NTNU
Norwegian University of
Science and Technology

Challenges in End-to-End Encrypted Group Messaging

Tjerand Silde

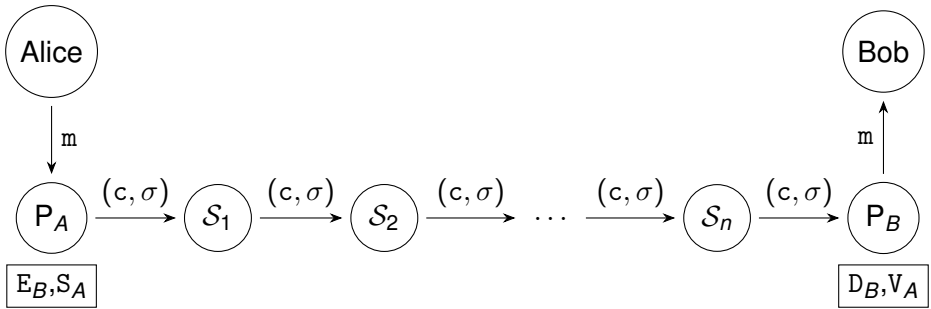
This Work

"Where the Rubber Meets the Road" = Implementing Group Messaging in Practice

- Minimal Requirement: End-to-End Encryption
- Analyze: Challenges, Treadeoffs and Features
- Document: Applications Used in Practice:

  Signal, Whatsapp, Wire, Keybase, Threema, Crypho,...
- Compare with Messaging Layer Security Standardization Effort.
- Study the Design, not the Code.

End-to-End Encryption for Alice and Bob



Authenticated Key Exchange doesn’t mean Authenticated Parties

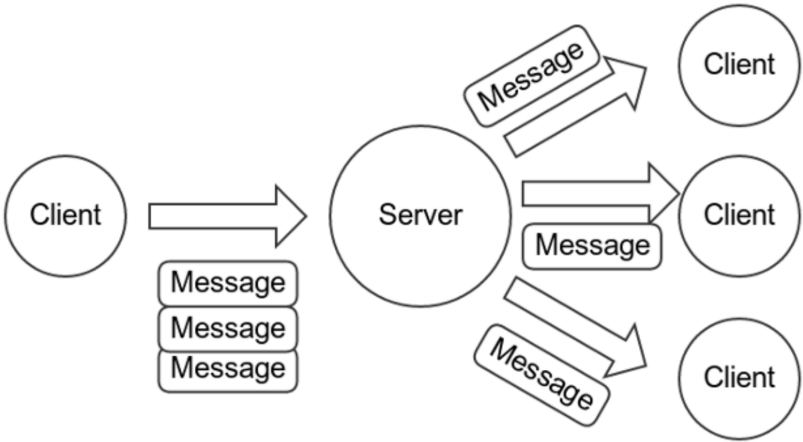
Scott Hanselman

@shanselman

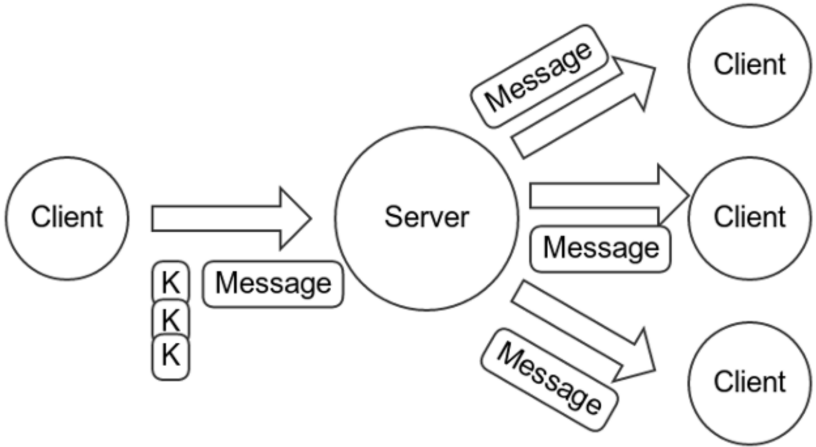
Follow

HTTPS & SSL doesn't mean "trust this." It means "this is private." You may be having a private conversation with Satan.

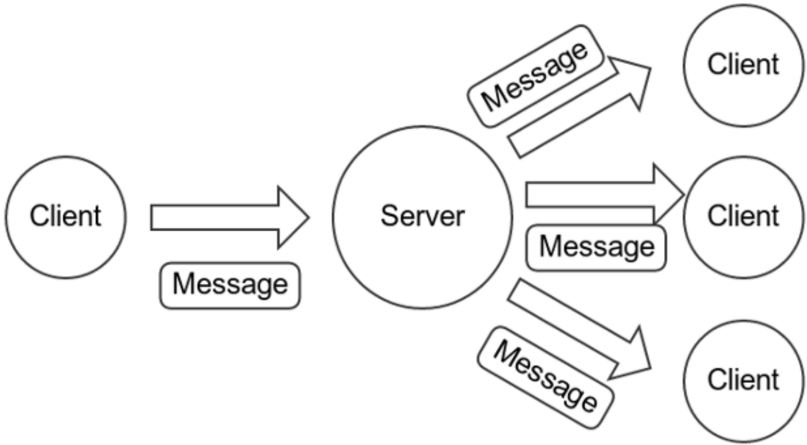
Encrypt Message Individually to Everyone in the Group



Encrypt Decryption Key to Everyone in the Group



Encrypt with Group Key Known to the Group Members



Challenges I

- Forward Secrecy and Post-Compromise
  - Double Ratcheting
  - Message Dependent Keys
- Authentication of Members
  - Trust Only First Use (TOFU)
  - External Social Graph
  - Security Numbers

Challenges II

- Adding or Removing Members
  - List Structure
  - Tree Structure
  - "Lazy" Update
- Multi-Device Users
- Privacy of Social Graph
  - Use Software Guard Extensions for Set Intersection
  - External Social Graph
  - Server Knows All Metadata

Challenges III

- Synchronization of Conversations
  - Ordering Messages
  - Acknowledge Messages
- Communicating with Offline Parties
  - Pre-Shared Pre-Keys with Server
  - Only Use Static Public Keys
- Backup and Restore Conversations
  - No Access to Backups
  - Local Encrypted Backup
  - Plaintext Backup in Cloud

Challenges IV

- Metadata Leakage and Server Knowledge
  - Encrypted Metadata
  - Anonymous Credentials
- Deniability of Messages
  - Ephemeral Keys instead of Signatures
  - Shared MAC-Keys for Groups
- Efficiency and Denial of Service
- Censorship resistance and Domain Fronting

Thank You! Questions?

Email: tjerand.silde@ntnu.no

Slides: `www.tjerandsilde.no/talks`