Computer security has become one of the most important concerns in the entire discipline of computing. The recent explosive growth of the Internet and the World Wide Web has brought with it the need to protect sensitive communications over the open networks. In the past, security violations were generally done by young adults, just for fun. But as technology and usage of the internet increased, there is always the threat of planned attacks (cyber terrorists), where the loss of money could be large in billions. Hence the need for secure connection will arise. A robust solution for this is provided by VPN (Virtual Private Networks) and SSL (Secure Socket Layer) protocols in my research. In the recent past SSL protocol has revolutionized the area of VPN (Virtual Private Network). To set up secure communication from virtually any Internet-connected web browser, SSL based VPN products permit users to do such a thing. To implement a secure remote access, it is easier and resourceful than its predecessor (IP Sec).

In my research paper in which security of client – server communication is achieved by principles of security, like Authentication and Encryption. There are two sides of this application
server side and client side. Without certification, client can't communicate with the server. The SSL handshake-protocol message flow involves client and server negotiating a common cipher suite acceptable to both parties. The application based on RSA algorithm, using for encryption especially for data sent to server. A certificate is issued to each server and client using key tool commands. Private keys are protected by a password in key store. Client and server can thus communicate with each other only if the certificate has been issued to both. Once issued a secure and safe communication link is established. It gives an insight into the different attacks on the internet, and how the data can be sent securely through SSL.

References

Index Terms

Computer Science  Security

Keywords