Research Journal of Management Sciences ____ ISSN 2319–1171
Vol. **2(7),** 33-37, July **(2013)** *Res. J. Management Sci.*

Impact of M-Commerce in Mobile Transaction’s Security

Anand Bajpai
Career Degree College, Lucknow, UP, INDIA

Available online at: www.isca.in
Received 21st October 2012, revised 21st December 2012, accepted 12th January 2013

Abstract

Really the modern world is so advance in technologies since portable network accessible devices and techniques. In the era of wireless technologies which are available in mobile, PDA, Laptop as well as in any PC (personal computer), anyone can get access anywhere- anytime. So we can say it wireless communication which may be called as anywhere- anytime communication. Due to this type of communication, it is very easy to access as well as transfer the information from anywhere-anytime. Today Information technology has connected the whole world on a one land which is called as electronic network land. This land has enabled two types of commerce: i. E-commerce, ii. M-commerce. The M-commerce has enriched the global market and advanced the whole business scenario. The business suddenly moved from regional land to global land because of access and reach of E-commerce and M-commerce. M-commerce is one of the derived technology from E-commerce. E-commerce is the mother of M-commerce. But the question comes up to the enterprise that whether enterprise architectures and designs are able to secure our e-business? Concerning the issues related to the above question I have found one key solution for it which would be capable of handling the issues of security of data assets beyond the enterprise boundaries. Now the concept as well as the approach for the security issue is E-security. But How? So we will find out also the solution for this question. Strategy and the solution need to be addressed in a more fundamental way than firewalls, SSL or PKI.

Keywords: Secure mobile transaction, mobile transaction, secured transaction, e-transaction, electronic transaction security.

Introduction

In today’s scenario where technology is getting very much advance day by day, and people are getting used to the mobile or wireless application, the key message is anytime anywhere communication and transferring of any information. Many technological considerations need to be examined in order to actualize such a message. Integral to enabling anytime-anywhere communication and transmission of data and information is a sound secure system. Hence a robust trust model in any mobile transaction becomes significant.

Generally a mobile transaction occurs when a client accesses the web-enabled services of a merchant and after necessary negotiations and communications, decides to place an order and make payment[1]. The order and payment information is transmitted from the mobile device to a base wireless station and from there, through the mobile communication infrastructure of the service operator, to the wireless application gateway of the merchant. In a typical mobile computing environment, one or more of the transacting parties are based on some wireless handheld devices. However, security over the mobile platform is more critical due to the open nature of wireless networks. Furthermore, security is more difficult to implement on the mobile platform because of the resource limitation of mobile handheld devices. Therefore, security mechanisms for protecting traditional computer communications need to be revisited so as to ensure that electronic transactions involving mobile devices can be secured and implemented in an effective manner[2].

Objectives

The main objective of this paper is to discuss the issues of a security in mobile transactions. This paper tries to give the solution for mobile transactions using the tool E-security. The major driver for E-security is WAP. It describes security strategies for the successful online transaction and the possible solution in a more fundamental way than firewalls, SSL or PKI.

3G Network Based Mobile Devices

Before 3G networks, there wasn’t too much trouble a mobile user could get into. The primary activity was simply placing and receiving voice calls. Mobile data was somewhat limited to the mobile operator’s walled garden and also the relatively slow data speeds. While the subscriber could browse news stories and even download some content such as ringtones, all of the content was primarily kept under the mobile operator’s control, thus limiting the exposure to security threats[3]. However, as the mobile network and devices both become more open, the risk of security attacks have increased.

Many mobile users get frustrated when going from an open computer device to having to use a closed mobile device. Therefore, the trend in the mobile industry is towards opening up the phone. Many of the smart phones are run on open software such as Android, Symbian, or Windows Mobile. These operating systems provide much more user flexibility in terms of loading applications and customizing the phone.

Fraud prevention steps while doing online transaction

Credit card fraud can be a significant problem for customers, merchants, and credit card issuers[4]. Liability for fraudulent transactions belongs to the credit card issuer for a card present, in-store transaction, but shifts to the merchant for "card not present" transactions, including transactions conducted online[5]. This means that the merchant does not receive payment for a fraudulent online transaction. Fortunately, there are steps you can take to significantly limit your risk as an online merchant.

The following important fraud prevention steps should be adhered to:

Choose a payment services provider that is well-established and credible. Your provider should also have in-depth experience in and a strong track record for transaction security. Make sure your payment gateway provider offers real-time credit card authorization results. This ensures that the credit card has not been reported as lost or stolen and that it is a valid card number. One of the simplest ways to reduce the risk of a fraudulent transaction is to use Address Verification Service (AVS). This matches the card holder billing address on file with the billing address submitted to ensure that the card holder is the card owner. Use Card Security Codes, known as CVV2 for Visa, CVVC for Master Card, and CID for American Express®. For American Express, the code is a four-digit number that appears on the front of the card above the account number. For Visa and MasterCard, the code is a three-digit number that appears at the end of the account number on the back of the card. The code is not printed on any receipts and provides additional assurance that the actual card is in possession of the person submitting the transaction. Watch for multiple orders for easily resold items such as electronic goods purchased on the same credit card. Develop a negative card and shipping address list and cross-check transactions against it. Many perpetrators will go back to the same merchant again and again to make fraudulent transactions.

Wireless Application Protocol (WAP)

WAP is "an open, global specification that empowers mobile users with wireless devices to easily access and interact with information and services instantly." WAP is currently the only publicly available solution for wireless communication and enables M-Commerce where Internet data moves to and from wireless devices. WAP-enabled phones can access interactive services such as information, location-based services, corporate information and inter-active entertainment. WAP is targeted at various types of Bluetooth enabled mobiles[6].

Wap Security Model

WAP have added advantages to the programming model. They are: WTA i.e. Wireless Telephony Support, and Push. In case of WAP model, all the applications and contents are specified in a well-known format which is based on World Wide Web (WWW). Data transportation is done by using some standard of www communication protocols.

Cyber Security

Cyber security has been an important topic in the today's scenario. In fact, a recent study by the Center for Strategic and International Studies wrote, "Cyber security is among the most serious economic and national security challenges we face in the twenty-first century". For a company to achieve effective mobile commerce security and ultimately consumer trust the security mechanisms will constitute as a security risk. The mechanisms are:

Authorization: It means ensuring authorized uses of systems and performance of business functions by authorized users only.

Authentication: Authentication is establishing that parties to an electronic transaction or communication are who they claim they are.

Integrity: Ensuring that data on the host system or in transmission are not created, intercepted, modified or deleted illicitly.

Confidentiality: Warranting that data are only revealed to parties who have a legitimate need to know it or have access to it.

Availability: Ensuring that legitimate access to information and services is provided. It should be available every time when it is required.

Non-repudiation: If a party to some transaction or communication later denies that it has ever happened, some mechanism is in place to facilitate dispute resolution.

Privacy - Ensuring that customers' personal data collected from their electronic transactions are protected from indecent and/or unauthorized disclosure.

Public Key Infrastructure

Public key infrastructure (PKI) is a system of digital certificates[7], certification authorities, and other registration authorities that provides solutions to enable a secure mobile commerce. The theory of PKI is presented as follows:

Public Key Cryptography: Public key infrastructures are based on public key cryptography, which uses two keys: a private key that is kept a secret, and a public key that can be divulged publicly. An interesting property of this pair of keys is that to decrypt messages encrypted with one, the other is needed. The keys are said to be asymmetric. The most popular algorithm for public key cryptography is RSA[8].

Digital Signatures: Digital signatures can ensure the authenticity of transaction parties, integrity, and non-repudiation of transmissions. A digital signature is created when the document to be transmitted is enciphered using a private key. The process of enciphering the document using the private key authenticates the document, since the document could only have been enciphered using the private key of the owner. A digitally signed document or message is unalterable after the signature[9]. The recipients can verify the signature by deciphering using the public key. In real world, documents are not completely encrypted to save time. In such cases one-way hash functions are used. A hash uses a one-way mathematical function to transform data into fixed length digest called a hash, which is subsequently enciphered[10]. The verification of the signature involves reproducing the hash generated from the received message and comparing it with the deciphered original hash[11].

A Joint-Signature Scheme

A joint-signature scheme acts as an alternative to traditional digital signatures[12]. This scheme is based on collaborative use of one-way hash functions and traditional digital signatures with the network operator. This scheme not only reduces the mobile computation costs, but also provides lower communication cost as opposed to other digital signature security schemes[13]. This joint-signature scheme is based on the hypothesis that if a third party, like the network provider which has with ample computation and communication resources, signs a digital signature containing a secret that is only shared between the customer and the merchant, then the merchant can treat the digital signature as a joint signature originated from the customer and signed by the third party/network provider.

Transaction Authentication Number - Tan

A Transaction authentication number or TAN is used by some online banking services as a form of single use one-time passwords to authorize financial transactions. TANs are a second layer of security above and beyond the traditional single-password authentication. TANs are believed to provide additional security because they act as a form of two-factor authentication. Should the physical document or token containing the TANs be stolen, it will be of little use without the password; conversely, if the login data are obtained, no transactions can be performed without a valid TAN.

Mobile Tan (mTAN)

mTANs are used by banks in Germany, Austria, Poland, the Netherlands, Hungary, South Africa and some other countries in the world. When the user initiates a transaction, a TAN is generated by the bank and sent to the user's mobile phone by SMS. The SMS may also include transaction data, allowing the user to verify that the transaction has not been modified in transmission to the bank[14]. However, the security of this scheme depends on the security of the mobile phone system. In South Africa, where SMS delivered TAN codes are common, a new attack has appeared: SIM Swap Fraud. A common attack vector is for the attacker to impersonate the victim, and obtain a replacement SIM card for the victim's phone from the mobile network operator. The victim's user name and password are obtained by other means (such as key logging or phishing). In-between obtaining the cloned/replacement SIM and the victim noticing their phone no longer works; the attacker can transfer/extract the victim's funds from their accounts[15]. Most Web sites today, especially those that allow e-commerce or e-transactions through the exchange of credit card information, are employing security measures to ensure that sensitive personal information can't be captured as it goes from browser to server. Even so, many people won't consider making a purchase from their computers. Now imagine having that purchase originate from a wireless handset. In addition to having the information goes out over the public Internet, it also goes out over the air from the handset.

Crucial to addressing those concerns will be the Wireless Access Protocol (WAP), a key piece of the effort to get traditional Internet access and services down to wireless handsets[16]. WAP, which can be used with existing wireless networks such as GSM and CDMA, allows traditional Web and Internet content to be made accessible to very small wireless handsets. Wireless SSL The main security component of the WAP specification is the *wireless transport layer security* (WTLS) protocol, which essentially defines security procedures for wireless Internet transactions. WTLS is based on Transport Layer Security, formerly known as Secure Sockets Layer, or SSL. WTLS provides a multitude of security features, including data integrity, privacy and authentication. The basic WAP security model, involves three major components. The Web server, which can be located at the site of either a content provider of wireless operator, delivers Web pages and enables online transactions. Typically, subscribers would have access to multiple Web servers depending on the number and type of services[17].

In secure sessions, the Web server would serve up content encrypted with SSL in the same manner as encrypted content moves from Web servers to traditional wired browsers. The SSL encrypted traffic goes out over the Internet and hits a WAP gateway, which is generally hosted by the wireless operators. The WAP gateway is becoming known more as a WAP server, because next-generation products can function as both application server and gateway. The gateway can be viewed as the heart of a WAP solution in general and of WAP-enabled security[18]. Because the WAP handset is limited in terms of memory and battery life, a number of tasks that would exist at the browser level have been moved to the gateway.

Deploying Strong Security for Worldwide Commerce

Until recently, strong 128-bit encryption was not exportable. The United States Department of Commerce has approved the issuance of certificates for 128-bit encrypted communications—the highest level of encryption ever allowed across United States borders. With a 128-bit Global Server ID, your 128-bit customers can now enjoy unparalleled security when visiting your Web storefront site. The Global Server ID is a septillion times more secure than any other product.

Visa and Mastercard Take Different Approaches to Authentication

Online merchants could face integration hassles as they deploy forthcoming and competing credit card payer authentication technologies from Visa USA and MasterCard International Inc. The technologies, Visa's Verified by Visa and MasterCard's Secure Payment Application service, take distinctly different approaches[19]. Visa performs authentication on the merchant site, whereas MasterCard handles it on the customer's PC automatically, using a previously downloaded applet. As a result, merchants that accept credit cards will be required to support two authentication mechanisms. Furthermore, some observers speculate the companies' respective systems may be no more successful in gaining market acceptance than the ill-fated Secure Electronic Transaction (SET) authentication protocol, a protocol spearheaded by Visa and MasterCard. Visa sweetened the bait for its system recently when it announced that online merchants using Verified by Visa will have no liability for any transactions processed by the service[20]. Verified by Visa, also known as Visa Payer Authentication authenticates credit card users with a password and requires no client software. MasterCard's Secure Payment Application service, which the Purchase, N.Y., company will pilot in April, also uses a password or PIN and requires an applet for authentication. MasterCard and Visa, which formerly cooperated, now find fault with each other's approaches[21]. Visa's service, for instance, will extend transaction processing times, take customers off the merchant sites for authentication, and require complex integration. MasterCard's service, Visa countered, amounts to a digital wallet, which consumers have been loath to use. About the only thing MasterCard and Visa seem to agree on is that SET, which was launched in December 1997, was a failure. SET required long download times for customers, used clumsy digital certificate technology, and created integration hassles for merchants and banks that issued the credit cards. But with Visa and MasterCard now going separate ways, some merchants see little reason to try authentication technology. You're creating another layer of complication[22]. After customers go through the trouble of giving you their credit card number, they now have the problem of remembering one more password.

Authentication and Billing

A major concern with anything going out over a wireless network, especially with secure content, is making sure subscribers are able to validate themselves to the network. For traditional wireless voice, users have different ways to authenticate themselves to the network, depending on what their provider requires. For most, it's enough to type in a code to the handset keypad, which then unlocks the phone[23]. Once the phone is unlocked, any type of phone call can be made. In some cases, a PIN is required. Authentication schemes for wireless data likely will incorporate existing models, but they will also move beyond it. The nice thing about wireless networks is they already have a mechanism to authenticate handsets to the network worked out. All the things an operator uses to protect against fraud on voice networks apply equally to the data side. The steps are: i. Each vendor has an agreement with WSP or with consortium of providers, ii. The consumer initiates transaction with the vendor, iii. Consumer receives service/product, iv. WSP pays vendor, v. Consumer receives a bill from WSP

Customer information is kept behind a firewall for additional protection. Another measure to ensure that only authorized users reach certain WAP content is to perform authentication at the application layer.

Conclusion

It is essential for both businesses and consumers to be aware of the implications of trading online and taking account of these two particular issues will assist businesses in the smooth operation of trading via the WAP/Internet. M-Commerce security is a very crucial issue that needs further research to introduce efficient and effective solutions. In this article, I have tried to cover various security concerns. We have to think over the issues like privacy, authentication, authorization and encryption for the secure transactions over web and wireless. Encryption alone is not sufficient. Unauthenticated SSL certificates provide confidentiality and integrity, but lack the third-party authentication necessary to:

Verify that the user is actually visiting the company's Web storefront and not an imposters site. Allow the receiver of a digital message to be confident of both the identity of the sender and the integrity of the message.

Ensure safe online transactions that protect both customers and your business.

There are, however, some problems and issues that include (i) the real security of such systems is still not well understood, (ii) difficulty of generating suitable curves, and (iii) relatively slow signature verification. Time will answer in future.

References

1. Santosh K. Misra, Nilmini Wickamasinghe Security of a Mobile Transaction: A Trust Model ISSN: 1389-5753 (Print) 1572 9362 (Online)/ Volume 4, Number 4 / October, 2004 accessed on **(2012**)

2. Peikari C. and Fogie S., "Maximum Wireless security", 1st Edition ed: Sams Publishing, **(2002)**

3. He L.S. and Zhang N., "A new signature scheme: joint-signature," presented at Proceedings of the 2004 ACM symposium on Applied computing, Nicosia, Cyprus, 2004 accessed on **(2012)**

4. Vacca, John R., Identity Theft, Prentice Hall PTR, **(2003)**

5. "Establish Trust to Protect and Grow Your Online Business," © 2003 VeriSign, Inc, 2003 accessed on **(2011)**

6. Vacca, John R., i-mode Crash Course, McGraw-Hill Professional, **(2001)**

7. Special Issue of IEEE Communication Magazine on E-Commerce, September, **(1999)**

8. Towards Digital e-Quality, US Govt. Working Group on Electronic Commerce, **(1998)**

9. Denial Amor and Addison Wesley, The E-business Revolution, **(1996)**

10. Greenstein and Feinmann, E-Commerce, Tata McGraw Hills, **(1996)**

11. Goel Ritendra, E-Commerce, New Age International Publishers, **(1995)**

12. Benjamin R.I. and Wigand R.T. , Electronic Commerce: Effects on Electronic, **(1995)**

13. Markets, Journal of Computer-Mediated Communication, **(1994)**

14. http://www.scottish-enterprise.com/ebusiness **(2012)**

15. http://www.researchandmarkets.com/reports/314548**(2012)**

16. http://www.phone.com/pub/Security WP.pdf **(2012)**

17. http://www.wmrc.com/businessbriefing/pdf/mcommerce2001/book/byrne.pdf **(2012)**

18. http://www.s2.chalmers.se/iths/pdf/Digital%20signature%20tutorial.pdf **(2011)**

19. http://www.tdap.co.uk/uk/archive/billing/bill(fml0012).htm **(2011)**

20. http://eai.ebizq.net/web integration/olden 1.html **(2011)**

21. http://www.iol.co.za/index.php?art_id=vn20080112083836189C511499IOL:"Victim's SIM swap fraud nightmare" **(2011)**

22. http://computer.org/internet **(2011)**

23. http://www.misq.org/discovery/MISQD_isworld **(2011)**