Mathematical Problems of Computer Science 46, 50--54 , 2016.

Selection of Methods to Provide End-to-End Email Traffic Security

Arthur S. Petrosyan and Gurgen S. Petrosyan

Institute for Informatics and Automation Problems of NAS RA
e-mail: arthur@sci.am, gurgen@sci.am

Abstract

The goal of the research described in this paper is to select methods of securing Email traffic. While it is known that Email service is not secure by default, both end users and service providers can implement available securing mechanisms to ensure end-to-end Email traffic security as much as possible. Latest developments and research in this area, like SMTP MTA Strict Transport Security (STS) and SMTP TLS Reporting are presented. This paper includes a best practice configuration of protection methods for both Mail User Agent (MUA) and Mail Transfer Agent (MTA). Recommendations given are oriented for the Members of Academic Scientific Research Computer Network of Armenia (ASNET-AM) in regard to secure use of ASNET-AM Email Service.

Keywords: Email, Security, SMTP, MTA, Strict Transport Security, STS, TLS, Mail User Agent, MUA, Mail Transfer Agent, MTA.

1. Introduction

Despite so many other ways of communication today, Email is still one of the widely used and popular ways to exchange information. Since Email is not an online service and is based on a store-and-forward model (Picture 1), implementing end-to-end Email traffic security can be a complex task, depending on several parties to support and implement specific configuration requirements. This includes configuration of both Email Clients, called Mail User Agent (MUA) and Email Servers, called Mail Transfer Agent (MTA). Generally speaking Email security can mean two measures:

1. Connection Security
2. Data Security

This paper is focused on the measures of Connection Security in view of latest developments in this field. Implementing Connection Security for Email means encryption of Email traffic during network transfer.

Email message always originates at MUA and is then transferred to MTA for further delivery via other MTAs to the appropriate user's mailbox, from which the recipient can fetch it using its own MUA. So end-to-end Email traffic security could be achieved only in case all parties use the secure methods of communications. End-to-end Email communication presented in Picture 1 can be divided into two main parts: MUA-MTA communication and MTA-MTA communication.

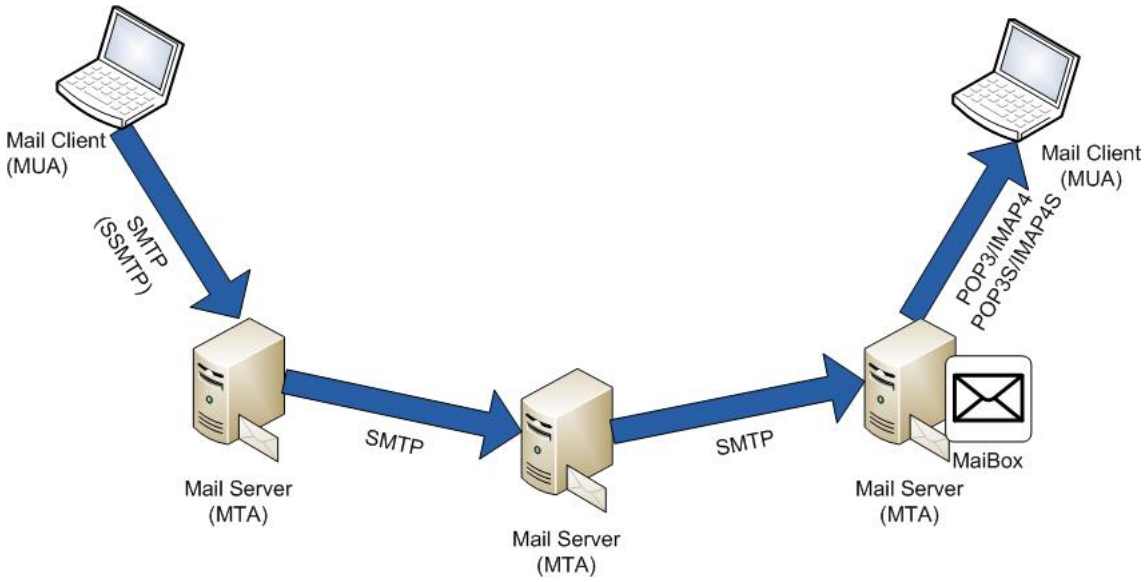

Fig. 1. Email store-and-forward model.

2. MUA-MTA Communication

MUA-MTA connection security means encryption of data during network transfer. For Email it can be implemented in two ways: SSL/TLS and STARTTLS.

Both options provide the same level of connection security but there is some important difference. The "SSL/TLS" method means: "always encrypt connection or don't connect at all". The "STARTTLS" method means: "encrypt connection if both ends support TLS, otherwise connect without encryption". So, STARTTLS can be treated as less secure, because not only can it failback to insecure data transfer without notification, but because it's also subject to Man-in-the-Middle (MitM) attack [1].

STARTTLS as an extension of the SMTP, IMAP and POP3 protocols (SMTPS, IMAPS, POP3S) enables establishing an encrypted connection with the support of the SSL/TLS Protocol without separate special network port for encrypted communication. Although separate ports are registered for the SMTPS, IMAPS and POP3S protocols, the use of standard port enables the usage of both protected and unprotected communication [2].

But that's the issue for users, who use STARTTLS, because by using it, they choose to get Email service work at any price, even sacrificing the connection security for just having their Email work. And that will surely happen if the MTA doesn't provide SSL at least at that time. On the other hand, if users configure MUA to use SSL/TLS method and specify only separate

special network port for encrypted communication for SMTP and IMAP/POP3, then the user can be sure, that at least MUA-MTA connection is encrypted and secure. ASNET-AM Memebers are urged not to use STARTTLS, but use SSL/TLS instead for MUA-MTA connection [3].

3. MTA-MTA Communication

In case of MUA-MTA communication the decision to use encrypted communication can be freely made by the end user (the owner of MUA). But in case of MTA-MTA communication, which is the next step of forwarding the Email message, it is out of the end user control. That part of the chain is to be properly configured by the administrator of MTA.

Unfortunately, today most of MTAs are accepting non-encrypted connections from other MTAs for backward compatibility. It means that currently we can't be sure that our Email traffic passes the Internet securely. As described above for MUA-MTA connection regarding STARTTLS method is also true for MTA-MTA connection. Here also use of STARTTLS can be treated as not reliable and vulnerable to man-in-the-middle (MitM) and encryption downgrade attacks. Thus, STARTTLS for MTA-MTA connection does not guarantee either message confidentiality or proof of server authenticity.

A brief description of the security issue with STARTTLS mechanism follows. When a STARTTLS-enabled MTA wants to establish an SMTP session with another MTA, it first initially asks the remote MTA if it supports SSL or not. And that process is not encrypted. So if an attacker intercepts this unencrypted communication and alters the handshaking process to trick the original MTA into believing that the remote MTA doesn't support encrypted communication, it can trick original MTA to use non-SSL communication, i.e., perform encryption downgrade, even in case the real remote MTA can talk SSL.

Latest developments and research in this area are trying to improve the situation. For example, the new SMTP MTA Strict Transport Security (STS) mechanism is now being actively developed by Google, Yahoo!, Microsoft, LinkedIn and other big companies as an Internet-Draft document [4]. SMTP MTA STS has been designed to enhance the email communication security. This new proposal has been recently submitted to the Internet Engineering Task Force (IETF). The primary goal of SMTP STS is to prevent MitM attacks that have compromised past efforts like STARTTLS at making SMTP a more secure protocol.

The use of SMTP MTA STS would force MTA-MTA communication to be always encrypted.

SMTP MTA STS mechanism will enable administrators of MTAs to:

- declare MTAs ability to receive TLS-secured connections
- declare particular methods for certificate validation
- request that sending MTA report upon
- and/or refuse to deliver messages that cannot be delivered securely.

SMTP MTA STS can protect MTA-MTA communication against MitM attacks. It is designed to rely on certificate validation process via TLS identity checking. The new email security standard will check if recipient MTA supports SMTP MTA STS and has valid and up-to-date encryption certificate published in its DNS zone. If it does successful encrypted MTA-MTA communication will take place and Email traffic will securely pass on. Otherwise, the connection will be dropped and notification about the reason will be generated.

Of course, SMTP MTA STS is an attempt to improve the situation where STARTTLS fails. But since the SMTP MTA STS mechanism is only a draft proposal right now, we need to wait

for it to become usable. But even before that almost any MTA can be configured to strictly use SSL. For example, Postfix MTA has an approptiate option ‘smtpd_tls_security_level’ [5], which can be turned on and set to the value ‘encrypt’. This way administrator of MTA can enforce the use of TLS, so that the Postfix MTA accepts no mail without encryption, by setting "smtpd_tls_security_level = encrypt". Unfortunately, this will bring many problems in a real MTA, because many MTAs are not able to talk SSL today. So much of Email traffic will just be dropped. That is why it is currently not recommended to have such configuration in case of a publicly-referenced MTA [8]. In Postfix MTA default configuration this option is off by default and should only seldom be used.

Example:

```
/etc/postfix/main.cf:
   smtpd_tls_security_level = encrypt
```

4. Conclusion

According to the investigations presented above it becomes clear, that currently there is no way to achieve total end-to-end security of Email traffic. For MUA-MTA communication part Email traffic security currently can be obtained, but it mostly depends on the MUA correct configuration. Best practice configuration discussed above is important to be used, i.e., using strict transport security measures both for incoming and outgoing Email traffic, but avoiding the use of STARTTLS mechanism, to be sure encryption always takes place. ASNET-AM Members are strongly recommended to use only "SSL/TLS" method, when configuring MUAs. For MTA-MTA communication part Email traffic security currently is in the state of development until the SMTP MTA STS mechanism becomes a standard and will be implemented at least by the major parties managing the Email traffic in the Internet. It can be expected then to provide proper end-to-end Email traffic security.

References

[1] RFC4949 - Man-in-the-Middle (MitM) attack. https://tools.ietf.org/html/rfc4949
[2] RFC7435 - Opportunistic Security: Some Protection Most of the Time. [Online]. Available: https://tools.ietf.org/html/rfc7435
[3] A. Petrosyan, E. Prokhorenko and M. Khachatryan, “Securing E-mail Service in ASNET-AM Network”, *Proceedings of the Conference CSIT’2015*, Yerevan, pp. 249-250, 2015.
[4] SMTP MTA Strict Transport Security. Internet-Draft, [Online]. Available: https://tools.ietf.org/html/draft-ietf-uta-mta-sts-01
[5] Enabling TLS in the Postfix SMTP server, . [Online]. Available: http://www.postfix.org/TLS_README.html#server_cert_key

Submitted 04.07.2016, accepted 12.11.2016.

Էլ. փոստի տվյալների ամբողջական հոսքի անվտանգության մեթոդների ընտրություն

Ա. Պետրոսյան և Գ. Պետրոսյան

Ամփոփում

Այս հոդվածում նկարագրված հետազոտության նպատակն է փնտրել այնպիսի մեթոդներ, որոնք կապահովեն էլ. փոստի տվյալների փոխանակման ամբողջական անվտանգությունը: Ինչպես հայտնի է էլ. փոստի ծառայությունն ի սկզբանե անվտանգ չէ: Այդ պատճառով վերջնական օգտագործողները և ծառայությունների մատակարարները կարող են կիրառել հնարավորինս շատ հասանելի էլ. փոստի տվյալների ամբողջական հոսքի անվտանգության ապահովման մեխանիզմներ: Հոդվածում ներկայացված են այդ բնագավառում վերջին մշակումները և հետազոտությունները, ինչպիսիք են՝ SMTP MTA Strict Transport Security (STS) և SMTP TLS Reporting: Այս հոդվածում ներառված են պաշտպանության մեթոդների լավագույն կարգավորումների առաջարկությունները՝ ինչպես Mail User Agent (MUA)-ների, այնպես էլ Mail Transfer Agent (MTA)-ների համար: Առաջարկությունները հիմնականում նախատեսված են Հայաստանի ակադեմիական գիտահետազոտական կոմպյուտերային ցանցի (ASNET-AM) անդամների կողմից էլ. փոստի ծառայությունից անվտանգ օգտվելու համար:

Выбор методов обеспечения безопасности трафика электронной почты «из-конца-в-конец»

А. Петросян и Г. Петросян

Аннотация

Описанные в статье исследования имеют цель поиска способов обеспечения безопасного трафика электронной почты «из-конца-в-конец». Как известно, служба электронной почты не является безопасной по умолчанию, поэтому необходимо, чтобы как конечные пользователи, так и провайдеры почтовых услуг реализовывали как можно больше доступных механизмов защиты обеспечения безопасности трафика электронной почты «из-конца-в-конец». В статье представлены последние разработки и исследования в этой области, такие как SMTP MTA Strict Transport Security (STS) и SMTP TLS Reporting . Статья содержит рекомендации по выбору наилучшей конфигурации методов защиты как Mail User Agent (MUA), так и Mail Transfer Agent (MTA). Рекомендации в основном ориентированы на членов академической научно-исследовательской компьютерной сети Армении (ASNET-AM) для безопасного использования службы электронной почты сети ASNET-AM.