The Cipher Mail Transport Protocol Interface

Jonathan Moroney

February 17, 2016

Contents

1 High level overview **1**

2 Deep Dive **2**
2.1 OHAI 2
2.2 MAIL 2
2.3 KEYREQUEST <USER> <DOMAIN> 2
2.4 NOOP 2
2.5 LOGIN <USER> 2
2.6 HELP 2

1 High level overview

The Cipher Mail Transport Protocol (CMTP) uses a text based, command/reply interface similar to that of the Simple Mail Transport Protocol (SMTP). The commands for CMTP have been designed to make stateless implementation easy. All commands are ASCII strings terminated by a line feed (\n). ASCII is used over utf-8 for commands as each ASCII character corresponds to one byte.

OHAI

This command is used to identify a CMTP client to a CMTP server. This is the CMTP analog to SMTPs HELO/EHLO though there are no parameters that follow.

MAIL

This command is used to initiate a mail transfer. After the command is issued the CMTP server should expect a self describing CMTP message to follow and should reply after it has been received.

KEYREQUEST <USER> <DOMAIN>

This command is used to request a public key for some user on some domain. The parameters USER and DOMAIN are null terminated.

NOOP
: This command does nothing but prompt a reply from the CMTP server.

LOGIN <USER>
: This command is used to initiate a user login.

HELP
: This command is used by users that need to RTFM.

OBAI
: This command is used to terminate a connection.

2 Deep Dive

2.1 OHAI

The OHAI command is in place to prevent SMTP clients from seeing a CMTP server as a valid SMTP server. Conveniently OHAI is four characters long which should mean even the oldest SMTP client should fail in a defined way when attempting to connect to a CMTP server.

2.2 MAIL

The MAIL command is a stand alone command which servers only to tell the CMTP server that a message is to follow. The CMTP message is self describing in length so that a server knows when it has received the entire thing. Subsequently no state is needed in order to pass a message.

2.3 KEYREQUEST <USER> <DOMAIN>

UNDER CONSTRUCTION

2.4 NOOP

The NOOP command exists because SMTP has a NOOP command. This may be removed if a better reason for existence cannot be found.

2.5 LOGIN <USER>

UNDER CONSTRUCTION

2.6 HELP

The help command exists because people will be dumb given the chance and in that inevitability the help command is here to... help.