Design and Development of E-mail Security Protocols and Forensic Tools: A Research Proposal

M. Tariq Banday
Design and Development of E-mail Security Protocols and Forensic Tools: A Research Proposal

M. Tariq Banday
Department of Electronics & Instrumentation Technology
University of Kashmir, Hazratbal, Srinagar
E-mail: sgrmmb@yahoo.com

Abstract—E-mail system is continuously being misused to carry out attacks in the cyberspace despite improvements in protocols and procedures underlying it. From spamming to cyber terrorism, e-mail system is being exploited every now and then. Owing to e-mail message’s easy proxy, often no tangible conclusion is drawn from its forensic investigation conducted to identify its sender. New threats from e-mail date spoofing, terrorist use of e-mail, multilingual e-mail messages, etc. have raised more security considerations. E-mail has become prevalent in every way and as such constant improvements in its security, operating procedures, and forensic investigation have become a critical requirement. The purpose of this paper is to discuss proposal for conducting research in the design and development of new and improved e-mail security protocols and forensic tools. The proposal proposes conduct of research in four distinct but substantially related areas of e-mail namely: security protocols, security procedures, forensic tools and legal resolutions. Besides devising improvements in the existing protocols and procedures, the study would also lead to the design of new protocols and procedures for detection of e-mail date spoofing, filtering and forensics of terrorist e-mails, and filtering of contaminated multilingual e-mail message. The proposal begins with a brief introduction to e-mail flow and security problems in it. Next, it presents a literature review of e-mail security protocols and procedures. It later portrays the significance and objectives of the proposed study. The proposal also provides proposed methodology and work plan of the study.

Keywords—Network Security, E-mail Security, E-mail Forensics, Spoofing, Spamming, Phishing, date spoofing

I. INTRODUCTION

E-Mail, a global communication infrastructure service is a highly distributed service involving several actors playing different roles for accomplishing end-to-end mail transfer. This system is an integration of several hardware components, software components, services and protocols. The integration provides interoperability between its users and among the components along the path of transfer. Several communicating entities called e-mail nodes which are essentially software units working on application layer of TCP/IP model are involved in the process of e-mail delivery. The e-mail architecture using SMTP is shown in figure 1. The architecture specifies relationship between logical components of e-mail system for creation, submission, transmission, delivery and reading processes of an e-mail message. Different nodes in this architecture are: Message/Mail User Agent (MUA), Message/Mail Store (MS), Message/Mail Submission Agent (MSA), Message/Mail Transfer Agent (MTA), Message/Mail Delivery Agent (MDA), Relays, Gateway, Other Agents, Web Server (WebServ), and Mail Server (MailServ). They perform different functions in this architecture which is beyond the scope of this paper. Since, almost all e-mails communication directly or indirectly uses SMTP, nodes working on lower layers e.g. bridges and routers representing options to send e-mail without using SMTP are not considered in this architecture. Further, proprietary nodes used for internal deliveries at sending and receiving servers are also not considered in this architecture.

There are multiple paths for transmission of e-mail message from the author to the receiver. Every path utilizes certain protocols which include SMTP, Add on protocols of SMTP, non-SMTP protocols, HTTP, MAP, and other internal protocols for node to node transfer of the message. Paths ABCDEFGHIK, ABDEFGHIJK OR ACBDEFGHIK or ACBDEFGHIJK are considered as good mail by the Sender Policy Forum (SPF). These paths will be taken in case the e-mail is send using a webserver or an e-mail application like MS Outlook. Mails following through other paths are either fully or partially non-SMTP based or uses non-standard transfer modes which are often suspected to contain viruses and spam. Various notification messages Delivery Status Notification (DSN), Message Disposition Notification (MDN), Out Of Office (OOO) messages, etc. are send to the sender by the system.

E-mail messages include transit handling envelope and trace information in the form of structured header fields which are not stripped after messages are delivered, leaving a detailed record of e-mail transactions. A comprehensive analysis of these headers can be used to map the networks traversed by messages, including information on the messaging software and patching policies of clients and gateways, etc.

II. ORIGIN OF THE PROBLEM

The primary e-mail protocols namely SMTP and ESMTP have various inherent vulnerabilities. The capability of e-mail to transmit executable files and other similar contents using Multi-Purpose Internet Mail Extensions (MIME) and e-mail access at public places where anonymous use is easy has increased its vulnerability. They lack security features for privacy of the sender, authentication of sender, integrity of e-mail message, non-repudiation by sender and consistency of e-mail envelope which permit it to be spoofed by forging its headers or by sending it anonymously. Cybercriminals misuse it for various illegitimate purposes

Available online at http://www.bepress.com/banday/11/download
DOI: 10.13140/RG.2.1.1569.2888.
including abuses like spamming, phishing, cyber bullying, child pornography, sexual harassment, racial vilification, etc. Internet infrastructure crimes through Denial of Services and Directory Harvesting Attacks are also being carried out using e-mail. Viruses, worms, Trojan horses, hoaxes, and other malicious programs with intent to spread them over the Internet are also transmitted through e-mail. These injudicious uses of e-mail cause many technological problems like misuse of storage space, wastage of computational resources, and network conjunction besides creating severe legal issues. Firewalls, anti-viruses, anti-spam filters, scanners and filters prevent e-mail abuses but are insufficient to make e-mail communications completely secure. E-mail may contain a forged date which may be ahead or before the actual date it was sent thus spoofed in date. Such e-mails can cause manifold of problems including confusions, wastage of time of their recipient, threats to time scheduled activities like e-commerce, e-tendering, e-evaluation, e-transactions, etc. Multilingual e-mail or non-English e-mail messages cannot be scanned by the current filters and as such there is a threat that such messages can include spam or malicious content. Cyber forensic e-mail analysis is employed to collect credible evidence to bring criminals to justice. E-mail forensics refers to studying the source and content of e-mail message as evidence, identifying the actual sender, recipient and date and time it was sent, etc. However, often no tangible conclusion is drawn from its forensic investigation to identify its sender owing to its easy proxy.

III. INTERDISCIPLINARY RELEVANCE

With the advent of World Wide Web, e-mail has emerged as one of the most widely used tool for communication over the Internet. The e-mail traffic on the Internet has increased manifold due to its wide array of applications. It is used for multimedia, e-commerce and e-governance purposes. Further, it is also used for carrying out financial transactions and distribution of documents and archives of diverse natures. The domain of applications of e-mail is not limited to any particular discipline or branch. It is extensively being used in private, corporate, government, business, academic and other sectors.

IV. LITERATURE REVIEW

A. International Status

The ability to provide privacy of the sender, authentication of sender, integrity of e-mail message, non-repudiation by sender and consistency of e-mail envelope and protection against mail forgery is secure messaging [1]. Various add-on protocols that work on top of SMTP aim to add secure messaging features to SMTP. Several anti-spam procedures have been developed to automatically classify incoming e-mail messages into spam or legitimate classes for preventing mail forgery. Further, various approaches and software tools are being used to investigate e-mail messages for their forensic investigations.

E-mail Security Protocols

End to end symmetric or asymmetric cryptographic schemes or encrypted secure channel between the sender and the receiver during SMTP transactions are used by security protocols that add privacy to SMTP. Anti-spoofing standards that either use IP addresses or digital signatures to validate sending domain have also been developed that help an e-mail system at the receiving end to detect the spoofing of addresses and as such enables it to decide how to handle
incoming e-mail. Following figure lists various e-mail security protocols following a short description of each.

Secure Socket Layer (SSL) [2] creates a secure socket connection between the sending and receiving MTAs to encrypt SMTP transactions. Secure SMTP over Transport Layer Security (TLS) RFC 2487 provides confidentiality and data integrity through encryption over the Transport Layer between two or more servers. It is made up of TLS Record and TLS handshake protocols that create a secure channel for e-mail traffic between the sending and receiving servers. Privacy-Enhanced Mail (PEM) [3] is an encryption technique devised by Internet Architecture Board but it lacks flexibility as it requires every participating e-mail entity to trust a single Certification Authority. Pretty Good Privacy (PGP) [4], [5] is a public-key encryption technique to protect E-mail and data files with no secure channels needed for prior exchange of keys. It combines the convenience of the Rivest-Shamir-Adleman (RSA) public key cryptosystem with the speed of conventional cryptography, message digests for digital signatures, data compression before encryption, good ergonomic design, and sophisticated key management. GNU Privacy Guard (GPG) [6] is an open standard of PGP like OpenPG. Secure Multi-purpose Internet Mail Extensions (S/MIME) [7], [8] adds cryptographic security to e-mails through MIME encapsulation using Digital Signatures. Certified Server Validation (CSV) [9] validates the IP address of SMTP client and determines whether Domain Name administrator has authorized the client to send mail or not. It also specifies a mechanism for querying an assessment service about the client’s Domain Name. Bounce Address Tag Validation (BATV) [10] addresses bounces which are misdirected handling notices by permitting the sender to digitally sign ‘MailForm’ bounce address. Lightweight MTA Authentication Protocol (LMAP) [11] is a DNS-based approach to determine whether a mail is from clamed address or not. Reverse Mail eXchange (RMX) protocol [12] defines an envelope oriented scheme for domain validation through reverse lookup into DNS server for RMX record of the sending domain for verification of sending MTAs permission to send mail. Designated Mailer Protocol (DMP) [13] is similar to RMX but uses a DMP record which is a TXT record compatible with DNS. RMX and SPF/SenderID and DMP are reverse lookup schemes similar to one another in many ways. Sender Policy Framework also called Sender Permitted Form (SPF) [14] is a DNS based anti-forgery method. It queries the DNS with the domain name specified in the ‘MailFrom’ command and determines whether the IP address of the previous hop-MTA is registered under that name. SenderID also called Sender ID Framework (SIFD) [15] checks the DNS lookups against ‘from’ name fileid if no from field is present in the envelope. DomainKeys Identified Mail (DKIM) [16] is a Domain level encryption based e-mail signings protocol that adds authentication, authenticity and integrity to e-mail.

![Figure 2: E-mail Security Protocols](image)

Anti-Spam Procedures

Lack of message integrity within SMTP permits e-mail forgery through distribution of spam and phishing e-mails.

Anti-spam procedures aim to detect e-mail forgery and are use diverse methods for detection. These include methods based on filtering, change of process of e-mail transmission, and anti-spam protocols. It is beyond the scope to discuss...
methods in each group in this write up. However, a typical classification of anti-spam procedures is given in figure 3.

Filters classify incoming e-mail messages in at least two classes; one class with normal e-mails and the other with spam, phishing and dangerously infected e-mails. They provide security against mail forgery through mail classification. They apply learning and non-learning algorithms at servers, routers [17] and destination clients. James Carpinter and Ray Hunt [18] and Enrico Blanzieri and Anton Bryl [19] have performed a comprehensive literature survey of anti-spam procedures. Anti-spam methods like zmail [20] differential e-mail delivery [21] proof of work [22] and CAPTCHA [23] suggesting change of existing e-mail protocols, propose inclusion of additional steps in e-mail sending process. Rate Throttling [24] also called shaped or economic filtering, Greylisting [25], Behaviour Analysis [26] and information hiding [27] also called Identity Hoping [28] or Address Obscuring Techniques (AOTs) [29] suggests a local change in the incoming or outgoing or transmission process of the e-mail message.

E-mail Forensic Investigation

E-mail forensics refers to the study of source and content of e-mail as evidence to identify the actual sender and recipient of a message, data/time of transmission, detailed record of e-mail transaction, intent of the sender, etc. This study involves investigation of metadata, keyword searching, port scanning, etc. for authorship attribution and identification of e-mails scams. Various approaches that are used for e-mail forensic are described in [30] include header analysis, bait tactics, server investigations, and network device investigation. Besides mandatory headers, custom and MIME headers appearing in the body of the message are also analyzed for sender mailer fingerprints and software embedded identifiers.

Various software tools have been developed to assist e-mail forensic investigation. These include eMailTrackerPro [31], EmailTracer [32], Adcomplain [33], Aid4Mail Forensic [34], AbusePipe [35], AccessData’s FTK [36], EnCase Forensic [37], FINALEMAIL [38], Sawmill-GroupWise [39], Forensics Investigation Toolkit (FIT) [40], Paraben (Network) E-mail Examiner [41], etc. These analyse headers of e-mail messages to detect the IP address of the originating machine. These tools often have abuse reporting features, e-mail classification option, and support multiple encryption techniques like Credant, SafeBoot, Utimaco, EFS, PGP, Guardian Edge, Sophos Enterprise and S/MIME. Commonly supported e-mail types are: Lotus Notes NSF, Outlook PST/OST, Exchange EDB, Outlook Express DBX, Eudora, EML (Microsoft Internet Mail, Earthlink, Thunderbird, Quickmail, etc.), Netscape, AOL and RFC 833.

B. National Status

Given its global and multidisciplinary nature, researchers the world over including India are actively involved in the design and development of e-mail security protocols, forensic tools and legislative measures but no e-mail security protocol to India specific requirements has been made. Further, very little work has been done on the National level to develop e-mail forensic tools and no separate legislation in India exists to deal with the problems of spam.

EmailTracer [32] is an Indian effort in cyber forensics by the Resource Centre for Cyber Forensics (RCCF) which is a premier centre for cyber forensics in India. It develops cyber forensic tools based on the requirements of law enforcement agencies. Among several other digital forensic tools, it has developed an e-mail tracer tool named EmailTracer. This tool traces the originating IP address and other details from e-mail header, generates detailed HTML report of email header analysis, finds the city level details of the sender, plots route traced by the mail and displays the originating geographic location of the e-mail. Besides, it has keyword searching facility on e-mail content including attachment for its classification.

Governments have introduced anti-spam legislations to protect consumers and businesses to ensure confidence in online commerce and protect interests of stakeholders. These legislations have introduced different parameters. There is no separate legislation in India to deal with the problem of spam. Some researchers [42] have discussed possible parameters which an anti-spam legislation in India, as and when enacted. These parameters have been analyzed in the light of trans-border legislative developments. However, legislation alone cannot prevent spam. It is to be combined with technological measures.

V. Significance of the Study

Illegitimate activities through e-mail system are carried out by Cybercriminals who remain underground to evade any possible legal action against them. These misuses include:

- Abuses like spamming, phishing, sexual harassment, cyber bullying, racial vilification, child pornography, etc.
- Transmission of viruses, hoaxes, worms, Trojan horses, and other similar malicious programs with intent to spread them,
- Internet infrastructure crimes through Denial of Services (DoS) and Directory Harvesting Attacks.

Technological problems including misuse of storage space, wastage of computational resources, and network conjunction besides various severe legal issues are caused due to these misuses. A highly technical spammer or phisher may also evade packet filters and spoof the source IP address of their packets to indicate that the message is from a trusted domain [43]. Senders can lie about their true identities in various ways by using or misusing different techniques that include: Spoofering [44], Unauthorized Networks: [45], Open Mail Relays [46], Annomizers or re-mailers [47], Open Proxy [48], SSH Tunnel or Port-Redirector [49], Botnets [50], and Untraceable Internet Connections [51, 52]. E-mail provides the perfect vehicles for terror groups to communicate with each other, to spread their message, to raise money and to launch cyber-attacks. In some cases it is possible to intercept the communication or reach the attacker or the place where from the crime has been committed but given to the fact that e-mail messages can be spoofed or encrypted it may not always possible. E-mail has
remained the most favorite communication tool for terror
groups to claim responsibility for bombing or creating other
unlawful activities. Investigation of the e-mail message
calming terror responsibility has not always been able to
identify the attacker. Highly techno terror groups through
spoofed e-mail messages may not only confuse a country’s
defense or investigating teams but can also waste time and
resources of the country.

Protocols offering security [53] and anti-spam filters
capable to perform mail categorization have been developed
to secure e-mail service against sender-spoofing. However,
the use of some of these protocols is very limited due to
limited technical skill of users or unawareness about their
existence [54], besides, their use has not been made
mandatory. E-mail forensic investigation is carried out by
using various techniques and software tools, however, they
may prove to be ineffective due to lack of co-operation
between different service providers. Also, spammers
constantly change spam sending techniques and its structure
to evade security procedures and protocols, leaving scope for
e-mail forgery and e-mail crime raising the need for e-mail
forensic analysis. Further, new threats from e-mail date
spoofing, terrorist use of e-mail, multilingual e-mail
messages, etc. have raised new security considerations
calling for research for designing of new and improved e-
mail security protocols and forensic tools. Furthermore,
inventions of new means and changing tactics of the
cybercriminals make e-mail security and forensics an active
area of research.

VI. OBJECTIVES OF THE STUDY

The objectives of the study are given hereunder:

1) To identify limitations of the e-mail security
protocols, analyze and evaluate their effectiveness in e-mail
servers.

2) To suggest methods to improve efficiency of e-mail
servers in detecting spoofed e-mails from domains that do
not follow any standard anti-spoofing protocol.

3) To design a new e-mail security protocol for
detection and stopping sender spoofing, and date spoofing.

4) To analyze exiting e-mail security procedures and
evaluate their effectiveness and limitations.

5) To develop new security procedures for filtering
spam and threat e-mails from legitimate e-mails.

6) To devise a spam filter capable to filter multilingual
e-mail messages.

7) To carry out detailed header analysis of various
multiple tactic spoofed e-mail messages and to explore
various possibilities for detection of spoofed headers and
identification of their originators.

8) To analyze difficulties faced by investigators while
forensic investigation of an e-mail message and work
towards their solutions.

9) To analyze e-mail forensic software tools in terms of
their efficiency and to develop new forensic tool to extract
credible evidences from e-mail messages.

10) To analyze techno-legal solutions to the problem of
spam and phishing followed in various countries and
suggest techno-legal solutions for India.

VII. PROPOSED METHODOLOGY

The proposed project involves research and development
in four distinct but substantially related areas of e-mail,
namely a) security protocols, b) security procedures, c)
forensic tools and d) legislative measures. Each area involves
literature survey followed by analysis of existing techniques
under varying parameters to determine their efficiency,
effectiveness and usability. The infrastructural facilities
required to execute the proposed project would be created
along with literature survey and analysis of existing
techniques. Research towards development of algorithms for
new e-mail security protocols and procedures and
improvement in the existing ones shall be carried out after
infrastructural facilities have been created in the department.
The developed algorithms shall be designed and
implemented to evaluate their performance. Analysis of
existing e-mail forensic tools shall be carried out in terms of
techniques used by each to determine their effectiveness.
Research towards design and implementation of new e-mail
forensic tool that employs the use of new and improved
security techniques developed in the proposed project shall
be undertaken. The developed protocols, procedures and
forensic tool shall be thoroughly analyzed under varying
parameters and conditions to ascertain their limitations.
Improvements in the developed techniques shall be
undertaken to eliminate the limitations discovered through
analysis. Techno-legal analysis of anti-spam legislatures of
various developed countries shall be carried out to determine
most optimum measures that can be followed in India to
cater to the problems of spam.

VIII. PLAN OF WORK

The project can be taken up for a tenure of three years.
The proposed plan of work is given in table 1 below:

<table>
<thead>
<tr>
<th>Year</th>
<th>Plan of Work</th>
</tr>
</thead>
<tbody>
<tr>
<td>1st Year</td>
<td>Literature survey of e-mail security protocols, anti-spam protocols and</td>
</tr>
<tr>
<td></td>
<td>forensic techniques and tools.</td>
</tr>
<tr>
<td></td>
<td>Procurement of necessary software &amp; hardware tools.</td>
</tr>
<tr>
<td></td>
<td>Creation of Infrastructure facilities in terms of development of Wi-Fi and</td>
</tr>
<tr>
<td></td>
<td>wired network security and digital forensics laboratories.</td>
</tr>
<tr>
<td></td>
<td>Procurement and installation of SSL and Digital Certificates on</td>
</tr>
<tr>
<td></td>
<td>experimental e-mail accounts and websites.</td>
</tr>
<tr>
<td>1st Year</td>
<td>Development of new algorithms, protocols, and procedures for specific</td>
</tr>
<tr>
<td></td>
<td>segments of e-mail security.</td>
</tr>
<tr>
<td>2nd Year</td>
<td>Design, implementation and evaluation of the developed algorithms, protocols,</td>
</tr>
<tr>
<td></td>
<td>and procedures.</td>
</tr>
<tr>
<td>2nd Year</td>
<td>Development of new automated e-mail forensic software tool, Design,</td>
</tr>
<tr>
<td></td>
<td>implementation and evaluation of the developed e-mail forensic tool.</td>
</tr>
<tr>
<td>3rd Year</td>
<td>Refining the developed e-mail security algorithm and forensic tool in terms</td>
</tr>
<tr>
<td></td>
<td>of efficiency, user friendliness and usability.</td>
</tr>
</tbody>
</table>

Table 1: Proposed plan of work

IX. COLLABRATIONS

To meet the objectives, for some segments of the project
that pertain to legal issues, active collaboration with law
experts teaching and/or practicing cyber laws is mandatory.
The collaborative efforts would highly facilitate analysis of techno-legal measures adopted in various countries and subsequently suggesting measures for India to regulate spam and other cybercrimes. The collaboration would also help analyze IT Act and proposed cyber security policy of India and to compare and contrast them with those of various other countries.

X. INFRASTRUCTURAL REQUIREMENTS

Apart from some basic hardware and software tools, the study and design would require network security and digital forensic laboratories. These laboratories must have various vital software and hardware tools to carry out the research on the topic. These include a Blade server, high performance server, manageable routers, wireless access points, firewall security appliance, voice bundle router desktop, different cables, NetSim server, hardcopy, shadow, forensic duplicator, Forensic Toolkit, EnCase forensic software, Device seizure software, password recovery toolkit, network e-mail examiner besides various other e-mail detective software’s. Online subscription of few journals and periodicals besides Proxy less Internet access for IP level investigations will be required throughout the study. Further, SSL Certificate, Digital Certificate, Domain Name, Hosting Service, and E-mail accounts, are required to work with security protocols.

CONCLUSION

Cybercriminals hide themselves behind proxy or ammonizers or by using any other technique to evade e-mail security protocols and procedures. The forensic investigation of e-mail does not always result in a concrete decision. New threats from e-mail date spoofing, terrorist use of e-mail, multilingual e-mail messages, etc. have raised more security considerations. Thus, calls for research to design novel and improved e-mail security protocols and procedures and improved forensic tools are not only imperative but also challenging. Further, inventions of new means and changing tactics of the cybercriminals and its impact on cyber security makes e-mail security and forensics an active area of research.

REFERENCES


Available online at http://www.bepress.com/banday/11/download
DOI: 10.13140/RG.2.1.1569.2888.


EmailTracer, http://www.cyberforensics.in.


FINALeMAIL, http://finaldata2.com


Forensics Investigation Toolkit (FIT), http://www.edecision4u.com/FIT.html


