# Securing XMPP End-to-End

Matt Miller

IETF 89 - London

# OTR: In the Wild

- OTR == “Off the record”
- Used by numerous multi-protocol clients …
- … but has issues
  - no stable reference yet
  - covers chat plaintext only
  - problems with multiple devices
  - “Invents” new crypto

# WIP: draft-miller-xmpp-e2e

- Overcomes issues with previous efforts
  - Protects “whole” stanzas – and only stanzas
  - Works with multiple devices simultaneously
  - Re-uses JOSE
- But has issues
  - PFS still undefined
  - No store/forward

# Call to Arms

- Need reviewers and/or authors
- Open to different ideas