



International Journal of Emerging Technologies in Computational and Applied Sciences (IJETCAS)

www.iasir.net

Fault Detection and Deployment of Security Mechanisms in E-mail Systems

Kulvinder Singh Handa^a, Sanjeev Dhawan^b

^{a, b} Faculty of Computer Science & Engineering, University Institute of Engineering & Technology (U.I.E.T), Kurukshetra University, Kurukshetra (K.U.K)- 136 119, Haryana, INDIA.

E-mail: {kshanda_rsdhawan@rediffmail.com}

Abstract: This paper presents the realistic flaws and design implementation of security mechanisms in current e-mail services for unauthorized access. A thorough study is carried out to discuss the existing design of current e-mail systems, and furthermore, a virtually feasible design has been presented, which can completely vanish the role of any type of misuse, online fraud and attack in an online system. It has been argued that individuals or groups can now use cyberspace to threaten government, or terrorize the citizens of a country by cracking into a government or military maintained Website or most importantly when they use electronic mail (e-mail). However, to deal with such type of Internet threats, we should be aware of the basic functionality, nature and possible security concerns which can be taken while accessing the Internet. This paper has been organized into four parts: part I discusses the basic usage and general working and specific problem domain of an e-mail system, part-II presents the one of the weaknesses of present Web-based free e-mail service providers like: Rediffmail.com, Gmail.com, Hotmail.com, Yahoo.com, Mail.com, Lycosmail.com and Zapakmail.com. Basically, these e-mail services configure accounts for users and these Web-based e-mail services allow users to access their e-mail from any Web, part III describes the mechanism for Internet security and e-mail authentication on the basis of digital certificates, secure e-mail pattern and the deployment of Advanced Digital Signature Services (ADSS) server, and part IV gives the conclusions and future trends, which should be incorporated to implement efficient security mechanism not only for receiving external e-mail data but also for retrieving and checking the data stored at respective e-mail server for a particular account.

Keywords: Digital certificates, e-mail system and threats, Internet security, secure e-mail pattern.

I. Introduction

Electronic mail (generally known as e-mail) is a method of sending and receiving formatted messages and files over the Internet from source to destination. The files are generally sent in the form of attachments along with e-mails. Depending upon the Internet traffic, an e-mail message can go anywhere in the world in a few seconds. Internet Service Providers (ISPs) issue e-mail addresses in the form of *username@domainname*. Post Office Protocol, version 3 (POP3) and Internet Message Access Protocol, version 4 (IMAP4) are two major protocols used for accessing e-mails from servers. POP3 is used to store e-mail messages on a remote server until a user chooses to view the message and download them onto a local machine. IMAP4 is also used to store e-mail on a remote server, but allows users to manipulate e-mail messages directly on the server without downloading the messages. However, POP3 servers require users to download e-mails before viewing, accessing e-mails from different machines. But, IMAP4 allows users to leave messages on the server, so that users can access e-mails from multiple machines without distributing the messages among the servers. Although an e-mail has a simple structure and it can send messages only in NVT-7 (Network Virtual Terminal) bit ASCII format. Due to this, it is also having some limitations. For example, it cannot be used for languages that are not supported by 7-bit ASCII characters (such as German, French, Russian, Chinese, Japanese, and Hebrew etc.). Furthermore, it cannot be used to send binary files, video or audio data. So, Multipurpose Internet Mail Extensions (MIME) is a supplementary protocol that allows non-ASCII data to be sent through e-mail. Moreover, MIME acts as software that transforms non-ASCII data to ASCII data and vice versa. The current version of MIME is 1.1 and it consists of five headers that can be added to the original e-mail header section. Finally, to send the message from one server to another server, most e-mail systems use Simple Mail Transfer Protocol (SMTP) [1] [2] [3] [4].

II. Requirement and Evolution of E-mail

The Web has significantly changed the behaviour and expectations of human beings in the areas of information retrieval, knowledge sharing and collaborative working. With the advancement of World Wide Web commonly known as WWW, the world has shrunk down, and it has truly become a magnificent force for the people who are using the facility of WWW for fulfilling their different needs. The WWW was created in 1989 by British scientist Sir Tim Berners-Lee, working at the European Organization for Nuclear Research (CERN) in Geneva, Switzerland, and released in 1992. Since then, Berners-Lee has played an active role in guiding the development of Web standards (such as the markup languages in which Web pages are composed). The working of the Web is based on hyperlinks which are used to navigate between documents (called 'Web pages') with the help of a program called a Web browser. A Web

browser is a software application, which enables a user to display and interact with text, images, videos, music, games and other information typically located on a Web page at a Website. Some of the Web browsers currently available for personal computers include Internet Explorer, Netscape Navigator, Mozilla Firefox, Safari, Opera, Google Chrome, Flock, Arachne and AOL Explorer etc. Web and the Internet have brought significant changes in information technology and their related scenarios. Today email is one of the promising applications available on the Internet. It can take days to send a hard copy letter across the country and weeks to go around the world. To save time and money, more and more people are relying on electronic mail. It's fast, easy and much cheaper than the postal service. E-mail is an electronic message sent from one device to another. While most messages go from computer to computer, e-mail can also be sent and received by mobile phones, PDAs and other portable devices. With e-mail, you can send and receive personal and business-related messages with attachments, such as photos, documents, music, video clips and software programs. Let's say you have a business with sales agents working around the country. How do you communicate with them without running up a huge phone bill? E-mail is the best way to go. A postal letter makes stops at different postal stations along the way to its final destination, similarly, e-mail passes from one computer, known as a mail server, to another as it travels over the Internet. Once it arrives at the destination's mail server, it's stored in an electronic mailbox until the recipient retrieves it. This whole process can take seconds, allowing you to quickly communicate with people around the world at any time of the day or night. To receive e-mail, you need an account on a mail server. This is similar to having a postal box where you receive letters. One advantage over regular mail is that you can retrieve your e-mail from any location on earth, provide that you have Internet access. Once you connect to your mail server, you download your messages to your computer or wireless device, or read them online. The following figure 1.1 shows the basic working of an e-mail system.

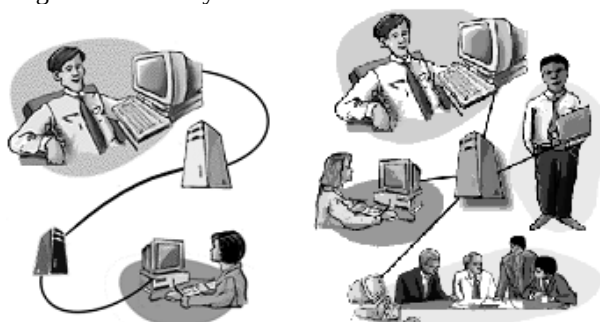


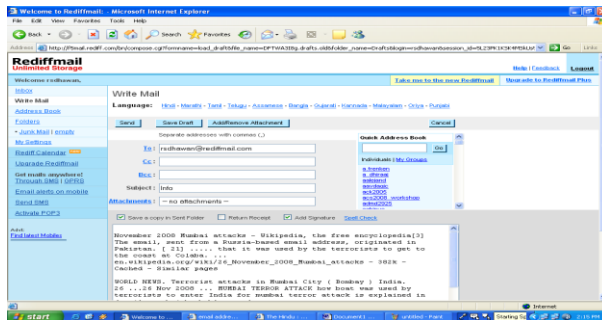
Figure 1.1 shows the working of an e-mail system [5].

In this paper an attempt has been made to trace out the practical observations (in context to their security levels) behind some of top most e-mail service providers viz. *Rediffmail.com*, *Gmail.com*, *Hotmail.com*, *Yahoo.com*, *Mail.com*, *Lycosmail.com* and *Zapakmail.com*. These service providers are having a large number of users e-mail accounts. Today, when the researchers are involved to find out a solution for faster data exchange by introducing Semantic Web, (in which data is given well-defined meaning through the use of a series of enabling client-server based Web technologies), but on the other side no one has observed the potential risks that can affect any country drastically in concern to the security of their citizens. So, this paper is designed to addresses one of the top most flaws of current e-mail service providers, which can be used by the terrorists to build up collaborative workability to share their information secretly. To avoid these kinds of threats, each and every country should take necessary steps to screen out the messages of the free e-mail service providers. Therefore, each and every e-mail account must be observed by incorporating new security standards and protocols. This paper traces some of the possibilities not to send threats e-mails form one e-mail server to another server and also to store the threats e-mails onto the same server.

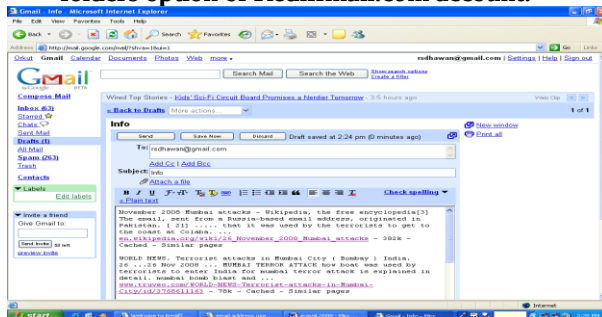
III. Specific Problem of Computer Fraud

Computer fraud is the use of computer systems to commit a fraud. In many cases, the computer has replaced manual records, and the false input document has been substituted by manipulating data held in a computer system. This manipulation does not need to be sophisticated. The jobs of people in the same office or at different locations with different user ID and passwords on the same PC means that a forged payment instruction or any other secret information may be approved simply by logging on to a computer with a stolen supervisor's logon. At the other extreme, the use of the Internet and e-mail with "sniffer" programs to capture user's passwords and credit card details can only exist because of the global explosion in the use of networked computers. Many organizations will be at risk from a specific type of computer fraud. Therefore, the investigator should be able to identify the likely culprits, the methods of manipulation, and the means of conversion or diversion of funds. There is a difference between computer fraud and computer crime. These terms are often used interchangeably with little distinction made between them although substantial differences between them exist. It has been observed that about half of reported frauds are committed by insiders who have authorized access to the computer system. When investigating cases of potential computer fraud, it is vital to establish the system of the organization's authorization procedures. Today e-mail is having the following major problems areas: (i) E-mail Security Concerns, (ii) E-mail Ownership, and (iii) Organizational Liability. E-mail has considerably changed the ability of businesses to interact swiftly, and indeed global business has embraced the e-mail system wholeheartedly. However, e-mail also gives organizations a degree of vulnerability. Aside from employees using it for personal correspondence, e-mail can be used to damage and crash organizations' networks.

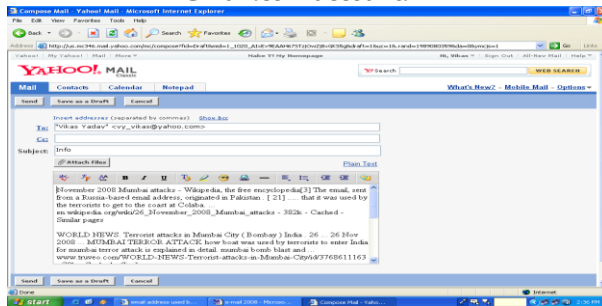
Forwarding 'Trojan Horse' programs or even simple virus hoaxes are often enough to overload a system. Using e-mail through such systems can easily be disguised or obscured the original message. Because a sender's identity can be concealed, sensitive business information can be safely forwarded to an unauthorized address. Therefore, organizations must now be concerned with the consequences of the actions of any disgruntled or rash employees. Once an e-mail message has left a company's system, it may travel through any number of foreign e-mail systems before reaching its destination. An e-mail transmission can quite easily be intercepted or compromised without the use of encryption software. Therefore, without a security-enhanced e-mail system, the receiver of an e-mail message has little assurance that the e-mail is authentic. E-mail addresses can be easily 'spoofed' or cloned by a knowledgeable user, and moreover, any e-mail that is not encrypted can be read by anyone with access to it. Even encrypted e-mail may be cracked if the encryption or key is weak enough. In fact, one of the emerging security problems concerning e-mail is the huge volume of space required to archive old messages. In some organizations, people are regularly asked to delete more e-mail messages those are no longer needed after a certain amount of time (e.g., one or two months). The following snapshots from 1 to 8 give you an idea that how embarrassing the uses of existing e-mail services.



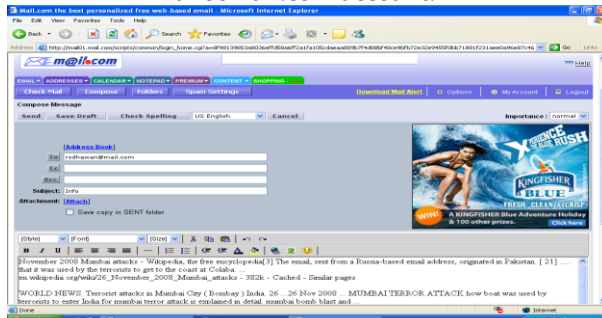
Snapshot (1) shows the saved draft message in folders option of Rediffmail.com account.



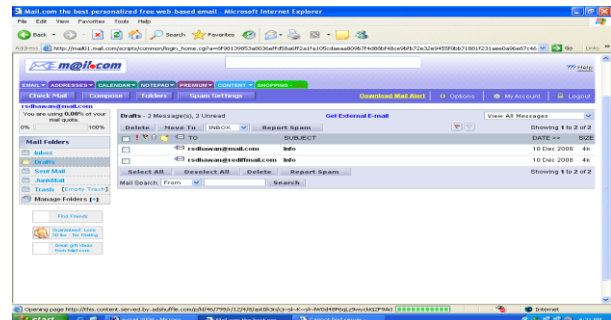
Snapshot (2) shows the saved draft message in the Gmail.com account.



Snapshot (3) shows the saved draft message in the Yahoo!mail.com account.



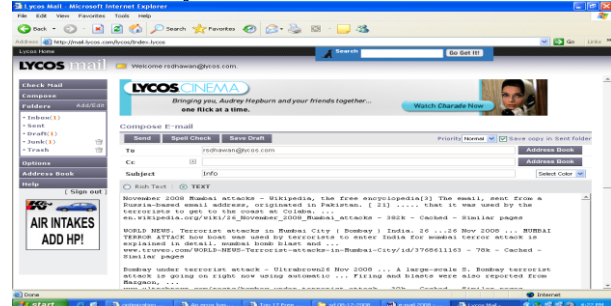
Snapshot (4) shows one of saved draft messages in the Mail.com account.



Snapshot (5) shows the saved draft messages in the Mail.com account.



Snapshot (6) shows the saved draft messages in the Lycosmail.com account.



Snapshot (7) shows one of saved draft messages in the Lycosmail.com account.



Snapshot (8) shows one of saved draft messages in the Zapakmail.com account.

These snapshots provide the view of the stored messages in the draft option available in each and every e-mail account. In these e-mail services, any individual can easily store their messages without sending to any other e-mail account. By simply insert the message in the compose message window or write option, one can directly save the message in its own existing e-mail account (let us consider you are having an e-mail account *xyz@gmail.com*; then after composing the message and without sending the same to someone, you can easily save the message by clicking the save draft option available in the Gmail account or any other corresponding account). The terrorists' group can easily acquire (and most probably they might have used) this type of existing weakness. Generally, the terrorists operate in a group and without sending the e-mail to their concerned member, they can create one e-mail account (let us say: *xyz@gmail.com*) and all the members can easily log on to the same account. Because the password is available to each and every member of that terrorist group and as a result, the terrorists can easily open the account by sitting at their own locations to carry out their functions. In this type of activity no e-mail is send from one server to another. The fact is that the information exchange is available to each and every member of that terrorist group in a unique manner. It is very much difficult to capture such type of stored information, because the message is not forwarded to any other e-mail account from which the IP address can be obtained. Moreover, they are not sending their e-mails form one server to another. Another possible area on which the terrorists are operating is that they are jumping their e-mails from one server to another, and they generally use a number of intermediate servers to send their information and messages to its final destination. For the cyber cop or for an investigating person, it is quite difficult to access these types of crimes. Therefore, the proper Internet Protocol security schemes should be maintained in the existing e-mail accounts, so that one cannot misuse the e-mail systems [6] [7].

A. Terrorism Issues for Governments

As more and more aspects of human life become dependent on computers and the Internet, the risk for terrorism grows. One of the greatest challenges and threats to businesses and governments is information warfare. Everything that is computer-dependent or linked to an organization's telecommunications is threatened. A telephone system, a city's power, water supply, a hospital's communication system and hotels are all potential targets. It is argued that individuals or groups can now use cyberspace to threaten governments, or terrorize the citizens of a country. Cracking can become terrorism when an individual cracks into a government or military maintained Website.

B. Threatening Terrorist Attacks on Mumbai

In the recent terrorist attacks in Mumbai the forensic experts have determined that an e-mail claim of responsibility for 26th November, 2008 terror attacks was first generated on a computer located in Pakistan. A group calling itself the 'Deccan Mujahideen' issued this e-mail. On the basis of the Internet Protocol (IP) addresses used to send the mail, computer specialists at India's RAW found that the Russia-based e-mail address is used to send the document, which was opened early on 26th November, 2008. A computer user based in Pakistan opened this e-mail account. Furthermore, the government sources said RAW experts have determined the e-mail address by using specialised analytical software. They also said that the document was generated using voice-recognition software, which allowed dictated text to be typed in the Devnagari font. Mumbai, a metropolis of more than 17 million, is the financial capital of India. The first terror mail sent before the Ahmedabad blast on 26th July, 2008 was from the e-mail Id: *alarbi_gujarat@yahoo.com* from IP Address: 210.211.133.200. It was traced to Kenneth Haywood's house in Navi Bombay, but he was completely innocent. The Haywood's unsecured wi-fi router was misused by terrorists to send terror mail. Because the log system was disabled, the investigating team was unable to find out the details of the Medium Access Control (MAC) address of the culprit. The second mail was sent on 31st July, 2008 from *alarbi_gujarat@yahoo.com* from IP Address: 202.160.162.179. It was traced to the Medical College at Vaghodiya in the state of Gujarat. The cops faced difficulties tracing the second mail as it was sent using a proxy server and a fake mail script. Finally, the cyber cop managed to trace the original IP address. The third mail was sent on 23rd August, 2008 from *alarbi.alhindi@gmail.com* from IP address: 121.243.206.151. It was traced to the Khalsa College at Bombay. It was again another case of an unsecured wi-fi router, which was misused to send the mail. The fourth mail was sent on 13th September, 2008 from *al_arbi_delhi@yahoo.com*, traced to Kamran power limited at Bombay. Similarly, the wi-fi router was misused to send the same mail. The major problems faced by the team were that all these mails were traced to exact IP addresses. But, the ISPs (Internet Service Providers) never responded in time. Hence, this proves that you have to be alert and follow certain practices to avoid such misuses of unsecured wi-fi routers. Therefore, a wi-fi router should never be configured as an unsecured connection as it opens the possibility for intruders to misuse the connection [8] [9]. Usually, ISPs configure the phone numbers or mobile numbers as default network key in router. In such cases, such default network keys should be changed as soon as possible. On configuring unsecured connection, enabling the logging system is must as it helps one to get MAC address of the machines, which uses the wi-fi router. A couple of more practices should also be used if the router is configured as an unsecured connection. One is installation of the packet capturing software or

wireless local area network (WLAN) analyzing software, which will ensure tracking the machines using the wi-fi router. The other one is to bind the MAC address with the router. This will only allow authenticated machines to connect with the router. One should also maintain all types of logs at least for a period of six months. Therefore, ISPs should maintain records pertaining to event log, security Log and surfing activity logs for at least six months to track and monitor the activities of any registered subscriber in order to trace out the activities within seconds. ISPs should thoroughly verify information before providing the Internet connection, because in many cyber crime cases the applications carried fake identities. Some ISPs have even installed wi-fi hotspots in public places like restaurants, coffee shops, shopping malls and hotels. One can easily buy prepaid Internet card to use the service without submitting any proof or documents. ISPs should also ask for some photo identity proof before issuing these prepaid cards. The ISPs should give access to government authorities and investigation agencies to their real time dynamic IP addresses database to easily trace the culprits. ISP and E-mail service providers should also put filtering mechanisms in their event logs for words being used like 'LeT', 'naxal', 'al arbi', 'jihad', 'mujahideen'. They must also send alerts to government agencies if someone is signing up with e-mail ids with combination of any of such key words [10].

C. Benefits to the Criminal

The virtual cyber scammer is really no different than the traditional scam artist of the real world. However, the online scam artist has many advantages over the traditional scam artist. The online scam artist can target a tremendously large audience without ever having to come into physical contact with those they plan to deceive. Furthermore, the online scam artist doesn't need much time, effort or money to reach their intended audience. It may take only fifteen minutes or so for the online scammer to compose and send a customized e-mail message to millions of people. It would take months if not more, for the traditional scam artist to accomplish such a task. This is just one reason why many scammers are making their way into cyberspace. Not only is it easy for cyber scammers to deceive others online. It is also easy for them to cover their tracks. With the use of aliases and anonymous re-mailers they can hide their identity and location. Furthermore, because the perpetrator and victim may be a far distance from one another, multiple jurisdictions may be involved; this makes the situation more difficult to deal with. There is no proper organisation to which people in the India can report all Internet based crime. There are a number of organisations that claim that they do this but in fact do not; these include NIC, Police Forces, the Home Office, and CBI etc. On December 17, 2008 in the Lok Sabha of India the two new anti-terror bills for setting up the National Investigation Agency (NIA) and amending of the Unlawful Activities (Prevention) Act have been proposed. For whatever reason, the people do not like to report that they have been scammed; many of them fear a police investigation. As is said in management consultancy: (i) If you can't see it, you can't measure it, (ii) If you can't measure it, you can't manage it, and (iii) If you can't manage it you can't control it. Without the ability to measure, with a fair degree of accuracy and robustness, the scale of the problem it is impossible to devote the resources necessary to address financial or any other crime on the Internet [13].

IV. Mechanisms for Internet Security and E-Mail Authentication

Nowadays it is very easy to forge e-mail by forging the sender identification. Anyone could send you mail pretending it came from me. Or, if you like, anyone could send Internet e-mail to your boss, looking like it came from you. Someone could send a death threat to the President of the India in your name. They say the security forces are obliged to investigate all death threats against the President, so don't do this to someone as a joke. It is also quite easy for someone to alter the content of e-mail after it has left your machine: this requires more technical skills than the simple forging of a return address, but standard Internet e-mail provides no protection against it. Commercial e-mail systems used within a company, such as Lotus Notes, have solved this problem: they authenticate the sender of all messages, and the software used to read e-mail checks this. They can also certify that e-mail has been altered since it was sent. You can get this level of security with your Internet e-mail and it doesn't cost a cent. You need to install a digital certificate on your computer. Digital signatures prove that from where the actual e-mail comes from and that it has not been altered in transit. If you establish the habit of using digital signatures for important e-mail, you will have a lot of credibility. The digital signature allows you to encrypt e-mail so that no one can read it except the recipient. PGP in particular offers this levels of encryption that will take Nobel prizes to break. There are two popular standards of digital signatures which you can use at no cost: SMIME digital certificates, and PGP. I concentrate here on the SMIME digital certificates; but both are widely accepted Internet standards. SMIME is a lot easier to set up; PGP offers better and more versatile security. The bad news is that is almost impossible to use digital certificates with Web-based e-mail like Hotmail.com, Yahooemail.com, Rediffmail.com, mail.com.

A. Digital Certificates and Keys

A digital certificate is like a passport. The certificate contains different parts, most importantly a private key and a public key. The keys work together to verify that the e-mail came from the "reply to" address. They do this by attaching a digital signature to your e-mail; the verification happens at the receiving end. The digital signature guarantees the correctness of the sender's claimed e-mail address, and guarantees that the message has not been

altered after it was sent. A digital signature is generated by your e-mail software and your private key, working together. These electronic keys are clever: your message's signature can only have been generated by your private key, and it works according to Internet standards (either SMIME or PGP). So the sending and receiving software can be different. The SMIME standard is supported by Internet Explorer/Eudora/Safari/Netscape Messenger/Mozilla/Thunderbird, and Outlook Express. With digital keys, you can also encrypt a message so that it is only readable by the recipient. Signing a message proves that from where it came from. If anyone can read the message in transit through the Internet will invalidate the signature. Encrypting makes sure the message is unreadable during transit. When you send a signed a digitally e-mail, your e-mail software sends to the recipient three things: (i) The message, (ii) Your public key, and (iii) The digital signature (a large number). If you sent a signed message to someone who has old e-mail software that does not process digital signatures, 2 and 3 appear as an attachment full of numbers and strange text. If you need a digital ID card, called a certificate. You can get this for free, from <http://www.thawte.com/>. Do this for Netscape, Internet Explorer or Opera). Another well-known provider is Verisign, but you have to pay for an ID that signs e-mail. Thawte is just as good, and free. There are a few steps to go through and the installation process may take half-an-hour before your passport number ready. The table 1 shows a list of top Web server software vendors published in a Netcraft survey in September 2008.

Vendor	Product	Web Sites Hosted	Percent
Apache	Apache	91,068,713	50.24%
Microsoft	IIS	62,364,634	34.4%
Google	GWS	10,072,687	5.56%
lighttpd	Lighttpd	3,095,928	1.71%
nginx	nginx	2,562,554	1.41%
Oversee	Oversee	1,938,953	1.07%
Others	-	10,174,366	5.61%
Total	-	181,277,835	100.00%

Table 1 shows the market structure of top most Web servers.

B. Secure E-Mail Pattern

A pattern is a logical model of technology that can be reused and leveraged across the organization. It is a blueprint that identifies components at a design or logical level (for example, a data server or an application server), and shows the roles, interactions, and relationships of components at that level. The following figure 1.2 section details the secure e-mail pattern.

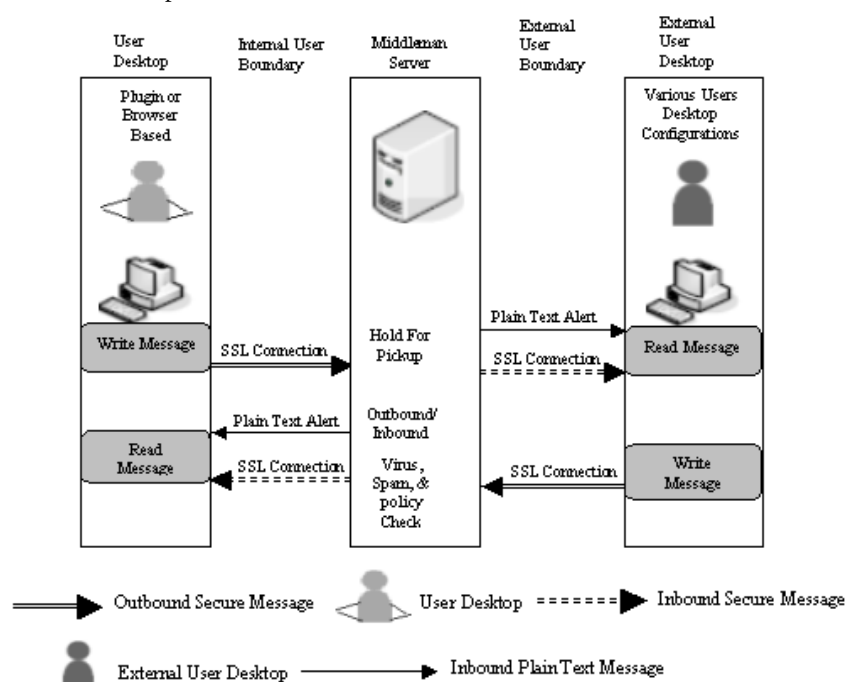


Figure 1.2 secure e-mail middleman pattern.

The secure middleman solution of figure 1.1 identifies a logical and functional combination of various secure e-mail architectures. The pattern relates following two streams: (i) Internal user message origination and receipt by an external user, and (2) external user message origination and receipt by an internal user. Outbound and

inbound virus, spam and policy checks occur at the middleman server location. The secure e-mail middleman pattern consists of the following core components: (a) Internal user desktop: It resides inside the NIH boundary and writes and reads secure e-mail messages. The desktop can either employ a plug-in or be browser-based. Outbound messages are secured inside the internal user boundary and transmitted via plain text to the e-mail gateway server. The transfer of secure or encryption status occurs at the gateway server. The secure message is then transmitted to a middleman server, which is outside of the internal user boundary, for relay to an external user recipient. Inbound message alerts are communicated via plain text alert and delivered by secure SSL connection, (b) Internal user boundary: It points from the internal user desktop. The internal user boundary will maintain control over all activities and messages remaining within its infrastructure, (c) Middleman server: It provides the environment where the message is no longer exposed to unauthorized parties during transmission. This boundary is applicable to both inbound and outbound messages. The middleman server provides the means to establish trust between internal users and external users in order to facilitate final delivery of secure messages. External users will login to a Web server to retrieve their secure e-mail via Secure Sockets Layer (SSL), (d) External user boundary: It points from external user desktop through the External user's infrastructure. Depending on the disposition of the external user (i.e., partner, non-affiliate or other), and (e) External user desktop: It resides inside the external user boundary and writes and reads secure e-mail messages. Consequently, the external user desktop can have various configurations [9] [11].

C. Deployment of Secure E-Mail Server Architecture

Today e-mail is one of the most popular applications on the Internet. It has earned this position due to its clear business and other reliable benefits. However for several years, there has been a dramatic rise in e-mail fraud and phishing. Header field in an e-mail message or the message content itself can no longer be trusted. It is easy to spoof these details, allowing attackers to create and use false identities with minimum effort. The recent substantial fraud committed at a leading European bank is one of the concrete and clear evidences in which e-mails are trusted blindly without any security checking. To overcome such threats in electronic communication, the advanced digital signature services server should be incorporated and this will act as a solution for digitally signing and verifying any type of electronic document. Therefore, the contents of the e-mails can be easily trusted and the identity of its authors, reviewers and observers can be automatically verified. So, this technology will involve: Signing outgoing e-mail attachments using digital signatures, verifying incoming signed e-mails, verifying incoming signed e-mail attachments, signing outgoing e-mails and archiving outgoing e-mails. The functions of secure e-mail advanced digital signature services server (ADSS) will support both SMTP and POP3 protocols. A future version of the product will provide extended functionality to provide e-mail archiving as well as e-mail encryption/decryption services. A typical deployment of secure e-mail server is shown below in figure 1.3, with an existing e-mail server handling e-mails as normal, but then routing these to the secure e-mail server for signing. If the matcher rules determine that the e-mail requires signing then the mailer sends a signing request message to ADSS server. The secure e-mail server can also be used to sign and archive received e-mails and attachments to provide evidence of what has been received and when it was received from external sources.

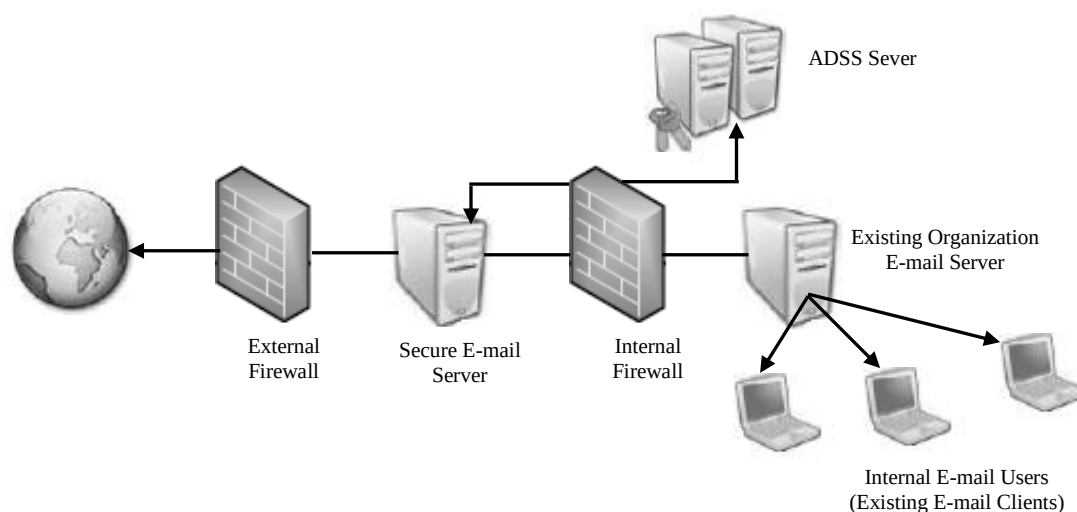


Figure 1.3 shows the deployment of ADSS server.

Finally, this secure e-mail server will filter or configure the e-mails on the basis of following options: (i) Matcher processing options: The matcher will be configured to meet organizational needs. The e-mails can be filtered based on the following: (a) Test matches within the from field, to field, cc field, bcc field, subject field, and e-mail body, (b) Attachment present and properties within the PDF documents, XML data, and other file

types, such as Office documents, and (c) Whether the e-mail is already signed digitally, and (ii) Maillet processing options: The maillet will be configured as needed to provide a range of services, e.g.: Sign an attachment (according to the attachment type or policy), verify an attachment (according to the attachment type or policy), sign the e-mail (including any attachments), verify the e-mail (including any attachments), archive the e-mail, encrypt the e-mail, decrypt the e-mail. If you are interested to verify the digital signatures then various options are possible (a) if the signature is trusted, then the e-mail can be passed to intended recipient with the results shown in the e-mail body or as an attachment, or (b) if the signatures are not trusted, then the e-mail can be forwarded to a security person for review and action. The handling of received encrypted e-mails and e-mails will be effective in the year 2009 or 2010. As mentioned above that the secure e-mail server maillet can specify the ADSS server signature profile for the attached document. Moreover, the digital signature should be placed on a page (or pages) for a particular PDF document or for any other compatible document. An example of digital signature appearance is shown below:

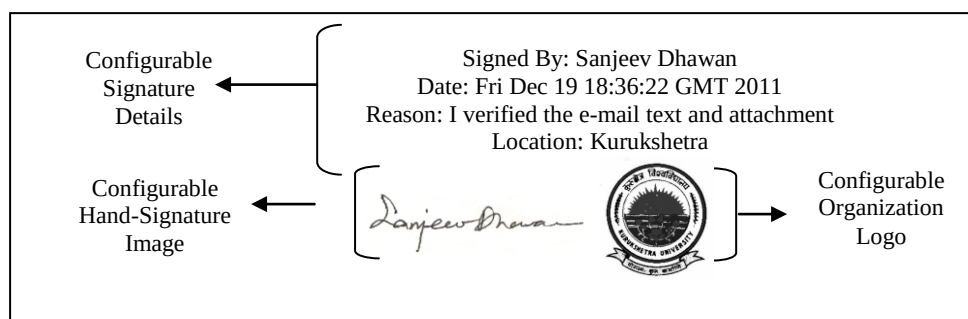


Figure 1.4 shows an example of digital signature used to send secure e-mails.

V. Conclusions and Future Predictions

There has been a tremendous growth in the Internet that has been almost exponential over the period 1992-2007, but this must slow down as the world becomes saturated with Internet access. There has been dramatic growth in computer crime on the Internet during the same period. Of the crimes committed using computers many are traditional crimes using Internet as a tool that is cheap. This can extend the reach of the criminal and allows a great degree of anonymity as well as confused jurisdictional and legal issues. Moreover, the only new crime really is Malware as this could not be propagated so easily without the Internet, but originally was distributed by floppy disk. This has been extensively used in the India and abroad in many disputes. There are legislative and other issues for funding of both implementing and managing information security by individuals as well as organisations to give the investigators to investigative computer related crimes. Finally, one should understand that we are dealing with twenty-first century crimes, and still we are committed on technology founded in the twentieth century. On the other side the majority of the cyber crimes are been investigating by a police force whose concepts were founded in the eighteenth century, and in the same cases the sentencing is usually carried out by judges who appear to be living in the seventeenth century to handing down such unjustified sentences. All of the above facts are based on laws and philosophies that are more relevant to the sixteenth century.

In near future, the Internet will be everywhere and persistent in everyday life. The house will be Internet driven - there are already Internet aware fridges in circulation. There will be continued and increasing reliance on the Internet as a major component of the critical infrastructure. Many of today's utility services will become controlled by the Internet, examples being the electric grid, gas, telephones (voice over IP), emergency services, banking and transport. The capabilities and opportunities provided by the Internet have transformed many legitimate business activities, augmenting the speed, ease, and range with which transactions can be conducted whilst also lowering many of the costs. Criminals have also discovered that the Internet can provide new opportunities for them. The dark side of the Internet not only involves fraud, theft, pervasive pornography, and paedophile rings, but also drug trafficking and criminal organizations. New technology now and in the future will create more opportunities for crime by: (i) Providing easier access to systems, premises, goods and information, (ii) Removing geographical obstacles to crime, (iii) Increasing the scale of potential rewards, and (iv) Increasing secrecy in committing crime or consuming its proceeds. The global aspect of this problem has been highlighted by the Council of Europe in its draft Convention on Cyber-crime, the first international treaty to address e-crime and IT abuse [12]. Moreover, you have to be very careful by having all the necessary precautions as secure connections in configuring your IP address, MAC address, subnet mask address, wi-fi router configuration, socket interface level, proxy connection or even IP security over geosynchronous satellite links [8] [9] [10] [11]. Otherwise, it is quite possible that someone could knock your door to arrest you on charges of sending terror e-mails and it will really disrupt you that the terror e-mails were actually sent from your IP address, which is actually acquired by someone due to your unsecured settings in the Internet options of your personal system. In summary, there are few new crimes using computers or the Internet - most of them could exist in one form or another without either the computer or the Internet. Hence each and every country should take necessary steps to

strengthen their cyberspace and to reform their law and enforcement agencies to fight against this serious issue for carrying out scams using computers or the Internet

VI. References

- [1] William Stallings, “*Data and Computer Communications*”, Prentice Hall of India (PHI), New Delhi, 2004.
- [2] Thomas A. Powell, “*The Complete Reference HTML & XHTML*”, Tata McGraw Hill (TMH) New Delhi, Fourth edition, 2005.
- [3] H. M. Deitel, P. J. Deitel & A. B. Goldberg, “*Internet & World Wide Web How to Program*”, Pearson Prentice-Hall, New Delhi, India, Third Edition 2006.
- [4] Behrouz A. Forouzan, “*Data Communications and Networking*”, Tata McGraw Hill (TMH) New Delhi, Fourth edition, 2006.
- [5] URL: http://www.learnthenet.com/english/html/20how_2.htm
- [6] Kent, S. “*Security Architecture for the Internet Protocol*”, RFC2401, November 1998.
- [7] Zhang, Y., Singh, B. “*A Multi-Layer IPSec Protocol*”. Internet Draft, April 2000.
URL: <http://www.wins.hrl.com/people/ygz/ml->
- [8] Sanjeev Dhawan, “*Analogy of Promising Wireless Technologies on Different Frequencies: Bluetooth, WiFi, and WiMAX*”, International Conference on Wireless Broadband and Ultra Wideband Communication (AusWireless-2007), Australia, Published in IEEE On-line Proceedings.
- [9] Karambir, Sanjeev Dhawan, Kulvinder Singh. “*Pervasive Computing: Security and Automisation of Personal Area Networks*”, 2nd International conference on Intelligent Systems and Networks (IISN-2007), Computational Intelligence Laboratory & MAIMT Jagadhri, Haryana, India.
- [10] URL: <http://www.itexaminer.com/>
- [11] Sanjeev Dhawan, Rakesh Kumar, Kulvinder Singh, “*Performance Prediction Metrics for Broadband Data Security over Satellite Links*”, National conference on ‘IT Research & Applications-2007’, MAIMT, Jagadhri, Haryana, India.
- [12] CECC 2002 - Council of Europe Convention on Cyber Crime.
- [13] URL: <http://legal.practitioner.com/computer-crime/index.htm>