ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 1, Issue 2, November 2012

Design and Simulation of an E-Mail Proxy Firewall

Oluwaseyitanfunmi Osunade

Abstract*— Electronic mail (e-mail) services are the most used on the Internet. They carry messages, documents and pictures within the mail or as attachments from one connected device to another device. Internet services, such as electronic mail (e-mail), are provided by Internet Service Providers (ISPs) or business organizations such as Yahoo!, Google and Hotmail. The high frequency and volume of messages transmitted through the e-mail servers is enormous. Not all the messages transmitted are useful to the receivers because some are marketing messages, unsolicited advertisements and malicious messages. E-mail service providers use several methods to protect their clients from such unsolicited e-mails. In this study, the focus is on preventing unsolicited e-mails from being routed to e-mail boxes using the proxy firewall method. An e-mail proxy software was designed using a search and match algorithm and then developed into Java executable code to be run on an e-mail server. The proxy software, placed between the e-mail server and the network, uses a set of tables to perform the filtering of e-mails and placement of e-mails into boxes. The software developed, called Proxy Firewall, is to protect the clients' e-mail box from unsolicited malicious mails. The software was tested and the results are presented in this paper.

***Index Terms*— Databases, E-Mail, Information Filtering, Information Flow Controls, Java.**

I. INTRODUCTION

The firewall is a system or group of systems that enforces an access control policy between two or more networks. The firewall can be thought of as a pair of mechanisms: one which exists to block traffic, and the other which exists to permit traffic. Some firewalls place a greater emphasis on blocking traffic, while others emphasize permitting traffic. Probably the most important thing to recognize about a firewall is that it implements an access control policy. If you don't have a good idea of what kind of access you want to allow or to deny, a firewall really won't help you. It's also important to recognize that the firewall's configuration, because it is a mechanism for enforcing policy, imposes its policy on everything behind it.

A proxy server (sometimes referred to as an application gateway or forwarder) is an application that mediates traffic between a protected network and the Internet. Proxies are often used instead of router-based traffic controls, to prevent traffic from passing directly between networks. Many proxies contain extra logging or support for user authentication. Since proxies must ``understand" the application protocol being used, they can also implement protocol specific security (e.g., an FTP proxy might be configurable to permit incoming FTP and block outgoing FTP).

Proxy servers are application specific. In order to support a new protocol via a proxy, a proxy must be developed for it. One popular set of proxy servers is the TIS Internet Firewall Toolkit (``FWTK") which includes proxies for Telnet, rlogin, FTP, the X Window System, HTTP/Web, and NNTP/Usenet news. SOCKS is a generic proxy system that can be compiled into a client-side application to make it work through a firewall. Its advantage is that it's easy to use, but it doesn't support the addition of authentication hooks or protocol specific logging.

The SMTP (simple mail transfer protocol) server is the web server in charge of mail services. Whenever you send a piece of e-mail, your e-mail client interacts with the SMTP server to handle the sending. The SMTP server on your host may have conversations with other SMTP servers to actually deliver the e-mail.

E-mail stands for electronic mail, for the vast majority of people right now; the real e-mail system consists of two different servers running on a server machine. One is called the SMTP server. The SMTP server handles outgoing mail. The other is either a POP3 server or an IMAP server, both of which handle incoming mail. POP stands for Post Office Protocol, and IMAP stands for Internet Mail Access Protocol. A typical e-mail server looks like this:

The treatment of the project topic is taken from the view point of an ISP .As an ISP there are many security threats being faced, these attacks can come in different forms and through different routes. One of these many routes is the SMTP (simple mail transfer protocol), and these attacks can come in the form of spam.

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 1, Issue 2, November 2012

As an ISP I will allow my clients direct access to the internet. Practically there are three networks the internet, the DMZ, and the intranet. The DMZ (demilitarized zone) is where all the servers will be placed i.e. the dns server, the SMTP server etc. The intranet is the ISP's internal network. The ISP's internal network will also have an SMTP server this is necessary because the ISP provides mail services for its clients also this mail service is similar to that of other public mail service providers like yahoo, for example the client will have an e-mail address as such clientname@isp.com. The aim of this work is to design and develop proxy software capable of preventing spam emails emanating from blacklisted websites.

II. LITERATURE REVIEW

Computer networks are vulnerable to many attacks such as social engineering when someone pretends to be a legitimate system user or administrator tricking people into revealing secrets; war dialing is when someone uses computer software and a modem to search for desktop computers equipped with modems that answer, providing a potential path into a corporate network; Denial-of-Service (DOS) attacks overwhelm a computer network denying legitimate users of the computer network access; protocol-based attacks take advantage of known or unknown weaknesses in network services; host attacks are vulnerabilities in the operating systems or in the system set up; password guessing; and, eavesdropping of all sorts, including stealing e-mail messages, files, passwords, and other information over a network connection by listening in on the connection. Firewalls can help protect against some of these attacks. A firewall is a system or group of systems that enforces an access control policy between two or more networks. The actual means by which this is accomplished varies widely, but in principle, the firewall can be thought of as a pair of mechanisms: one, which exists to block traffic, and the other, which exists to permit traffic. Some firewalls place a greater emphasis on blocking traffic, while others emphasize permitting traffic.

The Internet, like any other society, is plagued with the kind of jerks who enjoy the electronic equivalent of writing on other people's walls with spray paint, tearing their mailboxes off, or just sitting in the street blowing their car horns. Some people try to get real work done over the Internet, and others have sensitive or proprietary data they must protect. Usually, a firewall's purpose is to keep the jerks out of your network while still letting you get your job done.

Some firewalls permit only email traffic through them, thereby protecting the network against any attacks other than attacks against the email service. Other firewalls provide less strict protections, and block services that are known to be problems. Generally, firewalls are configured to protect against unauthenticated interactive logins from the ``outside" world. This, more than anything, helps prevent vandals from logging into machines on your network. More elaborate firewalls block traffic from the outside to the inside, but permit users on the inside to communicate freely with the outside. The firewall can protect against any type of network-borne attack if you unplug it. Firewalls are also important since they can provide a single ``choke point" where security and audit can be imposed. Unlike in a situation where a computer system is being attacked by someone dialing in with a modem, the firewall can act as an effective ``phone tap" and tracing tool. Firewalls provide an important logging and auditing function; often they provide summaries to the administrator about what kinds and amount of traffic passed through it, how many attempts there were to break into it, etc.

Because of this, firewall logs are critically important data. They can be used as evidence in a court of law in most countries. You should safeguard, analyze and protect your firewall logs accordingly. Firewalls can't protect against attacks that don't go through the firewall. Many corporations that connect to the Internet are very concerned about proprietary data leaking out of the company through that route. Unfortunately for those concerned, a magnetic tape, compact disc, DVD, or USB flash drives can just as effectively be used to export data. Another thing a firewall can't really protect you against is traitors or idiots inside your network. While an industrial spy might export information through your firewall, he's just as likely to export it through a telephone, FAX machine, or Compact Disc. CDs are a far more likely means for information to leak from your organization than a firewall. Firewalls also cannot protect you against stupidity. Users who reveal sensitive information over the telephone are good targets for social engineering; an attacker may be able to break into your network by completely bypassing your firewall, if he can find a ``helpful" employee inside who can be fooled into giving access to a modem pool. Before deciding this isn't a problem in your organization, ask yourself how much trouble a contractor has getting logged into the network or how much difficulty a user who forgot his password has getting it reset. If the people on the help desk believe that every call is internal, you have a problem that can't be fixed by tightening controls on the firewalls.

Firewalls can't protect against tunneling over most application protocols to Trojans or poorly written clients. There are no magic bullets and a firewall is not an excuse to not implement software controls on internal networks or

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 1, Issue 2, November 2012

ignore host security on servers. Tunneling ``bad'' things over HTTP, SMTP, and other protocols is quite simple and trivially demonstrated. Security isn't ``fire and forget''.

Lastly, firewalls can't protect against bad things being allowed through them. For instance, many Trojan Horses use the Internet Relay Chat (IRC) protocol to allow an attacker to control a compromised internal host from a public IRC server. If you allow any internal system to connect to any external system, then your firewall will provide no protection from this vector of attack.

Firewalls can't protect very well against things like viruses or malicious software (malware). There are too many ways of encoding binary files for transfer over networks, and too many different architectures and viruses to try to search for them all. In other words, a firewall cannot replace security-consciousness on the part of your users. In general, a firewall cannot protect against a data-driven attack--attacks in which something is mailed or copied to an internal host where it is then executed. This form of attack has occurred in the past against various versions of *send mail*, *ghost script*, scripting mail user agents like *Outlook*, and Web browsers like *Internet Explorer*. Each site is a little different from every other in terms of what attacks are likely to be used against it. Some recurring themes do arise, though.

SMTP Server Hijacking (Unauthorized Relaying):This is where a spammer will take many thousands of copies of a message and send it to a huge list of email addresses. Because these lists are often so bad, and in order to increase the speed of operation for the spammer, many have resorted to simply sending all of their mail to an SMTP server that will take care of actually delivering the mail. Of course, all of the bounces, spam complaints, hate mail, and bad PR come for the site that was used as a relay. There is a very real cost associated with this, mostly in paying people to clean up the mess afterward. The Mail Abuse Prevention System Transport Security Initiative maintains a complete description of the problem, and how to configure every mailer on the planet to protect against this attack.

1) Exploiting Bugs in Applications : Various versions of web servers, mail servers, and other Internet service software contain bugs that allow remote (Internet) users to do things ranging from gain control of the machine to making that application crash and just about everything in between. The exposure to this risk can be reduced by running only necessary services, keeping up to date on patches, and using products that have been around a while.

2) Bugs in Operating Systems: Again, these are typically initiated by users remotely. Operating systems that are relatively new to IP networking tend to be more problematic, as more mature operating systems have had time to find and eliminate their bugs. An attacker can often make the target equipment continuously reboot, crash, lose the ability to talk to the network, or replace files on the machine. Here, running as few operating system services as possible can help. Also, having a packet filter in front of the operating system can reduce the exposure to a large number of these types of attacks. And, of course, choosing a stable operating system will help here as well. When selecting an OS, don't be fooled into believing that ``the pricier, the better''. Free operating systems are often much more robust than their commercial counterparts

Cheswick and Bellovin, in the definitive text on Internet firewalls, said an Internet firewall has the following properties: it is a single point between two or more networks where all traffic must pass (choke point); traffic can be controlled by and may be authenticated through the device, and all traffic is logged.

a) Packet filtering

Since routers are commonly deployed where networks with differing security requirements and policy meet, it makes sense to employ packet filtering on routers to allow only authorized network traffic to the extent possible. The use of packet filtering in those routers can be a cost-effective mechanism to add firewall capability to an existing routing infrastructure. As the name implies, packet filters specify packets to filter (discard) during the routing process. These filtering decisions are usually based on contents of the individual packet headers (e.g., source address, destination address, protocol, port). Some packet filter implementations offer filtering capabilities based on other information, but we consider these under the heading of stateful inspection described below.

Generally speaking, packet filtering routers offer the highest performance firewall mechanism. However, they are harder to configure because they are configured at a lower level, requiring you to have a detailed understanding of protocols[2].

Packet filtering is typically implemented on two kinds of platforms

- General purpose computers acting as routers
- Special purpose routers

Application proxies

An application proxy is an application program that runs on a firewall system between two networks .The host on which the proxy runs does not need to be acting as a router. When a client program establishes a connection “through” a proxy to a destination service, it first establishes a connection directly to the proxy server program. The

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 1, Issue 2, November 2012

client then negotiates with the proxy server to have the proxy establish a connection on behalf of the client between the proxy and the destination service. If successful, there are then two connections in place: one between the client and the proxy server and another between the proxy server and the destination service. Once established, the proxy then receives and forwards traffic bi-directionally between the client and service. The proxy makes all connection-establishment and packet-forwarding decisions; any routing functions that are active on the host system are irrelevant to the proxy.

As with packet filtering, application proxies are available on both special purpose proxy machines and general purpose computers. Generally speaking, application proxies are slower than packet filtering routers. However, application proxies are, in some ways, inherently more secure than packet filtering routers. Packet filtering routers have historically suffered from implementation flaws or oversights in the operating system's routing implementation on which they depend. Since packet filtering capabilities are "add-ons" to routing, they cannot correct or compensate for certain kinds of routing flaws.

As a result of making more complex filtering and access control decisions, application proxies can require significant computing resources and an expensive host upon which to execute. For example, if a certain firewall technology running on a UNIX platform needs to support 200 concurrent HTTP sessions, the host must be capable of supporting 200 HTTP proxy processes with reasonable performance. Add 100 FTP sessions, 25 SMTP sessions, some LDAP sessions, and some DNS transactions and you have a host that needs to sustain 500 to 1,000 proxy processes. Some proxies are implemented using kernel threads (which can dramatically reduce resource requirements) but resource demands remain high.

Stateful Inspection or Dynamic Packet Filtering

We use the terms stateful inspection or dynamic packet filtering to refer to a more capable set of filtering functions on routers. Packet filtering is restricted to making its filtering decisions based only on the header information on each individual packet without considering any prior packets. Stateful inspection filtering allows both complex combinations of payload (message content) and context established by prior packets to influence filtering decisions. As with packet filtering, stateful inspection is implemented as an "add-on" to routing, so the host on which the stateful inspection function is executing must also be acting as a router.

The principle motivation for stateful inspection is a compromise between performance and security. As a routing "add-on," stateful inspection provides much better performance than proxies. It also provides an increase in the level of firewall function than simple packet filtering. Like proxies, much more complex access control criteria can be specified and like packet filtering, stateful inspection depends on a high quality (i.e., correct) underlying routing implementation.

III. METHODOLOGY

This work used simulation as the methodology for developing and testing the e-mail proxy software. The design consists of simple identifiable units that were written in Java programming language while the database was developed in Microsoft Access. The units interacted based on the input from the send mail interface and the blacklist file.

IV. PROPOSED DESIGN

The proposed e-mail proxy firewall is made up of four components. They are

- A send mail interface for sending e-mail
- A database which contains the following
  - Incoming mail: this is a table that contains the list of mails that are allowed to get to the server and the e-mail box.
  - Filtered mail, this table contains the e-mails with the corresponding sender and receiver that are not allowed to get to the server,
  - Blacklist is the list of blacklisted IP addresses which is loaded using the autoloader
- Autoloader: this loads the blacklisted IP addresses from a text data-file into the blacklist table, this has no interface.
- Server : this is a simulation of an actual mail server

Fig. 1 below shows the different components of the design and their interaction in protecting e-mail boxes from spam and unsolicited e-mails.

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 1, Issue 2, November 2012

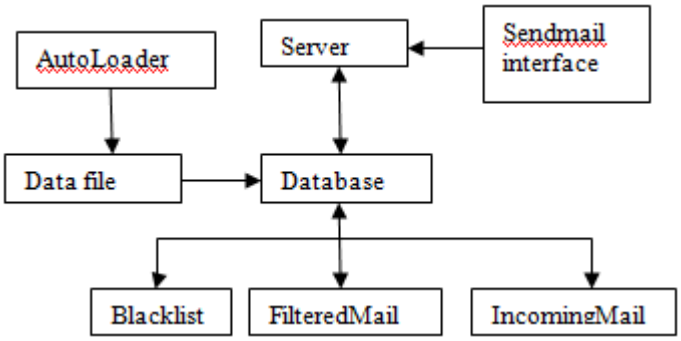

Fig. 1: Components of E-Mail Proxy Firewall System

V. PROGRAM ALGORITHM

The algorithm for the proposed system is given below:

Start server
Wait for server initialization reply
Start autoloader
Blacklisted IP list is loaded into database file
Sendmail is activated
Mail is sent to the server
If mail is coming in
If IP address of incoming mail on blacklisted list
Filter and put in filtered list
Else
Put in incoming list
EndIf
If connection to internet is made
List is downloaded into data-file
Autoload list into blacklist table
Else
Use previous downloaded list
Endif

"Principal" (e.g., "principal investigator") and "principle" (e.g., "principle of measurement"). Do not confuse "imply" and "infer." Prefixes such as "non," "sub," "micro," "multi," and "ultra" are not independent words; they should be joined to the words they modify, usually without a hyphen. There is no period after the "et" in the Latin abbreviation "*et al.*" (it is also italicized). The abbreviation "i.e.," means "that is," and the abbreviation "e.g.," means "for example" (these abbreviations are not italicized).An excellent style manual and source of information for science writers is [9].

VI. RESULTS

The software is capable of running on any Win32 platform. Figure 2 shows the start of the simulated e-mail server.

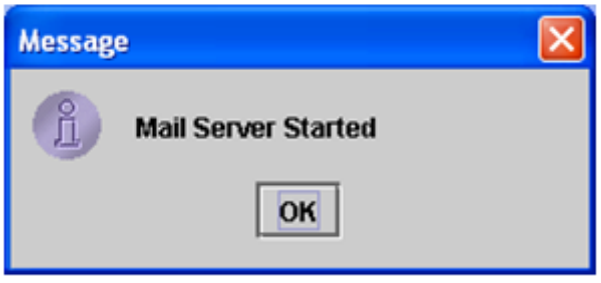

Fig 2: Visual confirmation that Mail Server is started

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 1, Issue 2, November 2012

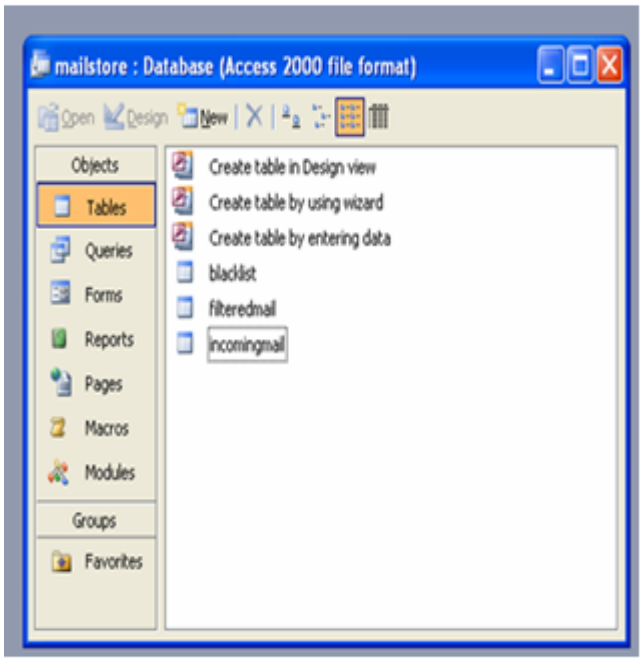

Fig 3: View of the database

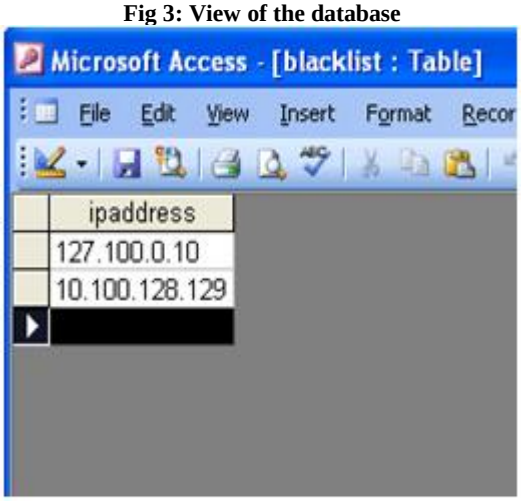

Fig 4: Blacklist table

The list of IP addresses for websites that send out unwanted e-mails is contained in the Blacklist table shown in Figure 4. The list is obtained from a website offering such services or it can be created if the expertise is available.

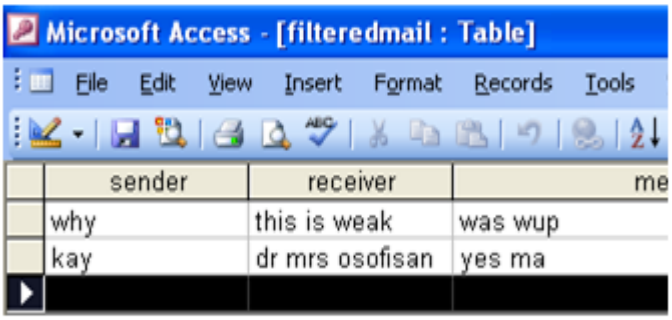

Fig 5: Filtered Mail Table

Figure 5 shows all e-mails that have been blocked from being delivered to the client's e-mail box. The senderip, last column in the figure, contains some of the IP addresses on the Blacklist table.

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 1, Issue 2, November 2012

Fig 6: Incoming Mail Table

The table in Figure 6 displays e-mails that have been checked against the blacklist table and found deliverable to the client's e-mail box. The e-mails do not originate from IP addresses on the Blacklist table as shown in the last column of the table.

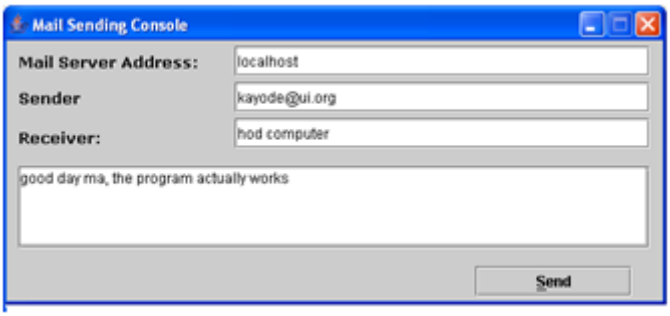

Fig 7: Send Mail Interface

1) Unexpected results are reported.
2) Because replication is required for scientific progress, papers submitted for publication must provide sufficient information to allow readers to perform similar experiments or calculations and use the reported results. Although not everything need be disclosed, a paper must contain new, useable, and fully described information. For example, a specimen's chemical composition need not be reported if the main purpose of a paper is to introduce a new measurement technique. Authors should expect to be challenged by reviewers if the results are not supported by adequate data and critical details.
3) Papers that describe ongoing work or announce the latest technical achievement, which are suitable for presentation at a professional conference, may not be appropriate for publication in a TRANSACTIONS or JOURNAL.

VII. CONCLUSION

The e-mail proxy firewall software was developed based on filtering which offers the ability to control the kind of e-mail the clients' receive. The system is designed to filter client e-mails going to the server, using the Internet Protocol address of the server where the e-mail is coming from, and based on the filtering performed, it should put the e-mails in their appropriate table and provide information to the tables . The software uses a list of already known senders of unwanted e-mails based on their Internet Protocol address. The list is regularly updated so as to keep the proxy software working efficiently. Packet filtering functionality can be added to improve the performance of the firewall.

REFERENCES

[1] Avolio and Blask. 1998. Application Gateways and Stateful Inspection: A Brief Note comparing and contrasting. Retrieved on February 20, 2011 from http://www.avolio.com/apgw+spf.html.

[2] Chapman, B. and Zwicky, D. 1992. Building Internet Firewalls. Retrieved on February 20, 2011 from http://www.ora.com/ .

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 1, Issue 2, November 2012

[3] Cheswick, W. and Bellovin, S. XXXX. Firewalls & Internet Security. Addison-Wesley Press. Retrieved on February 20, 2011 from http://www.aw.com/cp/Ches.html .

[4] Coopers & Lybrand. 1997. Microsoft Proxy Server Security Evaluation. Coopers & Lybrand, L.L.P., Information Technology Security Services.

[5] Federico A. 1998. Firewall and Internet Security, the second hundred (Internet) Year.Avolio Consulting.

[6] McCrea P.; Smart B.; Andrews M. 1998. Blocking Content on the Internet: a Technical Perspective.

[7] McGobbon, S.M. 2000. Firewall and Internet Security. Retrieved on February 20, 2011 from http://secinf.net/fw/steph.

[8] Oliver and Chapman. 1996. Data Processing and information Technology. Ashford Colour Press, Gosport.

[9] CISCO. 2000. Cisco PIX Firewall and Stateful Firewall Security. White Paper. Retrieved on February 20, 2011 from http://www.cisco.com/warp/public/cc/pd/fw/sqfw500/tech/nat_wp.htm.

[10] Windows NT magazine. 2000. The Power of packet filtering. Retrieved on February 20, 2011 from http// www.win2000mag.com/Articles/Index.cfm? ArticleID=7735.

[11] Zwicky, Elizabeth D and Cooper, Simon. 2000. Building Internet Firewalls. Sebastopol: O'Reilly and Associates. Page 76.

[12] H.M. Dietel and P.J. Deitel. 2003. Java. How to programming series. 3rd edition.

[13] Design the firewall system. Retrieved on February 20, 2011 from www.cert.org/security-improvement/practices/p053.

[14] Matt Curtin and Marcus Ranum. 2011. Internet Firewalls: Frequently Asked Questions. Retrieved on February 20, 2011 from www.interhack.net/pubs/fwfaq/

[15] Cheswick, bellovin and rubin. 2005. Firewalls and internet security. 2nd edition.

[16] How e-mails work. Retrieved on February 20, 2011 from www.howstuffswork.com.

[17] Firewall definition, application proxy definition. Retrieved on February 20, 2011 from www.webopedia.com.

[18] Firewall and internet security. Retrieved on February 20, 2011 from www.phptr.com/articles/article.

[19] The Spamhaus Project - SBL.htm. Retrieved on February 20, 2011 from www.spamhaus.com.

AUTHOR BIOGRAPHY

Oluwaseyitanfunmi Osunade, Dept of Computer Science, University of Ibadan, Nigeria. E-mail: o.osunade@ui.edu.ng