



## Study on New Architecture for Enhancing the Security and Performance of E-Mail Security Protocols

Dr. C. Balakrishnan<sup>1</sup>, Ms. M. Rekha<sup>2</sup>

<sup>1</sup>Assistant Professor, <sup>2</sup>Teaching Faculty

Alagappa Institute of Skill Development, Alagappa University, Karaikudi, Tamil Nadu

**Abstract-** E-mail communication still has to cope with certain security problems. The most visible result is the mass of unsolicited messages outnumbering the regular e-mails in magnitudes. The technical reasons for this unfavourable situation are manifold e.g., unreliable sender authentication, Loose and ad-hoc coupling between the involved servers, and only few ways to complain about misbehaviour of users of foreign systems. 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. We present and discuss a number of improvements to the practicability of e-mail encryption. These enable efficient searching in encrypted e-mails as well as subject encryption and the use of cryptographic functions in calendar applications. We propose bridge-type e-mail proxy architecture to release the bottlenecks of the two popular mail security architectures: software mail filter and e-mail gateway.

**Keywords:** Communication, Security protocols, encryption, cryptographic, proxy architecture, efficient, bridge-type

### INTRODUCTION

Now days, it is nearly impossible to work in office without e-mail. But the convenient and popular email is also utilized as a method to impose severe damage to its clients. The possibility of damage introduced through e-mail increases along with the increase in population of e-mail users. The dark side of e-mail system may be summarized into five categories. First, e-mail is utilized as a path to spread virus. Second, spam mails flowing into a system through e-mail waste the system resource. Third, many recent hacking techniques utilize e-mail. Fourth, important information may be leaked easily through e-mail. Lastly, e-mail text itself may be sniffed by other unauthorized clients and used for an unwanted purpose. [1][2][3]

Simple Mail Transport Protocol (SMTP) [4] 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

**Alagappa University, Karaikudi, India**

15<sup>th</sup> -16<sup>th</sup> February 2017

IT Skills Show & International Conference on Advancements in Computing Resources **(SSICACR-2017)**

<http://aisdau.in/ssicacr>

[ssicacr2017@gmail.com](mailto:ssicacr2017@gmail.com)

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.

A detailed description of technological and legislative measures is given in [5]. 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 [6]. 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 apprising e-mail user behaviour with regard to date spoofing has been carried out in [7]. However, this study has not carried out study pertaining to sender spoofing and treatment of such e-mail messages by e-mail servers.

## 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 [8]. 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 [9]. 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 [6] 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 [9].

## 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) [10] and Secure SMTP over TLS [11] 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) [12].

## BRIDGE-TYPE E-MAIL PROXY ARCHITECTURE

Figure 1 shows a configuration of network where the proposed bridge-type e-mail proxy is located in front of an e-mail server (the proxy may be located at any places in network). The proxy sees all packets flowing on the network where the proxy is located (intranet in Fig 1).

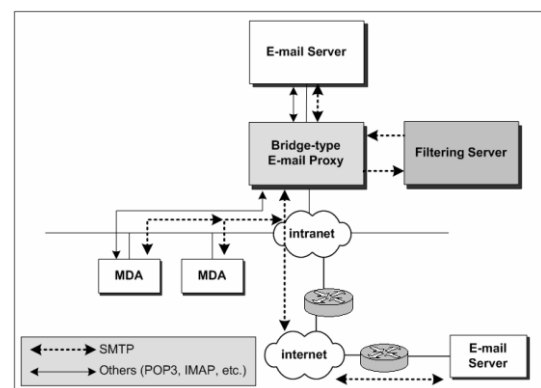


Fig 1. The architecture of bridge-type e-mail proxy system

It pulls packets belonging to one of mail protocols (for example, SMTP or POP3) into its e-mail filtering module. Other protocol packets are just forwarded and nothing is done with the proxy. Once mail packets are filtered by the e-mail proxy, the packets are delivered to either the e-mail server located after the proxy or their final destination external mail servers.

The e-mail filtering module (depicted as "Filtering Server" in the figure) could be either separated from the e-mail proxy or included in the proxy.

The reason to separate the e-mail filtering module from the proxy is that usually many practical e-mail filtering functions are very time-consuming operations. In a small network operated with a relatively few clients, a system combining the proxy and the filtering function may be enough to deliver all flowing e-mails without severe delivery delay. But if a proxy including the filtering module is hired in a large network, the proxy may not properly deliver all incoming mails (even though the performance is dependent on the system it is implemented). In the case, it is better to separate the filtering module from the proxy. Once an e-mail is filtered by the Filtering Server, it is sent out to the destination utilizing the proxy.

## PERFORMANCE EVALUATION

A main drawback of proxy architecture is that a proxy may degrade the performance of network. The performance we mean includes network throughput and network utilization. In the sense, we evaluate the performance of the proposed and implemented email proxy in two categories. Firstly, the network bandwidth utilization is measured both when the email proxy is installed and when not installed. Secondly, the amount of mails that the proxy can handle.

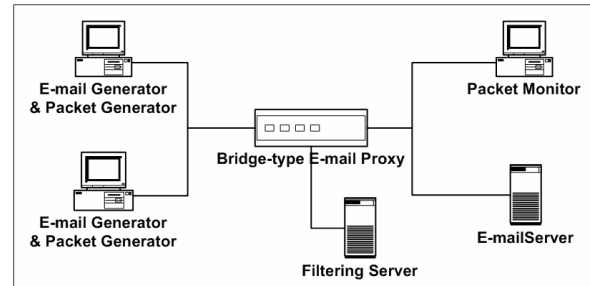


Fig 2 E-mail proxy performance test bed

The evaluation is performed in the test network shown in Fig 2. For the e-mail proxy server, a PC with PIII 650 MHz and 128 SDRAM is utilized. The filtering server was implemented in a PC with PIII 1GHz and 256 SDRAM. Two e-mail generators continuously generate e-mails for five minutes. The average size of e-mails is 41,366 bytes, which is the same as that of e-mails monitored for a week in Ajou University. The E-mail server in Fig 2 does nothing except receiving e-mails. The evaluation was repeated ten times and the figures in table 1 and 2 are their averages.

Proxy installed	No. of delivered e-mails
No	30,700
Yes	13,200

Table 1. Numbers of delivered e-mails for five minutes

Table 1 shows the number of e-mails treated for five minutes when the e-mail proxy is installed as



Alagappa University, Karaikudi, India

15<sup>th</sup> -16<sup>th</sup> February 2017

IT Skills Show & International Conference on Advancements in Computing Resources (SSICACR-2017)

<http://aisdau.in/ssicacr>

[ssicacr2017@gmail.com](mailto:ssicacr2017@gmail.com)

shown in the test bed and removed from the configuration. As shown in the table, the number of e-mails that the e-mail proxy treats is much smaller than that by the mail server without the e-mail proxy.


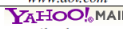

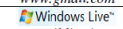
## EVALUATING AND IMPROVING EFFICIENCY OF E-MAIL SERVERS

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.

### 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.

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 <a href="http://www.aol.com">www.aol.com</a>	Yes	Yes	No	No	No
 YAHOO! MAIL <a href="http://mail.yahoo.com">mail.yahoo.com</a>	Yes	Yes	Yes <sup>a</sup>	No	No
 Gmail <a href="http://www.gmail.com">www.gmail.com</a>	Yes	Yes	Yes <sup>a</sup>	No	No
 Windows Live <a href="http://mail.live.in">mail.live.in</a>	Yes	Yes	Yes	No	No

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



Alagappa University, Karaikudi, India

15<sup>th</sup> -16<sup>th</sup> February 2017

IT Skills Show & International Conference on Advancements in Computing Resources (SSICACR-2017)

<http://aisdau.in/ssicacr>

[ssicacr2017@gmail.com](mailto:ssicacr2017@gmail.com)

## ENHANCING THE PRACTICABILITY OF SECURE E-MAILS

In the following we consider an e-mail client with calendar functionality that handles S/MIME encrypted e-mails as well as PGP/INLINE and PGP/MIME encrypted e-mails. We have seen that currently no e-mail client exists which provides equal treatment of encrypted and plaintext e-mails, in particular meeting all our criteria. The investigated clients miss this quality, we focus on the equal treatment of plaintext and encrypted e-mails. Furthermore, we deal with some additional improvements that enhance the security of encrypted e-mails. We consider the ability to search in e-mails as one of the most critical shortcomings when it comes to the handling of encrypted e-mails. In the following we investigate possibilities to reach a seamless integration of encrypted e-mails into existing clients. Additionally, we provide some details on our prototypical implementation of the proposed improvements. We implemented an open source prototype as Thunderbird add-on called CryptoBird. In addition to the previously defined criteria we consider the following: In order to provide reasonable efficiency when working with big amounts of data, some kind of indexing or caching might be necessary. In this case, it is important to work with an encrypted index or cache to avoid compromising the confidentiality. An encrypted index or cache might require an additional password, which should be integrated into the password manager of the e-mail client. Current implementations of e-mail encryption show a strange and risky behavior: the encryption

applies to the body only and does not include the header, especially not the subject line. To meet the user's expectation when encrypting a message, some kind of header encryption has to be applied to encrypted e-mails. This way the user is not lulled into a false feeling of security when encrypting e-mails.

## CONCLUSION

We have proposed a new architecture for e-mail filtering system. The proposed bridge-type e-mail proxy screens all packets flowing on network. The packets belonging to e-mail protocols are processed with e-mail filtering process but other protocol packets are just forwarded. The e-mail proxy architecture has several merits over the existing mail filtering techniques. We have implemented the proposed e-mail proxy on an embedded system and a PC. The empirical study done on the implemented email proxies showed that the throughput and bandwidth reduction by the e-mail proxy are not serious at all.

## References

- [1] Jay Chaudhry. "The e-mail battlefield: build a defense," May, 2002 .
- [2] Hal Beghel, Email-The Good, "The Bad, and the Ugly," Communication of ACM, Vol.40, No.4, April 1997.



**Alagappa University, Karaikudi, India**

15<sup>th</sup> -16<sup>th</sup> February 2017

IT Skills Show & International Conference on Advancements in Computing Resources (SSICACR-2017)

<http://aisdau.in/ssicacr>

[ssicacr2017@gmail.com](mailto:ssicacr2017@gmail.com)

- [3] Lorrie Faith Cranor and Brian A LaMacchia, "SPAM!," Communication of ACM, Vol. 41. No.8, August 1998
- [4] Klensin, (2001) 'Simple Mail Transfer Protocol' IETF RFC 2821.
- [5] Mir, F.A., Banday, M.T. (2010). "Control of Spam: A Comparative Approach with special reference to India",.
- [6] Banday, M.T., Qadri, J.A. (2010). "A Study of E-mail Security Protocols,"
- [7] Banday, M.T., Mir, F.A., Qadri, J.A., Shah, N.A. (2011). "Analyzing Internet E-mail Date Spoofing",
- [8] C. E. Landwehr, C. L. Heitmeyer, and J. D. McLean, (2001) "A security model for military message systems: Retrospective," Naval Research Laboratory, Wasgington, DC, 2001
- [9] R. Oppliger, (2004 ) "Certified Mail: the next challenge for secure messaging", Communications of ACM, Vol. 47, No. 8, pp. 75-79.
- [10] Tahir Elgamel, and Kipp E. B. Hipman, (1997) "Secure Socket Layer Application Program Apparatus and Method" U.S. Patent No:5657390.
- [11] P. Hoffman, (2002) "SMTP Service Extension for Secure SMTP over Transport Layer Security", IETF RFC 3207.
- [12] S. Suzuki and M. Nakamura, (2005) "Domain Name System—Past, Present and Future", IEICE Transactions of Communication, E88b (3), pp. 857-864.