Advanced Engineering Technology and Application
An International Journal

@ 2012 NSP
Natural Sciences Publishing Cor.

Securing Proxy Server using Encryption Techniques: Theory, Design and Implementation

Humaira Habib Awan[a], Aihab Khan[b], Murad Khan[c]

[a] *Department of Computer Science, Fatima Jinnah Women University, Rawalpindi, Pakistan.*
[b, c] *Department of Computing and Technology, Iqra University, Islamabad, Pakistan.*
Email:[a] humaira_habib87@yahoo.com, [b]aihabkhan@yahoo.com, [c]muradkhan23@gmail.com

Received: Jul 8, 2011; Revised Oct. 4, 2011; Accepted Jan. 6, 2012
Published online: 1 May 2012

Abstract: Proxy server is an important communication agent for secure communication between a client and a proxy server. The usage of a proxy server cannot be limited to Local Area Network (LAN). It can also be used on a Wide Area Network (WAN). To enhance the security of communication between clients and servers we proposes a secure model to made communication between client and proxy server more secure by using encryption algorithms. We test different encryption algorithms and found that Advanced Encryption Standard (AES) provides more secure communication between a client and a proxy Server. Simulation results show that the proposed scheme performs better in case of using AES as compared to other encryption algorithms. We conclude that the proposed model enables secure communication among user and proxy server.

Keywords: Proxy server; Advanced encryption standard; Local area network; Wide area network;

1 Introduction

With the huge information data growth in internet network service, how to increase the data transmission capacity for communication network is an important problem. Wavelength-Division Multiplexing (WDM) optical network can use the same fiber to support multiple optical channels, and can provide an ultra high-speed transmission. Such optical networks promise data transmission rates than the current high level of electronic networks [1-2]. So the WDM network is regarded as a long backbone transmission network. With the rapid development of the WDM technology, WDM optical communication network will be the future development direction of network construction [3]. To transmission network, most of the existing infrastructure network is still built in voice transmission, in accordance with the present technology, voice communications can be transmitted through the packet network and be ability to carry multi-service circuit switched networks [4].

Nowadays most of the research work focuses on the secure communication between a client and a proxy server. A client sends a request to a server for a resource, but before reaching this request to the server it is passed through a proxy. A proxy server is then used to provide the request resource either by connecting to the server or by serving it from a cache. A Proxy server works with web browsers and servers, or other applications. These applications contain processing emails by supporting network protocol suits. Which can be hypertext transfer protocol (HTTP) and the protocols used for designing server and also for assembling information on an internet protocol (IP) network. A Proxy server can also be used to provide security to the information which can be in form of text or hypertext markup language (HTML) pages. There are different type of proxy servers like Forward Proxy (PF), Open Proxy (OP) and Reverse Proxy (RP). A FP is used to take requests from internal network and forward it to the internet. An OP is used to forward a request to inside a network and outside to anywhere on the internet. A RP is used to transfer a request from internet to servers on internal network. A proxy server can be used for filtering, caching, DNS, logging and eavesdropping, gateways to private networks and accessing services anonymously. A proxy server can be implemented as web proxy, suffix proxy and transport proxy. In case of web proxy server, the client send HTTP request for web pages, it will pass from the proxy server, where proxy server apply filter rule, hide sensitive information and send the request to the web server. A proxy server can be used to enhance the performance of network by using different advanced techniques in which most common is caching technique. A user first sends a request to connect to a proxy server for onward communication. An attacker can intercept this request and forward it to attacker proxy server, by this way user starts communication with an unknown proxy and attacker behaves like a benign user by using source IP address of compromised user. The reason an attacker gets to all these information is that the communication between user and proxy server is not secure. In this research an attempt is made to secure the communication between user and proxy server by employing encryption algorithms

The rest of the paper is organized as follows: Section 2 outlines related work, Section 3 presents framework overview and Section 4 presents the results and the paper is concluded in Section 5.

2 Related Work

To guarantee more enhanced secure communication between proxy server and a client Ziqing Mao et al. [1]. Design a comprehensive web-service based link-translating proxy, Address-Bar-Only Proxy (ABOProxy). A client can send its data to proxy server while using an address-bar. The uses of sub-domain mapping techniques entirely eliminate the need to translate or even to find relative links in content. The Proxy in design provides simplicity, robustness, security, load time and scalability. Paul Reeser et al. [2] proposed a model-based approach for the Web server performance evaluation and design an enhanced analytic queuing model of Web servers that can be used in dynamic server-side computing in a distributed environment. The model forms an excellent basis for a decision support tool to allow system architects to predict the behavior of new systems prior to deployment, or existing systems under new workload scenarios. Ravi Chandra et al. [3] presents the delegate, a proxy-based architecture that enables a user to access web sites without disclosing personal information to untrusted machines. Delegate enforces rules at the proxy to detect and prevent session hijacking. A simple keystroke logger, a common payload of many viruses, records and transmits the secret information e.g. passwords, credit card numbers, PIN numbers entered into these machines.

There are attacks that can exploit protocol suits. These attacks can be done by intruder from inside and outside network. A technique based on intrusion detection called stateful protocol analysis is used to stop these attacks. Rocky et al. [4] presents a model based on packet filtering technique embedded in transport layer. The type of proxy used by said author is capable of handling multiple security functions ranges from user or host level authentication to session logging. This technique encapsulates packets between a transport level proxy server and transport level proxy client. TLP client reside above UDP/IP layer. The data flows from client to UDP/IP and then to the internal IP network. A transport layer proxy is then used to scan incoming traffic using different security functionalities and pass this traffic to external proxy server. The model is successful in many ways but it slower down the speed of data movement because each packet is filtered for different security purposes. An approach used by Siu et al. [5] for protecting multimedia data and objects. The author presents secure proxy system for audio and video streaming applications. This system uses asymmetric reversible parametric sequence. This system is able to provide following functionalities: data confidentiality during transmission, end to end transmission, against proxy intruders and member collusion. The system uses multi key RSA technique. An encryption configuration parameter is also use to increase the quality of audio and video against the unauthorized parties. Author depend his work with practical implementation and simulation results. Jung et al. [6] proposes a proxy system for accessing and sharing media contents. The proposed system uses DLNA proxy system for secure communication and sharing information between AV devices in the home. The system works in four different phases. In first phase DLNA Media Proxy Server register its IP address using user authentication and authorization details. Second it broadcast a message for discovering devices and information for services. Third phase is for media contents retrieving, it shows media content list through a message. And lastly a device can sends a request for specific media contents. The DMA get this information from internet via DMPS. There is device that does not have any hardware system for connecting to internet. They make a bridge connection with host computer to connect internet. H. Karen et al. [7] present a work that provides security for small network enabled devices to connect with host computer. A proxy system is designed that supports small network enabled devices and also supporting organization policies. This system uses web proxy tunneling techniques with some security features for better deployment, security related and routing problems. Peter Wurzinger et al. [8] propose a technique based on a server side solution for preventing cross site scripting attacks. The proposed system uses a reverse proxy system that interrupts all HTML responses and also change the state of a web browser for script enabled contents. This system is named as secure web application proxy, SWAP. The system can be deployed on clients. Using this system we can get rid of vulnerabilities in web applications. The systems capture every HTML response and check it for javaScript contents. The system is modified during run time for differentiating benign and malicious java Script contents. The system is good but it handles only java Script contents. A three tier model is presents by Dwen-Ren Tsai et al. [9] for protecting information of social networking sites. A client sends information to the social networking web sites using a proxy. This proxy is used to detect security threats on social networking websites. This system can handle web based security threats like malware, phishing attack etc. The proxy also checks information coming from server to the client for any malicious behavior. If a web page is found to be black list the proxy send a warning to the client side.

3 Proposed Model

In this research a model is designed proposed for secure communication between a proxy and a client. It basically consists of a Client and Proxy Server environment. The basic approach followed in this system is to prevent the Client and Proxy Server communication from the external intruders. For this purpose a cryptographic algorithm AES (Advanced Encryption Standard) has used to make the network communication more secure. The system works as follows.

A user can use proxy server by sending an HTTP request to it. The Proxy server will check the status of the request. If the request sent to proxy server is encrypted it will be processed otherwise proxy server will send an acknowledgement to the user to send data in encrypted form. Once the user send encrypted request to the proxy server the proxy server will decrypt the request and will forward this request to the required destination.

The data coming from the outside network will be checked for authentication by the proxy if it is authenticated the proxy server will forward this data to the user.

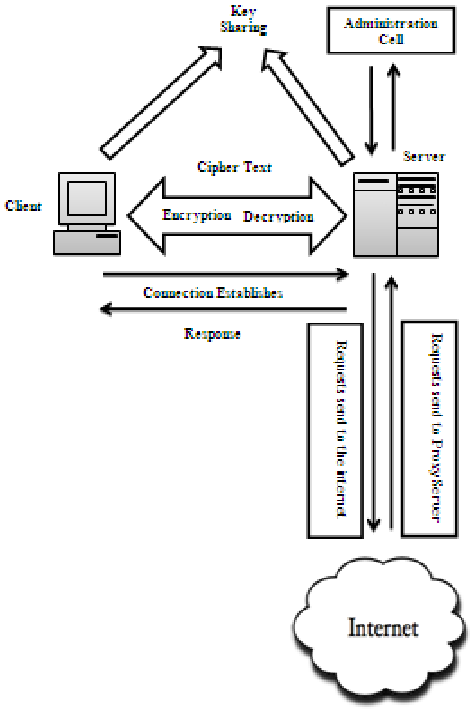

Figure 1: Data flow in proposed model.

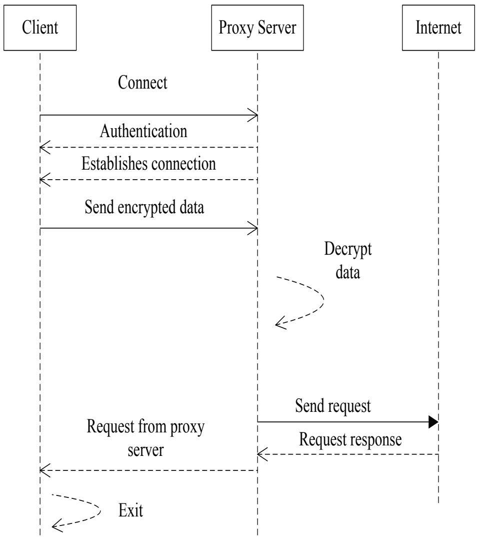

Figure 2: Connection flow Diagram

The user can decrypt this data for further processing.

The Encryption is done through Advance Encryption Standard. AES uses a key of 128 bit; it is very difficult for an attacker to guess this key. This strong authentication has shown some good results against other encryption schemes.

The working of the model is shown in following diagram.

The figure shows that how a client can make connection with proxy server and how proxy server can accomplishes its tasks.

4 Results

The system is checked over different scenarios. We quantify time in seconds taken by a client to establish a connection with a webserver using proxy and without proxy. The result of this experiment is shown in following figure.

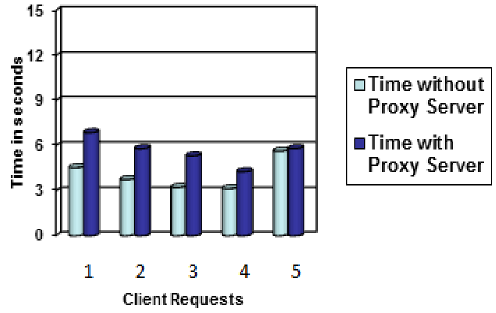

Figure 3: Time in seconds with and without a proxy server.

Following table shows time in seconds while a client is browsing with and without proxy.

Table 1 Time in seconds with and without a proxy server.

Options Requests	Without Proxy	With Proxy
1	4.5429675	5.32765
2	3.75	4.2714
3	3.236718	5.81304
4	3.149675	5.32765
5	5.6388	4.2714

Following graph shows time in seconds of browsing while a proxy processing a request with and without an encryption and decryption.

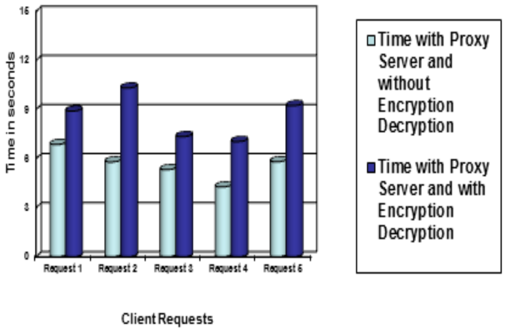

Figure 4: Time in seconds while a proxy server processing different requests with and without encryption and decryption.

Following table shows time in seconds while processing a request with and without encryption.

Table 2 Time in seconds while a proxy server processing different requests with and without encryption and decryption.

Options Requests	Time with Proxy Server without Encryption Decryption	Time with Proxy Server and with Encryption Decryption
1	6.8671875	8.91276
2	5.80229	10.32018
3	5.32765	7.35013
4	4.2714	7.04398
5	5.81304	9.23864

5 Conclusion

We designed a model for secure transition of data flow between a client and a proxy server. The system is able to protect network connection between a user and a proxy server from external and internal intruders. As technology changes, it is become very difficult to control and get the behavior and pattern of intruders in intranet. The proposed model is design to protect the communication between a user and proxy server. The reason is to protect this communication is to achieve data integrity. In most of the networks internal user attacks are more frequent hence this model can be applied in such scenarios. Further contribution to this model can be achieved by applying hash functions to more secure this model.

Refrences

[1] *Z. Mao and C. Herley, "A Robust Link-Translating Proxy Server Mirroring the Whole Web," ACM SIGAPP Applied Computing Review, vol. 11, no. 2, Nov 2008.*

[2] *P. Reeser and R.Hariharan, "An Analytic Model of Web Servers in Distributed Computing Environments," Telecommunication Systems, vol. 21, pp. 283-299, 2002.*

[3] *T.W.V.D.H. Mehrotra, K. E.Seamons and N. Venkasubramanian R. Jammalamadaka, "Delegate: A Proxy Based Architecture for Secure Website Access from an Untrusted Machine," in in Proceedings of 22nd Annual Computer Security Applications Conference, 2006.*

[4] *R.K.C Chang, "Transport layer proxy for stateful UDP packet filtering," in ISCC 2002 Seventh International Symposium on Computers and Communications, 2002. Proceedings., Taormina, Italy, 2002, pp. 595 - 600.*

[5] *S.F Yeung, "A multikey secure multimedia proxy using asymmetric reversible parametric sequences: theory, design, and implementation," IEEE Transactions on multimedia, vol. 7, no. 2, pp. 330 - 338 , April 2005.*

[6] *Jung-Tae Kim, "Implementation of the DLNA Proxy System for Sharing Home Media Contents ," IEEE Transactions on Consumer Electronics, vol. 53, no. 1, pp. 139 - 144, Feb 2007.*

[7] *H.K Lu, "A Proxy Agent for Small Network-Enabled Devices," in IEEE International Performance, Computing and Communications Conference, 2008. IPCCC 2008,*

Austin, Texas, Dec, 2008, pp. 445 - 449.

[8] C. Platzer, C. Ludl, E. Kirda and C. Kruegel P. Wurzinger, "SWAP:Mitigating XSS Attack susing a Reverse Proxy," in Software Engineering for Secure Systems, Vancouver, Canada, 2009, pp. 33 - 39.

[9] A. Y Chang, S-C.Chung and Y.S.Li D-R.Tsai, "A proxy-based real-time protection mechanism for social networking sites," in IEEE International Carnahan Conference on Security Technology., San Jose, CA, Oct 2010, pp. 30 - 34.