The Cipher Mail Transport Protocol Design

Jonathan Moroney

March 3, 2016

1 Design

1.1 Interface

The cipher mail transport protocol (CMTP) is designed to be a simple mail transport protocol (SMTP) replacement and to use much of the existing infrastructure used by SMTP. CMTP is not meant to be a high security system, but rather as a way to raise the security of email without interfering with how email works (from a user perspective) With regard to infrastructure CMTP server discovery is done through Domain Name System (DNS) queries for mail exchange (MX) records. Using MX records solves the problem of finding servers on the internet to process messages and makes the process of searching much easier. However, there are many SMTP clients on the internet and eventually there will be a connection attempt from an SMTP client to a CMTP server. This cross talk issue imposes an immediate constraint on CMTP in that it should speak a familiar language and given that SMTP has an ASCII command set so too does CMTP. The CMTP commands are described in the interface document, but it's worth stating here that the choice of the initiation command 'OHAI' was chosen for

1. 'OHAI' is a four character string and thus compatible with the earliest versions of SMTP. As such any SMTP client/server should fail in a defined way when speaking to a CMTP server/client.

2. 'OHAI' is a greeting and is consistent with 'HELO' from SMTP and 'ELHO' from ESMTP.

3. 'OHAI' makes me smile and I hope it makes you smile too.

1.2 Network

CMTP is designed to be an open network. That is actors (Servers and users) are free to enter and exit at will. There is no central authority nor is there a system of communicating entry or exit from the network. This is like SMTP where any organization can set up their own server and communicate with

the likes of google, microsoft, apple, etc... The ability of the small to be on equal footing with the large is of personal importance and is reflected here.

1.3 Keys

The crux of any crypto system is to manage keys and CMTP handles this in the context of an open network with end users in mind. As such CMTP does not provide authentication for keys, but does provide a transparent key distribution system. Users are able to search for a retrieve the public keys of others without even being aware of the keys. This is facilitated by the KEYREQUEST command which takes two parameters (User and domain) and returns a public key. The domain's CMTP server is found through DNS and the request is made to the holder of the MX record. If you're aware of man in the middle attacks this may sound like a terrible idea, but recall that CMTP is only aims to be confidential and not authenticated. Should DNS ever become an authenticated protocol CMTP will reap the benefits of authentication as well.