International Journal Of Business Management
Available at www.ijbm.co.in
ISSN NO. 2349-3402
VOL. 2(1),2015

Empirical Study in the Security of Electronic Payment Systems

Anita Goyal[1]
Jaswinder Kaur[2]

Abstract

The financial institutions seek to cut the cost of mediators through direct deal with the consumers and share information with the Internet users as well as encourage customers to pay on-line. One of the main problems faced by Organizations in terms of dealing and paying on-line that Internet users are worried and unwilling to send sensitive information through the Internet. In fact customers are scared that during the transactions hackers and Internet interlopers will steal their information. This study suggests that there are some security features such as authentication, authorization, privacy and encryption can influence user's perceptions of security for electronic finance transactions and contribute toward enhancing customers' perceptions that the e-finance transactions are secure and safe to send through sensitive information and pay on-line.

Keywords: Electronic Payment, Authentication, Authorization, Privacy, Encryption.

1 Assistant Professor, Rayat-Bahra University, Mohali
2 Assistant Professor, Rayat-Bahra University, Mohali

Introduction

The emergence of Internet, the improvement of Information Technology, and the fast growth of wireless telecommunication between organizations and individuals have affected the financial system greatly and also have increased the use of Electronic Finance E-Finance locally as well as globally [1].

E-Finance has affected businesses, individual consumers and has also reform the trading relationships. Most organizations need to adopt the new technology in the new environment and enhance their businesses efficiency to gain competitive advantage and to succeed in the global economy.

One of the new challenges in the competitive and global economy is E-Finance including electronic payment. E-finance technology is considered one of the most important factors to gain competitive advantage in the global economy.

Therefore organizations try to improve the interchange of information and electronic payment, and enhance the means of transactions between trading partners (suppliers and customers). This can be through breaking the barriers that restrict information sharing. When the volume of transactions and information sharing increases; the level of the associated risk will also increases. Therefore organizations need to ensure the

International Journal Of Business Management
Available at www.ijbm.co.in
ISSN NO. 2349-3402
VOL. 2(1),2015

security of data and the system itself to protect the users' information being shared [2], [3].

Today most organizations seeks to complete their data interchange with E-Finance and gain from the associated cost saving and convenience offered to consumers, at the same time they need appropriate security system to ensure that during the financial transactions and electronic payment, all customers' information will be protected. The researchers noticed that privacy is a significant important factor influencing e-businesses and E-Commerce [4].

Therefore electronic payment technology need to provide security mechanisms as a sufficient safeguards in the form of digital signatures, encryption and Web seal assurances…etc, whereby e-finance users perceptions can be gained. The fast growth of Internet and E-Finance usage require a fast and similar growth in security system to satisfy the E-Finance) users especially those who use the electronic payment transactions.

Literature review

2.1 Evolution of Electronic Payment

Organizations were used to deal with financial dealings in the traditional way such as paper work. But with advent of communication and internet technology most of financial procedures dealt with it electronically. However the appearance of internet and the development of electronic communications technology impact significantly the growth of E-Finance. Accordingly E-finance defined as the provision of financial services and market using electronic communication and computation [5].

Electronic payment systems initiated since a quit long time. However in industrialized countries the interbank payment system was operated using telephone networks and mainframe networks. Furthermore, in 1970s Automated Clearing House (ACH) created in the US) in order to make payment of wages and other essential payments. Meanwhile European Giro system implement electronic format in order to reduce paper work as it is in credit cards organizations. On the other hand, the number of Automated Teller Machine (ATM) has increased from 18,500 in 1980 to 324,000 in 2000 and then increased by time to be well spread in the recent years [6].

2.2 Internet Banking Instruments

The Internet banking refers to the deployment over the Internet of retail and commercial banking services with individual and corporate clients including bank transfers, payments, settlements, documentary collections, credits, card business and others [7].

International banking statistics from the Bank of International Settlements and the European Central Bank shows that the popular payment instruments used for the payment of day-to-day purchases include cash, checks, debit cards, and credit cards. In general, EPS can be classified into five categories [8], [9], [10], [11], which are listed below.

International Journal Of Business Management
Available at www.ijbm.co.in
ISSN NO. 2349-3402
VOL. 2(1),2015

1. Electronic-cash: transactions are (transactions which are) settled via the exchange of electronic currency.
2. Pre-paid card: customers use a pre-paid card for a specified amount by making an entry of the unique card number on merchant sites. The value of the card is decreased by the amount paid to the merchant.
3. Credit cards: a server authenticates consumers and verifies with the bank whether adequate funds are available prior to purchase; charges are posted against a customer's account; and the customer is billed later for the charges and pays the balance of the account to the bank.
4. Debit cards: a customer maintains a positive balance in the account, and money is deducted from the account when a debit transaction is performed.
5. Electronic checks: an institution electronically settles transactions between the buyer's bank and the seller's bank in the form of an electronic check.

2.3 Limitations of Traditional Payment Systems in the Context of Online Payments

There are three factors stimulating the development of electronic payment systems: reduced operational and payments processing costs, growing online commerce and decreasing the costs of technology, Reduction of costs is one of the key reasons for research and development of EPSs. The central impetus for e-commerce and e-business is to provide a more efficient service, mainly in terms of costs. So, paying online with traditional payment systems such as credit cards is rather paradoxical, given that credit cards are one of the most expensive of all reachable mainstream payment means for both end consumers and merchants, defeated perhaps only by paper checks [12].

There are several limitations of traditional payment systems in the context of e-commerce can be outlined. Existing payment systems, such as credit cards, are inadequate for retail customer digital business from the following viewpoints as:

Lack of usability: Accessible payment systems for the Internet need from the end user to present a great amount of information, or make payments using complex elaborated web site interfaces. E.g. credit card payments via a web site are not the easiest way to pay, as these need entering wide amounts of personal data and contact details in a web form [13], [14].

Lack of security: Presented payment systems for the Internet are an easy target for stealing money and personal information. Clients have to give credit card or payment account details and other personal information online. This data is sometimes transmitted in an un-secured way. In practice this happens even in spite of introduction of secure transactions mechanisms, such as Secured Socket Layer. Providing these details by mail or over the telephone also entails security risks [13], [15], [16].

Lack of trust: Customers tend not to trust offered systems with the long history of fraud, misuse or low reliability. In the present situation, money loss by customers is quite possible when using existing payment systems, such as credit cards for Internet payments. Potential customers often mention this risk as

International Journal Of Business Management
Available at www.ijbm.co.in
ISSN NO. 2349-3402
VOL. 2(1),2015

The Proposed Protocol

This paper is introduced an efficient protocol, and make a simple comparison between the proposed protocol and the above described pay-word protocol. Also, gauging the efficiency and security of the protocol will take place in section 6. However, any such protocol should contain at least four schemes, registration scheme, blind signature scheme, transaction scheme, and redemption scheme. The proposed protocol adopts the same procedures of the pay word scheme except the blind signature scheme. Thus, in this section, we will introduce a new blind signature scheme using discrete logarithm problem [13]. We will show this improvement makes the pay-word protocol more efficient and keeps all other characteristics balanced.

Bank (*B*) Merchant (*M*)

Customer (*U*)

MU=(IDM,CU,Wo,EC,IM)SKS MU,P = (Wi,i) P = (Wi,i)
CU=(IDS,IDU,AU,PKU,EU,IU)SKS

5.1 Blind Scheme

The user gives a withdrawal request to the bank before his order for some service from merchant. The steps of the scheme are as follows:

Step 1: Bank

1.1. Generate an arbitrarily prime number p
1.2. Select a generator g of the multiplicative of group
1.3. Pick the private key d such that $1 < d < p < 2$
1.4. Finds the public key $y = g^d \mod p$
1.5. Determine the public key (p, *g, and y*) and private key (*d*)
1.6. Pick a random number $z < p - 2$
1.7. Send z to the user

Step 2: User

2.1. Pick a random integers v and u
2.2. Finds $f = v\, y * h\,(m)(\, u\, 2 + 1) \mod p$
2.3. Send (*e*, *f)* to the bank, where e represents an upper limit of cash that the user can use.
2.4. Pick an arbitrary integer c
2.5. Finds $k = v * c \mod p$
2.6. Pass $a = (k)\, y * (u - z) \mod p$ to the bank

Step 3: Bank

3.1. Finds $a^{-1} \mod p$
3.2. Finds $j = h\,(e)\, d * (f\,(z^{\,2} + 1) * a^{-2})2 * d \mod p$
3.3. Pass $(a^{-1}\, 1, j)$ to the user

Step 4: User

4.1. Finds $w = (u * z + 1) * a^{-1} * (k)\, y = (u * z + 1)(u - z)^{-1} \mod p$
4.2. Finds $x = j * v\ 2 * (c)\ 4 \mod p$ The parameter (e,w, x) is the signature on message*m*.

International Journal Of Business Management
Available at www.ijbm.co.in
ISSN NO. 2349-3402
VOL. 2(1),2015

However, one entity can verify this signature by checking whether x^{y}= (j *v2 *(c)4) y mod p

5.2 Example

Step 1: Bank

1.1. Suppose p = 113

1.2. Assume a generator g =2

1.3. Suppose the private key d =11

1.4. Find the public key y = gd mod$p$=211mod113=14

1.5. Determine the public key (p =113, g = 2, y =14) and private key (d =11)

1.6. Suppose z = 7

1.7. Send z = 7 to the user

Step 2: User

2.1. Assume v =10 and u = 17

2.2. Find f = v y * h (m) (u 2 * 1) mod p

=10 ^{14} *h (8) (17^2+ 1) mod113

=10^{14} *h (8) 10 * (8) (290) mod113

=41

2.3. Send (e = 6, f = 41) to the bank. Where e represents an upper limit of cash that the user can use.

2.4. Suppose c = 15

2.5. Finds k = v * c = 10 *15mod 113 = 37

2.6. Finds a = (k) y * (u - z) mod p 37 * (17* 7) mod=113

= 12

2.7. Pass a = 12 to the bank

Step 3: Bank

3.1. Find a^{-1} mod p

12^{-1} mod113

12*66 mod113 = 1

3.2. Finds j = h (e) d * (f (z2 +1) * a^2)2*d mod p

= h (6)11 * (41(72 =1) *12=2)2*11 mod113

=h $(6)^{11}$(41*50 * 62) mod113

= h 11 22 (362797056) * (127100) mod113

=19

3.3. Pass (a^{-1} , j) = (66 ,19) to the user

Step 4: User

4.1. Finds w = (u * z +1) * a^{-1} * $(k)^{y}$ = (u * z +1) (u - z)$^{-1}$ mod p

= (17 * 7 +1) * 66* $(37)^{14}$ = (17 * 7 +1) (17 - 7) $^{-1}$mod113

=12 = (17 * 7 +1) $(10)^{-1}$ mod113

= 12 = (120) (34) mod113

= 12 = 12

4.2. Finds x = j * v 2 * (c) 4 mod p

International Journal Of Business Management
Available at www.ijbm.co.in
ISSN NO. 2349-3402
VOL. 2(1),2015

= 19 *102 * (15)4 mod113
= 19 * 100 * 50625 mod 113
= 92
The parameter (e = 6, w =12, x = 92) is the signature on Message. However, one entity can verify this signature
By checking whether x^{y} (j * v2 * (c) 4) y mod p 9214
= (19 *102 *154)14 mod113 18
= (19 *100 50625)14 mod113
=18

Forgery Detection

The user U gets the bank B signature on m prior to any transaction. But, in order to process an accurate
Redemption, the merchant M should have information of the payment transaction. It is almost unfeasible for any
Entity to forge the user U payment without knowing the private key d. Thus, the opponent cannot forge signature. But to successfully achieve the verification of the formula x^{y} (j * v2 * (c)4) y mod p , an opponent has to calculate x where $x = j * v$ 2 * (c) 4 mod p provided the results of $h(e)$, h (m) and w . However, it is computationally intractable to obtain the value of d without solving the discrete logarithm that is hard to
Solve such a problem. Thus, the opponent is unable to forge the signature.

5.4 Efficiency

In the e-payment protocol, the profit acquired by a merchant is little in every transaction. It is unwise to check
The transaction employing a complicated technique that leads the average cost of the protocol more than the profit. On the other hand, large calculation in e-payment is not wise. In order to gauge efficiency of the proposed
Protocol, we compare the enhanced blind scheme with the pay-word scheme [4]. The time complexity of the
Remaining scheme stays the same in both protocols. We employ the following notation to gauge the efficiency of
The schemes. *Tm:* Calculation time for hash function operation *Ta:* Calculation time for addition in modular
Multiplication *Tm:* Calculation time for multiplication modular exponentiation Table 1: Computations of efficacy in blinding scheme.

Protocol Name Blinding Scheme

The pay-word protocol 5**Tm* * 9**Ta* * 5**Tm* Proposed protocol 4**Tm* * 8**Ta* * 4**Tm* actually, the modular exponentiation is a costly operation in comparison with addition or hash function operations. As a result it is simple to observe from Table 1 that the proposed protocol is more efficient than the pay-word protocol. Furthermore, when any entity computes and obtains small public key y , then the proposed protocol

International Journal Of Business Management
Available at www.ijbm.co.in
ISSN NO. 2349-3402
VOL. 2(1),2015

becomes more efficient. This makes public key operations quicker while the secret key operations remaining unchanged. In this case, when an entity uses the short public key attack, he cannot succeed with this try since every signature is being randomized by certain random numbers. So, the proposed protocol decreases expensive exponential operation and has better time efficiency.

Conclusion

In this paper, we described the characteristics of epayment protocol and evaluated one of the most important

E-payment protocols that relied on a hash chain. The hash chain typed scheme gives anonymity security characteristic besides other security features of e-payment protocol. The use of the blind signature scheme and hash function makes the protocol more efficient and guarantees the payment untraceable. Though, we notice that the blind scheme of the protocol takes significantly more computing time and we present an alternate blind scheme using the discrete logarithm that gives more efficiency than the existed protocol. The research accomplished in this paper has vast future prospects and can be extended towards a substantial protocol using hash function so that the modular exponentiation and costly operation can be avoided and also security depth can be reached.

Reference

[1] A.Tiwari, S. Sanyal, A. Abraham, J. Knapskog, and S. Sanyal, "A Multi-factor Security Protocol for Wireless

Payment-Secure Web Authentication Using Mobile Devices", IADIS International Conference Applied

Computing, 2007, pp.160-167.

[2] S. van, A. Odlyzko, and R. Rivest, T. Jones and D. Scot,"Does anyone really need micropayments", proceeding of the International Conference of Financial Cryptography, LNCS 2742, Springer, 2003, pp. 69-76.

[3] L. Jun, L. Jianxin, and Z. Xiaomin, "A System Model and Protocol for Mobile Payment", Proceedings of the IEEE International Conference one-Business Engineering (ICEBE’05), 2005. [4] R. Rivest, and A. Shamir, "Pay-word and MicroMint: Two simple micropayment schemes", International Journal of Network Security, Vol. 2, No. 2, 2001, pp. 81-90.

[5] D. Chaum, Fiat, and M. Naor, "Untraceable electronic cash", Proceeding Advances in Cryptology, LNCS 403, Springer, 1988, pp. 319-327.

[6] M. Hwang, and P. Sung, "A study of micro-payment based on one-way hash chain", International Journal of Network Security, Vol. 2, No. 2, 2006, pp 81-90.

International Journal Of Business Management
Available at www.ijbm.co.in
ISSN NO. 2349-3402
VOL. 2(1),2015

[7] R. Rivest, "Electronic lottery tickets as micropayments", Proceeding of the International Conference of Financial Cryptography, LNCS 1318, Springer, 1997, pp. 307–314.
[8] E. Foo, and C. Boyd, "A payment scheme using vouchers", Proceeding of the International Conference of Financial Cryptography, LNCS 1465, Springer, 1998, pp. 103-121.
[9] M. Baddeley, "Using e-cash in the new economy: An economic analysis of micro-payment systems",
Journal of Electronic Commerce Research, Vol. 5, No. 4, 2004.
[10] J. Tellez, and J.Sierra, "Anonymous Payment in a Client Centric Model for Digital Ecosystem", IEEE DEST, 2007, pp. 422-427,
[11] R.Rivest, A. Shamir, and L. Adleman, "A Method for obtaining digital signatures and public-key cryptosystems", Communications of the ACM, Vol. 21, No. 2, 1978, pp. 120-126.
[12] D.Stinson, Cryptography: Theory and Practice, CRT Press, 2006.
[13] M. Al-Fayoumi, and S.J. Aboud, "Blind Decryption and Privacy Protection", American Journal of Applied Sciences, Science Publications Vol.2, No. 4, 2005, pp. 873- 8