The Cipher Mail Transport Protocol Interface

Jonathan Moroney

February 22, 2016

Contents

1 Command 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 null character (\0). ASCII is used over utf-8 for commands as each ASCII character corresponds to one byte.

1.1 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.

1.2 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.

1.3 KEYREQUEST <USER> <DOMAIN>

The KEYREQUEST command takes at least one parameter and at most two. The user parameter is required while the domain parameter is not. Each parameter is null terminated. In the case that the domain parameter is not present the CMTP server should assume that the user is local to it. The reply format is
[Version][UserPublicKey][\0][ServerSigOfKey][\0].
Errors and messages use a similar reply format but with the Version = 0 which corresponds to the plaintext crypto case
[Version][Message][\0][ServerSigOfMessage][\0].
In this way delays and 'no key' messages can be passed back to the client.

1.4 NOOP

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

1.5 LOGIN <USER>

The LOGIN command takes one parameter and returns an encrypted copy of the users private key along with a clear text message which the server expects the user to sign and return. The private key is encrypted with a symmetric cipher and so signing the clear text message is sufficient to verify a user login. The message can be randomly generated on each login attempt to prevent replay attacks.

1.6 HELP

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

1.7 OBAI

The OBAI command is in place to terminate a connection. Connections may terminate for other reasons (time outs, tcp connection breaking, etc...), but OBAI allows for a graceful exit.