EFFECTIVENESS AND LIMITATIONS OF E-MAIL SECURITY PROTOCOLS

M. Tariq Banday

P. G. Department of Electronics and Instrumentation Technology
University of Kashmir, Srinagar - 6, India
sgrmtb@yahoo.com

ABSTRACT

Simple Mail Transport Protocol is the most widely adopted protocol for e-mail delivery. However, it lacks security features for privacy, authentication of sending party, integrity of e-mail message, non-repudiation and consistency of e-mail envelope. To make e-mail communication secure and private, e-mail servers incorporate one or more security features using add-on security protocols. The add-on security protocols provide a reasonable security but have several limitations. This paper discusses limitations of e-mail security protocols, analyzes and evaluates their effectiveness in e-mail servers. It also proposes methods to improve efficiency of e-mail servers in detecting spoofed e-mails from domains that do not follow any standard anti-spoofing protocol. Further, it presents results of studies carried out to appraise e-mail user practice; knowledge of security protocols and their confidence in e-mail system.

KEYWORDS

E-mail Security, SMTP Security Issues, Sender spoofing, S/MIME, SPF, DKIM, SenderID, E-mail Security Protocols

1. INTRODUCTION

Simple Mail Transport Protocol (SMTP) [1] was originally designed for a smaller community of users which was assumed to be well behaved and trust worthy. As such no heed was paid towards incorporating security protocols in it. But with its growth, this trust was breached, owing to lack of adequate security mechanism in it. Several technological and policy changes were made to SMTP servers to make e-mail system secure without creating incompatibility between older and newer systems. These include SMTP session refusal to unauthorized servers through IP address verification, refusal of e-mail relaying, restriction on use of certain SMTP commands like EXPN, verification of e-mail envelope and headers, limiting the size of e-mail message and filtering. These security features were updated, upgraded and some of them have been standardized. These security features fall under two broader categories namely technological and legal solutions. Technological solutions include solutions that suggest process or protocol change or use of one or more add-on security protocol or use of some machine learning or non-machine learning filtering technique. In some parts of the globe specific legislative measures are in vogue to deal with legal issues arising from security lacunas of e-mail systems. A detailed description of technological and legislative measures is given in [2]. Add-on security protocols are widely adopted measures to provide security in e-mail systems. A review of prominent add-on security protocols along with their working has been carried out in [3]. These protocols either use cryptographic techniques or encryption or some domain validation standards. A detailed survey of e-mail servers in dealing with problem of date spoofing and apprizing e-mail user behaviour with regard to date spoofing has been carried out in [4]. However, this study has not carried out study pertaining to sender spoofing and treatment of such e-mail messages by e-mail servers.

The remaining paper is organized as follows: Section 2 introduces e-mail security and enlists security issues of SMTP. Section 3 describes limitations of the e-mail security protocols.

Section 4 analyzes e-mail servers of some Commercial E-mail Service Providers. It also presents possible approaches to improve their efficiency. Section 5 appraises e-mail user practices, their knowledge of security protocols and also evaluates their confidence in e-mail system through a study which is followed by conclusion.

2. SECURITY ISSUES IN SMTP

Security in Information and Communication Technology is defined as adequate protection of information against unauthorized disclosure, unauthorized modification and unauthorized withholding [5]. It has a close relationship with privacy as insecure information cannot ensure users privacy. In E-mail messaging, security can be defined as the ability of the system to provide i) privacy, ii) sender authentication, iii) message integrity, iv) non-repudiation, and v) consistency [6]. These parameters are briefly described below:

i. Privacy guarantees confidentiality of a message transmitted over open medium which otherwise can be intercepted or altered.
ii. Sender authentication is the verification of the claimed identity of the sender.
iii. Message integrity refers to policies that ensure security against mail forgery which includes policies to stop transmission of spam e-mails; phishing e-mails and e-mails containing viruses, etc.
iv. Non-repudiation means non-denial by sender; an e-mail sender should not be able to disown an e-mail sent by him due to weak security mechanism.
v. Consistency refers to uniformity of both header and body of the message from source to the destination.

E-mail system consists of a number of hardware and software components that follow some defined standards. These standards also include standards for message addressing and formatting and a number of related protocols. Simple Mail Transport Protocol [1] is the primary and the most widely adopted protocol for e-mail delivery. It lacks security features for privacy and authentication of sending party. E-mail in plain text passes from sender to recipient through many intermediaries like routers, and mail servers. It is thus, inherently vulnerable to both physical and virtual eavesdropping as malicious attackers who gain access to these intermediaries can read e-mails. Further, E-mail Service Providers (ESPs) have capabilities to store copies of e-mail messages even when these are deleted by the users from their mailboxes [6].

It has no mechanism to authenticate the sender or other trusted fields in any way. It does not verify or validate the senders e-mail address or other header fields. As such senders can lie about their true identities [7], date and time of creation of message, return address and other details which result in security challenges of different types.

It has no security feature for message integrity and as such it is possible to send spam and phishing e-mails. Spam e-mails cause several problems like network conjunction, misuse of storage space and computational resources, loss of work productivity and annoyance to users, legal issues as a result of pornographic advertisements and other objectionable material, financial losses through phishing and other related attacks like spread of viruses, worms and Trojan Horses, and Denial of Services and Directory Harvesting attacks [8].

It also does not provide any protocol for achieving non-repudiation that would not make possible for sender to disown his e-mails. The consistency of the header is also not ensured. Transporting MTAs could make changes to the message that may be anecdotally attributed to

the sender [9]. Other protocols used with SMTP that include protocols like POP3 [10] for message pull and Secure Hyper Text Transfer Protocol for Webmail are also not foolproof against network sniffers and man-in-the middle attacks.

3. LIMITATIONS OF E-MAIL SECURITY PROTOCOLS

SMTP servers incorporate one or more security features using several add-on e-mail security protocols to make communications secure and private. These protocols use diverse technological means like encryption, symmetric and asymmetric cryptography and domain validation through IP address verification and digital signatures. Several varieties of anti-spam filter have been developed to ensure message integrity. The add-on security protocols provide a reasonable security but have several limitations. This section discusses chief security protocols and their limitations.

Secure Socket Layer (SSL) [11] and Secure SMTP over TLS [12] are encryption based methods that respectively create encrypted secure channel between the sending and receiving MTA's at sockets and transport layers. They are simple methods to obtain e-mail privacy without efforts of the end user but Secure SMTP over TLS guards only the path between client and server and not the endpoints that are authenticated by certifying authorities and not the Domain Name System (DNS) [13].

Cryptography based encryption techniques for e-mail security includes Privacy-Enhanced Mail (PEM) [14], Pretty Good Privacy (PGP) [15], GNU Privacy Guard (GPG) [16] and Secure Multi-purpose Internet Mail Extensions (S/MIME) [17, 18]. PEM lacks flexibility and more seriously requires trusting a single Certificate Authority (CA) infrastructure which is the reason for its almost negligible adoption [19]. PGP and GPG are PKI based scheme with sporadic adoption and as such are limited to a smaller user community.

S/MIME is a protocol for adding cryptographic security services to e-mails. S/MIME requires no change in the sending and receiving MTAs or the e-mail transmission process because this functionality can be added to the client software installed at sending and receiving clients. In its basic form it provides sender authentication, non-repudiation of sender, message integrity and message security using encryption and digital signatures. The basic security services permit to send and receive signed messages, encrypted messages and signed and encrypted messages. It is a widely used protocol than any other security protocol but it has several deficiencies. A recipient can forward an e-mail along with digital signature to third party without the consent of sender thus posing a security threat to the sender's privacy [20]. Another limitation with S/MIME is its inability to guarantee non-repudiation through keys in situations where keys are lost [21]. Digital signatures are aimed at message integrity against advertisers who modify e-mail in transit and counterfeit forged sender addresses but are a week line of defense against phishers and spammers [21] who can cleverly craft e-mail addresses to trick recipients in believing the source. To use S/MIME both sender and receiver need to purchase digital signatures from authorized certification authorities. S/MIME imposes mobility restrictions as users need to install certificates on clients from where they want to access e-mail and it cannot be used effectively through Webmail programs as these do not have S/MIME capabilities. It requires Mail Access and Retrieval protocols such as POP3 and IMAP which are not offered with free e-mail accounts by most ESPs. Since S/MIME besides offering basic security services also offers different optional services which may differ for each implementation of S/MIME, therefore it may not be interoperable and provide reasonable assurance to users. The level of security provided by S/MIME depends upon the robustness of its underlying cryptographic algorithms and PKI profile which may vary in implementations. S/MIME and PGP do not ordinarily sign the message headers making it possible to be modified at various intermediaries. S/MIME and PGP do not necessarily involve domain owners, thus permitting retiring users of a

company to continue to use their signatures [22]. Other issues pertaining to PKI based encryption protocols are concerns of key distribution [21], key renewal and key management [23] and issues pertaining to correspondence with unfamiliar correspondents [24]. Further, PKI based encryption security protocols require a compatible mail systems [25] and highly skilled users.

IP address based anti-spoofing standards include Certified Server Validation (CSV) [26], Bounce Address Tag Validation (BATV) [27], Lightweight MTA Authentication Protocol (LMAP) [28] Sender Policy Framework also called Sender Permitted Form (SPF) [29] and SenderID [30] also called Sender ID Framework (SIDF). CSV only covers the current client/server SMTP hop as the client specifies operator's Domain Name in the EHLO command. CSV, BAVT and LMAP have severe limitations in comparison to other DNS based anti-spoofing techniques namely SPF and SenderID.

SPF and SenderID are DNS based anti-forgery measures that allow receiving MTAs to verify that the message is coming from an expected IP address. SPF is aimed to validate that a message was sent by the sender domain specified in the SMTP 'MailFrom' command. Domain validation is performed during the SMTP transactions before the delivery of the complete message. In SPF, the receiving server queries the DNS server 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. SPF theoretically requires every intermediate MTA to have a SPF record in the DNS but this can be simplified to boundary MTAs only.SPF is a combination of Reverse Mail Exchange (RMX) and Designated Mailer Protocol (DMP). SenderID like SPF and has combined SPF and Microsoft's CallerID technologies. SenderID differs from SPF in the manner that the former operates at message header layer and the latter operates at the message envelope layer. SenderID uses different SPF record format than SPF. In SenderID the 'From' header field is validated against that specified in SPF record queried from DNS server. Although deployment and usage of SPF/SenderID is quite simple but it has significant administrative problems with redirected traffic such as when going through a third party forwarding service. The role of 'MailFrom' command is to specify the Notification Handler address which might be different from other origination information making registration of all of the MTAs in the path problematic. In some applications it may be desired to specify different return address but cannot because SPF/SenderID binds the sender's entity in the 'Return-path' field. Further, SPF cannot stop phishing attacks having fake content from outbound e-mail MTAs which are having correct return address. Further, neither SPF nor SenderID guarantee message privacy or integrity.

Domain Key Identified Mail (DKIM) [31] is a cryptography-based e-mail signing protocol meant to add e-mail authentication, authorization and integrity at domain level to SMTP. It combines two techniques namely Yahoo supported DomainKeys and the Cisco supported Identified Internet Mail. DKIM sending domains can have individual policies with respect to requirement for DKIM signing, requiring it to provide authentication for all, some or no e-mails. In DKIM, the sending domain generates public and private key pairs for each sending MTA and publishes the public keys and policies to the DNS under a "_domainkey." namespace. The receiving MTA verifies DKIM signature by checking it against the sending MTAs public key made available through DNS. It is quite possible that DKIM signature is verified by the intermediate domains before forwarding it to the next hop. DKIM also allows 3rd party to sign messages on behalf of the sending organizations as long as the 3rd party has necessary private keys making it possible to aggregate a number of different domains. An optional DKIM feature named DKIM Sender Signing Practice (SSP) [32] lets receiving domains know policies used by sending domains in signing e-mails using DKIM by making sending domains publish this policy. Lightweight E-mail Signatures (LES) [33] proposes use of identity based signatures to specify internal methods that can distinguish one user from the other within a particular DKIM

domain so as to detect identify spoofing within a domain. DKIM does not provide encryption but still can be used at top of those which provide it like S/MIME. DKIM also does not guarantee protection against mail damage which may result in case any intermediate mail gateway changes either envelope or body of the e-mail during transit. DKIM although a promising technique for anti-spoofing requires e-mail server software/hardware upgrades, adds overhead due to cryptographic processing and adoption at both sending and receiving domains. Sending MTAs must have some internal mechanism to distinguish one e-mail user form other on the same domain. E-mail policies are globally visible through DNS server in both DKIM and SPF/SIDF but their wider adoption could create an additional load on the DNS server.

Currently SPF, DKIM and S/MIME are dominant and standardized e-mail security protocols. A comparison of different features provided by them is given in table 1.

Table 1. Comparison of E-mail Security Protocols

Feature	**SPF/ SenderID**	**S/MIME**	**DKIM**
Standardization	SPF: RFC 4408 (Experimental) SenderID:RFC5518 (Proposed Standard)	RFC 3851 (Proposed Standard)	RFC 4871 (Proposed Standard)
Secure against Eavesdropping	No	Yes	No
Transparent to User	Yes	No	Yes
Message Readable to ESP	Yes	No	Yes
Message Privacy	No	Yes	No
Authentication Type	Domain	Individual	Domain
Certificate Type	Not Required	X.509	No Specific
Message Integrity	No	Yes	Yes
Webmail Access	Yes	Limited	Yes
Non-repudiation	No	Yes	No
Overloads at User/client level	No	Yes	No
Additional Costs	No Additional	Higher	No additional
E-mail Mobility	Yes	Limited	Yes

The comparative statement if different features if e-mail security protocols presented above in a tabular form reveals that no single add on security protocol to SMTP provides all of the required security features. SPF/SenderID and DKIM are not secure against eavesdropping, do not guarantee message privacy and non-repudiation but do not add overheads to the users. Further, they are transparent to users and add no additional cost to users. On the other hand S/MIME can ensure security against eavesdropping ensures privacy and integrity of message but is not transparent to user and also adds additional costs to users.

There are several groups of anti-spam procedures that perform filtering at servers or clients. Filtering does not require any change in the existing e-mail system. There are many limitations of filtering procedures that include sneaking, format and language dependence, passive approach, predictable behavior and various classification errors especially false positive and

false negative. The methods suggesting complete or partial change in the e-mail protocols pose compatibility challenges and as such their use is restrained.

4. EVALUATING AND IMPROVING EFFICIENCY OF E-MAIL SERVERS

Availability of free e-mail accounts with or without POP3 and IMAP access through some commercial e-mail service providers has increased the popularity of this very Internet application. However, this has also increased the security risks as spammers and hackers try to reach more and more people through this application for their illicit financial gains. Several anti-spoofing standards like SenderID/SPF and DKIM successfully validate sending domains. They are not, however, strictly being used in all e-mail servers. Spoofed e-mails from domains that do not follow any standardized anti-spoofing standard are not detected by receiving e-mail servers.

4.1. Feature Evaluation of E-mail Servers

The current authors analyzed e-mail servers of some commercial ESPs to evaluate their features and effectiveness of security protocols installed on them against sender spoofing. Test e-mail accounts were created on these servers and the features offered by each were analyzed.

It has been found that most of the Webmail programs under study use security protocols and have features for header analysis, custom signature, vocational response, custom filter, spam guard with custom blacklisting. But some of them lacked basic features like detailed header analysis and custom message filtering. A few ESPs provide secure HTTPS access through their Webmail programs. Most of these ESPs provide help to their users on their respective websites but no ESP provides a detailed security tutorial nor do they provide adequate information about e-mail security issues and training about best practices to overcome them.

To analyze the treatment of sender spoofing e-mail by servers of ESPs, test e-mail accounts were subjected to sender spoofed e-mails from domains following some security standard and also from domain following no security standard. A bulk e-mail utilities capable to include spoofed sender name, return-path and 'From' address was used to send spoofed e-mails. It has been found that DKIM complaint domains before delivery of message correct 'From' address field in e-mails if spoofed by the sender. Further, domains following SPF/Sender ID do not accept e-mails if spoofed. The results of analysis of the treatment of sender spoofed e-mails from non-DKIM/SPF complaint domains is provided in Table 2 below.

Table 2. Treatment of Sender Spoofed E-mails by Commercial E-mail Service Providers

Email Service Provider (ESP) Webmail	Accepts Sender-Spoofed Emails		Displays Name in Email Listing	Classifies Sender-Spoofed Emails as Spam	
	Username Only	Username & Domain		Username Only	Username & Domain
AOL mail *www.aol.com*	Yes	Yes	No	No	No
YAHOO! MAIL *mail.yahoo.com*	Yes	Yes	Yes$^{\alpha}$	No	No
Gmail *www.gmail.com*	Yes	Yes	Yes$^{\alpha}$	No	No
Windows Live *mail.live.in*	Yes	Yes	Yes	No	No

Email Service Provider (ESP) Webmail	Accepts Sender-Spoofed Emails		Displays Name in Email Listing	Classifies Sender-Spoofed Emails as Spam	
	Username Only	Username & Domain		Username Only	Username & Domain
www.inbox.com	Yes	Yes	Yes[α]	No	No
web.mail.com	Yes	Yes	Yes	No	No
mail.rediff.com	Yes	Yes	Yes	No	No
il.zapak.com	Yes	Yes	Yes	No	No
www.hushmail.com	Yes	Yes	Yes[α]	No	No
www.gmx.com/mail.html	Yes	Yes	Yes	No	No
mail.gawab.com	Yes	Yes	Yes[α]	No	No
www.fastmail.fm	Yes	Yes	Yes[α]	No	No
mail.ovi.com	Yes	~~No~~	Yes[α]	No	NA
lavabit.com	Yes	Yes	Yes	No	No

[α] When pointing to name, it also displays senders email address.

It has been found that most of the servers under study used some e-mail security protocol but continue to accept sender-spoofed e-mails, spoofed either in username only or in both username and domain name from domains that do not use anti-spoofing protocols. However, signatures in the headers do indicate that the e-mail has arrived from a domain that does not follow some compatible security protocol. Some domains also provide a visual indication to the users in browsers but others do not. Further, some domains display a human friendly name while listing e-mail in mail folder and others use human friendly name as well as use e-mail address in the listing. This human friendly name can be misleading and its forgery is difficult to know without opening the e-mail.

The extensive header analysis revealed that spoofed e-mails send from some domains that do not follow any standard anti-spoofing protocol do contain the original 'From' address in the 'Trace' header field which is ignored by the receiving servers.

4.2. Improving Efficiency of E-mail Servers

The headers of e-mail message are in plain text and are organized in field groups namely 'Origination Date', 'Originator Address', 'Destination Address', 'Information', 'Resent' and 'Trace'. When messages are introduced into the transport system, they are often pre-pended with additional 'Trace' fields. Headers comprise of name and body separated by a colon. Field body may be composed of any US-ASCII characters except Carriage Return (CR) and Line Feed (LF) characters. Long header fields may be 'folded' i.e. split into multiple lines for convenience by inserting Carriage Return and Line Feed (CRLF) characters before any White Space Characters (WSP) i.e. Horizontal Tab (ASCII value 9) and the Space (ASCII value 32).

Trace information is inserted at the beginning of the message when an SMTP Server receives a message for delivery or further processing by each MTA. This trace is in the form of Trace Fields consisting of 'Return-Path' and 'Received' fields and is defined as follows:

1) **Return-*Path Line*** = *"Return-Path:" FWS Reverse-Path <CRLF>*
2) **Time-*stamp-line*** = *"Received:" FWS Stamp <CRLF>*
3) **Stamp** = *From-domain By-domain Opt-info ";" FWS date-time*
4) **From-*domain*** = *"FROM" FWS Extended-Domain CFWS*
5) **By-*domain*** = *"BY" FWS Extended-Domain CFWS*
6) **Extended-*Domain*** = *Domain / (Domain FWS "(" TCP-info ")") / (Address-literal FWS "(" TCP-info ")")*
7) **TCP-*info*** = *Address-literal / (Domain FWS Address-literal)*
8) **Opt-*info*** = *[Via] [With] [ID] [For]*
9) **Via** = *"VIA" FWS Link CFWS ;"Via" is primarily of value with non-Internet transports*
10) ***With*** = *"WITH" FWS Protocol CFWS*
11) **ID** = *ID" FWS String / msg-id CFWS*
12) **For** = *"FOR" FWS 1*(Path / Mailbox) CFWS*
13) **Link** =*"TCP" / Addtl-Link*
14) **Addtl-*Link*** = *Atom Additional standard names for links are registered with the Internet Assigned Numbers Authority (IANA)*
15) **Protocol** = *"ESMTP" / "SMTP" / Attdl-Protocol*
16) **Attdl-*Protocol*** = *Atom ;Additional standard names for protocols are registered with the Internet Assigned Numbers Authority (IANA)*

The header analysis of the spoofed e-mails have revealed that 'Extended-Domain' (line numbered 6) part of the 'Received' field often contains the original sender address for e-mails received from some domains that do not follow any standard anti-spoofing protocol. A listing of headers of such mail with slight modification to hide the identity of sender, receiver and the domain involved is shown below:

1) **Return-Path:** <spoofed@spoofed.com>
2) **Received:** from CompX.internal (CompX.internal [a1.b1.c1.d1])
   by CompY.internal (ComputerY) with LMTPA; Tue, 29 Dec 2009 16:47:40 -0500
3) **X-Sieve:** CMU Sieve 2.3
4) **X-Spam-charsets:** plain='utf-8', html='utf-8'
5) **X-Resolved-to:** bob@bob.com
6) **X-Delivered-to:** bob@bob.com
7) **X-Mail-from:** spoofed@spoofed.com
8) **Received:** from mx3.MTAEngine.com ([a1.b1.c1.d2])
   by CompZ.internal (ComputerZ); Tue, 29 Dec 2009 16:47:40 -0500
9) **Received:** from alice.com (Unknown [a3.b3.c3.d3])
   (using TLSv1 with cipher DHE-RSA-AES256-SHA (256/256 bits))
   (No client certificate requested)
   by mx3.MTAEngine.com (Postfix) with ESMTPS id AXXX999
   for <bob@bob.com>; Tue, 29 Dec 2009 16:47:39 -0500 (EST)
10) **Received:** from SpoofedName ([a4.b4.c4.d4])
    (Authenticated user alice@alice.com)

by alice.com
(using TLSv1/SSLv3 with cipher AES256-SHA (256 bits))
for bob@bob.com;
Wed, 30 Dec 2009 03:07:04 +0530
11) **From:** "spoofed" <spoofed@spoofed.com>
Subject: spoofed subject
12) **To:** "bob" <bob@bob.com>
13) **Content-Type:** multipart/alternative; charset="utf-8";
boundary="qBZgvkMZ83jSnbQ4rTqYSoIg6y=_sXVOTU"
14) **MIME-Version:** 1.0
15) **Content-Transfer-Encoding:** 8bit
16) **Organization:** spoofed
17) **Date:** Wed, 30 Dec 2009 03:06:54 +0530
18) **X-Truedomain-SPF:** None
19) **X-Truedomain-DKIM:** None
20) **X-Truedomain:** Neutral
21) **Message-ID:** <xxx-abcd-99999-9999999999-9@storeabc.internal>

The headers specify that the mail is for bob@bob.com and has come from spoofed@spoofed.com having a user friendly name spoofed. The return path of the mail is also spoofed@spoofed.com. This listing also indicates that the mail has not come from a domain following some anti-spoofing standard like SPF and DKIM (lines numbered 18, 19 and 20). Besides other headers, the mail also contains 'Received' header that has multiple occurrences (at lines numbered 8, 9 and 10). The 'Received' header at line numbered 10 contains (Authenticated user alice@alice.com) which reveals the sender's original identification. This reveals that the original sender is alice@alice.com and not spoofed@spoofed.com. This trace information is added to the 'Received' field by some sending domains as an additional parameter named as Authenticated user or Authenticated sender. Currently, ESPs do not take this trace information into consideration for reporting spoofed e-mails. The efficiency against spoofing can be improved by comparing this trace information with the 'From' header field.

5. USER STUDY

An e-mail communication takes place at least between two users. To make this communication private and secure both users need to know and use security protocols. Further, their ESPs should implement compatible security protocols. The author augmented earlier study reported in [3] by conducting user studies with about 1600 e-mail users registered with different commercial and corporate ESPs, to appraise their e-mail practice and knowledge of security protocols. The results of this study are presented in figure 3. The authors also conducted another study to ascertain user confidence in e-mail communication system. About 100 users were made aware of the security and privacy issues of e-mail system and later were trained thoroughly in the use of existing security protocols and header analysis. The results of their confidence in e-mail system in terms of security and usability of security protocols before and after trainings are presented in tables 4 below.

Table 3. User E-mail Practice and Awareness of Security Protocols

Parameters	Results
User Practice	
Use of Webmail Programs	85%
Use of Anti-Virus and other related Software's	43%
Use of Encryption/Authentication Protocols like S/MIME or PGP	15%
Use of Headers Analysis for e-mail authentication	0.50%
User Knowledge	
Awareness about SPAM and SPAM Filters	88%
Awareness about filter classification errors	55%
Awareness about Spoofing	21%
Awareness about SPF/DKIM and other transparent security protocols	19%
Awareness about non-transparent security protocols like S/MIME	25%
Awareness about e-mail headers other than frequently used headers	12%

Table 4. User Confidence in E-mail Communication

User Confidence Parameters	Before Training	After Training
Users considering e-mail as highly secure	32%	85%
Users considering e-mail Security Protocols highly usable	45%	90%

It has been found that most of the users use Webmail interfaces to send and read e-mails. Less than 50% e-mail users have anti-virus, anti-spam and anti-spyware software's installed on their clients and less than half of them update virus definitions regularly. Very less number of users uses encryption/authentication protocols like S/MIME or PGP for securing their e-mails. Header analysis is being done by only a negligible number of users before trusting an e-mail source. Most of the users are aware of spam, spam filters and filter classification errors. Spoofing is not known to most of the users. Some users are aware of security protocols like DKIM, SPF/SenderID and S/MIME but very less are aware of all e-mail headers. The results obtained through these studies reveal that: 1) most of the users have limited knowledge of security issues, 2) existing security protocols are not used by most of the e-mail users, and, 3) user confidence in e-mail is poor. Further, it was also found that most of the users are feeling that information transmitted through e-mail is not only insecure but also the delivery of e-mail is not guaranteed. They were of the opinion that usability of security protocols is limited. The results of training were encouraging as confidence level of users on an average improved considerably in each individual parameter.

6. CONCLUSION

Add-on e-mail security protocols use encryption, PKI based cryptographic techniques, IP address verification and DNS based domain validation for providing security against spoofing and other e-mail threats. However, no protocol independently provides all required security features. Further, domains that are not compatible with security protocols continue to pose security threats by allowing transmission of spoofed e-mails that are not detected by receiving domains using security protocols. Spoofed e-mails from some domains that do not support add

on security protocols can be detected by analyzing trace header field which is not currently done by receiving domains. E-mail users are losing confidence in e-mail security because they have insufficient awareness of security protocols and only some of users use them to secure their e-mails. There is a need to undertake a major educational campaign to aware e-mail users about e-mail security issues and train them in use of security protocols and procedures.

REFERENCES

[1] Klensin, (2001) 'Simple Mail Transfer Protocol' IETF RFC 2821.

[2] Mir, F.A., Banday, M.T. (2010). "Control of Spam: A Comparative Approach with special reference to India", Journal of Information Technology Law, UK, 19(1), pp.22-59, DOI: 10.1080/13600831003589350, URL: http://dx.doi.org/10.1080/13600831003589350.

[3] Banday, M.T., Qadri, J.A. (2010). "A Study of E-mail Security Protocols," eBritian, ISSN: 1755-9200, British Institute of Technology and E-commerce, UK, Issue 5,Summer 2010, pp. 55-60, available online at: http://www.bite.ac.uk/ebritain/ebritain_summer_10.pdf.

[4] Banday, M.T., Mir, F.A., Qadri, J.A., Shah, N.A. (2011). "Analyzing Internet E-mail Date Spoofing", Journal of Digital Investigation, UK, 7, pp. 145-153, doi:10.1016/j.diin.2010.11.001.

[5] C. E. Landwegr, C. L. Heitmeyer, and J. D. McLean, (2001) "A security model for military message systems: Retrospective," Naval Research Laboratory, Wasgington, DC, 2001, http://www.chacs.nrl.navy.mil/publications/CHACS/2001/2001landwehr-ACSA.pdf, accessed 20 November 2009.

[6] R. Oppliger, (2004) "Certified Mail: the next challenge for secure messaging", Communications of ACM, Vol. 47, No. 8, pp. 75-79.

[7] M. Jakobsson and S. Myers (Eds.), (2006) "Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft", Adobe E-Book, Wiley Publication, ISBN: 978-0-470-08609-4.

[8] T. R. Surmacz, (2007) "Reliability of e-mail delivery in the era of spam", International Conference on Dependability of Computer Systems, DepCoS-RELCOMEX'07*,* 198 – 204.

[9] Apu Kapadia, (2007) "A Case (Study) For Usability in Secure E-mail Communication", IEEE Security & Privacy, pp. 80-84.

[10] P. Tzerefos, C. Smythe, I. Stergiou and S. Cvetkovic, (1997) "A comparative study of Simple Mail Transfer Protocol (SMTP), Post Office Protocol (POP) and X.400 Electronic Mail Protocols. Proceedings of the 22nd Annual IEEE Conference on Local Computer Networks, pp. 545 – 554.

[11] Tahir Elgamel, and Kipp E. B. Hipman, (1997) "Secure Socket Layer Application Program Apparatus and Method" U.S. Patent No:5657390.

[12] P. Hoffman, (2002) "SMTP Service Extension for Secure SMTP over Transport Layer Security", IETF RFC 3207.

[13] S. Suzuki and M. Nakamura, (2005) "Domain Name System—Past, Present and Future", IEICE Transactions of Communication, E88b (3), pp. 857-864.

[14] S. T. Kent, (1993) "Internet Privacy Enhanced Mail" *Communications of ACM,* Vol. 36, No. 8, pp. 48-60.

[15] PGP, (nd) "Pretty Good privacy (PGP)", http://www.pgp.com, accessed 25 August, 2009.

[16] W. Koch, (nd) "The GNU privacy guard", http://www.gnupg.org, accessed 7 September 2009.

[17] B. Ramesdell, (2004) "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1 message specification", Internet Engineering Task Force (IETF), RFC 3851.

[18] B. Ramesdell, (2004) "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1 Certificate Handling", Internet Engineering Task Force (IETF), RFC 3850.

[19] S. Garfinkel, (2009) "Signed, Dealed and Delivered", CSO Online, www.csonline.com/read/040104 /shop/html, accessed 25 November.

[20] C. Moris and S. Smith, (2007) "Towards usefully Secure E-mail", IEEE technology and Society Magazine, pp. 25-34.

[21] Federal Trade Commission, (2005) "Florida Man Settles FTC Charges of Sending Illegal Spam and Making False "Human Growth Hormone" Product Claims", 15th June 2005, http://www.ftc.gov/opa/2005/06/creaghanharry.shtm, accessed 25 August 2009.

[22] B. Leiba and J. Fento, (2007) "DomainKeys Identified mails (DKIM): Using Digital signatures for Domain Verifcation", CEAS 2007, Fourth Conference on E-mail and Anti-Spam, August 2-3, 2007, Mountain View, California USA.

[23] Y. Zhang, T. Cui, and H. Tang, (2008) "A new secure e-mail scheme based on Elliptic Curve Cryptography Combined Public Key", In proceedings of 2008 IFIP International Conference on Network and Parallel Computing, pp. 336-340.

[24] L. Harn and J. Ren, (2008) "Design of Fully Deniable Authentication Service for E-mail applications", IEEE Communication Letters, Vol. 12. No. 3 pp. 219-220.

[25] Hunt and Courane, (2004) "An analysis of tools used for the generation and prevention of spam" Computers & Security, Vol. 23. No. 2, pp. 154-166.

[26] D. Crocker, J. Leslie and D. Otis, (2005) "Certified Server Validation (CSV)", IETF Internet Draft, http://tools.ietf.org/html/draft-ietf-marid-csv-intro-02, accessed 25 September, 2009.

[27] J. R. Levine, (2005) "Experiences with Greylisting", Second conference on e-mail and anti-spam, http://www.ceas.cc/papers-2005/120.pdf, accessed 5, August 2009.

[28] B. Adida, (2007) "Lightweight MTA Authentication Protocol (LMAP) Discussion and Comparison", Proceedings of the 14th ACM conference on Computer and communications security, pp. 48-57.

[29] M. Wong and W. Schlitt, (2006) "Sender Policy Framework (SPF) for Authorizing Use of Domains in E-MAIL, version 1", Internet Engineering Task Force (IETF), RFC 4408.

[30] J. Lyon and M. Wong, (2006) "Sender ID: Authenticating E-mail", Internet Engineering Task Force (IETF), RFC 4406.

[31] E. Allma, J. Callas, M. Delany, M. Libbey, J. Fenton and M. Thomas, (2007) "DomainKeys Identified Mail (DKIM)", Internet Engineering Task Force (IETF), RFC 4871.

[32] E. Allman, M. Delany and J. Fenton, (2007) "DKIM Sender Signing Practices", IETF Internet draft, work in progress.

[33] B. Adida, D. Chau, S. Hohenberger and R. L. Rivest, (2006) "Lightweight E-mail Signatures (Extended Abstract)", In Fifth Conference on Security and Cryptography for Networks (SCN'06), Vol. 4116 of Lecture Notes in Computer Science, pp. 288-302.

Author

M. Tariq Banday was born in 1969. He did his M. Sc., M. Phil. and Ph. D. Degrees from the Department of Electronics, University of Kashmir, Srinagar, India in 1996, 2008 and 2011 respectively. He did advanced diploma course in computers and qualified UGC NET examination in 1997 and 1998. At present he is working as Sr. Assistant Professor in the Department of Electronics & Instrumentation Technology, University of Kashmir, Srinagar, India. He has to his credit several research publications in reputed journals and conference proceedings. He is a member of Computer Society of India, International Association of Engineers and ACM. His current research interests include Network Security, Internet Protocols and Network Architecture.