A new protocol for credit card Transaction systems

M. Koleini, M. Berenjkoub, M. Dakhil Alian
Department of Electrical and Computer Engineering, Isfahan University of Technology.
Emails: masoudkoleini@yahoo.com, brnjkb@cc.iut.ac.ir, mdalian@cc.iut.ac.ir

Abstract

In these days, buying goods on the Internet is growing fast and vast amount of money transmits on the Internet. Credit card transaction is a popular means for buying things or services on the open networks. Many credit card payment protocols have been designed up to now; the most famous protocol in this field is Secure Electronic Transaction (SET). This protocol is based on a technique named dual signature and uses PKI as an important infrastructure for getting more secure. But implementation of this protocol designed by credit card suppliers was expensive and using this protocol for customers was very difficult, because they should have a thick wallet and valid certificate on their machines for transaction. So, companies like Visa and MasterCard tried to design other protocols that were less expensive to implement and easier to use. In this way, MasterCard designed UCAF/SPA protocol and Visa designed 3D Secure. This protocol focuses on 3D Secure, a protocol that supports Merchants against unauthenticated transactions. But this protocol has some weaknesses against man in the middle attack. It has been shown that Merchant or another person can open a web page like issuer authentication page on buyer's machine so he can sniff buyer's password. This paper describes benefits and problems of 3D Secure protocol and proposes a new password based payment protocol; which has the core of 3D Secure as the basis. Then a comparison between proposed protocol and 3d Secure would be presented.

Keywords: Credit Card, Fraud, SET, UCAF/SPA, 3D Secure and Payment protocol

1. Introduction

The 2004 EP Study shows that there were 44.5 billion electronic payments made in the United States during 2003 with a value of $27.4 trillion [1]. The large value of credit card transactions results in increase of the amount of fraud in electronic payments. This fraud has grown due to the lack of authentication in credit card transactions especially in transaction using SSL as the only means of security. It has been estimated that 8 percent of online sales were lost in 1999. Online fraud is estimated at 10 percent of sales in 2000 rising 14 percent in 2003 [2]. Estimation shows that about 50% of Internet transactions are paid for by means of credit cards. But this is only 2% of all credit card business; most of which takes place at Point of Sale (POS), e.g. in shops, restaurants and hotels [1]. So, having a good means for a secure credit card transaction can reduce credit card fraud. Good authentication can reduce fraudulent payments on the Internet. It is expected that nearly 80% of all e-commerce chargebacks and fraud, and a substantial proportion of customer complaints, could be eliminated with the use of authenticated payment [3]. New protocol designs are based on good authentication of cardholder. So, stolen credit card numbers cannot be used for any transaction on the Internet based on authentication methods. But these methods have their pros and cons. In these days, expense and ease of use of protocols can affect their security strength. It means if one protocol is a secure protocol but it's implementation is difficult or it is not easy to use for cardholders and Merchants, it cannot be successful in business world. In this paper, some important credit card protocols and their specifications are discussed. In continue some details of 3D Secure protocol are described. According to the problems of 3D Secure, a new protocol will be proposed and a comparison between 3D Secure and proposed protocol will be presented at the end.

2. Credit Card Protocols

The first important protocol designed by IBM, Microsoft, Europay, Netscape and some other companies, is "Secure Electronic Transaction" (SET). SET uses cryptography protocols to protect credit

card transactions on the Internet. MasterCard and Visa published the Implementation of the SET in 1996. The key feature of SET protocol is using dual signature based on digital certificate. It has been shown that SET is the most powerful payment protocol by now and it provides non-repudiation to cardholders and Merchants. But some practical problems made it unsuccessful in implementation. Having a thick wallet that must be installed on cardholder's machine, a digital certificate for cardholder and large computations made it too costly and difficult to implement. In this protocol, cardholder cannot use another computer for his transaction. Issuers and Acquirers should distribute software and manage the issuing and re-issuing digital certificates. Despite upgrading SET to 3D SET, this protocol became obsolete. MasterCard moved to design another protocol namely UCAF/SPA, which had easier implementation than that of SET. Visa designed and implemented 3D Secure protocol too. Also other companies designed other protocols but those didn't become as widespread as 3D Secure and UCAF/SPA.

New protocols are based on three-domain model. This model has cardholder and his issuer in one domain, Merchant and his Acquirer in another and an interoperability domain as the last. The issuer issues card for the cardholders, enrolls them in the system and is responsible to authenticate them during transaction. From April 2002, liability of repudiated payments; which is the result of unauthenticated transactions has shifted from Merchants to the issuers. Acquirers have agreement with Merchants to participate them in Internet transactions. Interoperability domain facilitates electronic transactions between these two domains, by means of providing some required services.

2.1. UCAF/SPA Protocol

MasterCard designed UCAF/SPA protocol for better authenticating the cardholders in transaction flow. SPA (Secure Payment Application) was designed to meet several goals, including the reduction of chargebacks for Issuers and Acquirers, the rapid adoption by Merchants, and the support for debit/credit transactions and for real/virtual/pseudo account numbers [4]. In this protocol, Merchant doesn't need to install any plug in on his server, but simply needs to insert UCAF hidden field in his website software. But cardholder needs to install a thin wallet on his computer. Everybody that wants to have a transaction can use this wallet. This protocol is a password-based one. It means that authentication of cardholder is based only on username and password. So this protocol doesn't use PKI as a base. As a result, UCAF/SPA is easy to use but it is not fully guaranteed about non-repudiation. It has a cryptographic value named AAV (Accountholder Authentication Value) as the proof of transaction and the parameters related to it. The transaction flow of this protocol is simple and more complete description can be found in [4].

2.2. 3D Secure Protocol

Design of 3D Secure is base on what Visa claims: "As of July 2001, chargeback rates for Internet purchase transactions are several times the system average, and Internet-related fraud cases constitute a significant percentage of all reported fraud cases. The majority of the chargeback reasons are fraud-related or cardholders claiming non-participation" [3]. So Visa tried to migrate to a new protocol, which was able to authenticate person who wants to make e-commerce transaction as the authorized cardholder. SSL client and SSL server certificates provide security of channels. Authentication is the most important part of this protocol. It is expected that nearly 80% of all e-commerce chargebacks and fraud, and a substantial proportion of customer complaints, could be eliminated with the use of Authenticated Payment [3]. Figure 1 shows the transaction flow of 3D Secure protocol.

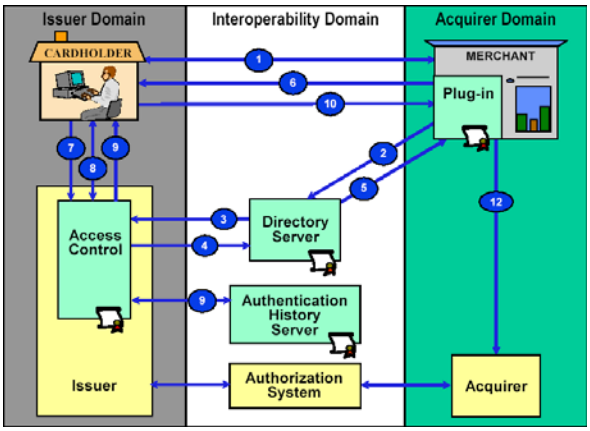

Fig .1 Purchase Transaction in 3D Secure [5]

In this protocol, cardholder needs only his browser to make a purchase. But Merchant needs to install a plug-in on his server. The transaction steps is as below:

1- Customer sends card information to the Merchant.
2- Merchant checks credit card number validity using interoperability domain (Directory Server)
3- If valid, Directory Server (DS) checks enrollment of card number in issuer's server.
4- Issuer responds enrollment response.
5- Directory Server responds validity and enrollment response to Merchant.
6- If valid, Merchant asks card issuer for cardholder authentication via shopper device.
7- Issuer server (ACS) receives the request.
8- Issuer authenticates cardholder through his password.

9- Issuer signs the respond and sends it back to the Merchant via cardholder device and stores information.
10- Merchant receives the response
11- Merchant verifies issuer signature
12- Merchant send authorization request to Acquirer.

A complete description of 3D Secure protocol is presented in [5].

3. Security analysis of 3D Secure protocol

3D Secure has some advantages like ease of use for cardholder, mobility of users, authentication by issuer, centralized authentication history for dispute resolution and less complexity than 3D SET [3]. This protocol has less PKI complexity than 3D SET and only uses digital signature of issuer in a portion of the protocol. But this protocol has some vulnerability including complexity of Merchant implementation, disclosure of credit card information to the Merchant, faking the Access Control Server (ACS), increased number of Internet links and so on [3]. Some other problems that can bring into account are:

1- Sniffing in customer's node
2- Commercial SSL certificates in customer's channels with the strength of 40 bit
3- The ability to send forge order description from Merchant to issuer.

3.1. Attack to 3D Secure protocol

Lack of an observer on the customer's computer makes the 3D Secure vulnerable to some man in the middle attacks. One of them has presented in [6]. Figure 2 shows the message flow of this attack.

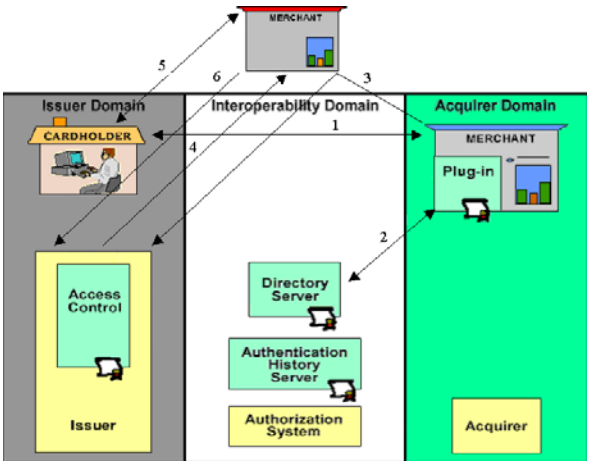

Fig.2 Attack on 3D Secure

In this attack, cardholder goes to the Web Page of Merchant and sends his card information to him. Merchant has a computer in another location, which is related to him. He sends authentication request to cardholder issuer through the middle computer. Issuer opens the authenticating page on the middle computer and asks for entering password. The middle computer opens a page just like this page on cardholder's computer. Cardholder sends his password to the middle computer. Middle computer sends cardholder's password to the issuer. Delivery of goods to the customer completes the transaction. But now, Merchant has all the information of cardholder credit card without any suspicious situation. For details of this attack and how much it could be successful refer to [6].

4. A new credit card transaction protocol

As mentioned before, the lack of an observer on cardholder's computer can simplify the transaction from one point of view. But on the other hand, it may lead to an insecure e-commerce business. In the new approach, it is recommended to install a thin wallet on cardholder's computer that is able to transfer transaction messages and perform a secure hash function. This protocol is based on the structure of 3D Secure protocol. In this password-based protocol, cardholder wallet can authenticate both Merchant and issuer and it doesn't send card information on the Internet. Before introducing the protocol steps, it is useful to be considered some issues:

1- 128-bit SSL can protect the channels from eavesdropping, but without client certificate, it is intractable to authenticate correctly. 40-bit SSL without certificate (in cardholder's computer) can get more privacy, but cannot be fully trusted.
2- Using digital signature by some principals such as Issuer and Acquirer is recommended.
3- Using electronic wallet in cardholder's computer as an observer.
4- Using username and password for authentication and getting more security.
5- Nobody except Merchant knows about orders.

The protocol includes the following steps as depicted in Figure 3:

1- Customer goes to Merchant's web page. After selecting the goods, he enters the payment process. In this section, Merchant sends order description and transaction identifier (TID) to the customer's wallet.
2- Wallet sends following information namely "BuyerComment" to the Merchant:

   "*TID, Issuer ID, Hash (PIN, Username, Exp Date), Hash (TID, Issuer ID, Hash (PIN, Username, Exp Date)*"

In which PIN is the credit card number of the cardholder and "Exp Date" is the expiration date of credit card number.

3- Merchant sends buyer information and some information related to the payment process for Internet Payment Service Provider (IPSP). In some resources, IPSP is called "Payment Gateway". The channel between Merchant and IPSP has been secured by 128-bit SSL with client and server certificates.

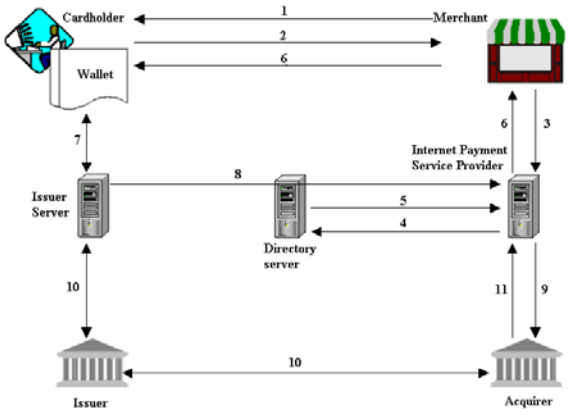

Fig.3 New protocol message flow

4- IPSP extracts Issuer identifier from credit card information and sends payment information to the Directory Server in the interoperability domain.

5- In the Directory Server, there exists a database that has different partitions for each Issuer and in each partition; there exists credit card numbers, which are sorted according to the Hash (PIN, Username, Exp date) as shown below:

Issuer A

Hash (PIN1, Username1, Exp Date1), PIN1, Username1, Exp Date1
Hash (PIN2, Username2, Exp Date2), PIN2, Username2, Exp Date2
.....

Issuer B

Hash (PIN1, Username1, Exp Date1), PIN1, Username1, Exp Date1
Hash (PIN2, Username2, Exp Date2), PIN2, Username2, Exp Date2
.....

Directory Server searches Hash (PIN, Username, Exp date) and extracts the PIN, Username and Exp Date related to it if it exists. Then he creates the following expression namely "DSComment":

"*Hash (PIN, Username, Exp Date, TID, Hash (Order Description)), Issuer"*

Note that nobody can make this message except who has the PIN, Username and Exp Date.

6- IPSP should send DSComment to the cardholder wallet. There are two options to do this. IPSP can send the message directly to the cardholder wallet if it has received his IP. Next, IPSP can send the message via existing SSL channels between IPSP and Merchant and also Merchant and cardholder.

7- Cardholder's wallet has order description and gets the hash of it. Then by the use of current and previous information, he computes DSComment and ensures that it to be exported from the Directory Server. The integrity of this message can authenticate the Merchant from proving of his ability to contact with the Directory Server. Now, the wallet should ask the Issuer to authenticate the cardholder. So it sends the following statement to the Issuer:

"Hash (PIN, Username, Exp Date)"

Issuer has a database like the Directory Server database. This database has cardholder's password in addition to other information like PIN, Username and Exp Date. After inspecting that this statement exists in the database, Issuer extracts the information, creates a nonce and sends the following statement back to the wallet:

"Hash (nonce, PIN, Username, Exp Date, Password), nonce ⊕ Hash (PIN, Username, Exp Date, Password)"

It is clear that nobody can create the statement except who knows all PIN, Username, Exp Date and Password. In this protocol, not only password doesn't go through the transmission lines purely, but also eavesdropper doesn't have a chance to perform dictionary attack to realize the password. After that cardholder receives this statement, he calculates Hash (PIN, Username, Exp Date, Password), extracts the nonce from the statement, checks Hash (nonce, PIN, Username, Exp Date, Password) and ensures that who has sent this statement knows all of the information about the credit card. Then he replies Issuer by the Hash (nonce) to ensure it about his password knowledge.

8- The Issuer checks the statement and after authenticating, creates an encrypted number that contains important information about this payment. The encryption can be done by Issuer private key. It signs this number with some information related to this payment and sends it to the Merchant through existing SSL sessions or directly by a new 128 bit SSL connection to the IPSP.

9- IPSP checks the signature and if it is correct, sends the authorization request to the Acquirer.

10- Acquirer sends the authorization request with the encrypted number to the Issuer. Issuer checks the validity and authorizes the payment.

11- Acquirer sends the Receipt to the IPSP to be delivered to the Merchant.

5. Security analysis of new protocol

In this section, some of the significant security issues of proposed protocol are described.

5.1. Using Username and Expiration date

In this protocol, using simply hash function of PIN, which has at most 16 digits, can give us only 9 unknown digits that generate a space which can be specify by only 13 bits. This is because that the first 6 digits of credit card number show the card type and Issuer code and last digit is check digit. So, using a good username together with expiration date can increase the entropy up to 50 bits [6], which is about 1000 time stronger than 40-bit SSL. Notice that this is computed with the assumption of dictionary attack.

5.2. SSL connection effects

Creating a SSL session can be so time consuming. So it is desirable to use an existing SSL session instead of establishing a new SSL session if it is possible. Some of SSL sessions can be existing sessions. For example, IPSP and Directory Server can create their new connections based on their previous SSL session during a run of the payment protocol. But the SSL connection between cardholder and Merchant and also cardholder and Issuer is a new connection in every payment. In this protocol, the use of SSL in cardholder channel is not necessary but using it can make some of the payment information like order description more private. Consequently, this protocol can reduce the number of new SSL sessions in comparison with 3D Secure.

5.3. Authenticating Merchant and Issuer to the cardholder

In 3D Secure, cardholder without any assurance of authenticating Merchant, sends his credit card information to him. Besides, cardholder doesn't authenticate his Issuer's web page. Both of these are because of the lack of an observer on cardholder's computer. In the proposed protocol, using of a wallet, which is simply capable to calculate a standard hash function helps cardholder to authenticate both Merchant and Issuer. To realize this purpose, it uses a simple password-based method. However, despite simplicity of method, it is resistant against dictionary attacks.

5.4. Weaknesses of the protocol

It seems that if the connection between cardholder and Issuer is eavesdropped, the content (Hash (PIN, Username, Exp Date)) can be used for replay attack to the Issuer. To avoid this attack, one stage should be added to the handshaking messages between cardholder and Issuer. Sending a nonce from Issuer to the cardholder and getting this nonce in the next message from the cardholder's wallet can prevent the replay attack, which is done by sending a vast number of messages from different IP addresses.

Using a wallet can make the electronic payment more complicated in comparison with 3D Secure. But as we saw, it makes the payment protocol more secure.

Searching the proposed database for Directory Server is more complicated than 3D Secure. Because if Hash function is 128 bits long, the search algorithm compares 16 byte values, however 3D Secure database uses less than 8 byte comparator function to search.

6. Comparison between 3D Secure and proposed protocol

Table 1 shows a comparison between 3D Secure and proposed protocol. Password sniffing is a weakness that exists in every password-based protocol. However, protocols that use wallet are more resistant against this attack, because wallet enters customer password automatically in authentication page. So, cardholder doesn't need to enter credit card password every time he wants to make a transaction. By using SSL in 3D Secure and also TID and nonce in proposed protocol, both protocols are resistant against existing replay attacks. In the worst case, if it is considered 1.5 bit entropy for every letter in dictionary attack, the proposed protocol creates a search space that is representable with 50 bits. It is clear that choosing a strong username and password can make dictionary attack unsuccessful. Authenticating issuer prevents faking Issuer that is a problem in 3D Secure protocol. Unlike 3D Secure, proposed protocol doesn't send pure credit card information to the Merchant and also order description to the Issuer.

Conclusions

In this paper, features and problems of previous and current credit card protocols were described. The main attention in this paper was on the current protocol of Visa, namely 3D Secure. The features and weaknesses of this protocol were discussed in continue, a new protocol on the basis of 3D Secure was proposed. As we know, there is always a trade off between security and complexity. Particularly, the new protocol can be implemented based on required level of security in particular application. However, proposed protocol, which remained still a password-

based protocol, is sufficiently resistant against dictionary attacks.

Table.1 Comparison between 3D Secure and proposed protocol

Criterion	3D Secure	Proposed protocol
Sniffing in cardholder's node	Weak	Weak
Replay attack to Merchant	Almost Strong	Almost Strong
Replay attack to Issuer	Almost Strong	Almost Strong (which nonce)
Brute Force attack	2^{40} (commercial SSL)	2^{50}
Issuer page fake	Weak	Resistant
Credit card Information	Disclose to Merchant	Private

References

[1] GigaABP Inc, Electronic Payment Put in Context, WhitePaper, March 2002

[2] Gpayments Inc., Pseudo Card Numbers, Authentication and Payment Solutions White Paper, March 2002.

[3] Visa International, "3D Secure Introduction", *Visa* International Service Association, Publication 70001-01, Version 1.0.2, September 26, 2002.

[4] European Committee for Banking Standards, *Secure Card Payments on The Internet*, Version 1.0, November 2002.

[5] Visa International, "3D Secure Protocol Specifications, Core Functions", Visa International Service Association, Publication 70000-01, Version 1.0.2, July 16, 2002, Errata as of January 20, 2004.

[6] Koleini, M. "Security in Electronic Payment Systems", MS Thesis, Isfahan University of Technology, February 2005 in Persian.