International Journal of Engineering (IJE)
Singaporean Journal of Scientific Research(SJSR)
Vol5.No.1 2013 pp 24-29.
available at:www.iaaet.org/sjsr
Paper Received :25-04-2013
Paper Accepted:18-06-2013
Paper Reviewed by: 1. John Arhter 2.Androues Kenal
Editor : Prof. Yuh-Shyan Chen

E-PAYMENT SECURITY

Abhishek bhol[#1], Ankur gupta[#2], Chaman singh[#3], Rajat Kumar[#4]
College of engineering Roorkee
India
[1]abhishekbhol18@gmail.com [2]ankurforwin@gmail.com [3]chaman091@gmail.com [4]myrajat.coer@gmail.com

ABSTRACT

This document gives all the details about electronic payment scenario from working of payment gateways, working of SSL and TLS, information about some modern threats to the e-payment system and proposed solutions for these type of threats.

Keywords **–** Payment gateway; SSL; TLS; Data Integrity; Asymmetric encryption; Symmetric encryption; Blocking; Message authentication code; Endpoint verification; Two factor authentication; Three factor authentication; One time passcode**.**

1. INTRODUCTION

Transaction is no longer limited to real world today. Witnessing the Internet reconnaissance happening in every modern country, most companies especially big brands have setup their own e-commerce sites with several payment options offered for secure online shopping and transaction. However, what we heard almost every day is transaction security issue like phishing scam happening all around the world.

If you're like the many consumers of digital goods you will surely be processing transactions online every so often. We know the companies are doing their job very hard to tighten the security, but as a consumer you must be well-prepared to tackle any possible transaction issue or trap**.**

Credit cards have made all of our lives easier. It's now simpler than ever to purchase new device, cloth, furniture, or anything online at the drop of a hat. However online phishing scams are still very popular and can be credited for thousands of identify theft cases each year.

An online store allows you to be open for business 24 hours a day, 7 days a week. Not only is this an important convenience for your customers, it also means more revenue for you. An online store also helps you to reduce your overhead costs since you don't need to hire reception staff and people to take orders. With the right payment processing tools, these functions are all done automatically for you. And lastly, an online store helps you to reach new markets across the country or even outside the country. A secure online store is no longer an option for a successful business; it's a critical step in managing and growing your business as in [1].

2. PAYMENT GATEWAY DURING ONLINE TRANSACTION

A payment gateway is an e-commerce application service provider service that authorizes payments for e-businesses. It is the equivalent of a physical point of sale terminal located in most retail outlets. Payment gateways protect credit card details by encrypting sensitive information, such as credit card numbers, to ensure that information is passed securely between the customer and the merchant and also between merchant and the payment processor as in [2].

3. HOW PAYMENT GATEWAY WORKS

A payment gateway facilitates the transfer of information between a payment portal (such as a website, mobile phone or IVR service) and the Front End Processor or acquiring bank. When a customer orders a product from a payment gateway-enabled merchant, the payment gateway performs a variety of tasks to process the transaction

1. A customer places order on website by pressing the 'Submit Order' or equivalent button, or perhaps enters their card details using an automatic phone answering service.
2. If the order is via a website, the customer's web browser encrypts the information to be sent between the browser and the merchant's web server. This is done via SSL (Secure Socket Layer) encryption.
3. The merchant then forwards the transaction details to their payment gateway. This is another SSL encrypted connection to the payment server hosted by the payment gateway.
4. The payment gateway forwards the transaction information to the payment processor used by the merchant's acquiring bank.
5. The payment processor forwards the transaction information to the card association (e.g., Visa/MasterCard), which routes the transaction to the correct card issuing bank.
6. The credit card issuing bank receives the authorization request and does fraud and credit or debit checks and then sends a response back to the processor (via the same process as the request for authorization) with a response code [eg: approved, denied]. In addition to communicating the fate of the authorization request, the response code is used to define the reason why the transaction failed (such as insufficient funds, or bank link not available). Meanwhile, the credit card issuer holds an authorization associated with that merchant and consumer for the approved amount. This can impact the consumer's ability to further spend (eg: because it reduces the line of credit available or because it puts a hold on a portion of the funds in a debit account) as in [3].
7. The processor forwards the authorization response to the payment gateway.
8. The payment gateway receives the response, and forwards it on to the website (or whatever interface was used to process the payment) where it is interpreted as a relevant response then relayed back to the merchant and cardholder. This is known as the Authorization or "Auth".
9. The entire process typically takes 2–3 seconds.
10. The merchant then fulfils the order and the above process is repeated but this time to "Clear" the authorization by consummating the transaction. Typically the "Clear" is initiated only after the merchant has fulfilled the transaction (eg: shipped the order). This result in the issuing bank 'clearing' the 'auth' (i.e.: moves auth-hold to a debit) and prepares them to settle with the merchant acquiring bank.
11. The merchant submits all their approved authorizations, in a "batch" (eg: end of day), to their acquiring bank for settlement via its processor.
12. The acquiring bank makes the batch settlement request of the credit card issuer.
13. The credit card issuer makes a settlement payment to the acquiring bank (eg: the next day)
14. The acquiring bank subsequently deposits the total of the approved funds in to the merchant's nominated account (eg: the day after). This could be an account with the acquiring bank if the merchant does their banking with the same bank, or an account with another bank.
15. The entire process from authorization to settlement to funding typically takes 3 days as in [4].

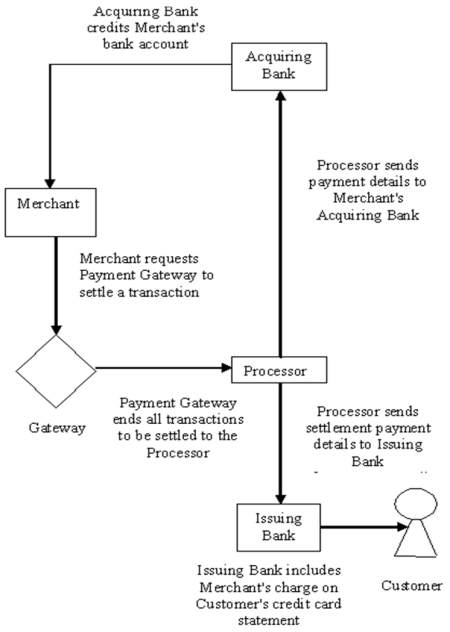

Figure. 1 Payment processing settlement

Many payment gateways also provide tools to automatically screen orders for fraud and calculate tax in real time prior to the authorization request

being sent to the processor. Tools to detect fraud include geolocation, velocity pattern analysis, black-list lookups, delivery address verification, computer finger printing technology, identity morphing detection, and basic address verification system checks.

4. WHAT IS SSL AND TLS?

Secure Sockets Layer (SSL) and Transport Layer Security (TLS) are cryptographic protocols for transferring information over the Internet in an encrypted, secure way. They utilize endpoint authentication and end-to-end encryption, providing authenticity, message integrity, and privacy. They also protect against session-replay attacks. SSL/TLS is widely used to securely send data over the Internet, however it is not a magic solution, and without an understanding of how the protocol works and how the underlying technologies it is at best difficult to fully utilize SSL/TLS and at worst easy to use SSL/TLS in an insecure manner as in ([5] - [7]).

The purpose of the Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols is to provide a mechanism for secure communications between two parties over a network which neither party has end-to-end control over and thus has the potential for third parties to intercept communication. The Internet is a good example of such a network. Fundamentally there are two aspects that need to be addressed, data integrity and end-point verification.

A. ***Data Integrity*** - When communication is made between two parties in a secure manner it is important that the data is received in its entirety, unmodified and without other parties being able to inspect or modify the communication. To provide data integrity SSL/TLS employs a variety of cryptographic techniques. Asymmetric and symmetric encryption is used to provide privacy by preventing third-parties from being able to access the contents of a message even if it is intercepted. This also provides protection against messages being removed and inserted. Message digests are used to protect against messages being modified.

   1) ***Asymmetric Encryption*** - Asymmetric Encryption, also commonly referred to as public key encryption, allows encrypted communication between two parties without the need for prior negotiation of secret keys. It is referred to as asymmetric encryption as different keys are used for encryption and decryption.

   2) ***Symmetric Encryption*** - Symmetric Encryption allows encrypted communication between two endpoints using a shared key. It is called symmetric encryption because the same key is used for both encryption and decryption.

   3) ***Blocking*** - Symmetric encryption algorithms tend to be block-based. That is they take a fixed amount of data and encrypt or decrypt it.

   4) ***Message Authentication Code*** - A Message Authentication Codes (MAC) are used to ensure that messages are not tampered with or otherwise corrupted during transit. This can be thought of as a digest of the message which includes a secret key. It is constructed when data is sent, and verified when it is received. It is not possible to reproduce the digest without knowing both the input text and the key, and thus a would-be attacker needs to know the secret in order to construct a valid MAC for a message that has been altered. For protection against replay attacks SSL and TLS include a monotonically increasing serial number is included in the input to the MAC.

B. ***Endpoint Verification*** - It is also important that when communication is made between two endpoints the endpoints are indeed who they claim that they are. In SSL and TLS this is achieved using certificates. During the course of establishing an SSL/TLS connection a message signed with the end-point's certificate is sent along with the certificate. The certificate itself is signed by a certificate authority, and it is in the certificate authority that the web of trust lies.

5. WORKING OF SSL

The SSL/TLS protocols run on layers beneath the application protocols (e.g. HTTP, SMTP, etc.) and above the TCP transport protocol. Both are able to use a number of (symmetric and asymmetric) encryption algorithms. Authentication is performed via certificates: digital objects signed by designated authorities (certificate authorities or CAs) confirming the identity of the party. Symmetric algorithms are used to encrypt the data transfer, while asymmetric is used during the authentication as in [8].

1. The general procedure of encrypted communication is the following: The client and the server select a method (encryption algorithm) for encrypting the communication.
2. The client authenticates the server by requesting its certificate. Optionally, the server can also request a certificate from the client, thus mutual authentication is also possible.

3. The client encrypts his message using symmetric a key.
4. The client transmits the message to the receiver.
5. The server decrypts the message using a symmetric key.
6. The communication between the parties can continue by repeating steps 3-5.

The server stores information (including the session ID and other parameters) about past SSL/TLS sessions in its session cache. Clients that have contacted a particular server previously can request to continue a session (by identifying its session ID); this can be used to accelerate the initialization of the connection.

Newer versions of certain protocols (e.g.: POP3, SMTP, HTTP) allow starting a TLS session from within an existing connection. This means that the client starts to communicate with the server using the regular, non-encrypted protocol, and later during the communication either of them can decide to switch to TLS-encrypted communication. This is possible within the same session; there is no need to rebuild the connection.

6. SOME MODERN THREAT

There are some modern threat in which the data displayed on the user browser window is not something what the server had sent. Similarly, what the server sees on the other end might not be what user had sent as in [9].

These types of attacks are invincible to security mechanisms like

A. ***SSL (Secure Socket Layer)*** – It is a cryptographic protocol for transferring information over the internet in an encrypted, secure way.
B. ***Two factor authentication*** - It includes two sources for secrets such as a One-Time-Passcode + user secret/password/pin.
C. ***Three factor authentication*** – It includes three sources for secrets such as a One-Time-Passcode + biometric + user secret/password/pin.

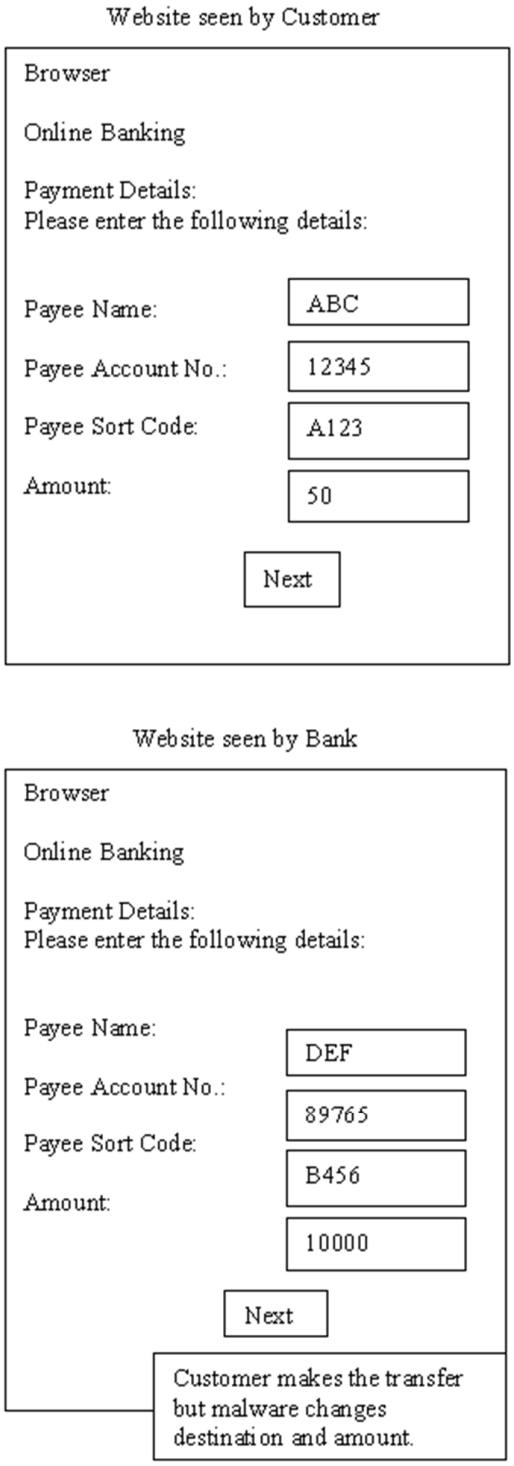

Figure. 2 Example of modern threat

These types of attacks are

- Hard to detect.
- Computers are easily affected.

- Traditional Strong Authentication doesn't help.
- Traditional Anti-Fraud Mechanisms and Risk-based Tools are Not Effective.

7. CURRENT SECURITY MECHANISM TO AVERT THESE TYPES OF ATTACKS

A. Out-of-Band (OOB) Authentication

- Can be compromised by waiting for the user to enter the onetime passcode and then overtaking the transaction.

B. Hardened Browser on a USB Drive

- Some security agencies provide with a hardware device which has a secure browser designed for online banking.
- But then there is some user inconvenience to always carry this additional hardware and also lack of accessibility of this to all.

C. Live CDs\Virtual Machines

- This includes booting from a Live CD or on a virtual machine when you want to do online transactions. Works but not comfortable for the end-user.

I. PROPOSED APPROACH TO AVERT THESE ATTACKS

A. ***Securing the onetime pass codes*** **-**

1) ***Current Scenario*** **-** First user request for One Time Passcode during transaction. Now during transaction Trojan or virus sends the One Time Passcode (OTP) to the attacker. Attackers use this code to initiate an illegal transaction.

2) ***Reconfirming the IP Address*** **-** One Time Passcodes can be made more secure if Banks confirm the IP Address from which the request for OTP came and the IP Address from which the request for transaction came are same. Since the OTP lasts for a short period of time there is very less probability that the owner of the account will use different internet connection to do the transaction.

B. Securing the confirmation page –

1) ***Using Images + Text for Confirmation*** **-** The Confirmation Page displays the account number in Image form also. Image includes some noise to make it difficult for automated reading. Image may not be single image but split images for enhanced security. The split images contain the account number in parts. The split images may not be aligned horizontally but on different angles. Sending the transaction details (Amount, Account from, Account to, date, etc.) to user mobile via SMS. A confirmation code may also be sent via SMS along with transaction details, and the customer must enter this one time confirmation code for transaction to continue successfully.

8. ADDITIONAL SECURITY MEASURES

A. ***Using Logo In The Image*** **-** User can set a logo which will be user specific. In case the attacker manipulates the image. The user can see the logo and check if the image was sent by the bank or not.

B. ***Confirmation on Mobile Phones*** **-** If the amount of the transaction is greater than a certain threshold amount (set by the user) then the details of the transaction should be confirmed by sending the details on the mobile number of the account holder.

Limitations of These Approaches

- Our approach is based on the fact that it is difficult for the virus or attacker to manipulate the image.
- Banks should be capable of generating the images with user specific logo.
- Network Bandwidth will be utilized more for sending the image for each transaction.

9. CONCLUSION

The transfer of money digitally has become common place in today's futuristic society. And our technocracy is quickly advancing into a better tomorrow. Purchasing online may seem to be quick and easy, but most consumers give little thought to the process that appears to work instantaneously. For it to work correctly, merchants must connect to a network of banks (both acquiring and issuing banks),

processors, and other financial institutions so that payment information provided by the customer can be routed securely and reliably. The solution is a payment processing service that connects your online store to these institutions and processors. Because payment information is highly sensitive, trust and confidence are essential elements of any payment transaction. This means the payment processing service should be provided by a company with in depth experience in payment processing and security.

REFERENCES

[1] Carat, G. (2002), ePayment Systems Database -Trends and Analysis, electronic Payment Systems Observatory (ePSO).

[2] Kim, Jinwoo, Jungwon Lee, Kwanghee Han and Moonkyu Lee, 2002. Business as Buildings: Metrics for the Architectural Quality of Internet Businesses. Information Systems Research, 13, 3, 239-254.

[3] The Daily (2004), Electronic Commerce and Technology, 16 April at: http://www.statcan.ca/daily.

[4] The Economist (2004b), .Online Payments. Paying Through the Mouse, 20 May.

[5] Bartlett, Alan and Richard Silverman "SSH: The Secure Shell The Definitive Guide." 31 July 2001. URL: http://www.snailbook.com/ (3 March 2003)

[6] Deitel, Harvey M., Paul J. Deitel & Tem R. Nieto. e-Business & e-Commerce How to Program. Upper Saddle River: Prentice Hall. 2001.

[7] Dierks, T. & C. Allen. "The TLS Protocol Version 1.0." January 1999. (16 February 2003)

[8] Freier, Alan O. and Philip Karlton and Paul C. Kocher. "The SSL Protocol Version 3.0."November 1999. (14 March 2003)

[9] Mantel, Brian, 2000. "Why don't consumers use electronic banking: Towards a theory of obstacles, incentives and opportunities," Federal Reserve Bank of Chicago, occasional paper series.

[10] Goldfinger, C. (2003), .Secure Electronic Payment on the Internet., prepared for the EC workshop on building technologies for next generation electronic exchanges infrastructures and related applications deployment at: http://europa.eu.int/ISPO/ifwg/payments/epayments_sept11999.html

[11] The Economist (2000), .Making Online Payments More Secure., 26 October, p. 107.

[12] The Economist (2004a), .A Perfect Market . A Survey of E-Commerce., 15 May.

[13] OECD (1999), OECD Guidelines for Consumer Protection in the Context of Electronic Commerce, Paris.

[14] OECD (2002a), Report on Consumer Protection for Payment Cardholders, 14 June.

[15] Pago (2005), Pago Report 2005: Success and risk factors in international E-payment – Recommendations on real purchasing transactions in 2004.

[16] Paunov, C. and G. Vickery (2004), .Online Payments Systems for E-commerce., Journal of Financial Transformation, Capco, Vol. 12, December.

[17] Paybox (2003b), Paybox Signs Contract with M-Net to Launch Mobile Payment in the Middle East, Public Relations, 30 September, http://www.paybox.net

[18] PricewaterhouseCoopers (PwC) (2003), Study on the Security of Payment Products and Systems in the 15 Member States, Final Report, 16 June.

[19] TowerGroup (2004), .Making Sense from Cents: Trends in the Rebirth of Electronic Micropayments.

[20] Walczuch, R and R. Duppen (2003), .Payment Systems for the Internet . Consumer Requirements., Department of Accounting and Information Management, Faculty of Economics and Business Administration, University of Maastricht, The Netherlands.

[21] https://panopticlick.eff.org/

[22] http://blog.fireeye.com/research/2010/02/man-in-the-browser.html

[23] http://www.safenetinc.pt/uploadedFiles/About_SafeNet/Resource_Library/Resource_Items/White_Papers__SFDC_Protected_EDP/Man%20in%20the%20Browser%20Security%20Guide.pdf

[24] http://download.entrust.com/resources/download.cfm/24002/