# Possible solutions to implement email transfer offering anonymity towards third parties

Martin Gwerder

Dezemer 2013

# Contents

# 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[2] 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.

1. There is not always an encryption available between a mail user agent (MUA) and the outgoing mail server.

2. There is no way to guarantee that a mail is being transferred encrypted between SMTP hosts.

3. There is no always an encryption available between a SMTP host and the MUA of the recipient.

4. 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.

5. 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 todays economy is growing the more is confidentiality and reliability a topic. Unfortunatley 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[8] 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[8, 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[2] and its predecessors. While the transfer protocol SMTP is quite compact, the protocol is enhanced with serveral 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

[2]

#### 2.1.1.1 Mail transport

[**RFC1870**]

#### 2.1.1.2 encryption

### 2.1.2 MIME

[5] [6] [7] [3] [4]

### 2.1.3 S/MIME

[10]

### 2.1.4  PGP

[9]

### 2.1.5  Sender Policy Framework

[12] [1]

### 2.1.6  Sender ID

[11]

### 2.1.7  DNS

#### 2.1.7.1  DNSSEC

### 2.1.8  Transport Protocols

#### 2.1.8.1  IPv4

[**RFC760**] [**RFC791**] [**RFC1180**] [**RFC792**] [**RFC919**] [**RFC922**] [**RFC950**] [**RFC793**]

#### 2.1.8.2  IPv6

[**RFC2460**]

#### 2.1.8.3  TCP

### 2.1.9  POP3

[**RFC1939**]

### 2.1.10  IMAPv4

[**RFC3501**]

## 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

[**RFC1087**]

# Chapter 3

# Analysis of current situation

## 3.1 Current state of common Technology

## 3.2 Current state of available Technology

## 3.3 Missing Gap

# Chapter 4

# Designing an approach

## 4.1 Defining system boundaries

## 4.2 Basic Requirements of an aproach

# Chapter 5

# Specifying a target solution

# Chapter 6

# Analysis of solution

## 6.1 User acceptance of the target system

## 6.2 Admin acceptance of the target system

## 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

# Appendix A

# Definitions

**MUA** A Mail User Agent

# Bibliography

[1]  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. 10).

[2]  J. Klensin. *RFC5321 Simple Mail Transfer Protocol*. 2008. URL: `http://tools.ietf.org/pdf/rfc5321.pdf` (cit. on pp. 5, 9).

[3]  J. Postel N. Freed J. Klensin. *RFC2048 Multipurpose Internet Mail Extensions; (MIME) Part Four: Registration Procedures*. 1996. URL: `http://tools.ietf.org/pdf/rfc2048.pdf` (cit. on p. 9).

[4]  J. Postel N. Freed J. Klensin. *RFC2049 Multipurpose Internet Mail Extensions; (MIME) Part Five: Conformance Criteria and Examples*. 1996. URL: `http://tools.ietf.org/pdf/rfc2049.pdf` (cit. on p. 9).

[5]  N. Borenstein N. Freed. *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. 9).

[6]  N. Borenstein N. Freed. *RFC2046 Multipurpose Internet Mail Extensions; (MIME) Part Two: Media Types*. 1996. URL: `http://tools.ietf.org/pdf/rfc2046.pdf` (cit. on p. 9).

[7]  N. Borenstein N. Freed. *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. 9).

[8]  Jonathan B. Postel. *RFC821 Simple Mail Transfer Protocol*. 1982. URL: `http://tools.ietf.org/pdf/rfc821.pdf` (cit. on p. 6).

[9]  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. 10).

[10] 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. 9).

[11] N. Williams. *RFC4401 Sender ID: Authenticating E-Mail*. 2006. URL: `http://tools.ietf.org/pdf/rfc4401.pdf` (cit. on p. 10).

[12]   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. 10).