser son argent sous toutes ses formes
- La disponibilité c'est à dire la possibilité d'utiliser son argent quand on le souhaite

Enfin, il y a bien sur des problèmes de sécurité comme dans toute application utilisant le réseau :

- D'une part la fiabilité du système, pour éviter la perte ou le vol d'argent
- D'autre part la confidentialité afin de protéger le client

Tous les acteurs du domaine se sont évertués à développer différentes solutions aux problèmes que nous avons cités, et nous allons maintenant détailler ces solutions.

3 Provenance de l'argent

Dans cette partie, nous allons nous attacher à détailler les différentes sources de l'argent électronique. Il existe différentes tendances mais toutes ont pour but la sécurité.
La premières source d'argent est la carte bancaire. Dans ce cas, les frais de transaction sont à la charge du commerçant. De plus, il est possible de différer ses paiements et on bénéficie d'une assurance auprès de son organisme bancaire. Actuellement, c'est la méthode la plus fréquemment utilisée.
Deuxième solution : l'utilisation directe de son compte bancaire régulier. L'argent se trouve à la banque du client et celui-ci doit fournir des informations confidentielles pour y accéder.
Une alternative est d'utiliser un compte spécial pour effectuer ses achats. L'argent est stocké sous une forme spéciale et on a recours à un intermédaire qui détient ou délivre l'argent au client. Dans le cas où l'argent est chez l'intermédaire, le client doit créditer son compte et l'intermédaire s'occupe des transactions. L'argent peut avoir différentes formes. Dans le cas où l'argent est chez le particulier, l'intermédiaire se contente de transformer l'argent sous forme électronique. Dans ce cas, il se pose le problème de la conservation des informations.

Enfin, il existe une méthode qui semble être l'avenir du paiement électronique (déja utilisée dans les téléphones mobiles) c'est la carte à puce. Elle nécessite cependant de disposer d'un équipement spécifique chez soi.

4 Les micro-paiements

Ce problème vient du fait que toute transaction a un coût qui est facturé. Or, dans le cas de montants très faibles, il se peut que ce coût soit non négligeable par rapport au coût de l'achat lui-même.
En effet, le coût d'une transaction peut être déterminé à l'aide de la formule suivante : X+(Y% du montant total de l'achat) où X est un montant fixe (par exemple 0.25 euros) et Y un pourcentage prélevé sur l'achat (par exemple 2%).
Pour remédier à cela, il existe plusieurs solutions. La première et la plus simple est de regrouper les achats avant facturation. Ceci suppose cependant que plusieurs achats soient effectués. On peut également utiliser in tiers de confiance qui est en relation avec les organismes financiers et qui se chargera du paiement. Enfin, on peut utiliser de l'argent électronique via un compte spécialisé crédité par le client. Dans ce cas, les frais de transaction sont supprimés mais en contre-partie des frais globaux ont été introduits.

5 La sécurité

La sécurité apparait comme un point essentiel d'un système de commerce électronique, mais qu'entend on par sécurité ? Il peut s'agir de sécuriser le canal de communication afin d'éviter toute intrusion dans une communication. Il peut s'agir aussi d'assurer la sécurité des données transmises, que ce soit en terme d'intégrité ou de confidentialité. Il y aussi tout un aspect authentification des acteurs, à savoir client, commerçant et organisme financier. Enfin, il y aussil'aspect juridique avec la protection des intervenants.

5.1 Intégrée au navigateurs

La première technique de sécurisation que nous allons aborder est celle directement intégrée aux navigateurs. Il s'agit essentiellement du protocole SSL mais nous dirons aussi quelques mots à propos de S-HTTP.

5.1.1 SSL

Le protocole SSL (Secure Socket Layer) a été développé à l'origine par la société Netscape et intégré à son navigateur. Aujourd'hui, la plupart des navigateurs web intègre SSL. Ce protocole assure trois services de sécurité :

- La confidentialité des données par chiffrement symétrique (DES, IDEA, 3DES, RC4,...)
- L'intégrité par l'utilisation de MACs (Message Authentication Code) basés sur des fonctions de hachage (MD5 ou SHA-1)
- L'authentification des entités par l'utilisation de certificats X.509 et des données grâce aux MACs

SSL est indépendant du protocole utilisé (HTTP,telnet,FTP,...). Lors de l'établissement d'une connexion SSL, il y a d'abord une phase de négociation des protocoles de cryptographie qui vont être utilisés entre le client et le serveur. Une fois ces choix effectués les échanges de données peuvent commencer et le canal est sécurisé.
Les principales faiblesses de SSL sont la taille des clés utilisées (128 bits recommandés) mais surtout le fait que l'authentification du client soit optionnelle ce qui constitue un risque important.

5.1.2 S-HTTP

S-HTTP pour Secure HTTP a été développé par CommerceNet à l'origine. C'est une couche au-dessus de HTTP et par conséquent ne fonctionne que pour HTTP et par conséquent est une couche plus haute que pour SSL. On a souvent placé S-HTTP et SSL comme concurrents alors qu'ils peuvent fonctionner en collaboration.
Un message S-HTTP se constitue de trois parties :

- Le message HTTP
- Les préférences cryptographiques de l'envoyeur
- Celles du destinataire

Il assure trois fonctions de sécurité : la confidentialité, l'authentification et la non-répudiation (chose que ne fait pas SSL). Mais il ne s'est jamais réellement imposé.

5.2 PGP

PGP (Pretty Good Privacy) est un protocole de confidentialité. Il combine les avantages de la cryptographie à clé secrète (rapidité) avec les avantages

de la cryptographie à clé publique/clé privée (facilité de mise en oeuvre). Pour cela le message est chiffré avec une clé de session à usage unique qui va servir également à déchiffrer le message (donc le message est chiffré rapidement). Ensuite, cette clé de session est chiffrée avec la clé publique du destinataire. On lui envoie le couple (clé de session chiffrée, message chiffré). Le destinataire utilise sa clé privée pour récupérer la clé de session avec laquelle il peut déchiffrer le message.

5.3 L'authentification

Nous étudions ici le protocole Kerberos. Celui-ci a pour but de décharger les applications du processus d'identification qui n'est pas leur vocation première. Dans ce protocole, on fait appel un serveur qui va se charger d'effectuer l'authentification des clients pour le compte des serveurs d'applications. Les utilisateurs doivent avoir une confiance aveugle dans le serveur kerberos, c'est à dire que toute authentification validée doit être acceptée par les serveurs applicatifs. L'authentification se fait au moyen de tickets délivrés au client. Le client demande une connection à un service au serveur kerberos. Si le client est potentiellement authorisé à y accéder alors kerberos demande l'authentification. Le client fourni alors un ticket crypté avec son mot de passe (connu du serveur). Si l'authentification est valide kerberos fournit au client deux tickets : le premier destiné au serveur d'applications que le client va juste propager et un second appelé ticket granting ticket qui va permettre de refaire appel au service pendant une certaine durée sans avoir à effectuer la phase d'authentification.

5.4 SET et C-SET

SET (Secure Electronic Transaction) a été développé par Visa et Mastercard afin de fournir une norme de chiffrement et d'authentification des opérations par carte bancaire sur Internet. En fait, le client va authentifier le commerçant et réciproquement. Pour ce faire, chacun sera enregistré auprès d'un tiers de confiance qui leur délivrera un certificat. Ainsi, une fois le client authentifié par le commerçant il reçoit un bon de commande et le certificat du commerçant. Une fois le commerçant authentifié, le client peut fournir ses informations bancaires que le commerçant va envoyer à sa banque qui traitera directement avec la banque du client pour authoriser le prélèvement. Il existe une autre version appelé C-SET (C pour card) où le client utilise sa carte bancaire directement via un lecteur de carte intégré à sa machine.

Dans ce cas là, on ne fait plus appel à un tiers de confiance.

6 Conclusion

Le paiement électronique est un domaine en plein essor où beaucoup d'entreprises tentent de s'implanter mais peu réussissent. Il existe aujourd'hui un problème au niveau juridique qui va nécessiter de définir des normes pour ce commerce spécifique afin de palier aux éventuels problèmes. De plus, il subiste encore une certaine méfiance des consommateurs vis à vis d'internet qui constitue un frein au développement du commerce électronique.

Références

[1] http ://developer.netscape.com/tech/security/ssl/howitworks.html. la page de netscape expliquant le fonctionnement de SSL.

[2] http ://web.mit.edu/kerberos/www/. la rubrique kerberos du MIT.

[3] http ://www.expertweb.fr/comel.htm. des informations sur les technologies employées dans le commerce électronique.

[4] http ://www.netbill.com/netbill/works.html. le principe de fonctionnement de netbill.

[5] http ://www.securiteinfo.com/crypto/ssl.shtml. une explication sommaire de SSL.

[6] http ://www.setco.org/. le site pour tout savoir sur le protocole SET.

[7] www.cartes-bancaires.com/. le site du GIE cartes bancaires.

[8] http ://www.rambit.qc.ca/plamondon/ecashind.htm, 1997. site sur le commerce électronique qui aborde tous les aspects.

[9] Gilles Dubertret. *Initiation à la cryptographie*. Number ISBN 2-7117-7087-7. Vuibert, 2002. un livre qui permet de comprendre les principes de base de la cryptographie.