JABBER/XMPP

THE PAST, THE PRESENCE & THE FUTURE

Daniel Gultsch

December 27th 2017 @ 34C3

MOTIVATION

- Single vendors are dangerous
- Open Source doesn’t help
- Phone numbers

JABBER/XMPP

- Provider independent
- IETF working group since 2002
- Extensions *published* by the XSF

JABBER OR XMPP?

- Jabber = Ecosystem (Email, Web)
- XMPP = Protcol (IMAP, SMTP, HTTP)

JABBER VS MATRIX

- Similiar goals
- Personal preference
- Gateways are flawed

2016

- Reliable & battery friendly [1]
- Multiple devices [1]
- Media transfer [1]
- Group chats
- Optional: E2EE [1]

[1] When using a modern client and server

STATE OF MOBILE XMPP IN 2016

- gultsch.de/xmpp_2016.html
- XMPP talk @ FrOSCon 2015, media.ccc.de

A CHOICE OF E2EE

- None
- OMEMO: Forward secrecy
- PGP: Server side archive

2017

DIRECT TLS / SNI

- Replaces STARTTLS
- Domain name / certificate selection
- Faster
- Public WiFi / Port 443

PUSH

- *something* happened
- Important on iOS
- Might become important on Android
- Server support / Proxies over App server

GROUP CHAT READ MARKERS

- XEP-0333
- small changes to XEP
- *Read to this point* UI

MESSAGE STYLING

- Not markdown
- Italic, bold, strikethrough & monospace
- Inspired by WhatsApp & Slack

AVATARS

- Two »competing« standards
- One simple solution

XEP 0084: USER AVATARS

- efficient interface
- only contacts can access

XEP 0153: VCARD-BASED AVATARS

- Data is public
- works in group chats

XEP-XXXX: USER AVATAR TO VCARD-BASED AVATARS CONVERSION

FUTURE

OMEMO BY DEFAULT

- Easier trust model
- World readable keys
- Deployment

EASIER TRUST MODEL

- TOFU is difficult to apply
- BTBV
- Trust everything by default
- Trust new keys
- After scanning a contact, stop trusting new keys from that contact

WORLD READABLE KEYS

- `publish_options`
- `mod_omemo_all_access`

DEPLOYMENT

- Every platform has at least one client
- omemo.top

OTR MUST GO AWAY

- Unreliable
- Doesn’t work with multiple devices
- Auto response loops

IMAGE THUMBNAILS

- XEP-0385: Stateless Inline Media Sharing
- OMEMO: Data URIs
- Size limit (10,000 bytes)

INITIAL LOGIN

- Initial login / discovery expensive
- Resume requires TLS and SASL

SPAM

- »Cyber criminals« spamming each other
- Be careful about publishing your JID
- Blocking made easy / No notifications
- Spam Reduction on yax.im

CONVERSATIONS V2.0.0

March 24th, 2018

GETTING STARTED

CLIENTS

- Conversations
- ChatSecure
- Gajim / Dino

SERVERS

- Self hosting
- Hosting
- Domain hosting

DEVELOPERS WANTED

- Go help out the existing clients!
- Tooling
- Compliance Tester
- Server Status page
- Google Summer of Code

QUESTIONS?

@iNPUTmice

gultsch.de

github.com/iNPUTmice/talks