



GNITED MINDS
Journals

*Journal of Advances in
Science and Technology*

*Vol. IV, No. VIII, February-
2013, ISSN 2230-9659*

SECURITY OF ONLINE PAYMENTS BY SSL (SECURE SOCKETS LAYER)

Security of Online Payments by SSL (Secure Sockets Layer)

Zahoor Ahmad Dar

Research Scholar (Computer Science), CMJ University, Shillong, Meghalaya

Abstract— All of us are a part of an age where everything is online. Such is the testimony of the boom that every possible thing which deals with consumers has gone online. On the internet numerous support services are provided to the customers. Online payment is a crucial process in e commerce. The payment activity requires the use of high security to protect online transactions from any unauthorized use on the internet. In some cases data is transferred in an encrypted form through a secured medium. Different payment mechanisms are available on the internet and each and every customer has the option of using the one that suits their requirement. Normally there are three common methods of payment which are e cash , e cheque as well as credit card. In this paper we analyze the various security measures which can be adopted for the security of the online payments.

Index Terms— Online payments, risks, SSL, Secure Sockets Layer, Protocol.

1. INTRODUCTION

Women have caught up with men in the last decade or so as far as online shopping is concerned. In the year 1998, 9 out of 10 online shoppers were men whereas now the ratio is 51 %. In the last ten years the number of online shoppers multiplied by 40 percent as well as the consumer spending increased manifold. The growth will continue and online shopping will evolve from a function to an experience.

There seems to be no difference between online as well as ordinary shopping. In the last ten years shopping has become an enjoyable experience with customer reviews as well as opinions about the products. This is also what inspires the modern Indian women. In addition to this online shopping does not have the same disadvantages as it used to have in the earlier days? Earlier people used to worry about the security of the online transactions and whether the delivery will be made on time. But all these things are of the past and online shopping has caught up big time in the world of today (Molenaar, 2010)

Email continues to be the most popular medium of communication and enticing the customers to go online and register does not always yield the desired results always. In addition to this the customers usually forget their user names along with passwords and this results in numerous calls being made to the call centre. In many programs it takes between 7 to 24 clicks to find and pay the bill which is far more than the experience worth repeating. Security features like phishing as well as identity theft are important barriers in online security. In the final analysis marketers are

finding it a difficult task to communicate the benefits to the consumers (Botha et al, 2002).

Phishing or spoofing as it is technically termed involves the sending of email messages to the members of online payment accounts such as banks , credit card companies as well as online payment services to update their records

2. HISTORY ABOUT ONLINE PAYMENTS

A merchant bank or a bank which is acquired is a bank that deals with both the buyers as well as the sellers (both buyers as well as sellers) that want to accept payment cards. In other words to process payments for transactions related to the internet the merchant must incorporate a merchant account. In this regard the business merchant has to provide some essential details before the bank grants him the permission to set up the account. This could be related to the business plan of his and questions concerning his credibility stature. The type of business also influences the bank's likelihood of granting an account. An example of a business like a weight loss scheme where money is returned back to the customers will not find enough takers. The banks assess the risk as well as the credit information provided. A new or risky business that aims to make \$ 5000 in sales a month has to keep \$ 2500 in the merchant account. One problem facing the online business is the level of fraud in online transactions is much higher than either in person or telephonic transactions of the same nature. The fact of the matter is that less than 10 % of the transactions are completed online through credit card but they account

for almost 70 % of the fraud. What is more alarming is that the percentage of online frauds is on the rise ever since the inception of ecommerce since 2008- 2009. But efforts have been stepped to decrease the frauds and some amount of success has been achieved in the recent days mainly due to the measures taken by the merchants (Schneider, 2011).

There are a variety of ways to utilize online payment but overall it boils down to three major options which are

- Your current bank- With functional click and mortar banks you can pay each bill as a onetime bill setting up payments for recurring bills, paying multiple bills at once and even set up future periodic payments. Payments to small electronic companies with no service can also be handled. In this regard one could also use a personal software programme for managing their budget as well
- Companies directly – You can go directly to the company's website or the utility company's website to sign up for the bill payment service. Essentially you are giving permission to both the bank as well as the company to deal with your financial information. One of the major advantages of signing up with a company is that you can view your complete bill history.
- Aggregation services- These companies offer their own independent online services. This service will gather and link all the online account information such as your credit card, utilities as well as mortgage company to name a few.
- Using a bill payment service with an aggregation service makes it convenient for you to pay all the bills from one website and have access to all your financial records (Lawrence, 2005).

Companies like Google processes the payment and then pays the merchant. In this regard the consumer does not need to remember the user name as well as the password of each and every merchant banker which he banks with. At any point of time he can review the history of the orders along with the payment details. Using PayPal as well as Google account is free for the users as they can set up their account in minutes and there are no extra charges associated with making the purchases as well. The fact of the matter is that consumers who are having such accounts are growing in numbers, but till 2008 any merchant banker could ever think of such a situation (Kimball and Rich, 2009).

3. HOW TO SECURE ONLINE PAYMENTS

Secure online payment processing and credit card transaction processing must be encrypted with strict back end security control systems to prevent unauthorized access to the private data of the customers (Kim and Solomon, 2012).

As the business includes the internet as part of their business models, they increase their chances of exposure to online threats risks as well as vulnerabilities. One has to remember that connecting to the internet means increasing the chances of exposure to hackers as well as thieves. Securing web applications along with securing front and back end systems are some of the methods which one could adopt.

In response to the growing concerns of the customers of using their credit card numbers on the internet companies have developed secure payment systems for e business. The most common forms of online payment systems are electronic cash as well as electronic wallets. In fact internet browsers like Firefox contain powerful encryption systems which is the powerful tool of encoding data for security purposes. When consumers see such an icon on the website they are aware of the fact that they are at a protected site.

An electronic wallet is another method of online payment in which a computer data file is stored at the e business site check out that not only contains electronic cash but credit card information as well as the address of an individual . In this regard consumers do not have to retype the information when they make purchase at a website. The mode of operation is pretty simple as the consumers simply click on the electronic wallet after selecting the items and all the information is transferred instantly (Boone and Kurtz, 2011).

Not surprising that ecommerce has its own set of challenges as the consumers are more concerned with protecting their data. Another secure online payment system is offered by the secure servers. Merchants using this system house their web sites on a secure server (Delta and Matsuura, 2010).

The question which needs to be understood how to secure your online payments, one of the methods in this regard would be to make your website as secure as possible. Each and every transaction should be protected so that everyone does not have the access to it in the first place. Setting up the mechanisms of online payments involves designing an interactive form which the users can fill in quiet easily and setting up form of payment. If you are accepting credit card payments already you may be quiet aware of the modalities involved in it.

If one does not accept credit card, they could set up a merchant banking account. In the midst of this entire if you do not want to have the hassle of setting up accounts relating to online payments then one could rely on third party charity donations for you. Websites such as Good as well as Network are perfect examples of websites in this sphere (Mutz and Murray, 2006).

As the masses tend to use the internet more and more they will become aware of the fact on what information to provide as well as what not. One needs to be truly protected while making online payments. In fact before entering the information on the website be assured of the fact that you are dealing with a trustworthy vendor. There is a quick way to figure out that you are dealing with a secured website as if after http there is and the answer pretty much readily solves itself (Johnson and Manning, 2010).

ET happens to be a message protocol which has been formulated by visa as well as master card. It secures credit card transactions over open networks like the internet. In this protocol the transaction has three major players which are the customer, the merchant as well as the bank of the customer. In addition to this it has three major principles which are

- All sensitive information between the three parties are encrypted
- All the three parties are required to authenticate themselves with certificates from the SET authority
- The merchant never uses the credit card number of the customer in plain text also

In fact the third feature makes the internet commerce more secured than the traditional card transactions such as pay by card in store. To some extent one may confer it to be more secure than SSL also.

4. ADVANTAGES RELATED TO ONLINE PAYMENTS

By allowing the users to purchase goods and services through the online platform you are allowing the users to pay for the goods as well as services at their own convenience. Many of the users of internet expect speed and ease of operations. Your online store is open throughout the day and you are enticing the customers to buy from you. In this regard freedom as well as independence play a big role as users are able to make their own purchases without relying on any individual. They do not need to wait for the assistance of a sales associate as well as a long period of approval as well. Automated online paying systems can benefit your business in the form of reduced costs. You need not pay someone for processing your transactions and you need not produce paper invoices. In the midst of all this think of the additional amount of time who can save in this regard. You will be able to focus on areas where the business needs you more. Before one accepts credit card payments they need to acquire an appropriate internet merchant banking account or utilize services like PayPal.

Doing business on the online platform is quite different from doing traditional business as the credit card as well as the card holder are not present at the time of sale. Some banks have no problems in issuing an internet merchant account as far as they are concerned. On the other side of things some banks are not all that keen in issuing a merchant account, so in this case you have to look for an alternative. One could also opt for a third party alternative also known as internet payment service. PayPal is an alternative to having your merchant account (Sweeney and Sweeney, 2011).

Other than all this mechanisms one could secure online payments if they have ISP enabled. This will help the customers to make payments with confidence or otherwise buyers will go to secured sites to make the payments. The online users are able to make transfer money quickly as well as safely. They work out to be a viable options for small business as well as the auction sellers. Another major advantage of the online services is that they are quick as well as easy to open and can be applied in a matter of few minutes (Simmons, 2004).

5. SSL AS SECURITY OF ONLINE PAYMENT

SSL commonly referred to as secured sockets layer which was developed by Netscape for securing the message transmission over the internet. It is not a payment technology but proposed as a means to secure the payments. It requires public key identification along with authentication, confidentiality and happens to be the security cornerstone in the domain of ecommerce. In fact the descendant of SSL is called the transport layer security and was proposed by the Internet engineering task force. There are slight difference between SSL and TLS but the protocol in both the cases tends to be the same (Janczewski, and Colarik, 2008).

To enhance the features of customer security most companies involved in e business use SSL to encrypt information as well as verify the authenticity of the senders as well as the receivers. It consists of a public as well as a private key (the software that encrypts the information) the public key is used to encrypt the information while the private key is used to decipher it. When a browser points to a domain with a SSL certificate the technology verifies the authenticity of the server as well as the visitor. VeriSign is one of the leading providers of SSL technology.

SSL provides a security handshake in which the client and the computer servers exchange a host of information. In this exchange of messages they agree upon the level of information they will use to exchange digital certificates and perform other tasks. Each and every computer without fail identifies the

other. It is not a problem if the client does not have a certificate as he is not the one who is sending the sensitive information. On the other side of the coin the server with whom the client is doing business ought to have a valid certificate. In other words one should be certain of the fact to which the commerce site belongs to in the first place. After the identification the SSL encrypts as well as decrypts the information flowing between both the computers. This literally means the information in the HTTP responses as well as requests is encrypted. The encrypted information includes the URL the client is requesting as well as any information which is requested in the form of forms. This might also include a credit card number as well. In short all information between the SSL enabled clients as well as the servers is recorded.

The question of utmost importance is SSL secure? Yes no doubt it provides the secured connection for payment transaction between the merchants as well as the consumers. In fact it is more secure than phone call or a postal mail delivery. In the midst of all this the security ends at the side of the merchant banker as the credit card information is not kept in any way (Joseph, 2006).

The SSL certificates allow the users to confirm a website's identity. The web browsers check the essential details along with the public portfolio is being issued by a competent authority or not. In fact the SSL server authentication is vital for securing e commerce transactions in which the users who send credit card numbers over the web in the first place would want to verify the identity of the server. This literally means that a user can send private data to a website being least worried about the misuse of it (Vacca, 2007).

6. CONCLUSION

The concept of online payments is increasing all the more in the world of today and is bound to increase with the passage of time. A host of advantages are related to it and no doubt there is a bright future associated with it also. But the grave area is the security aspect as lot of online users are still worried about the security as well as the privacy part in making online payments. eCash, PayPal as well as bill point are some of the effective tools which are used by most companies in making online payments.

In fact as e commerce booms it will be quiet easy as well as convenient to use online payments. New payment systems will be introduced to build trust as well as security for all the parties involved in the transaction. However for a payment system to gain popularity it must fulfil some basic conditions. These conditions are not only related to security but confidentially, ease of use as well as being free of cost to users are important points of consideration. In the present scenario SSL is a popular security mechanism in place which is virtually implemented by most of the organizations.

REFERENCES

1. Molenaar, C. (2010). Shopping 3.0: Shopping, the Internet Or Both? England: Gower
2. Botha, J., Bothma, C., and Geldenhuys, P. (2008). Managing E-commerce in Business. SA: Juta.
3. Schneider, G. (2011). Electronic Commerce. SA: Cengage.
4. Lawrence, J. (2004). The Budget Kit: The Common Cents Money Management Workbook. NY: Kaplan.
5. Kimball, C., Rich, J. (2009). Design and Launch an Online Web Design Business in a Week. Canada: Entrepreneur Media
6. Kim, D., and Solomon, M. (2012). Fundamentals of Information Systems Security. Canada: Jones and Bartlett
7. Boone, L., and Kurtz, D. (2011). Contemporary Business 2010 Update. NJ: Wiley
8. Delta, G., and Matsuura, J. (2011). Law of the Internet, Volume 2. USA: Aspen.
9. Mutz, J., and Murray, K. (2006). Fundraising For Dummies. NJ: Wiley.
10. Johnson, K., and Manning, S. (2010). Online Education For Dummies. NJ: Wiley.
11. Sweeney, S., and Sweeney, K. (2011). 101 Internet Businesses You Can Start from Home: How to Choose and Build. Canada: Maximum Press
12. Simmons, P. (2004). DIY Guide: How to publish your own ebook. UK: Password Publishing.
13. Janczewski, L., and Colarik, A. (2008). Cyber Warfare and Cyber Terrorism.
14. Joseph, P. (2006). E-Commerce: An Indian Perspective 2Nd Ed. Delhi: PHI.
15. Vacca, J. (2007). Practical Internet Security. Berlin: Springer.