Extremely Sensitive Communication Secure, Secret, and Private e-mail

Loek Sangers

UvA
KPMG

June 30, 2016

Research Questions

How can e-mail communication be changed to provide a trusted (secure, secret, and private) way of communication?

1. What are the requirements for secure, secret, and private e-mail?
2. What are the gaps in currently available solutions with regard to these requirements?
3. What system architecture enhancements can be provided to these solutions to fill these gaps?
4. What is the feasibility of implementing these system architecture enhancements?

Motivation

- Private communication
- SMTP not build for it
- State surveillance
- Existing solutions don't provide enough
  - StartTLS
  - OpenPGP
  - S/MIME

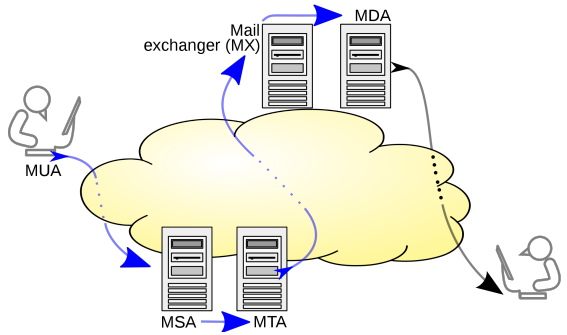
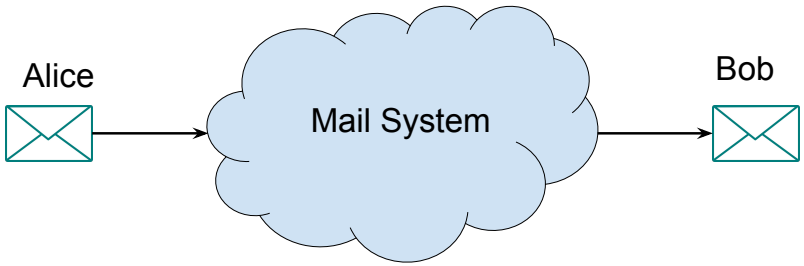


Figure 1: SMTP

Definitions

- Secure: Unreadable for anyone but sender and recipient
- Secret: Unknown that a message is submitted or retrieved by a specific user
- Private: Only two entities that know who both the sender and recipient are, are exactly those two



Requirements

- Secure
  - End-to-End Encryption
  - Perfect Forward Secrecy
- Secret
  - Purpose of traffic
  - Origin of traffic
- Private
  - Meta-data
  - Protected against compromised servers
  - Spam
  - Discoverable servers

Available Systems - Secure

- Requirements:
  - End-to-End Encryption
  - Perfect Forward Secrecy
- Client software
  - OpenPGP
  - S/MIME
  - opmsg
- Key validation
  - Certificate Authorities
  - Web of trust
- Key distribution
  - Out of band
  - Publishing

Available Systems - Secret

- Requirements:
  - Purpose of traffic
  - Origin of traffic
- Multi-purpose connection
  - HTTPS
  - VPN
- Anonymizing overlay network
  - Tor
  - I2P

Available Systems - Private

- Requirements:
  - Meta-data
  - Protected against compromised servers
  - Spam
  - Discoverable servers
- Anonymous remailers
  - Cypherpunk
  - Mixmaster
  - Mixminion
- Mix network
- Spam protection by opt-out
- Signatures

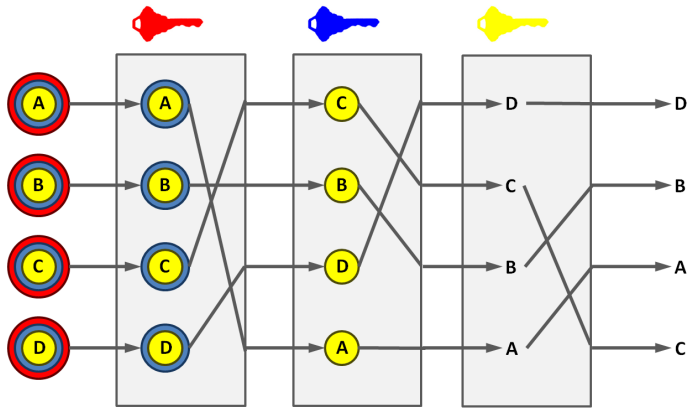


Figure 3: Mix Network

Solutions - Secure

- New key distribution system
  - Scalability
  - Perfect forward secrecy
- Including keys in messages
- Already being developed

Solutions - Secret

- Anonymizing overlay networks
  - Already exist
  - Could use broader adoption
- Multi-purpose connections
  - Already exist
  - Target server needs multiple purposes

Solutions - Private

- New Mix type
  - Multi-Binomial Shared Pool
  - Multi-Binomial Independent Pool
- Hash of content
- Server key rollover
- Spam
  - Signatures, both server and client
  - Expected format
  - Flagging spam senders in key distribution system
- Server discovery system

Proposed System - Message Content

1. Unencrypted message (fixed size)
2. Signed by Sender
3. Encrypted for Recipient
4. Signed with public key of Recipient
5. Encrypted for each server

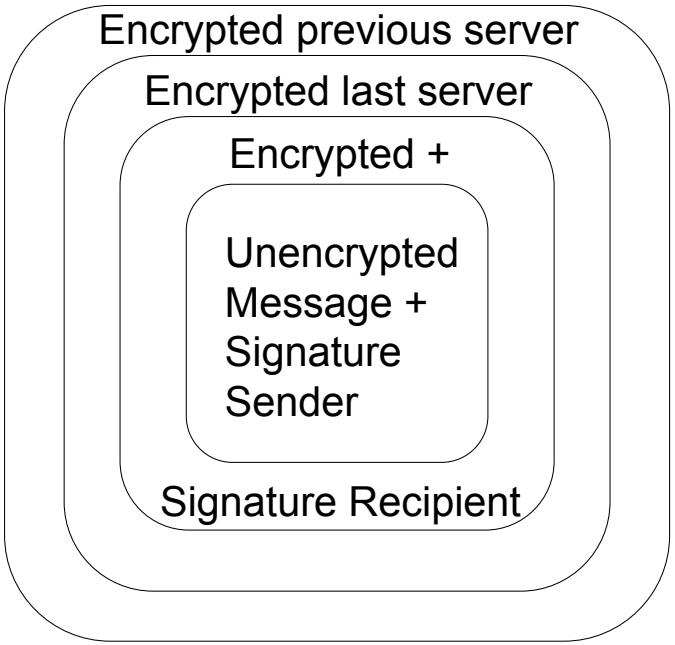


Figure 4: Content Encryption

Proposed System - Message Headers

- Fixed number of entries, each contains:
  - Address of next hop
  - Hash of content
  - Decryption key
- Entries moved up after being used
- Random entry appended at the end

Conclusion

- Secure, Secret, and Private e-mail is possible, but:
  - Key distribution system
  - Mail server discovery system
  - Client side software (stand-alone or browser plugin)
- Public adoption important
  - Profitable for companies
  - Demanded by public

Summary

- Requirements
- Available Systems
- Solutions
- Proposed System

Questions?

Use Cases

- Individuals
- Companies

Summary

- Requirements
- Available Systems
- Solutions
- Proposed System

Questions?

Resources

- Figure 1: "https://en.wikipedia.org/wiki/Simple_Mail_Transfer_Protocol#/media/File:SMTP-transfer-model.svg"
- Figure 3: "https://en.wikipedia.org/wiki/File:Decryption_mix_net.png"