BULETINUL Universităţii Petrol – Gaze din Ploieşti	Vol. LX No. 2/2008	71-76	Seria Matematică - Informatică - Fizică

Comparative Study of Internet Payment Security Protocols Based on Credit Cards

Ciprian Stanică-Ezeanu

ASE Bucureşti, Informatics Security Master, P-ţa Romană nr.6, sector 1, Bucureşti, 010374
e-mail : cystanica@yahoo.com

Abstract

The aim of this paper is to present a comparative study between the three most important Internet payment security protocols based on credit cards: iKP, SET and 3D-Secure. There are presented the advantages and disadvantages between those three payment security protocols for understanding why it was necessary to develop new types of protocols that would answer to as many request from the involved parties as possible.

Key words: *iKP, SET, 3D-Secure, payment, security*

Introduction

Once the web has spread, an the user have reached a critical mass, the trading companies, analysts and marketing experts thought that it is worth investing effort in putting together a new technology that would transform the web surfers into potential customers.

At the beginning, the web sites, contained contact information, promotions or even catalogues of products under the form of static HTML pages. The order of products was made through fax, telephone or e-mail. Everything was ok, unless the fact that for getting the products, the client had to pay the value of the products, and the money had to go all the way from the customer until the merchant. The payment was done by using classic mechanisms, through an account open by the merchant in a bank. This implied the customer had to go to a bank and to put the money and to initiate the transfer into the account of the seller. According to the policy of the merchant, in order to start the delivery process asked for a payment proof from the client, either by fax, or by other communications means. Even if they used their own distribution network, or a specialized postal service (post, DHL, etc.), this last phase was theoretically the longest.

One of the main difficulties that the merchants have to deal with when they wish to implement a system for electronic payments is providing a comfortable way of payment, secure, and easy to integrate in a system of online transactions.

This paper presents a comparative study between the three most important systems of payments based on credit cards.

Short History of Security Protocols

iKP which was in usage beginning with mid-1996, is actually the ancestor of SET. iKP is known for the longevity, security and the simplicity of the connection mechanism which made the its experience to be unique. SET appeared at the initiative of VISA and MasterCard, in order to satisfy other needs that iKP did, such as: information confidentiality (both the card owner and the seller had to be authenticated in order to protect al that were involved), independency from other protocols, platforms and operating systems, etc. [1].

However after 2000 new ideas for other protocols much better than SET, started to appear. Moreover since SET proved to be somehow a failure, especially because the actions of the seller were relatively complex. In fact there should have been established more communications with the customer, with the bank and with the payment gateway.

Seeing this lack of interest, a new payment scheme was created at the initiatives of Visa. Compared to SET, 3D-Sercure answers a simpler scheme and allows the integration of a much easier usage for the seller and the buyer. Most responsibilities are now transferred to banks. The main innovation in terms of security is the introduction of SSL/ TLS (at the beginning 3D-Secure was called 3D-SSL). Nowadays it is in general use (starting with 1st of March 2003) and it is supported by Visa, MasterCard, American Express, etc [2].

Comparative Discussion

iKP protocols (i-Key-Protocol, i = 1,2,3) form a family due to the different number of parties that put their public keys, raising the level of security and becoming more sofistacated as the number increases. [1]

- 1KP proposed that only the acquirer should put pairs of public keys.
  - it doesn't offer non-repudiation for the messages sent by the buyers and the sellers, only for the acquirer.
- 2KP implies that also the sellers should have a pairs of public keys and certificates.
  - offers non/repudiation to messages that come from the sellers and the acquirer.
- 3KP says that the buyers should also have their own set of public keys and certificates with public keys.
  - offers non- repudiation for all the involved parties(buyer, seller, acquirer).

Table 1. Comparison between iKP Potocols

The request marked with √ is accomplished, but in a way that could be discussed, while one that is marked with √√ is guaranteed fully accomplished and can be proven.

Requests/ Protocols	1KP	2KP	3KP
Acquirer			
A1. Proof of the Transaction offered by the Buyer. A2. Proof of the Transaction offered by the Seller.	√	√ √√	√√ √√
Seller			
S1. Proof of the Transaction offered by the Acquirer. S2. Proof of the Transaction offered by the Seller.	√√	√√	√√ √√

Buyer			
B1. Unauthorized Payment is impossible. B2 Proof of the Transaction offered by the Acquirer. B3. Certification and Autentification of the Seller. B4. Payment notification from the Seller.	√ √√	√ √√ √√ √√	√√ √√ √√ √√

The main reason for which these 3 types were created was development evolution: 1KP needs minimum PKI and was supposed to be developed immediately after it was proposed in 1995. While 2KP implies that the PKI involves all the sellers, the 3KP must involve both the sellers and the card owners.

Nevertheless, revising what really happened during the development of iKP and of its descendent SET, a protocol such as 1KP was not necessary. It can be noticed that SET is similar to 3KP, from the perspective of authenticating the card owner, of the seller and of the acquirer. In the case of SET, the seller must be able to identify also if the payment gateway is correctly authenticated.[1]

The main difference between SET and its predecessor iKP (especially 3KP) is in the functionality and complexity: iKP was created as a simple protocol that provides certain functions for the payment and it is therefore easily to understand and to analyze. SET was created to offer support for all the options that exist today for the operations of card payment and it is much more complex than iKP, and much harder to analyze, implement and use.

Comparisons can be made also by the point of view of confidentiality offered by the protocols of secure payments. In the case of iKP, during the payment, information such as PIN code, card number and other relevant aspects of the transaction (payment value, identity, etc) is sent encrypted with the public key of the acquirer. iKP protocols do not consider as secret the details of the order, and therefore does not crypt them.

For protecting this type of information other mechanisms are used (SSL or IPSec). This separation in the type of encryption of the order details is one of the main characteristics of iKP and must be compatible with other mechanisms of confidentiality protection.

SET uses the encryption RSA – 1024 to crypt the keys for the DES or 3DES sessions. In this way only the bank can read the card number. One thing that makes SET different from the other protocols is the use of dual signature. This dual signature was used to prevent the spreading of useless knowledge between the parts involved in the transaction, but only to those who are interested. In this way SET considered that the seller doesn't need to know the card number, and also the bank has no need to know what the client bought. By this, the security is guaranteed.

On one hand, there is less information known by the involved parties, and on the other hand the seller obtains the information about the OI (OI= Order Information) and PI (Payment Information) in a way that it is not linked.

The seller could send the PI to the bank. If the seller obtains another OI of the same client, he could say that this corresponds with the PI sent previously. The dual signature does not allow this fraud. A diagram regarding dual signature is presented in Fig.1.

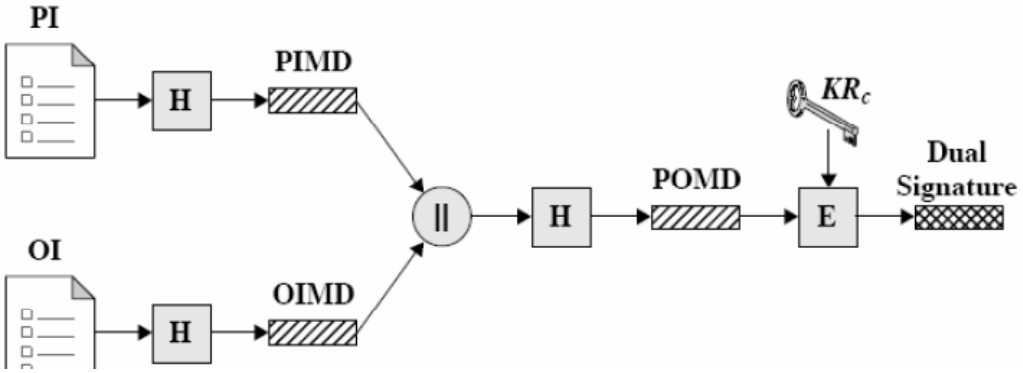

Fig. 1. Dual signature diagram [4]
PI=Payment Information; OI=Order Information; H=Hash function (SHA-1); ||=Concatenation; PIMD=PI Message Digest; OIMD=OI message digest; POMD=Payment Order message digest; E=Encryption (RSA); KR_C = Customer's private signature Key

For 3D-Secure, each entity in the scheme must support TLS Protocol in order to provide a safe connection. Architectural structure of 3D-Secure is shown in Figure 2.
Moreover it must support the RSA, 3DES and SHA algorithms. In the case of 3D-Secure, not like SET, the seller will dispose of the banking information of the client.

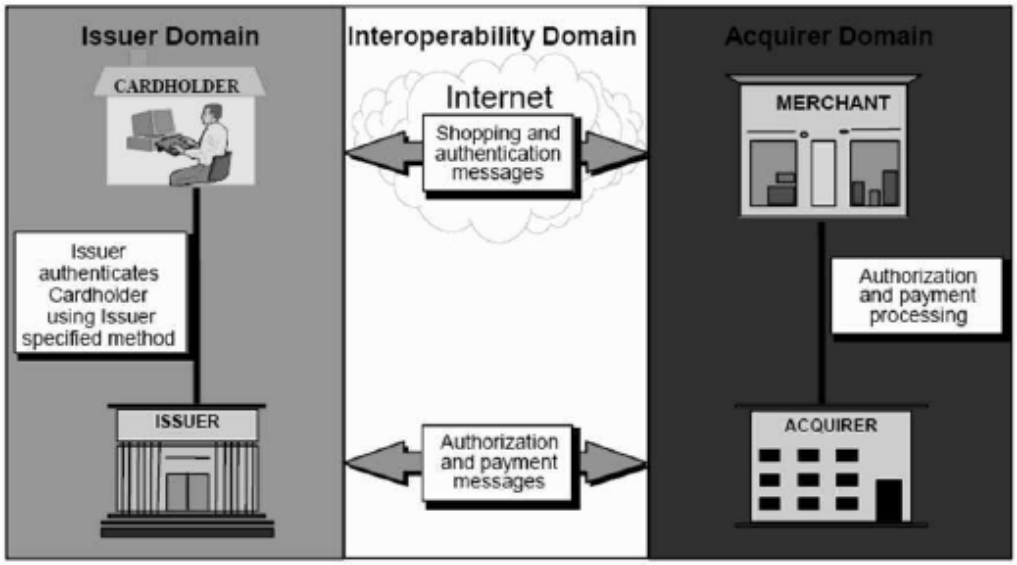

Fig. 2. 3D-Secure Architecture [3]

Using the "Three Domain Model" (3D-Secure) where the user is authenticated on the server hosted by the Issuer can prove to offer a great deal of freedom for the password mechanisms. Anyhow, the portability level is dependent on the authentication mechanism chosen by the Issuer and can be put at risk if the Issuer chooses a mechanism that needs a specific hardware or software on the user's device.

3D-Secure has the possibility to offer more channels of communication between the Card Owner and the ACS. This provides more opportunities for different new items like mobile phones, vocal response systems, etc.

Conclusions

Finally, the advantages and disadvantages of the newest Internet payment protocol 3D-Secure are [5]:

Advantages:

- Common protocol for Visa and MasterCard;
- Sustained by promotion programs, including exchanges of responsibilities between Visa and MasterCard;
- It could be easily proposed to the card owner, without being necessarily needed some extra hardware or software;
- Mobility for users from any places, including Internet Café or job's PCs;
- Card owners are enrolled by Issuer without any special register;
- Less complex then SET;
- It uses a method much more secure of authenticating the Card Owner during the transaction. This scheme is considered as an online alternative for Chip & PIN Cards, where the client is asked to type in a unique password set by the seller before the transaction is complete;
- Reduces the number of chargeback (repudiation from the buyer) received by the seller. A transaction authenticated 3D-Secure(where the client has offered authentication details to the Card Issuer) cannot force the seller to return the money in the case of a fraud, when the client does not admit that he himself used the card in the moment of the transaction. The seller is protected by the card Issuer against client repudiation and returning the money because the bank itself assumes full responsibility. This is the same for all the transactions that use 3D-Secure, when the seller uses 3D-Secure and the buyer doesn't, or when the card Issuer cannot offer validation possibilities to the client. In non-secure transactions, the responsibility belongs to the seller and in case of a fraud in the transaction, he is obliged to return the money. In conclusion 3D-Secure offers greater protection against using the cards in an illegal way.

Disadvantages:

- The complexity of implementing procedure by the seller. A Merchant Server Plug-in is needed and it can be obtained from an ISP or from an Acquirer;
- Payment Information (e.g. :card number, expiring date) can be seen on the Merchant Server;
- The seller is capable of sending the Card Owner to a false ACS, by this having the opportunity to obtain the User ID and password if the Card Owner is not alerted by the absence of the personal assurance message (PAM);
- A great number of links on the Internet (to the Server Directory, History Server and ACS);
- 3D-Secure doesn't automate the PAN introduction.

Kevin Evans, business development manager at ACI World-wide, who created payment gateways for the banks, explained the following: "SET, the original security system for online payments, is dead. On the other hand, VISA (an inventor of SET) developed 3D-Secure, a software that secures the money drawer of the seller. MasterCard developed UCAS as a rival. Instead of keeping the PKI inside the card, like SET did, it authenticates the Card Owner during the transaction by a user ID and password. Smart-Cards and biometrics can be added later".

Before, if a client was having a dispute with the seller, the seller was the one who covered all the expenses. Nowadays, Visa introduced new rules, saying that if the seller uses 3D-Secure, the issuer bank will have no right to pass the cost back to the seller.

References

1. Bellare, M., Garay, J., Hauser, R. - *Journal of Selected Areas in Communications*, Vol. 18, No.4, 2000
2. *** - www.romcard.ro
3. *** - http://www.visaeurope.com/merchant/handlingvisapayments/cardnotpresent/verifiedbyvisa.jsp
4. Yang Li, Yun Wang, - *Secure Electronic Transaction*, http://islab.oregonstate.edu/
5. *** - https://partnernetwork.visa.com/vpn/global/retrieve_document.do?documentRetrievalId=118

Studiu comparativ între protocoalele de securitate pentru plățile pe Internet pe baza cardurilor de credit

Rezumat

Scopul acestei lucrări este prezentarea unui studiu comparativ între trei dintre cele mai importante protocoale de securitate ale plăților pe Internet prin intermediul cardurilor de credit: iKP, SET şi 3D-Secure. Sunt prezentate avantajele şi dezavantajele acestor trei protocoale de securitate a plăților online pentru a înțelege de ce a fost nevoie să fie dezvoltate noi tipuri de protocoale care să răspundă cerințelor tuturor părților implicate într-o tranzacție.