hsgr lightning talks 201409

93 till ∞

Section 1

Why secure multiparty messaging so hard?

Introduction

- What is messaging?
- What is multiparty messaging?
- What is secure multiparty messaging?
- OTR
- mpOTR?

mpOTR Challenges

- Group Key Exchange (Broadcast or P2P?) (Dynamic?)
- Authentication
- Deniability
- Transcript Consistency
- Perfect Forward Secrecy
- How to do joins? Invites?

Future?

- moderncrypto.org [messaging] mailing list

Section 2

Pond

What is?

- Messaging based on end-to-end crypto and anonymity
- Slow crypto movement
- Written by agl

Properties

- End-to-end confidentality
- Perfect Forward Secrecy (TPM NVRAM supported)
- Traffic analysis defences (GPA doesn't know when messages were sent/received, or who is behind each home server)
- PAKE (EKE2) handshake
- Anti-spam
- Clean threat model

Section 3

Entry guards

Present

- FIND GRAPHS FROM TARIQ'S PAPER

Future (proposal 236)

- 3 guards $\rightarrow$ 1 guard
- Guards needs to be faster
- Increase guard lifetime?
- Guardiness load balancing?

More future

- Better data structures (How to detect network down events?)
- Guard fingerprinting
- Guard discovery attacks