University of ???

PhD Thesis

Possible solutions to implement email transfer offering anonymity towards third parties

Author:
Martin Gwerder

Supervisor:
unknown

December 13, 2013

Contents

List of Tables

List of Figures

Chapter 1

Introduction

This document describes a solution, which should offer anonymity against third parties when sending emails based on SMTP and the respective client protocols (e.g. IMAPv4 or POP3).

1.1 Overview over the current situation

SMTP as defined in RFC5321[10] is as of today (2013) state of the art transmission protocol for electronic mail. It is standardized in its current version since 2008 and is one of the few protocols, which is marked as "Standard". While the protocol delivers reliable mail transfer between two endpoint (mail servers) the anonymity of the message content towards any mail server is not given (For a detailed analysis see Analysis of current situation).

Anonymity against third party is not given due to the following facts.

- There is not always an encryption available between a mail user agent (MUA) and the outgoing mail server.
- There is no way to guarantee that a mail transfer between two SMTP hosts is encrypted.
- There is no always an encryption available between a SMTP host and the MUA of the recipient.
- Encryption based on top level protocols (such as S/MIME or PGP) do hide the message content. The sender, recipient, the subject and some technical information (eg. MIME-Headers) are always in plain available and not protected as such.

- Even if there is a reliable encryption between all endpoints and none of the intermediate servers are compromised sender and recipients might still be identified thru traffic analysis.

Keeping the message content confidential is more and more relevant in these days. The more the importance of mail transfer in today's economy is growing the more is confidentiality and reliability a topic. Unfortunately Secret Services have already discovered the significance of today's mail traffic and start to analyze those. With the presence of Secret Services in the internet, actively investigating data the importance of a reliable data channel for today's messages has become increasingly important.

Quick wins such as the use of "Onion Router Networks" (such as TOR) do not offer any additional security since the message content would be revealed in full to an eventual exit node and any mail server on its way to the recipient.

1.2 Problem statement

This work is an approach to extend the existing mail routing based on SMTP by an intermediate layer, which should offer anonymity against third party.

This work delivers the following results:

- A throughout analysis of current technology and its weaknesses.
  Although the Simple Mail Transfer Protocol (SMTP) is a well-implemented and well proven technology its weaknesses are well known. The SMTP protocol was originally defined in RFC821[21] by Johnathan B. Postel. At this time internet was only available to universities, some mayor companies and governments. The objective of Simple Mail Transfer Protocol (SMTP) is to transfer mail reliably and efficiently[21, p. 1]. Confidentiality or having a tamper proof protocol was no design goal. Over the years many standards arose trying to close some of the gaps. Most of them are being used but are not very common.

- An analysis of possible approaches to improve the current standards.
  Many standards and technologies do exist these days addressing parts of the issues mentioned above. A throughout research should be carried out to identify how can these technologies be combined to achieve the subsequent goals.

- A RFC document describing an approach offering a significant quality improvement of the existing solutions, which could be accepted by the internet community.

- A prototype reflecting at least the minimum baseline of the RFC document to reflect prove its functionality.
  A prototype should be offered to show the feasibility. The Prototype should be a reference implementation and offer a quick way to use the new technology. It should be distributed under the LGPL license to simplify distribution of the technology.

Chapter 2

Current situation

As of today the de facto standard for asynchronous mail transfer is SMTP as defined in RFC5321[10] and its predecessors. While the transfer protocol SMTP is quite compact, the protocol is enhanced with several standards for encryption, multimedia support and similar. A mail client offers today various support for a lot of sub-protocols. The following list is an excerpt of related sub-protocols which are either related to transport, reliability, identification or encryption.

2.1 Implemented protocols

2.1.1 SMTP

[10]

2.1.1.1 Mail transport

[11]

2.1.1.2 encryption

2.1.2 MIME

[4] [5] [6] [7] [8]

2.1.3 S/MIME

[23]

2.1.4 PGP

[22]

2.1.5 Sender Policy Framework

[27] [9]

2.1.6 Sender ID

[26]

2.1.7 DNS

[3]

2.1.7.1 DNSSEC

[12]

2.1.8 Transport Protocols

2.1.8.1 IPv4

[20] [17] [25] [18] [15] [13] [14] [19, p. 3]

2.1.8.2 IPv6

[2]

2.1.8.3 TCP

2.1.9 POP3

[16]

2.1.10 IMAPv4

[1]

2.2 Ground theory

2.2.1 Anonymity

2.2.2 Identification (data signage)

2.2.3 Encryption

2.2.4 Mix cascades

2.3 Other

2.3.1 Ethics of the Internet

[24, p. 1]

2.3.2 Possible legal issues

Chapter 3

Analysis of current situation

3.1 Current state of common Technology

3.2 Current state of available Technology

3.3 Missing Gap

3.4 Skeleton of Mails and mail transfer

Chapter 4

Designing an approach

4.1 Defining system boundaries

4.2 Basic Requirements of an approach

Chapter 5

Specifying a target solution

Chapter 6

Analysis of solution

6.1 User acceptance of the target system

From a perspective of a user Collected requirements to a mail system:

Requirement	cliteria	Weight
The System should transport mails fast under normal conditions	Mails should travel with at least 1MB/min	5
The System should transport mails reliable	Mails should always arrive or their status should be retrievable	9
The System should offer anonymity against spying from third parties	Neither original sender nor final destination or any part of the message content should be determinable by any part of the system except for the original sender and the final recipient.	9
The system must be easy to handle		8
The system must be easy to install	Installation should be almost a “single-click”-Thing. Details should be copied or accessed from the existing configurations.	5
continued on next page		

continued from previous page		
Requirement	cliteria	Weight

Table 6.1: User acceptance requirements

6.2 Admin acceptance of the target system

Collected requirements to a mail system from an admin perspective:

Requirement	Criteria	weight
The System should transport mails fast under normal conditions	Mails should travel with at least 10MB/min	5
The System should transport mails reliable	Mails should always arrive or their status should be retrievable	9

6.3 Possible attacks to the system

6.3.1 Generic DoS attacks

6.3.2 Attacks on the users anonymity

6.3.3 Reputaional attacks

6.3.3.1 Misuse for sending spam

Definitions

MUA A Mail User Agent. This user agent reads mails from a local storage and allows a user to read existing mails, create and modify mails.

Local MTA A local Mail Transfer Agent. This transfer agent reads mails to be sent to a remote account from a local storage and sends it to a MSA.

MSA A local Mail Sending Agent. This agent accepts mails to be sent to a remote MTA.

Bibliography

[1] M. Crispin. *RFC3501 INTERNET MESSAGE ACCESS PROTOCOL - VERSION 4rev1*. 2003. URL: http://tools.ietf.org/pdf/rfc3501.pdf (cit. on p. 6).

[2] S. Deering and R. Hinden. *RFC2460 Internet Protocol, Version 6 (IPv6) Specification*. 1983. URL: http://tools.ietf.org/pdf/rfc2460.pdf (cit. on p. 6).

[3] D. Eastlake, E. Brunner-Williams, and B. Manning. *BCP42 Domain Name System (DNS) IANA Considerations*. 2000. URL: http://tools.ietf.org/pdf/rfc2929.pdf (cit. on p. 6).

[4] N. Freed and N. Borenstein. *RFC2045 Multipurpose Internet Mail Extensions; (MIME) Part One: Format of Internet Message Bodies*. 1996. URL: http://tools.ietf.org/pdf/rfc2045.pdf (cit. on p. 5).

[5] N. Freed and N. Borenstein. *RFC2046 Multipurpose Internet Mail Extensions; (MIME) Part Two: Media Types*. 1996. URL: http://tools.ietf.org/pdf/rfc2046.pdf (cit. on p. 5).

[6] N. Freed and N. Borenstein. *RFC2047 Multipurpose Internet Mail Extensions; (MIME) Part Three: Message Header Extensions for Non-ASCII Text*. 1996. URL: http://tools.ietf.org/pdf/rfc2046.pdf (cit. on p. 5).

[7] N. Freed, J. Klensin, and J. Postel. *RFC2048 Multipurpose Internet Mail Extensions; (MIME) Part Four: Registration Procedures*. 1996. URL: http://tools.ietf.org/pdf/rfc2048.pdf (cit. on p. 5).

[8] N. Freed, J. Klensin, and J. Postel. *RFC2049 Multipurpose Internet Mail Extensions; (MIME) Part Five: Conformance Criteria and Examples*. 1996. URL: http://tools.ietf.org/pdf/rfc2049.pdf (cit. on p. 5).

[9] S. Kitterman. *RFC6652 Sender Policy Framework (SPF) Authentication Failure Reporting Using the Abuse Reporting Format*. 2012. URL: http://tools.ietf.org/pdf/rfc6652.pdf (cit. on p. 6).

[10] J. Klensin. *RFC5321 Simple Mail Transfer Protocol*. 2008. URL: http://tools.ietf.org/pdf/rfc5321.pdf (cit. on pp. 1, 5).

[11] J. Klensin, N. Freed, and K. Moore. *RFC1870 SMTP Service Extension for Message Size Declaration*. 1995. URL: http://tools.ietf.org/pdf/rfc1870.pdf (cit. on p. 5).

[12] B. Laurie, G. Sisson, R. Arends, and D. Blacka. *RFC5155 DNS Security (DNSSEC) Hashed Authenticated Denial of Existence*. 2008. URL: http://tools.ietf.org/pdf/rfc5155.pdf (cit. on p. 6).

[13] J. Mogul. *RFC922 BROADCASTING INTERNET DATAGRAMS IN THE PRESENCE OF SUBNETS*. 1984. URL: http://tools.ietf.org/pdf/rfc922.pdf (cit. on p. 6).

[14] J. Mogul and J. Postel. *RFC950 Internet Standard Subnetting Procedure*. 1985. URL: http://tools.ietf.org/pdf/rfc950.pdf (cit. on p. 6).

[15] Jeffrey Mogul. *RFC919 BROADCASTING INTERNET DATAGRAMS*. 1984. URL: http://tools.ietf.org/pdf/rfc919.pdf (cit. on p. 6).

[16] J. Myers and M. Rose. *RFC1939 Post Office Protocol - Version 3*. 1996. URL: http://tools.ietf.org/pdf/rfc1939.pdf (cit. on p. 6).

[17] J. Postel. *RFC791 INTERNET PROTOCOL DARPA INTERNET PROGRAM PROTOCOL SPECIFICATION*. 1981. URL: http://tools.ietf.org/pdf/rfc791.pdf (cit. on p. 6).

[18] J. Postel. *RFC792 INTERNET CONTROL MESSAGE PROTOCOL DARPA INTERNET PROGRAM PROTOCOL SPECIFICATION*. 1981. URL: http://tools.ietf.org/pdf/rfc792.pdf (cit. on p. 6).

[19] J. Postel. *RFC793 TRANSMISSION CONTROL PROTOCOL DARPA INTERNET PROGRAM PROTOCOL SPECIFICATION*. 1981. URL: http://tools.ietf.org/pdf/rfc793.pdf (cit. on p. 6).

[20] Jon Postel. *RFC760 DOD STANDARD INTERNET PROTOCOL*. 1980. URL: http://tools.ietf.org/pdf/rfc760.pdf (cit. on p. 6).

[21] Jonathan B. Postel. *RFC821 Simple Mail Transfer Protocol*. 1982. URL: http://tools.ietf.org/pdf/rfc821.pdf (cit. on p. 2).

[22] B. Ramsdell. *RFC2440 Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1 Message Specification*. 2004. URL: http://tools.ietf.org/pdf/rfc2440.pdf (cit. on p. 6).

[23] B. Ramsdell. *RFC3851 Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1 Message Specification*. 2004. URL: http://tools.ietf.org/pdf/rfc3851.pdf (cit. on p. 5).

[24] *RFC1087 Ethics and the Internet*. Internet Activities Board, 1989. URL: http://tools.ietf.org/pdf/rfc1087.pdf (cit. on p. 7).

[25] T. Socolofsky and C. Kale. *RFC1180 A TCP/IP Tutorial*. 1991. URL: http://tools.ietf.org/pdf/rfc1180.pdf (cit. on p. 6).

[26] N. Williams. *RFC4401 Sender ID: Authenticating E-Mail*. 2006. URL: http://tools.ietf.org/pdf/rfc4401.pdf (cit. on p. 6).

[27] N. Williams. *RFC4408 Sender Policy Framework (SPF) for Authorizing Use of Domains in E-Mail, Version 1*. 2006. URL: http://tools.ietf.org/pdf/rfc4408.pdf (cit. on p. 6).