{tag} {/tag}International Journal of Computer Applications
Foundation of Computer Science (FCS), NY, USA

Volume 175
-
Number 5

Year of Publication: 2017

Authors:

Lalit Mohan Joshi

10.5120/ijca2017915551

{bibtex}2017915551.bib{/bibtex}

Abstract

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 a 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 internet increased, there is always the threat of planned attack (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 side 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

1. A. O. Freier P. Karlton and P. C. Kocher. The SSL Protocol, Version 3.0. Netscape Communications, 1996, http://wp.netscape.com/eng/ssl3/draft302.txt (2003).

2. R. Rivest. The MD-5 Message-Digest Algorithm, RFC 1321. John Wiley and Sons, 1996, ftp://ftp.rfc-editor.org/innotes/rfc1321.txt (2003).

3. Charlie Scott, Paul Wolfe, and Mike Erwin, "Virtual Private Networks",Publisher: O'Reilly, Second Edition, ISBN: 1- 56592-529-7, pp.6-40.

4. R. Rivest, A. Shamir, and L. M. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems ", Communications of the ACM, v. 21, n. 2, Feb 1978, pp. 120-126.

5. Stephen Thomas, "SSL and TLS Essentials, Securing the Web",Publisher: Wiley, pp.12-14 & 37-60.

6. Giacomazzi, Poli, A. " Cost-Performance Optimization of SSLBased Secure Distributed Infrastructures"in Latin America Transactions, IEEE (Revista IEEE America Latina) Volume: 9 , Issue: 4 , Page(s): 550 – 556 in 2011.

7. C. J. Lamprecht, Aad and P. A. van Moorsel "Adaptive SSL: Design, Implementation and Overhead Analysis " in IEEE Computer Society, July 2007.

8. Norman Lim, Shikharesh Majumdar, Vineet Srivastava "Engineering SSL-based systems for enhancing system performance" in Proceedings of the 2nd ACM/SPEC International Conference on Performance engineering, March 2011.

9. Kapil Singh, Helen J. Wang, Alexander Moshchuk, Collin Jackson, Wenke Lee "Practical end-to-end web content integrity" in Proceedings of the 21st international conference on World Wide Web in ACM, April 2012.

10. Martin Georgiev, Subodh Iyengar, Suman Jana, Rishita Anubhai, Dan Boneh, Vitaly Shmatikov "The most dangerous code in the world: validating SSL certificates in non-browser software " Proceedings of the 2012 ACM conference on Computer and communications security ,October 2012.

11. Light, J. Ikejiani, O.K. "An efficient wireless communication protocol for secured transmission of content-sensitive multimedia data " in World of Wireless, Mobile and Multimedia Networks & Workshops IEEE Page(s): 1 – 6, April 2009

12. Norazah Abd Aziz, Nur Izura Udzir and Ramlan Mahmod,Performance Analysis for Extended TLS with Mutual Attestation for Platform Integrity Assurance,IEEE,2014.

13. LI Wei, XIANG Shuyue, CHEN Shuangbao, Improvement Method of SSL Protocol Identity Authentication based on the Attribute Certificate, International Conference on Computer Science and Service System,2012.

Index Terms

Computer Science Security

Keywords

Secure Socket Layer, Encryption, Security.