Securing E-mail Service in ASNET-AM Network

Arthur Petrosyan
Institute for Informatics and Automation Problems, NAS RA
Yerevan, Armenia
E-mail: arthur@sci.am

Eugene Prokhorenko
Institute for Informatics and Automation Problems, NAS RA
Yerevan, Armenia
E-mail: eugene@sci.am

Mary Khachatryan
Institute for Informatics and Automation Problems, NAS RA
Yerevan, Armenia
E-mail: mary@sci.am

ABSTRACT

This paper describes the technologies for secure E-mail access in the Academic Scientific Research Computer Network of Armenia (ASNET-AM). The goal is to provide recommendations to ASNET-AM Members to use E-mail service as much securely as possible. Solutions provided are in line with Campus Best Practice (CBP) documents of GÉANT pan-European research and education network.

Keywords

Networking, Email, E-mail, Electronic Mail, Mail Client, Mailserver, Mail Transfer Agent, MTA, Mail User Agent, MUA, Security, PGP, GPG, S/MIME, Encryption, Key, Certificate, Certificate Authority, Man-in-the-Middle attack, MiTM

1. INTRODUCTION

The Academic Scientific Research Computer Network of Armenia (ASNET-AM) is the National Research and Education Network (NREN) of Armenia. Created in 1994 and having over 20 years of experience in Networking and Information Technologies, ASNET-AM [1] provides various networking solutions to the Academic, Scientific, Research, Educational, Cultural and other organizations of Armenia, which are engaged in scientific and educational activity.

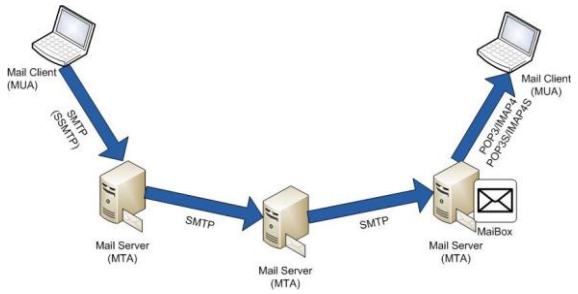
ASNET-AM continuously strives to provide more reliable and secure network services to its members. One of such widely used service is Electronic Mail (E-mail). E-mail service is not secure by default, neither in terms of network connections used, nor in terms of messages data.

Additional steps are required to implement security in E-mail service. In case administrators and users would implement the recommendations described in this paper, E-mail service use will become as much secure as possible.

2. CONNECTION SECURITY

E-mail is not an online service and is based on a store-and-forward model (Picture 1) [2]. It was developed at the time, when Internet was a much smaller place and had to provide simple store-and-forward messaging between people using different kinds of computers. E-mail messages were initially transferred completely in the open way, readable by anyone who could watch network traffic or access accounts. Surprisingly, e-mails sent using those wide-open methods still works.

But today the issue of email security becomes very important and e-mail users should understand potential dangers and know the ways to use e-mail service as much securely as possible.



Picture 1. E-mail store-and-forward model

Following are basic places where most people's e-mail can be compromised:

- on sender's device
- on the networks
- on the servers
- on recipient's device

It's clear from the above that basically e-mail security can mean two measures:

1. connection security
2. data security

Connection security means encryption of data during network transfer. For e-mail it can be implemented in two ways: SSL/TLS and STARTTLS.

Both options provide the same level of connection security. Difference in those methods is as follows. 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 [3].

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, though their use is not recommended, since the use of standard port enables the usage of both protected and unprotected communication [4].

Our opinion is that STARTTLS mostly can be used for data transfer between Mail Transfer Agents (MTA), i.e. mailservers, while SSL/TLS is better to be used between Mail User Agent (MUA), i.e. Mail Client and MTA. The reason is that connection between MTAs need to be expected unsecure for backward compatibility and STARTTLS provides this possibility. Also this means that even if we could use SSL/TLS for MUA-MTA or MTA-MUA connection, we can never be sure that the whole end-to-end data transfer for our e-mail message goes through the encrypted connections. It's because of the nature of e-mail model, which is store-and-forward one, that we can't control the communications between next pairs of MTA-MTA or MTA-MUA.

3. DATA SECURITY

Thus next e-mail security measures can be data security. This can be done by using:

- Secure/Multipurpose Internet Mail Extensions (S/MIME) [5]
- Pretty Good Privacy (PGP), GNU Privacy Guard (GnuPG or GPG) [6] [7]

Both options provide the same level of data security. The use of these methods ensures the protected e-mail exchange, including the authentication of the sender, proof of the integrity of the message and message content encryption. Both end parties in the communication (MUAs) need to use digital certificates [8].

The difference is that using of S/MIME requires digital certificates to be signed by real Certificate Authority (CA), which extends the security and serves to prove the authentication of the sender. On the other way the use of GPG is available at no cost and can be treated as a basic and simple way to securely exchange e-mail messages.

There exist free and open source MUA solutions for any operating system/platform, which enables the use of S/MIME or PGP/GPG.

For Windows/Linux/Mac operating systems **Mozilla Thunderbird** [9] MUA can be used together with **Enigmail** [10] a security extension.

For Mobile devices like smartphones or tablets **K-9 Mail** [11] open-source e-mail client can be used together with **OpenKeychain** [12] a security extension.

For Webmail interfaces like Gmail, Yahoo Mail or corporate webmails there is a very efficient **Mailvelope** [13] solution. It's a JavaScript based Web browser plugin and is supported by most browsers including Google Chrome, Mozilla Firefox, etc. The effect of Mailvelope is that it integrates directly into Webmail user interface and provides true data protection by not allowing an unencrypted message even to reach the webserver (where it can be saved as a draft, etc.).

4. CONCLUSION

E-mail service is truly not secure by default and any user using e-mail, should realize, that no total security can be achieved with e-mail, because any methods described require security measures to be taken at both ends. This is not always possible for every communication and for every recipient. Anyway methods described in this paper allow to use e-mail service as much securely as possible.

REFERENCES

[1] The Academic Scientific Research Computer Network of Armenia (ASNET-AM) http://www.asnet.am

[2] Email – Wikipedia Article
https://en.wikipedia.org/wiki/Email

[3] RFC4949 - Man-in-the-Middle (MiTM) attack.
https://tools.ietf.org/html/rfc4949

[4] RFC7435 - Opportunistic Security: Some Protection Most of the Time. https://tools.ietf.org/html/rfc7435

[5] RFC5751 - Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Message Specification
https://tools.ietf.org/html/rfc5751

[6] RFC4880 - OpenPGP Message Format
https://tools.ietf.org/html/rfc4880

[7] RFC5581 - The Camellia Cipher in OpenPGP
https://tools.ietf.org/html/rfc5581

[8] GÉANT Campus Best Practice Document
- Securing Service Access with Digital Certificates
http://services.geant.net/cbp/Knowledge_Base/Security/Documents/cbp-20_securing-server-access-with-digital-certificates.pdf

[9] Mozilla Thunderbird
https://en.wikipedia.org/wiki/Mozilla_Thunderbird

[10] Enigmail
https://www.enigmail.net

[11] K-9 Mail is an open-source e-mail client
https://play.google.com/store/apps/details?id=com.fsck.k9

[12] OpenKeychain
http://www.openkeychain.org/

[13] Mailvelope
https://www.mailvelope.com/