Blind Side of Secure Electronic Transaction

B. Sheeba

Abstract— **In this eventful world, everyone is living a dramatic role. Barely have we spent time in our home. We don't have adequate time to accomplish our family desires. So online shopping is the one of the tremendous alternative way to carry out our needs.**

The customers/users will sit in their home and they can view as many products/service in their desktop and they can decide on the product/service, pay the money through online the merchandise will reach home within couple of days. So the customers don't know what the phenomenon behind the screen is. So this is about blindsiding of secure electronic transaction.

Index Terms— **Secure electronic transaction, secure socket layer, key lengths, role of customer**

I. INTRODUCTION

Electronic commerce is universally known as e-commerce is the trading of products\services done by private or government through online social networks. In 1984 Compuserve Company instigated Electronic mall in Canada and USA. In 1989 Sequoia Data Corp, company initiated first internet based system for e-commerce [9].

The objective is to ensure the secure electronic transaction. But how? By using some of the protected protocols we can guarantee it. There are countless software and hardware running in the wake of the screen which the customer doesn't discern. These protocols do all the encryption and decryption to make the user's data and merchant's data safe and sound.

The secure socket layer (SSL) and transport layer security (TLS) these two protocols are extensively used today. These protocols endow with secure transaction between two machines functioning on internet or network.

II. BEHIND THE SCREEN

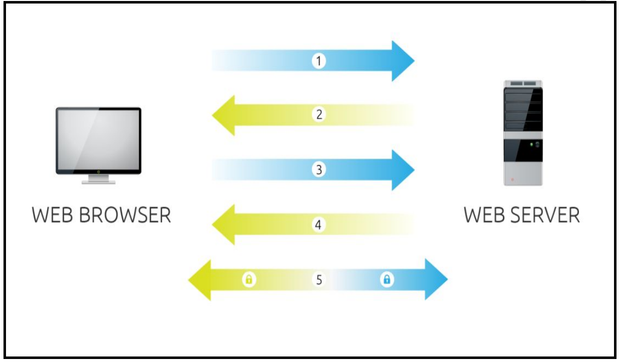
Customer thinking of a product, and selects the meticulous product on a website. Then studies about the product in online then be inclined to buy it. Then selects the quantity then make the order, will do payment, selects the bank, approach the payment (Credit card, Debit card, Net banking), enters the quantity and amount then authenticate the payment. The product will arrive at home within three days.

So the blind buyer is thinking every data he/she go through will arrive at the merchant straightforwardly and they drive the product to home. But behind the screen every distinct data will be encrypted by various key and they sent from side to side secured link. For the secure link we call for secure socket layer.

Manuscript received May 13, 2017

III. SECURE SOCKET LAYER

Secure socket layer establish link between browser and web server. This make certain that whatever data conceded in the link between browser and web server will be confidential [7].



The figure 1 represents the working of secure socket layer

1. The browser heaves the request to the web server to locate itself.
2. The SSL authenticate certificate and server's public key will be propel to the browser.
3. the browser encrypts and sends the symmetric session key before that browser counterpart the SSL authenticate certificate with the reliance CAs and then it finds that server is secured it can hope the certificate
4. Further server via its private key it decrypts the symmetric session key and fling back acknowledgement encrypted by session key so they can initiate the encrypted session
5. So by means of session key the Server and Browser at this instant encrypt all hand on data.

IV. KEY LENGTHS

In SSL layer 128 bit and 256 bit are key lengths with the assist of some algorithms and hashing function we can encrypt and decrypt the data. How difficult to encrypt the key? Envisage the key size considerably undersized so hackers realize it unproblematic for them to disengage the key. It will be thorny to decrypt the data if the key size is immense.

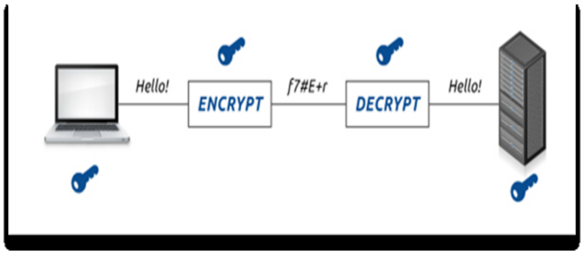


Figure 2 represents symmetric encryption

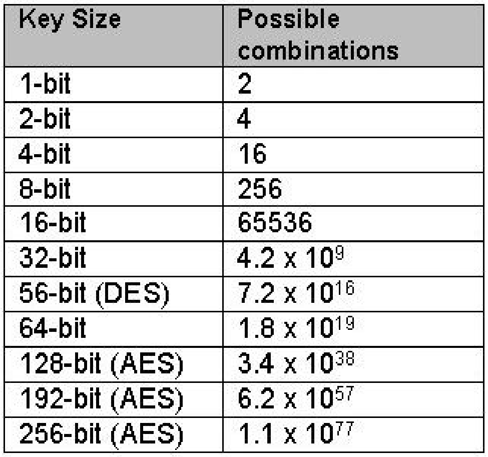
Symmetric encryption: both the sender and receiver necessitate the same key to encrypt and decrypt the data this is known as symmetric encryption

128-Bit Encryption

Thousands of years need to crack the code of 128 bit encryption as it will take 2^{128} combinations.

256-Bit Encryption

A longer key that provides a higher margin of security in encryption and decryption, as it will take 2^{256} combinations.
Nowadays 56-bit encryption is broadly used in symmetric encryption. Cracking a 256-bit key encryption will take twice as long as a 128-bit key encryption, which is 1,000,000 years needed practically.



Key Size	Possible combinations
1-bit	2
2-bit	4
4-bit	16
8-bit	256
16-bit	65536
32-bit	4.2×10^{9}
56-bit (DES)	7.2×10^{16}
64-bit	1.8×10^{19}
128-bit (AES)	3.4×10^{38}
192-bit (AES)	6.2×10^{57}
256-bit (AES)	1.1×10^{77}

Table 1 represents possible key combinations to decrypt the data according to key size

V. REVIEW OF LITERATURE

SET Secure Electronic Transaction Specification Book 1: Business Description states that to meet these needs, the SET Secure Electronic Transaction protocol uses cryptography to:

- Provide confidentiality of information,
- Ensure payment integrity, and
- Authenticate both merchants and cardholders.

This specification will enable greater payment card acceptance, with a level of security that will encourage consumers and businesses to make wide usage of payment card products in this emerging market [1].
One generally accepted approach to follow is suggested by Fites, et. al. [Fites 1989] and subsequently summarized by the 1997 Site Security Handbook (RFC2196) that includes the following steps [5].

- ➢ Identify what you are trying to protect
- ➢ Determine what you are trying to protect it from
- ➢ Determine how likely the threats are
- ➢ Implement measures which will protect your assets in a cost-effective manner
- ➢ Review the process continuously and make improvements each time a weakness is found

Techopedia explains *256-Bit Encryption* - 256-bit encryption is refers to the length of the encryption key used to encrypt a data stream or file. A hacker or cracker will require 2^{256} different combinations to break a 256-bit encrypted message, which is virtually impossible to be broken by even the fastest computers [4].
Typically, 256-bit encryption is used for data in transit, or data traveling over a network or Internet connection. However, it is also implemented for sensitive and important data such as financial, military or government-owned data. The U.S. government requires that all sensitive and important data be encrypted using 192- or 256-bit encryption methods [4].

VI. STEPS FOR SECURE TRANSACTION: CUSTOMER ROLE TO PLAY

- ✓ Personal computer or laptop is preeminent way to carry out online business deal /disbursement on every juncture
- ✓ Any person can hint their off the record data like A/c No, User ID and code word, if the customer carry out it on the civic machine
- ✓ At least for a month customer should have the inclination of shifting the password recurrently
- ✓ Keep serial of number changing the last digit alone along with some alphabets to remember the password
- ✓ Do not express the account details to stranger (through call or social network)
- ✓ there are possibilities it can reach in hands of hackers so do not write account details anywhere in your accessories

CONCLUSION

In e-commerce, exchanging data plays major role that carries business over the internet. It is extremely essential to exchange data between customers and merchant confidentially. A lot of mechanism could do with to design a protocol which will create a secured link between customer and merchant. In this paper we have seen in detail about Secure Socket Layer and how it works. The preeminent technique to exercise the presented set of rules is to pick the one which will toil in a precise e-commerce environment most powerfully.

REFERENCE

1. SET Secure Electronic Transaction Specification Book 1: Business Description Version 1.0 May 31, 1997
2. A Secure Electronic Transaction Payment Protocol Design and Implementation Houssam El Ismaili1 , Hanane Houmani2 , Hicham Madroumi3 Architecture of Systems Team - ENSEM, Hassan II University, 8118, Casablanca – Morocco – 2014
3. http://www.inet2000.com/public/encryption.htm
4. https://www.techopedia.com/definition/29703/256-bit-encryption
5. Fraser, B., (1997) RFC 2196 Site Security Handbook [Online] NWG. Available From: http://www.faqs.org/rfcs/rfc2196.html [Accessed: 31 October 2005]
6. http://coderevisited.com/
7. https://www.digicert.com/ssl.htm
8. AN ANALYSIS AND COMPARISON OF E-COMMERCE TRANSACTION PROTOCOLS - PURCHASING ORDER A Survey Paper for the completion of CMPE 298 by Judy Nguyen Summer 1999 SJSU
9. https://en.wikipedia.org/wiki/Secure_Electronic_Transaction