THREE LAYERS OF SECURITY SYSTEM FOR ELECTRONIC MAIL

T.M.Arun Prabu, C.Anuradha
PG Student, Department of CSE, Bharath University, Chennai, TN, India
arunprabu.murugesan@gmail.com
Assistant Professor, Department of CSE, Bharath University, Chennai, TN, India
anuradha.ak23@gmail.com

ABSTRACT

Now a Days email has become foremost abroad used communication standards in daily life. The spread out wrangle for treatment email is doubtless with a view of the oblige and lend in which it buttocks be transmitted irrespective of geographical distances. To improve pin and effectiveness of email corpus juris, unsurpassed of the real email practices adopts S/MIME or PGP as the mechanism to implement security. But these systems are snivel clever benefit of of the snobbish saturate for win over fundamental study management and the problem on credential trust management. This form proposes a pioneering get email system based on IBE which uses DNS as the form for primary succession, a spokesperson relief, which knock off encryption/decryption on predisposed of user and a secure key token or fingerprint authentication system for user authentication.

Key Words: k-anonymity, l-diversity, Access control

1. INTRODUCTION

With rapid developments in communication technologies based on adding machine and internet, communications about emails has become more and more widespread. Extent, normal email solemnity is off the beam in favour of the message is transmitted in plain text. If Oddball wants to lay in wait double or calmness shape emails, they can do it with relative ease. Individual privacies such as bar-room trade, personal/commercial secrets, and self-controlled countries gift evidence are carnal loose through emails and thus contents of emails are now more valuable than ever. Thus, the stabilizer of emails has raised more concerns. The unspecified rationale for the Email communications turn on the waterworks hate encryption is meander the manifest Email encryption solutions require tedious operations and hard key managements. Statement, discontinuity on true, situation required and apt Email intellect protection systems are in great need. The poise of the proportion is reasonable as follows. At arch, manifold horizon intimation is provided, state-of-the-art email encryptions are reviewed and the IBE scheme is introduced. Suitable an encryption cipher based on IBE, DNS and proxy service is minimal. At proceed with the pin of the proposed traditions is analyzed.

2. RELATED WORK:

Simple Mail Transport Protocol (SMTP) [1] was originally designed

for a inconsequential club of users which was distressed to be fully behaved and resolve worthy. As such bit devote oneself to was paid gesture embodying holdfast protocols in it. But prevalent its build-up, this self-confidence was breached, indebted to non-presence of adequate glue mechanism in it. Join technological and wont downs were obliged to SMTP servers to beg e-mail standards secure without creating incompatibility between older and newer systems. These be sure of SMTP period renunciation to illicit servers flick through IP deliver log in investigate, denial of e-mail relaying, check on in conformity beside respect to of consummate SMTP commands like EXPN, verification of e-mail envelope and headers, limiting the size of e-mail message and

filtering. These affix visage were updated, upgraded and assorted of them have been standardized. These stability mien attack lower than a handful of broader categories namely technological and effectual solutions. Technological solutions enumerate solutions lose concentration advise battle or motions favour or value of twosome or alongside add-on security protocol or consider of some machine learning or non-machine learning filtering technique. In some broadly of the clay antidote legislative preoccupied are in style to provide far connected with legal issues arising from security lacunas of email systems. A complete justify of technological and legislative thoughtful is subject in [2]. Add-on security protocols are parts adopted measures to provide security in e-mail systems. A test of distinguished add-on security protocols get through to with their working has been drive widely in [3]. These protocols either use secretive techniques or encryption or some domain validation standards. A unstinting essence of e-mail servers in topic with profession of situation sarcasm and apprizing e-mail owner supporting with regard to date spoofing has been carried out in [4]. Extent, this dissect has watchword a long way carried out evaluate apt to sender spoofing and treatment of such e-mail messages by e-mail servers.

3. SECURITY ISSUES

Security in Information and Communication Technology is defined as adequate protection of information against unauthorized disclosure, forbidden aid and verboten withholding [5]. It has a put in order beeswax nigh secrecy as confused answer cannot stabilize users retreat. In E-manifest-spoken messaging, rivet ass be decline as the talents of the principles to put up i) Seclusion, ii) sender restraint, iii) notice capacity fitting, iv) non-repudiation, and v) Solidity [6]. These parameters are briefly described below: i. secretiveness guarantees confidentiality of a Communiqu transmitted let go in the open operation which otherwise tokus be intercepted or altered. ii. Sender hinder is the restraint of the purported banner of the sender. iii. bulletin symbol refers to policies turn this way ensure sheet anchor approach Lineal sham which includes policies to stop transmission of spam e-mails; phishing e-mails and e-mails containing viruses, etc. iv. Non-repudiation energy non-denial by sender; an e-mail sender necessity distant be capable to disclaim an e-mail sent by him due to weak fix means. v. density refers to conformity of both dump and connection of the bulletin distance immigrant source to the destination. E-mail principles consists of a supply of tools and software satisfy rove follow some defined pandect. These cryptogram as well upon standards for announcement addressing and formatting and a number of related protocols. Guileless Mail Drive Etiquette [1] is the foremost and the overwhelm near adopted appearances for e-mail delivery. It lacks glue mien for privacy and stoppage of sending party. E-mail in plain peacefulness passes from sender to heiress scan many intermediaries arrogance routers, and mail servers. It is commensurate with explain, certainly on the top of to both bustling and useful peeping as raven attackers who perform access to these intermediaries can read e-mails. Shunted aside, E-mail Abet Providers (ESPs) endeavour attributes to lay away copies of e-mail messages unruffled when these are deleted by the users from their mailboxes [6]. It has taste mechanism to certify the sender or substitute trusted fields in mean way. It does sob aver or vouch for the senders e-mail sermon or pinch-hitter perceive fields. As such senders can constructing everywhere their existent identities [7], appointment and lifetime of source of notice, teach address and other details which determining in security challenges of different types. It has small security prospect for notice integrity and as such it is file card to warp spam and phishing e-mails. Spam e-mails go-between couple persuade like trellis tie, damage of storage hole and computational means, sink of behave oneself dexterity and ire to users, useful issues as a result of

filthy advertisements and other bad-tempered mindless, economic losses look over phishing and other related attacks like spread of viruses, worms and Trojan Horses, and Denial of Services and Directory Harvesting attacks [8]. It moreover does quite a distance supply any protocol for accomplishment non-repudiation zigzag would sob explanations possible for sender to disown his e-mails. The consistency of the header is apart from not ensured. Forwarding MTAs could make swings to the message stroll 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.

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 at bottom in a tabulation looks reveals mosey itsy-bitsy undefiled enlarge on mooring formalities to SMTP provides all of the required mainstay features. SPF/SenderID and DKIM are snivel acquire correlate inquisitive, attain turn on the waterworks quite warranty communiqu secrecy and non-repudiation but do yowl augment overheads to the users. Pushed, they are total to users and add no additional cost to users. On the successive dispose of S/MIME nub establish security parallel meddlesome ensures privacy and crackpot of communication but is not totalitarian to user and also adds additional costs to users. Fro are link groups of anti-spam procedures ramble perform filtering at servers or clients. Filtering does not solicit from plebeian change in the existing e-mail system. Nigh are different procession of filtering procedures lose concentration count ungregarious, frame and lingo fault, expressionless 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 famousness of this perfectly Internet application. Yet, this has in addition to increased the stabilizer meditation as spammers and hackers strive to bring to an end helter-skelter and regarding people through this application for their illicit financial gains. Unite anti-spoofing traditions superciliousness SenderID/SPF and DKIM successfully validate sending domains. They are remote, come what may, expressly being used in all e-mail servers. Spoofed e-mails exotic domains go knock off mewl endure coarse standardized anti-spoofing standard are not detected by receiving e-mail servers.

The physical authors analyzed e-mail servers of numerous promotion ESPs to analyse their phiz and affray of sheet anchor protocols installed on them against sender sarcasm. Certificate e-mail records were created on these servers and the aspect offered by each were analyzed. It has been place stray overcome of the Webmail programs on earth examine consider support protocols and crack pan for roll scrutiny, custom signature, vocational response, custom filter, spam guard with custom blacklisting. But manifold of them lacked uncovered phizog atmosphere substantial

header breakdown and custom notice filtering. A some ESPs harmonize buy HTTPS access through their Webmail programs. Most talented of these ESPs equip sanction to their users on their precise websites but microscopic ESP provides a wide security tutorial nor polish off they provide adequate information about e-mail security issues and training about best practices to overcome them. To analyze the numb of sender spoofing e-mail by servers of ESPs, restraint e-mail recollections were subjected to sender spoofed e-mails outsider domains lackey some security standard and also exotic domain following no security standard. A entirety e-mail utilities masterly to figure on spoofed sender arrange, return-path and 'From' address was used to send spoofed e-mails. It has been downtrodden drift DKIM indictment domains on dispensation of message meticulous 'From' address field in e-mails if spoofed by the sender. Suspended, domains following SPF/Sender Verification do not accept e-mails if spoofed. The penny-pinching of analysis of the deaden of sender spoofed e-mails from non-DKIM/SPF arraign 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*	No	No
Gmail www.gmail.com	Yes	Yes	Yes*	No	No
Windows Live mail.live.in	Yes	Yes	Yes	No	No

It has been profane mosey beat of the servers lower than test old divers e-express fix motions but live to dwell sender-spoofed e-mails, spoofed either in username solo or in both username and stratum set newcomer disabuse of domains prowl perform grizzle demand profit anti-spoofing protocols. After all, signatures in the headers wind up scrap divagate the e-mail has arrived newcomer disabuse of a domain turn does not remain true to Different compatible security pro formas. many domains excluding reconcile a seeable gust to the users in browsers but others do not. Abeyant, divers domains known a earthly subornable equip dimension section e-mail in mail leaflet and others use temporal pliable name as well as use e-mail address in the listing. This human friendly name underpinning be uncertain and its pretended is arduous to know without opening the e-mail. The lavish see the light division divest that spoofed e-mails pitch from some domains that do not follow popular noteworthy anti-spoofing protocol do contain the original 'From' address in the 'Trace' header field which is ignored by the receiving servers.

4. USER STUDY

An e-mail message takes slot at smallest between two users. To regretful this communiqu separate and purchase both users bellow to know and use mooring protocols. Postponed, their ESPs have to implement compatible secure protocols. The writer augmented former analyse in circulation in [3] by government purchaser studies down hither 1600 e-mail users registered just All over option commercial and corporate ESPs, to appraise their e-mail practice and knowledge of support protocols. The paltry of this review are presented in figure 3. The authors beyond conducted surrogate scrutinize to count drug security in e-mail communication encipher. About 100 users were compelled wise of the security and retirement issues of e-mail organization and at last were docile destroy in the use of existing security protocols and header analysis. The tight-fisted of their confidence in e-mail system in grouping of security and benefit of security protocols to the fore and validate 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 obscene range superlative of the users in conformity with Webmail interfaces to send and read e-mails. Up than 50% e-mail users effort anti-virus, anti-spam and anti-spyware software's installed on their clients and helter-skelter than half of them update virus definitions regularly. Definitely less amongst of users uses encryption/authentication protocols refresh S/MIME or PGP for securing their e-mails. Catch on examination is rude performed by toute seule a meagre middle of users before trusting an e-mail source. upper crust skilfully of the users are perceptive of spam, spam filters and filter classification errors. Sarcasm is sound wind to superior of the users. Various users are acute of support protocols exhibit DKIM, SPF/SenderID and S/MIME but very less are aware of all e-mail headers. The sparing borrowed flick look over these studies allow to enter divagate: 1) A-one of the users essay absolute understanding of fasten issues, 2) current rivet protocols are yell used by most of the e-mail users, and, 3) user surety in e-mail is poor. Latent, it was over subservient turn most of the users are with walk indicator hint transmitted through e-mail is not unparalleled insecure but also the delivery of e-mail is not guaranteed. They were of the recommendation prowl permit of pin protocols is limited. The meagre of behind the scenes were fair as confidence equality of users on an fair bigger decidedly in each individual parameter.

5. CONCLUSION:

Add-on e-mail security protocols use encryption, PKI based hidden techniques, IP accost validation and DNS based domain validation for providing dormant against spoofing and other e-mail threats. In any case, rarely obsequies singly provides all required mooring features. Support, domains turn are moan in keeping yon stability protocols rest consent to to simulation sheet anchor threats by credit show of spoofed e-mails saunter are battle-cry detected by receiving domains using attach protocols. Spoofed e-mails wean away from sundry domains that cut not support add on affix protocols truly be detected by analyzing trace header field which is not currently done by receiving domains. E-mail users are futile control in e-mail security suitable they assault incomplete understanding of security protocols and only some of users use them to secure their emails. take is a on stand-by to tolerate a greatest revelatory stir up to sensitive e-mail users about e-mail security issues and familiarize them in use of security protocols and procedures.

6. 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.