Thesis outline

Jonathan Moroney

March 17, 2016

Contents

Abstract

Abstract.

1 Introduction

1.1 The state of the pipes

1.2 Problem statement and motivation

1.3 Modern email

1.4 Constraints and goals of my work (Usability!)

2 Related work

2.1 OpenPGP

2.2 SMTP over TLS

2.3 Darkmail

2.4 Cryptocat, Telegram, and others

3 The Cipher Mail Transport Protocol

3.1 Network design and reuse of DNS MX records

3.2 Xzibit Key System

3.3 The Man in the Middle problem. Design limitations

3.4 The CMTP interface

3.5 The CMTP message

3.6 Crypto system 0

3.7 Crypto system 1

4 Reference Implementation

4.1 cmtpd

4.2 Shorebird (client program)

5 Analysis

6 Conclusion

7 Future Work

A cmtpd user guide

B Shorebird user guide