Chair of Network Architectures and Services
Department of Informatics
Technical University of Munich

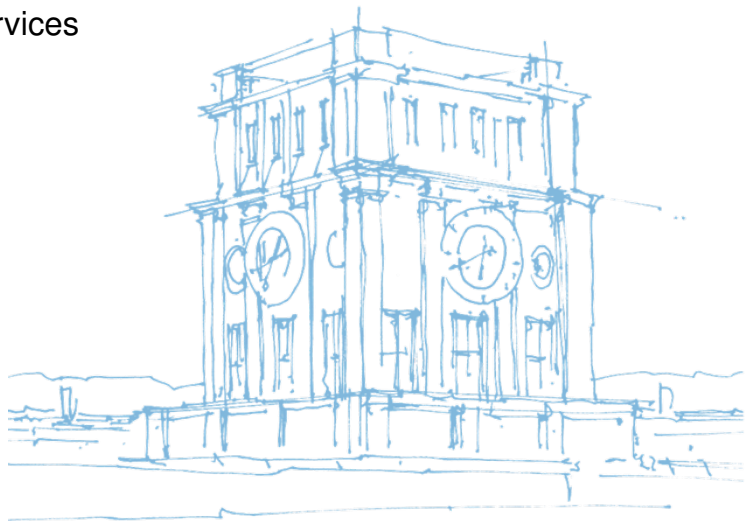
Automated Key Management for End-To-End Encrypted Email Communication

Final talk for the Guided Research by

Thomas Maier
advised by Benjamin Hof

Wednesday 4th April, 2018

Chair of Network Architectures and Services
Department of Informatics
Technical University of Munich



Agenda

Introduction

Related Work

Problem Analysis

Protocol Design

Evaluation

Future Work

Conclusions

Introduction

Problem & Motivation:

- Secure end-to-end email encryption is difficult to handle for end users [1, 2, 3].
- Usability issues $\Rightarrow$ Security problems
- One of the major impediments is the key exchange between end users
  $\Rightarrow$ Inability to ...
  - send and receive public keys
  - verify keys and signatures

Research Question:

How is it possible to automatically exchange authenticated public keys in order to make end-to-end encrypted mailing more usable?

Solution:

- Automated key exchange between end-users
- Implicit guarantee of authenticity
  (guaranteed mapping *key* $\rightarrow$ *user*)

Related Work

Solutions for Usable End-To-End Encryption

(Various solutions ⇒ Categorization necessary)

- Transparency frameworks
  - Certificate Transparency, CONIKS, Key Transparency
  - No authentication, but monitoring after publication
- Key servers
  - No authentication (e.g., HTTP KeyServer Protocol) ...
  - ... or an additional service handles credentials (e.g., Web Key Directory)
- Manual key verification and Web of Trust:
  - OpenPGP, p≡p (pretty Easy Privacy)
  - Secure channel necessary, bad usability [1, 2, 3]
- Mail provider approaches
  - Public Key Upload and Retrieval: DNS or isolated application
  - Assisting in Encryption: Usage of browser add-ons or proprietary implementations
  - Service Discovery: DNS or manual
  - Deployment Distribution: Isolated applications
- Client-side approach (Mailpile): Trust on First Use
- Guidelines (autocrypt): Protection against passive attacks only

Problem Analysis

Derivation of Addressed Problems from Related Work

Related Work $\Rightarrow$ Addressed Problems:

- Trust establishment
- Adoption and deployment
- Key authenticity and integrity
- Service discovery

Protocol Design

Proposed Solution

Two required workflows for key exchange:

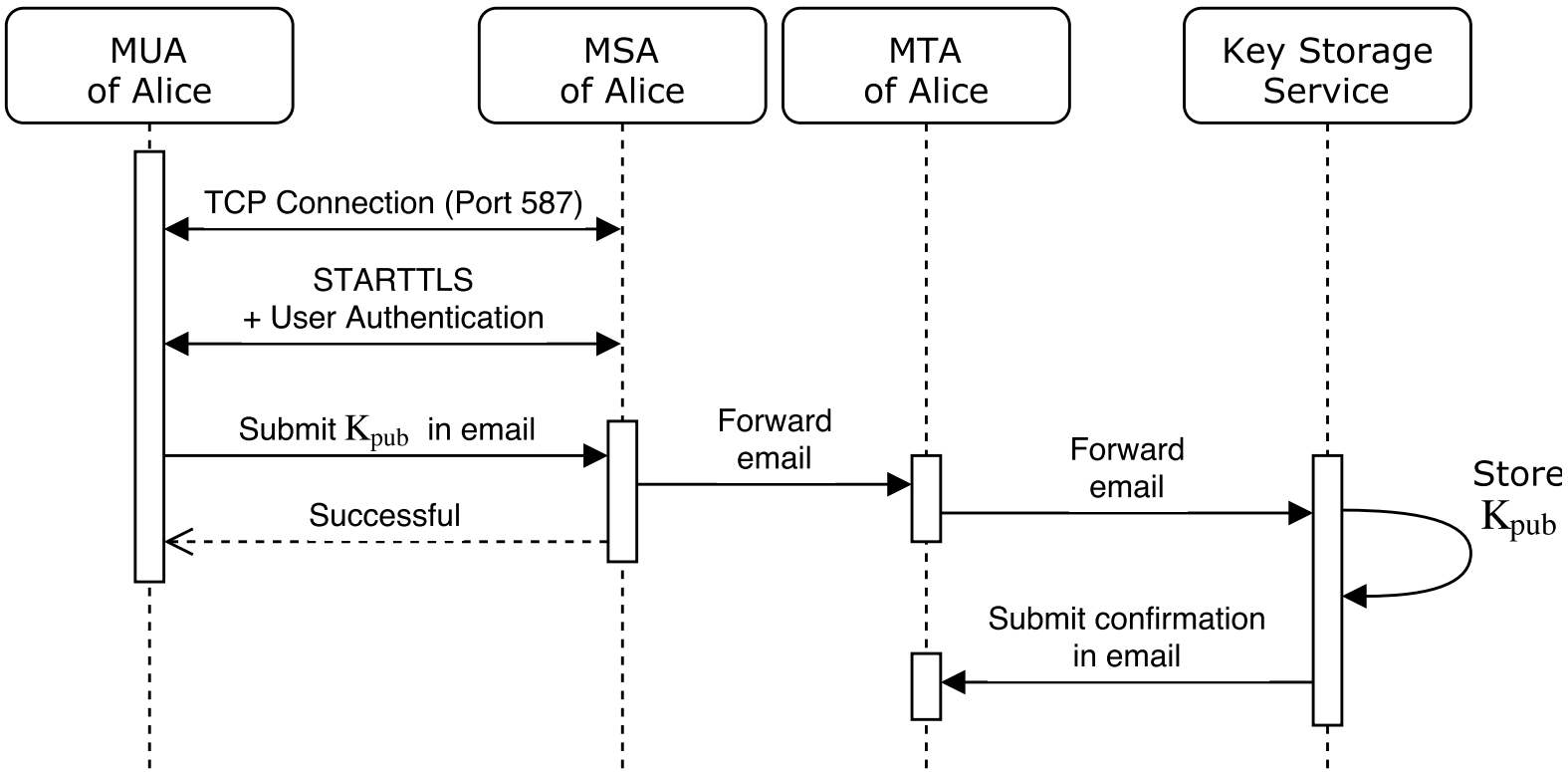
- Publication of a key K_{pub}
- Retrieval of a key K_{pub}

Addressed problems $\Rightarrow$ Design goals:

- Trust establishment
  $\Rightarrow$ Putting trust in mail provider
- Adoption and deployment
  $\Rightarrow$ Low costs (simple implementation and maintenance)
  $\Rightarrow$ High scalability (little amount of emails)
- Key authenticity and integrity
  $\Rightarrow$ Cryptographic verification
- Service discovery
  $\Rightarrow$ DNS lookups (`MX` records)

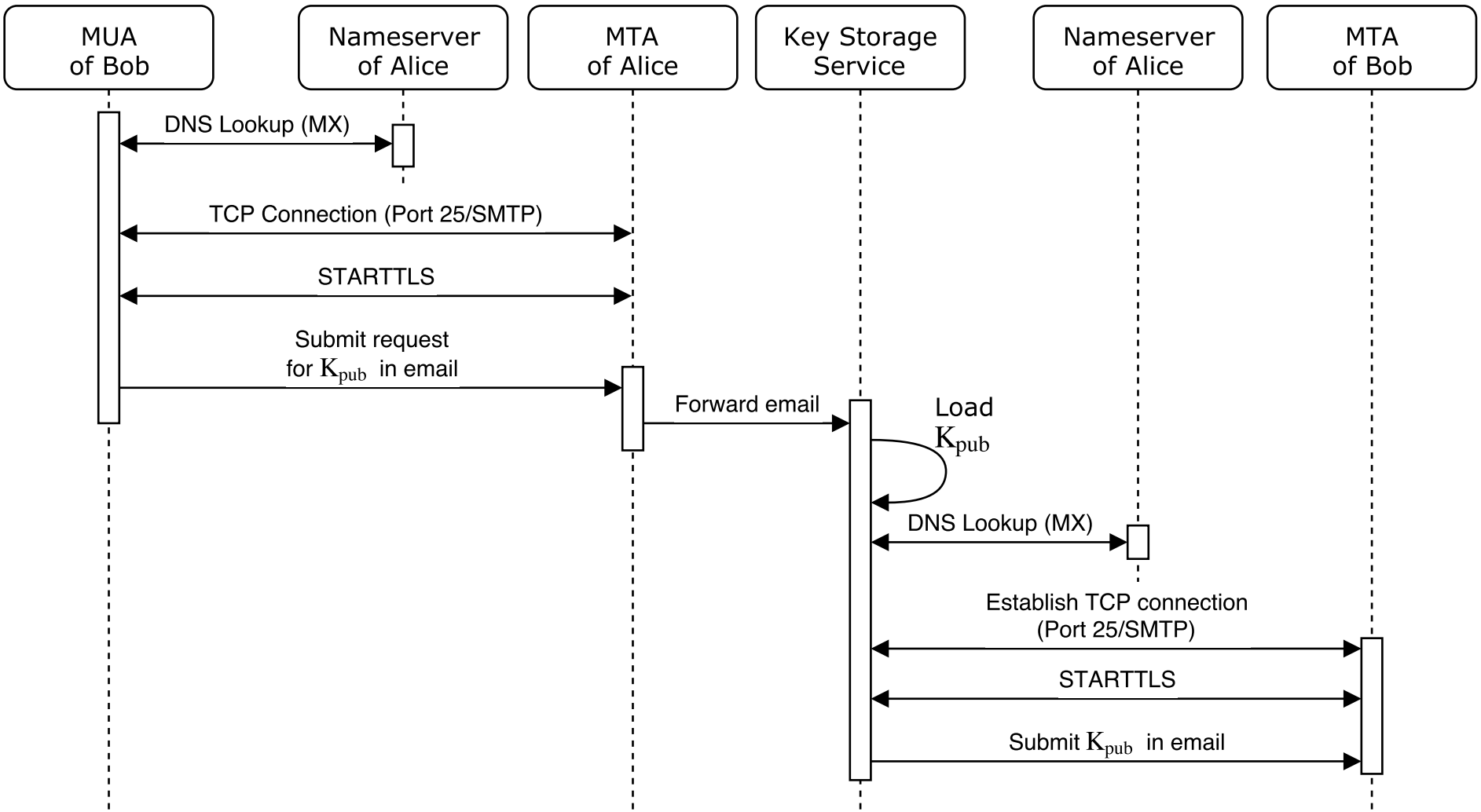
Protocol Design

Key Publication Protocol



Protocol Design

Key Retrieval Protocol



Evaluation

- Prove of Concept: Practical Implementation
- Design goals and implementation
  - Trust establishment with mail provider
  - Adoption and deployment: Low costs, high scalability
  - Key authenticity and integrity: Cryptographic verification
  - Service discovery with DNS
- Key revocation and expiration
- Complementary protocols

Future Work

- Security issues with DNS: *DNSSEC* or *DNS over TLS*
- Replacement of cryptographic primitives
- Key synchronization between servers
- Blocked email traffic (port 25)

Conclusions

- Many existing solutions
- Approach: Related Work $\Rightarrow$ Addressed Problems $\Rightarrow$ Design Goals
- Two workflows to automate key exchange for end-to-end encrypted mailing
- Trust in mail provider
- Usage of existing mailing infrastructure $\Rightarrow$ Simple deployment
- Prevention of passive and active attacks

Bibliography

[1] S. Ruoti, J. Andersen, D. Zappala, and K. Seamons.
Why Johnny Still, Still Can't Encrypt: Evaluating the Usability of a Modern PGP Client.
arXiv:1510.08555 [cs], Oct. 2015.
arXiv: 1510.08555.

[2] S. Sheng, L. Broderick, J. J Hyland, and C. Alison Koranda.
Why Johnny Still Can't Encrypt: Evaluating the Usability of Email Encryption Software.
ACM - Proceedings of the second symposium on Usable privacy and security, Nov. 2017.

[3] A. Whitten and J. D. Tygar.
Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0.
In *Proceedings of the 8th Conference on USENIX Security Symposium - Volume 8*, SSYM'99, pages 14–14, Berkeley, CA, USA, 1999. USENIX Association.