© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 08 Issue: 02 | January - March 2017
Paper is available at www.jrps.in | Email : info@jrps.in

HTTP SERVER SECURITY TO PREVENT ATTACKS ON COMMERCIAL: A REVIEW

[1]Sunil, Research Scholar,Department of CSE, Indus Instt. of Engg. & Tech, jind.
[2]Abhishek bhatnagar, A.P., Department of CSE, Indus Instt. of Engg. & Tech, jind

ISSN : 2278-6848
03
9 772278 684800
© International Journal for Research Publication and Seminar

ABSTRACT:- Hyper Text Transfer Protocol (HTTP) is an application-layer protocol used primarily on World Wide Web. HTTP uses a client-server model where web browser is client & communicates within web server that hosts website. Browser uses HTTP, which is carried over TCP/IP to communicate to server & retrieve Web content for user.

HTTP is a widely used protocol & has been rapidly adopted over Internet because of its simplicity. It is a stateless & connectionless protocol. Categories of attack could consist of passive monitoring of data communications exploitation by insiders, close-in attacks, harmful attacks through service provider & active network attacks. Information systems & networks usually offer targets & must be resistant within order to attack from full range of threat agents, from hackers to nation-states. System must be capable to restrict damage & recovery from occurrence of attacks. objective of research is to secure HTTP server from external attacks.

1. INTRODUCTION

HTTP concepts include idea that files can contain references to other files whose selection would elicit additional transfer requests. Any Web server machine contains, in addition to Web page files it can serve, an HTTP daemon, a program that is designed to wait for HTTP requests & handle them when they arrive. Your Web browser is an HTTP client, sending requests to server machines. When browser user enters file requests by either "opening" a Web file (typing in a Uniform Resource Locator or URL) or clicking on a hypertext link, browser builds an HTTP request & sends it to Internet Protocol address (IP address) indicated by URL. HTTP daemon in destination server machine receives request & sends back requested file or files associated within request.

Techopedia explains Hypertext Transfer Protocol

HTTP's simplicity is its greatest strength it is also its main drawback. As a result, Hyper Text Transfer Protocol - Next Generation (HTTP-NG) project has emerged as an attempt to replace HTTP. HTTP-NG promises to deliver a much higher performance & additional features to support efficient commercial applications in addition to simplifying HTTP's security & authentication features. Some of HTTP-NG's goals have already been implemented in HTTP/1.1, which incorporates performance, security & other feature improvements to its original version

HTTP/1.0.

A basic HTTP request involves following steps:

1. A connection to HTTP server is opened.
2. A request is sent to server.
3. Some processing is done by server.
4. A response from server is sent back.
5. The connection is closed.

2. LITERATURE REVIEW

Hailu Tegenaw (2015) within his research paper **"Application Aware Firewall Architecture to Enhance Performance of Enterprise Network (978-1-4799-7498-6/15©2015 IEEE)" stated that** performance of an enterprise network is affected not only by its protocol specification, its communication channel, design capacity & architecture of firewall but also by its implementation & traffic management. It was considered that Firewall is a perimeter security solution that is useful for addressing network traffic. It introduces a single point through which all traffic passes & as a result this creates performance bottleneck on enterprise network by increasing latency, reducing bandwidth & throughput.

Sangita A. Jaju(2015) within this research paper **"A Modified RSA Algorithm to Enhance Security for Digital Signature (978-1-4799-6908-1/15©2015 IEEE)"** stated that digital signature has been providing security services to secure electronic transaction over internet. Rivest, Shamir & Adlemen (RSA) algorithm was most widely used to provide security technique. Here they have modified RSA algorithm to enhance its level of security. This paper presents a fair comparison between RSA & Modified RSA algorithm along within time & security by running several encryption & decryption setting to process dataof different sizes. efficiency of these algorithms was considered based on key generation speed & security level. texts of different sizes were encrypted & decrypted using RSA & modified RSA algorithms. simulation result proves that within Modified RSA algorithm key generation is faster & this enhances security by two levels. RSA algorithm is faster than Modified RSA within terms of encryption & decryption speed.

Ayman Tajeddine, Ayman Kayssi, Ali Chehab, Imad Elhajj (Department of Electrical & Computer Engineering) (2014) presented a paper **"Authentication Schemes for Wireless Sensor Networks" within 17th IEEE Mediterranean Electrotechnical Conference, Beirut, Lebanon, 13-16 April 2014.**

In this paper, they discussed different authentication techniques suitable for severely constrained nodes within wireless sensor networks. They divide such techniques into three main categories based on symmetric cryptography, asymmetric cryptography, & hybrid techniques using both cryptographic methods. They discussed each category & deduce best cipher for each, namely, RC5 & IBE-ECC to be applied within a WSN. They also specify factors affecting decision of which category is best to use & different parameters affecting network within each category. Finally, they give a real network example & discuss appropriate choice of authentication scheme based on particular WSN needs.

3. TOOLS & TECHNOLOGY

Internet Information Services is an extensible web server created by Microsoft for use within Windows NT family.[2] IIS supports HTTP, HTTPS, FTP, FTPS, SMTP & NNTP. It has been an integral part of Windows NT family since Windows NT 4.0, though it may be absent from some editions & is not active by default.

IIS 6.0 & higher support following authentication mechanisms:

Anonymous authentication

1. Basic access authentication
2. Digest access authentication
3. Integrated Windows Authentication
4. UNC authentication
5. .NET Passport Authentication (Removed in Windows Server 2008 & IIS 7.0)[15]
6. Certificate authentication

IIS 7.0 has a modular architecture. Modules, also called extensions, can be added or removed individually so that only modules required for specific functionality have to be installed. IIS 7 includes native modules as part of full installation.

4. TREATS TO HTTP SERVER SECURITY

SECURITY THREATS

Categories of attack could consist of passive monitoring of data communications exploitation by insiders, close-in attacks, harmful attacks through service provider & active network attacks. Information systems & networks usually offer targets & must be resistant within within order to attack from full range of threat agents, from hackers to nation-states. System must be capable to restrict damage & recovery from occurrence of attacks.

5. CHALLENGES TO EXISTING NETWORK SECURITY

Much of theoretical work within cryptography is to cryptographic primitive algorithms within basic cryptographic properties & their relationship to other cryptographic problems. More complex cryptographic tools are then built from these basic primitives. Such primitives provide fundamental properties which are used in development of more complex tools called cryptosystems or cryptographic protocols that guarantee high-level security properties. Note however, that distinction between cryptographic primitives& cryptosystems, had been quite arbitrary; for example, RSA algorithm had been sometimes considered cryptosystem, & sometimes primitive. Eg. of cryptographic primitives consists pseudorandom functions, one-way functions, etc

Basic algorithm & terminology

RSA encryption & decryption are mathematical operations. These are exponentiation, modulo particular number. So **RSA keys** consist of numbers involved within this calculation, as follows:

1. **Public key** consists of **modulus** & **public exponent**;
2. **Private key** is consisting same **modulus** plus **private exponent**.

Proposed implementation

Here we are using HTTP filter to reject unauthenticated transmission of packets from server to client.

Here we have to enhance network security by customizing existing encryption techniques.

To study loopholes of existing security mechanisms & enhance security of network.

To program own socket server & corresponding client to prevent unauthentic access during data transmission.

To make use of more complex key during encryption & decryption.

To develop user interface to make client server communication.

6. CONCLUSION

During course of this thesis we have described in detail inspiration motivation behind our research its possible applications. A thorough exploration of both current previous efforts in Gesture recognition was revealed. Once this prelude was given we then offered a thorough description o f our system technologies incorporated. During design implementation an importance was made to keep system modular. This is to allow future enhancement would alleviate complexity of modifying or upgrading system. Individual components could simply be switched as long they interface within main system in a similar fashion.

REFERENCES

[1.] T. Kapuscinski M. Wysocki, "Hand Gesture Recognition for Man-Machine interaction", Second Workshop on Robot Motion andControl, October 18-20, 2001, pp. 91-96.

[2.] C. Yu, X. Wang, H. Huang, J. Shen K. Wu, "Vision-Based Hand Gesture Recognition Using Combinational Features", IEEE SixthInternational Conference on Intelligent Information Hiding andMultimedia Signal Processing, 2010, pp. 543-546.

[3.] P.S. Rajam G. Balakrishnan, "Real Time Indian Sign Language Recognition System to aid Deaf-dumb People", IEEE, 2011, pp. 737- 742.

[4.] A. Malima, E. Ozgur M. Cetin, "A Fast Algorithm for Vision- Based Hand Gesture Recognition for Robot Control", IEEE, 2006.

[5.] Manigandan M I.M Jackin, "Wireless Vision based Mobile Robot control using Hand Gesture Recognition through Perceptual Color Space", IEEE International Conference on Advances in ComputerEngineering, 2010, pp. 95-99.

[6.] D.Y. Huang, W.C. Hu S.H. Chang, "Vision-based Hand Gesture Recognition Using PCA+Gabor Filters SVM", IEEE FifthInternational Conference on Intelligent Information Hiding andMultimedia Signal Processing, 2009, pp. 1-4.

[7.] E. Koh, J. Won C. Bae, "On-premise Skin ColorModeing Method for Vision-based Hand Tracking", 13th IEEEInternational Symposium on Consumer Electronics (ISCE), 2009, pp. 908-909.

[8.] J.L. Raheja, K. Das A. Chaudhury, "An Efficient Real Time Method of Fingertip Detection", International Conference on Trendsin Industrial Measurements automation (TIMA), 2011, pp. 447- 450.

[9.] J. Rekha, J. Bhattacharya S. Majumder, "Shape, Texture Local Movement Hand

Gesture Features for Indian Sign Language Recognition", IEEE, 2011, pp. 30-35.

[10.] R. Gopalan B. Dariush, "Towards a Vision Based Hand Gesture Interface for Robotic Grasping", IEEE/RSJ InternationalConference on Intelligent Robots Systems, October 11-15, 2009, St. Louis, USA, pp. 1452-1459.