Website communications

Web based communication is defined as the sharing of information, words or ideas over a network of computers known as the internet.

A major factor in the success or failure of any web design project is communication.

Secure Socket Layer (SSL) technology allows web browsers and web servers to communicate over a secure connection.

In this secure connection, the data that is being sent is encrypted before being sent and then is decrypted upon receipt and before processing. Both the browser and the server encrypt all traffic before sending any data. SSL addresses the following important security considerations.

1. Authentication: During initial attempt to communicate with a web server over a secure connection. In this secure connection, the data that is being sent is encrypted before that server will present a web web browser with a set of credentials in the form of a server certificate.

2. Confidentiality: SSL responses are encrypted so that the data cannot be deciphered by the

third party and the data remains confidential.

3. Integrity: SSL helps guarantee that the data will not be modified in transit by the third party.

Secure Electronic Transaction (SET)

Secure Electronic Transaction (SET) is a system for ensuring the securing of financial transactions on the Internet.

With SET, a user is given an electronic wallet (digital certificate) and a transaction is conducted and verified using a combination of digital certificate and digital signatures among the purchaser, a merchant and the purchaser's bank in a way that ensures privacy and confidentiality.

Assume that a customer has a SET-enabled browser such as Netscape or Microsoft's Internet Explorer and that the transaction provider has a SET-enabled server.

1. The customer opens a MasterCard or Visa bank account. Any issuer of a credit card is some kind of bank.
2. The customer receives a digital certificate. This electronic file functions as a credit card for online purchase or other transaction. It includes a public key with an expiration date. It has been through a digital switch to the bank to ensure its validity.
3. Third-party merchants also also receive certificates from the bank. These certificate include the merchant's public key and the bank's public key.

4. The customer places an order over a web page, by phone, or some other means.
5. The customer's browser receives and confirms from the merchant's certificate that the merchant is valid.
6. The browser sends the order information.
7. The merchant verifies the customer by checking the digital ~~certificate~~ signature on the customer certificate.
8. The merchant sends the order message along to the bank. This includes the ~~key~~ bank's public key, the customer's payment information and the merchant's certificate.
9. The bank verifies the merchant and the message. The bank uses the digital signature on the certificate with the message and verifies the payment part of the message.
10. The bank digitally signs and sends authorization to the merchant, who can then fill the order.

What is the Role of RSA in E-commerce :

E-business is the most popular business there days. They deal with a lot of sensitive data of their customers. Security has become a tremendously important issue.

Technology has definitely been advanced but risk has increased as well with the increase of cyber crimes such as phishing, Hacking etc. So, by the use of cryptography, we can secure data.

The RSA algorithm is commonly used for securing communications between web browsers and e-commerce sites. The reason for this is the resistance to attack.

The ~~com~~ connection makes use of a secure Socket layer (SSL) certificate, which is created from the public and private keys.

The resulting pseudo-random number forms the basis for the certificate, which is installed at each end of the connection to ensure protected communications.

RSA

RSA implements a public-key cryptosystem, as well as digital signatures. In such cryptosystem, the encryption key is public and differs from the decryption key which is kept secret.

A public encryption method that relies on a public encryption algorithm, a public decryption algorithm and a public encryption key.

Using the public key and encryption algorithm anyone can encrypt a message. The decryption key is known only to authorized parties.

Operations of RSA :

The RSA algorithm involves four steps:

1. Key generation
2. Key distribution
3. Encryption
4. Decryption