Protection de la vie privée dans le système de paiement 3D-Secure

Aude Plateaux, Patrick Lacharme, Christophe Rosenberger

Protection de la vie privée dans le système de paiement 3D-Secure

Aude Plateaux, Patrick Lacharme et Christophe Rosenberger
prenom.nom@ensicaen.fr

Résumé

Les données personnelles sont nombreuses dans les architectures de paiement sur internet. Les protocoles de paiement comme 3D-Secure sont centrés sur l'authentification des utilisateurs et ne prennent pas en compte la protection de la vie privée. Cet article présente un état des lieux sur le sujet et propose une amélioration de 3D-Secure.

1 Introduction

Le commerce électronique s'est considérablement développé ces dernières années avec une utilisation importante du paiement sur internet. La fraude sur ce type de transactions a augmenté avec la même régularité et a obligé les institutions financières à proposer des systèmes de transactions sécurisées. Plusieurs directives sur la sécurité du commerce électronique ont vu le jour, comme les directives Européennes 2000/31/EC [Par00] et 2009/110/EC [Par09]. D'un autre coté, certains acteurs comme Paypal se sont spécialisé dans le paiement sur Internet en se proposant comme tiers de confiance entre le client et le site marchand. L'industrie bancaire s'est concentrée sur l'authentification des utilisateurs. Le premier protocole proposé fût le protocole SET (Secure Electronic Transactions, [S.E02]). Par la suite les protocoles de paiement ont été renforcés par l'utilisation d'un secret supplémentaire comme un lecteur CAP [Int04] ou l'envoi d'un OTP sur mobile avec le protocole 3D-Secure [Vis02]. Les résultats en termes de sécurité de ces protocoles sont variés [MA10, DMA09] et si le protocole SET a été largement étudié dans la littérature ([MS98, BMPT00, BPM02, BHM06]), le protocole 3D-Secure est lui très peu analysé, à l'exception d'étude partielles comme [MA10, PPWC06]. Quand à la protection des données personnelles elle a été simplement oubliée. Si SET assurait quelques propriétés de protection de la vie privée, tout a été abandonné dans 3D-Secure. L'objectif de cet article est de proposer un état des lieux sur la protection de la vie privée dans le protocole 3D-Secure, puis de proposer quelques améliorations permettant de renforcer la vie privée des utilisateurs sans que la sécurité de ce protocole ne soit remis en cause.

2 Paiement électronique et vie privée

La protection des données personnelles dans le domaine bancaire, et des systèmes de paiement à distance en particulier, doit faire l'objet d'une attention particulière. Par exemple, la CNIL s'intéresse aux grands fichiers du monde bancaire (FICOBA, FCC, etc..), mais aussi aux systèmes de paiement à distance. Ainsi elle rappelle dès 2003 que le numéro de carte bancaire est un réel outil d'identification pouvant être utilisé pour des utilisations secondaires commerciales ou la lutte contre la fraude [CNI03]. La CNIL recommande que l'utilisation secondaire commerciale du numéro de carte bancaire soit soumis au consentement de l'utilisateur et que le numéro soit chiffré de manière irréversible lors des transactions. On peut noter aussi que les banques sont parfois des filiales de groupes financiers plus importants où les données personnelles peuvent transiter d'une société du groupe à l'autre. La CNIL rappelle que cette pratique n'est pas illégale mais réclame le consentement de l'utilisateur [CNI08].

Il y a quatre acteurs toujours impliqués dans un protocole de paiement électronique. Le client qui souhaite réaliser un achat sur le site Internet d'un fournisseur de service SP et leur deux banques respectives. A ces quatres acteurs s'ajoute généralement un cinquième acteur (appelé directory server dans 3D-Secure), dont le rôle sera décrit plus loin. Les services de paiement commencent généralement par une authentification du client et l'ouverture d'un canal sécurisé entre le client et le fournisseur de service, avec le protocole SSL/TLS. Le client envoie ensuite ses informations bancaires comme le PAN (Personal Authentication Number), le cryptogramme visuel CVX2 et la date d'expiration. Certains sites se proposent comme partenaire de confiance, comme Paypal, où le client doit s'enregistrer lors de l'enrôlement en fournissant toutes ses données personelles. On peut toutefois se questionner sur l'utilisation secondaires de ces données puisque la politique de vie privée de Paypal [Pay12] spécifie qu'il est possible de *share some of your personal information with third parties*.

Le protocole SET fût développé par un consortium de sociétés de cartes de crédit comme VISA [VIS58] et MasterCard [MC66]. Ce protocole se déroule en deux pas : l'enregistrement et l'achat. Il assure la confidentialité et l'intégrité des données échangées, ainsi qu'une authentification mutuelle entre le SP et le client, à travers une autorité de confiance qui est la banque du SP. En termes de protection de la vie privée, le SP ne connaît pas les informations bancaires du client et la banque du client ne connaît pas la nature de l'achat de son client. Cependant, le client ne souhaite pas nécessairement faire confiance à la banque du SP et la banque du SP connaît donc l'identité du client. De plus, la banque du client connaît le SP. Enfin, le protocole SET est complexe à mettre en oeuvre pour le client car il demande l'installation d'un logiciel sur son ordinateur et l'utilisation d'un certificat. SET a donc été abandonné au profit de 3D-Secure.

3 Description du protocole 3D-Secure

Le protocole 3D-Secure est un système d'authentification à deux facteurs, utilisé dans les système de paiement sur internet, en plus du protocole SSL/TLS. Il fût développé par Visa en 2001 (décrit dans [Vis02]), mais d'autre organisations ont leur propre implémentation comme MasterCard avec *MasterCard SecureCode*, ou American Express avec *SafeKey*. Ce protocole comprend trois domaines à travers 5 acteurs, où le cinquième acteur, appelé serveur directory, correspond au troisième domaine en plus des deux domaines émétteur (le client et sa banque) et acquéreur (le SP et sa banque). Un module spécifique appelé MPI (Merchant Plug In) est implémenté sur le site web du fournisseur de service SP. Le protocole 3D-Secure se déroule de la manière suivante :

1. Le client envoie au SP son intention d'achat accompagné du PAN, du CVX2 et de la date d'expiration de la carte.
2. Le SP envoie une requête de verification au serveur directory.
3. Le serveur directory contrôle l'identité du SP, le numéro de carte et la banque du client et retrouve la banque émettrice où est enregistrée la carte du client.
4. La banque émettrice contrôle si le client est enregistré dans le programme 3D-Secure et envoie l'URL du client au SP.
5. Le SP envoie une requête d'authentification du client à travers cette URL, contenant les détails de l'achat, en ouvrant une fenêtre pop-up chez le client.
6. Le client s'authentifie auprès de sa banque par cette fenêtre.
7. La banque émettrice envoie au SP une confirmation de l'authentifcation du client, qui est enregistrée.
8. Le SP s'authentifie à sa banque, qui vérifie la nature de la transaction auprès de la banque du client et confirme l'autorisation de paiement au SP. La banque du client stoque les informations de paiement pour assurer la non-répudiation de la transaction.

Contrairement à SET, l'authentification du client est désormais faite par la banque du porteur de la carte (ce qui signifie que l'enrôlement et l'authentification du client est gérée par le domaine émetteur). La principale critique concernant la sécurité de ce protocole était que la banque émettrice demandait simplement la date de naissance du client pour cette authentification [MA10]. Néanmoins, beaucoup de banques se sont ensuite tournées vers l'utilisation d'un mot de passe à usage unique envoyé par SMS sur mobile, ce qui améliore clairement la sécurité du protocole.

4 Analyse de 3D-Secure et améliorations

L'authentification du porteur dans le protocole 3D-Secure est ainsi basé sur l'utilisation de deux canaux distincts (*Out-Of-Band*) et offre une certaine protection contre des attaques du type *man in the computer* causées par des virus informatiques [Sch05, LSH+11]. La confidentialité et l'intégrité des données dans 3D-Secure se base sur SSL/TLS. Le passage de SET vers 3D-Secure a toutefois supprimé toute notion de protection de la vie privée pour les utilisateurs. On peut noter en particulier les problèmes suivants :

1. Le client envoie toute ses informations bancaires au SP.
2. Le SP et la banque du SP connaîssent l'identité du client.
3. Les informations sur l'achat du client sont connues par la banque du SP et par la banque du client.

Le protocole peut être amélioré en utilisant le certificat de la banque du SP. Dans le protocole 3D-Secure, le CVX2 et la date d'expiration ne sont pas nécessaire. Ces données sont présentes uniquement pour la compatibilité avec les systèmes de paiement classiques existants. Ainsi, étant donné que l'authentification du client à sa banque est forte, ces deux éléments sont inutiles. On utilise alors le certificat de la banque du SP qui contient, en plus des informations standards, la clé publique du serveur directory. Il est alors nécessaire de modifier uniquement deux étapes (1. et 3.) du protocole. Dans un premier temps, le client n'envoie au SP que son intention d'achat et son PAN chiffré par la clé publique du serveur directory, cette clé étant présente dans le certificat de la banque du SP initialement fournit par le SP au client. Ensuite, dans l'étape 3., le serveur directory déchiffre le PAN avec sa clé privée et peut ainsi retrouver l'identité de la banque du client.

Cette amélioration permet ainsi de minimaliser la connaissance du SP concernant les informations bancaires du client, puisqu'il n'a plus accès au CVX2 et à la date d'expiration de la carte, celles-ci étant chiffrées par la banque du client. Néanmoins, toutes les exigences en matière de protection de la vie privée ne sont pas remplies, par exemple la banque du client connaît les achats du client. De plus, de manière générale, le client n'est pas anonyme vis-à-vis du cinquième acteur (le serveur directory). Cet acteur est nécessaire pour authentifier les banques entre elles, mais il est possible de mettre en oeuvre une architecture où le client est anonyme vis-à-vis de ce cinquième acteur. D'autres améliorations sont aussi possibles au niveau de la souveraineté des données ou au niveau de l'authentification des différents acteurs. Une critique plus générale sur l'authentification utilisée dans le protocole 3D-Secure concerne la réalité des deux canaux distincts lors de l'authentification du client, lorsque l'achat est réalisé par le smartphone qui reçoit le SMS.

5 Conclusion

Beaucoup d'informations personnelles sont transférées dans les systèmes de paiement à distance, concernant directement la problématique de la protection de la vie privée des utilisateurs. Les systèmes de paiement actuels comme 3D-Secure sont centrés sur l'authentification du porteur et ne servent pas à protèger les données personnelles auprès des différents acteurs. L'amélioration proposée ici permet de garantir plusieurs exigences concernant la protection de la vie privée des utilisateurs, tout en maintenant l'architecture globale de 3D-Secure.

Références

[BHM06] S Brlek, S Hamadou, and J Mullins. A flaw in the electronic commerce protocol SET. *Information Processing Letters*, 97(3) :104–108, 2006.

[BMPT00] Giampaolo Bella, Fabio Massacci, Lawrence Paulson, and Piero Tramontano. Formal verification of cardholder registration in SET. In *ESORICS*, volume 1895 of *Lecture Notes in Computer Science*, pages 159–174, 2000.

[BPM02] Giampaolo Bella, Lawrence C Paulson, and Fabio Massacci. The verification of an industrial payment protocol : The SET purchase phase. In *ACM CCS*, pages 12–20, 2002.

[CNI03] CNIL. Délibération portant adoption d'une recommandation relative au stockage et à l'utilisation du numéro de carte bancaire dans le secteur de la vente à distance, 2003.

[CNI08] CNIL. Guide banque, crédit : êtes vous fichés ?, 2008.

[DMA09] S. Drimer, S. Murdoch, and R. Anderson. Optimised to fail : Card readers for online banking. *Financial Cryptography and Data Security (FC'09)*, pages 184–200, 2009.

[Int04] MasterCard International. Chip authentication program functional architecture, September, 2004.

[LSH+11] S. Li, A. R. Sadeghi, S. Heisrath, R. Schmitz, and J. J. Ahmad. hpin/htan : A lightweight and low-cost e-banking solution against untrusted computers. In *Financial Cryptography and data Security (FC'11)*, volume 7035 of *Lecture Notes in Computer Science*, pages 235–249, 2011.

[MA10] S. Murdoch and R. Anderson. Verified by visa and mastercard securecode : or, how not to design authentication. *Financial Cryptography and Data Security (FC'10)*, pages 336–342, 2010.

[MC66] Mastercard worldwide, 1966. http ://www.mastercard.com/.

[MS98] Catherine Meadows and Paul Syverson. A formal specification of requirements for payment transactions in the SET protocol. In *Financial Cryptography and Data Sceurity (FC'98)*, 1998.

[Par00] European Parliament. Directive 2000/31/EC of the european parliament and of the council of 8 june 2000 on certain legal aspects of information society services, in particular electronic commerce, in the internal market, 2000.

[Par09] European Parliament. Directive 2009/110/ec of the european parliament and of the council of 16 september 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions, 2009.

[Pay12] Paypal. Privacy policy for paypal services, 2012.

[PPWC06] V. Pasupathinathan, J. Pieprzyk, H. Wang, and J.Y. Cho. Formal analysis of card-based payment systems in mobile devices. In *Australasian workshops on Grid computing and e-research*, volume 54, pages 213–220, 2006.

[Sch05] B. Schneier. Two-factor authentication : Too little, too late. *Communications of the ACM*, 48(4) :136, 2005.

[S.E02] S.E.T. Secure electronic transaction specification. *Book 1 : Business Description. Version*, 1, 2002.

[VIS58] Visa corporate, 1958. http ://corporate.visa.com/index.shtml.

[Vis02] Visa. 3D secure protocol specification, core functions, 2002.