International Journal of Scientific and Technical Advancements
ISSN: 2454-1532

Review and Analysis of Proxy Servers and Their Security Issues in Web Domain

Ashaq Hussain Dar[1], Fayaz Ahmad Fayaz[2], Syed Nisar Hussain Bukhari[3], Muneer Ahmad Dar[4]
National Institute of Electronics and Information Technology, J & K, India
Department of Electronics and IT, Ministry of communication and Information Technology, Govt. of India
E-mail: ashaq@nielit.gov.in[1], fayaz@nielit.gov.in[2], nisar.bukhari@gmail.com[3], muneer@nielit.gov.in[4]

***Abstract*—** A proxy server is a server acting as mediator for forwarding requests from clients and which in turn seeks resources from other servers [6]. Traditional proxy servers were used for variety of ethical roles like caching, bandwidth saving, logging /auditing, malware filtering etc. Essentially proxy servers manifested to add structure and encapsulations for data transmitted. Over the time proxy servers (particularly web proxy servers) are attributed for malicious activities like anonymous logging, breaching the security policy of the network, circumvent Internet filtering, masquerading the identity of the source etc. In this paper different types of proxy will be discussed like Forward proxies, Open proxies, Reverse proxies etc. Security aspects for committing online crimes while maintaining anonymity will be discussed.

***Keywords*—** Proxy, security, anonymous, web proxy.

I. INTRODUCTION

Using a proxy means that instead of communicating with the remote end directly, there is a middleman transmitting everything back and forth. There is a long list of reasons to use proxies, including the following:

- To prevent the remote end from knowing where the request came from (for security purposes).
- For caching: some proxies store the information that passes through them and supply the same content for a while (to speed up data delivery)
- To block unwanted resources based on keywords, URL's or other attributes, enforcing a policy.
- To bypass security / parental controls.
- To allow the browser to make web requests to externally hosted content on behalf of a website when cross-domain restrictions (in place to protect websites from the likes of data theft) prohibit the browser from directly accessing the outside domains.
- For logging and auditing usage in order to provide detailed statistics and reports.
- To prevent downloading the same content multiple times (and save bandwidth).
  - To bypass content filters (applied by other proxies).
  - For anti-virus purposes: proxies can scan files for malware before serving it to the client [1].
  - To prevent data leaks from behind the proxy sent outside [1].
  - For circumventing regional restrictions (make it look like resources were accessed from a different country).

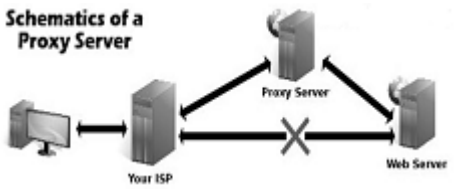

Fig. 1. Architectural view of Proxy servers [7].

II. TYPES OF PROXY

A proxy server may run right on the user's local computer or at various points between the user's computer and destination servers on the Internet.

A proxy server that passes requests and responses unmodified is usually called a gateway or sometimes a tunneling proxy.

A forward proxy is an Internet-facing proxy used to retrieve from a wide range of sources (in most cases anywhere on the Internet).

A reverse proxy is usually an Internet-facing proxy used as a front-end to control and protect access to a server on a private network, commonly also performing tasks such as load-balancing, authentication, decryption or caching.

III. FORWARD PROXIES

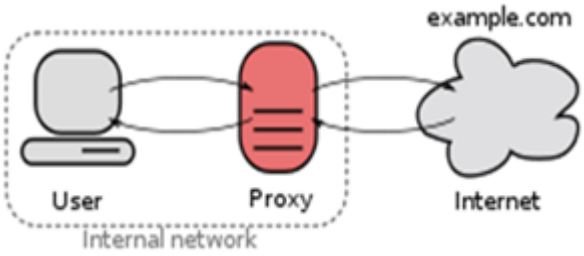

Fig. 2. A forward proxy taking requests from an internal network and forwarding them to the Internet [6].

Ashaq Hussain Dar, Fayaz Ahmad Fayaz, Syed Nisar Hussain Bukhari, and Muneer Ahmad Dar, "Review and analysis of proxy servers and their security issues in web domain," *International Journal of Scientific and Technical Advancements*, Volume 2, Issue 4, pp. 253-256, 2016.

Forward proxies are proxies where the client server names the target server to connect to.[5] Forward proxies are able to retrieve from a wide range of sources (in most cases anywhere on the Internet).

IV. Open Proxies

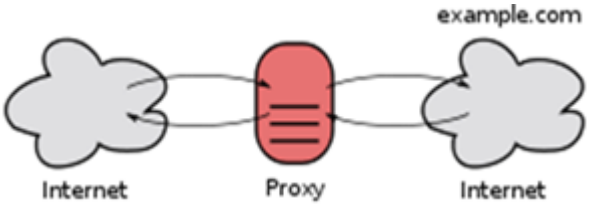

Fig. 3. An open proxy forwarding requests from and to anywhere on the Internet [6].

An open proxy is a forwarding proxy server that is accessible by any Internet user. An anonymous open proxy allows users to conceal their IP address while browsing the Web or using other Internet services. There are varying degrees of anonymity however, as well as a number of methods of 'tricking' the client into revealing itself regardless of the proxy being used.

V. Reverse Proxies

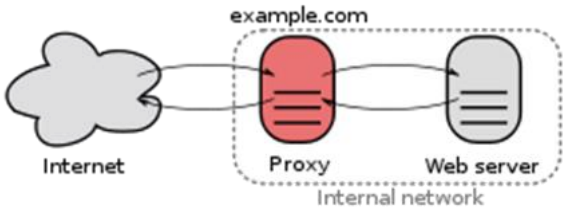

Fig. 4. A reverse proxy taking requests from the Internet and forwarding them to servers in an internal network. Those making requests connect to the proxy and may not be aware of the internal network [6].

A reverse proxy (or surrogate) is a proxy server that appears to clients to be an ordinary server. Requests are forwarded to one or more origin servers which handle the request. The response from the origin server is returned as if it came directly from the proxy server, leaving the client no knowledge of the origin servers.[5]

Reverse proxies are installed in the neighborhood of one or more web servers. All traffic coming from the Internet and with a destination of one of the neighborhood's web servers goes through the proxy server. The use of "reverse" originates in its counterpart "forward proxy" since the reverse proxy sits closer to the web server and serves only a restricted set of websites.

There are several reasons for installing reverse proxy servers:

- Encryption / SSL acceleration
- Load balancing
- Serve/cache static content
- Compression
- Spoon feeding
- Security
- Extranet Publishing

VI. Security Issues

One of the most successful vectors for gaining control of customer information and resources is through man-in-the-middle attacks. In this class of attack, the attacker situates himself between the customer and the real web-based application, and proxies all communications between the systems. From this vantage point, the attacker can observe and record all transactions. This form of attack is successful for both HTTP and HTTPS communications. For man-in-the-middle attacks to be successful, the attacker must be able to direct the customer to their proxy server instead of the real server. Lets look at what kind of MITM attacks can be used and under what scenario [7].

Here is a list of Different type of MITM attacks[3].

LOCAL AREA NETWORK: -

- ARP poisoning -
- DNS spoofing
- STP mangling
- Port stealing

FROM LOCAL TO REMOTE (through a gateway):

- ARP poisoning
- DNS spoofing
- DHCP spoofing
- ICMP redirection
- IRDP spoofing - route mangling

REMOTE:

- DNS poisoning
- Traffic tunneling
- Route mangling

However with respect to Identity Theft 'Transparent proxy attack' and 'DNS poisoning attack' are the most popular amongst Hacking community. Here is an articulate explanation of both these attacks:

- Transparent proxy attack [4].

In order to execute this attack the hackers try to trick the victim through below mentioned four easy steps. Step four explains analogy of MITM in case of Https [2].

STEP1

URL rewriting: Prepend all URL's with the attacker's host so that requests are routed through it. http://home.netscape.com/ becomes http://www.attacker.org/http://www.server.com/

STEP2

Pages are then requested through www.attacker.org, which functions as a proxy to fetch the true page (in this case, http://www.server.com/), applying any of the attacker's desired transformations in the process.

Ashaq Hussain Dar, Fayaz Ahmad Fayaz, Syed Nisar Hussain Bukhari, and Muneer Ahmad Dar, "Review and analysis of proxy servers and their security issues in web domain," *International Journal of Scientific and Technical Advancements*, Volume 2, Issue 4, pp. 253-256, 2016.

ISSN: 2454-1532

STEP3

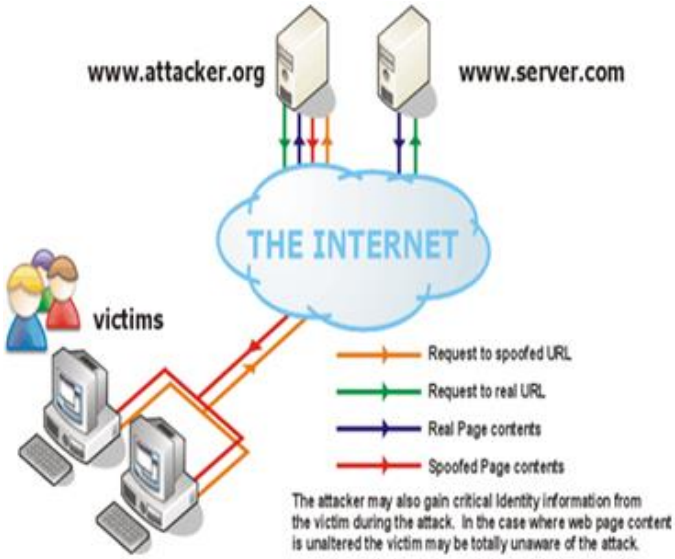

Fig. 5. Man in middle Attack [7].

STEP 4

After the above steps have been executed there is a secure connection between the victim and the attacker's host of which the victim is unaware as he is happy to notice that he has a secured connection hence his data is safe.

The attacker can then create a secure connection to the real host, decrypt the received data, apply transformations, re-encrypt for the victim, and send it on to him.` The Victim still remains uninformed however the Hacker has already achieved his goal.

- DNS Cache Poisoning

This is another popular MITM attack with hackers when it comes to "phishing". This attack is based on simple convention of Ip to host resolution .Here is how it works:

Every system has a host file in its systems directory in case of windows this file resides at the following location in case of windows:

C:\WINNT\system32\drivers\etc

Your computer also has a hidden system file called the Hosts file. This file can be used to hard code domain name translations and direct you to a different site. The file in you system looks like this:

Specimen of a normal Host file:

Copyright (c) 1993-1999 Microsoft Corp.
#
This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
This file contains the mappings of IP addresses to host names. Each
entry should be kept on an individual line. The IP address should
be placed in the first column followed by the corresponding host name.
The IP address and the host name should be separated by at least one
space.
#
Additionally, comments (such as these) may be inserted on individual
lines or following the machine name denoted by a '#' symbol.
#
For example:
#
102.54.94.97 rhino.acme.com # source server
38.25.63.10 x.acme.com # x client host
127.0.0.1 localhost

Normally if you try to visit www.citibank.com your computer sends the request to a DNS server to find out the IP address of that domain name. After the same has been resolved the request generated from your browser is forwarded to the Citibank Webserver.

Specimen of a normal Host file under DNS poisoning attack:

Copyright (c) 1993-1999 Microsoft Corp.
#
This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
This file contains the mappings of IP addresses to host names. Each
entry should be kept on an individual line. The IP address should
be placed in the first column followed by the corresponding host name.
The IP address and the host name should be separated by at least one
space.
#
Additionally, comments (such as these) may be inserted on individual
lines or following the machine name denoted by a '#' symbol.
#
For example:
#
102.54.94.97 rhino.acme.com # source server

Ashaq Hussain Dar, Fayaz Ahmad Fayaz, Syed Nisar Hussain Bukhari, and Muneer Ahmad Dar, “Review and analysis of proxy servers and their security issues in web domain,” *International Journal of Scientific and Technical Advancements*, Volume 2, Issue 4, pp. 253-256, 2016.

ISSN: 2454-1532

38.25.63.10 x.acme.com # x client host
127.0.0.1 localhost
XX.XX.XX.XX Citibank.com

However for a system under such attack Hosts file supercedes DNS records by adding an entry in the Hosts file with the domain name "citybank.com" and a different IP address to which your computer can be redirected. Rather than being sent to the true Citybank server your request will go to the address specified in the Hosts file.

In the above example XX.XX.XX.XX depicts the IP address of Hackers server which is hosting a fake login screen for the legitimate domain www.citibank.com.The victim thinks that he is passing his credentials to what he types as www.citibank.com in the browser bar. However the attacker has already achieved his goal! Once again the victim remains uninformed.

REFERENCES

[1] Zwicky, Elizabeth D.; Cooper, Simon; Chapman, D. Brent (2000). Building Internet Firewalls (2nd ed.)
[2] "Transparent Proxy Definition". ukproxyserver.org. 1 February 2011.
[3] "Vulnerability Note VU#435052". US CERT. 23 February 2009. Retrieved 14 August 2010.
[4] Wessels, Duane (2004). Squid The Definitive Guide. O'Reilly. p. 130. ISBN 978-0-596-00162-9.
[5] "Forward and Reverse Proxies". httpd mod_proxy. Apache. Retrieved 20 December 2010.
[6] Wikipedia Notes: http://en.wikipedia.org/wiki/Proxy_server
[7] Man in middle attack : http://www.contentverification.com/man-in-the-middle/

Ashaq Hussain Dar, Fayaz Ahmad Fayaz, Syed Nisar Hussain Bukhari, and Muneer Ahmad Dar, “Review and analysis of proxy servers and their security issues in web domain,” *International Journal of Scientific and Technical Advancements*, Volume 2, Issue 4, pp. 253-256, 2016.