ChatSecure

Free and open source OTR encrypted chat over XMPP
for iOS and Android.

@ChatSecure chatsecure.org

What is ChatSecure?

- Free and open source encrypted chat application
- Available for iOS and Android
- Interoperable with any XMPP + OTR client

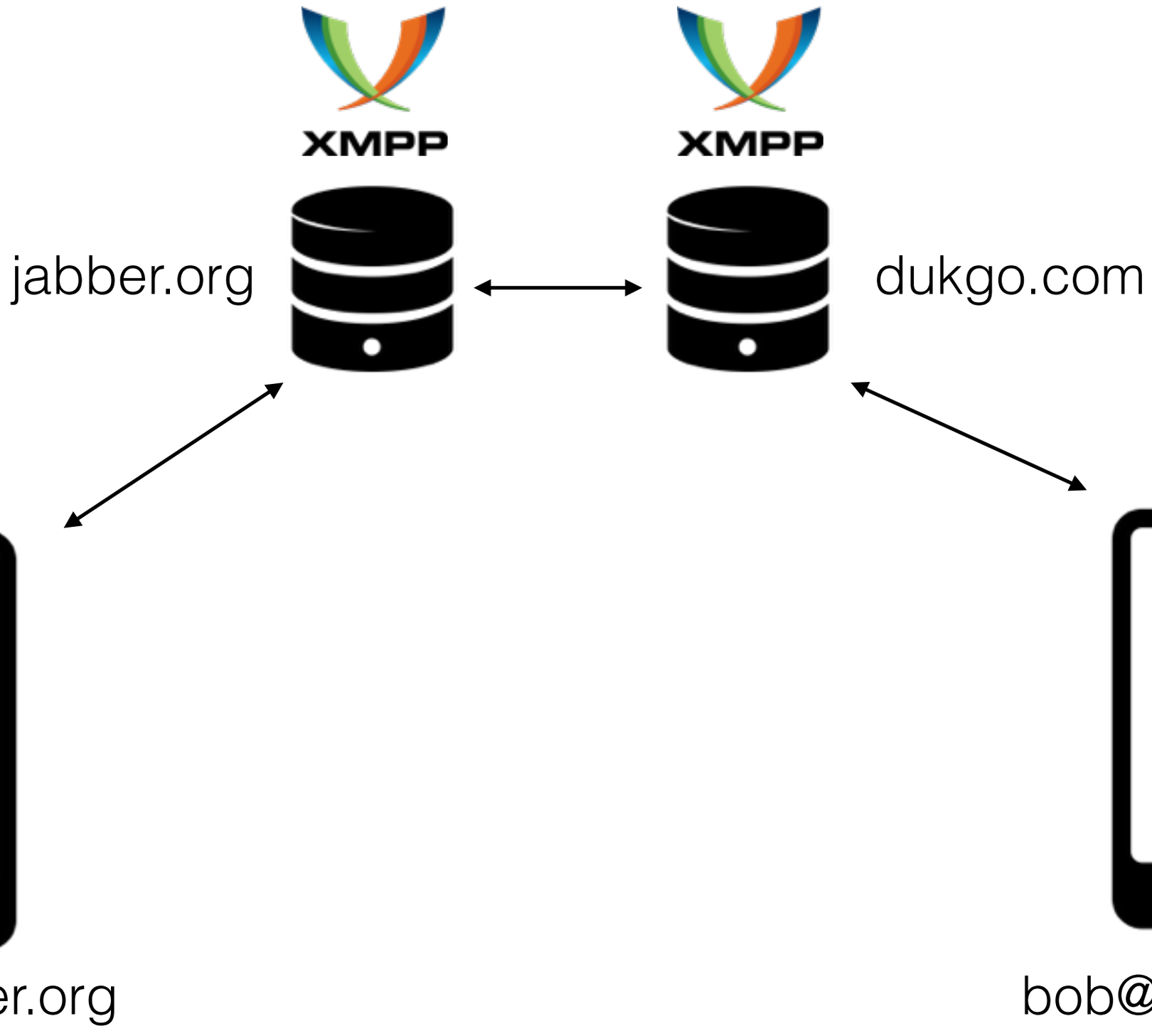
What is ChatSecure?

- XMPP for Google Talk, Facebook, Jabber support
- OTR for end-to-end encryption
- Tor for censorship resistance
- SQLCipher for local database encryption

Why XMPP?

- Decentralized (host your own server)
- Standardized
- Extensible
- Widespread implementation on desktop and mobile
- Supported by Google, Facebook (for now…)

XMPP Overview



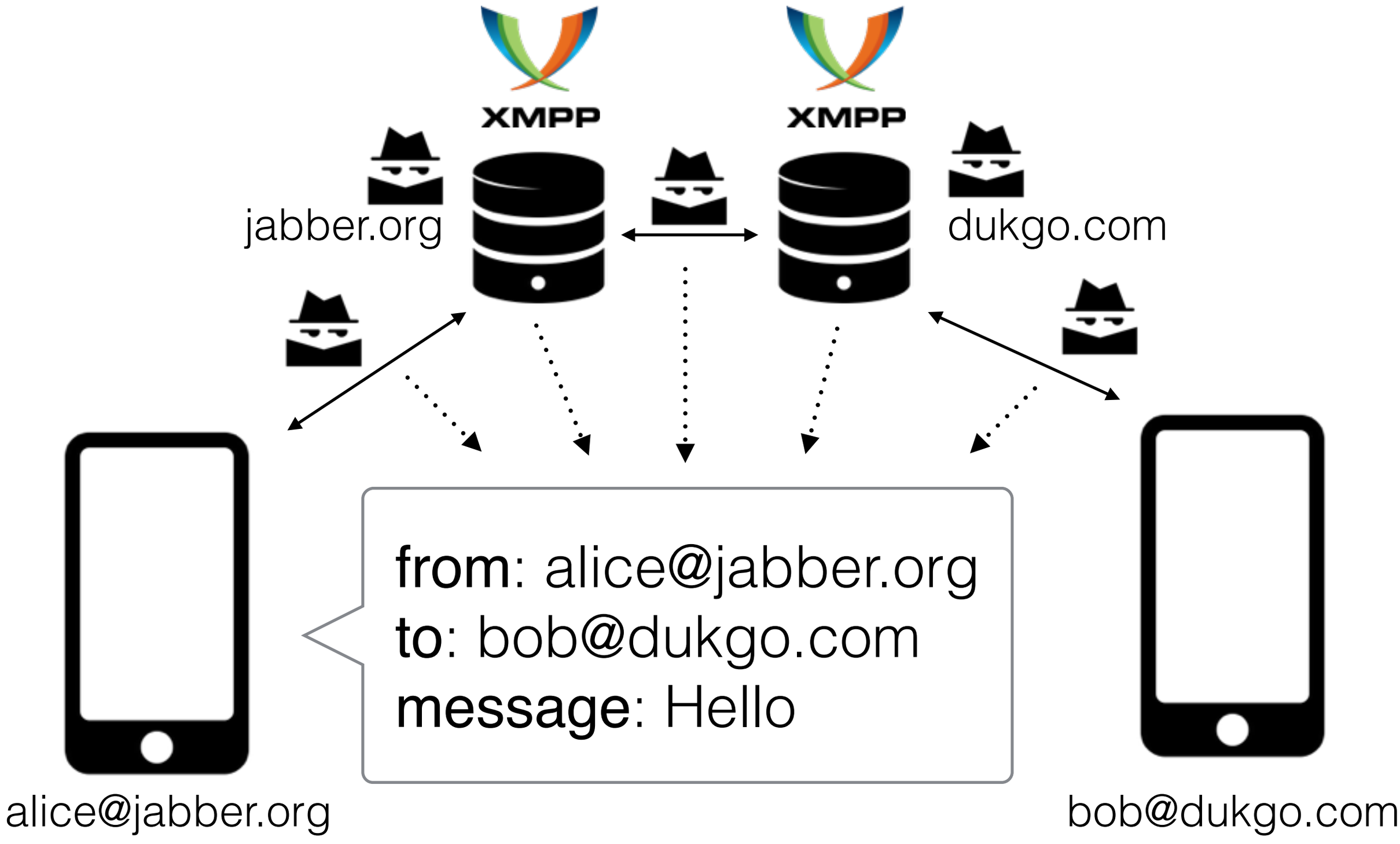
Why not XMPP?

- Not designed for mobile
- No widely implemented standard for push messaging
- These limitations are especially problematic on iOS

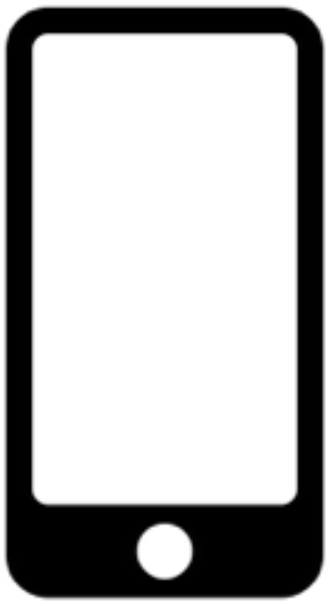
What is OTR?

- Widely deployed chat encryption protocol
- Designed by cryptographers Ian Goldberg and Nikita Borisov in 2004
- Features authenticated encryption, perfect forward secrecy, and deniability

Without OTR


XMPP
XMPP
jabber.org
dukgo.com
from: alice@jabber.org
to: bob@dukgo.com
message: Hello
alice@jabber.org
bob@dukgo.com

With OTR



alice@jabber.org

from: alice@jabber.org
to: bob@dukgo.com
message: ?
OTR:AAIDAQAAAAMAAAAEA
AAAwBst9inn2mWrtsl0xuJIbo
11fLGb04G5TtdjTK1JVDlI74y
HMu2VSCbYlOxkOp/
8MCyeY2wREI/w/jC/zaQ/
j5hx9LL4BFFsBeeDdarFrEI/
40STTc0ZUljV5X37iwM2il0tCA
QIfMleSQFS2m13UdwROyVM
tN….

Why OTR?

- Available in many open source chat clients
  - Adium (Mac), Pidgin (Windows, Linux)
  - Jitsi, Beem, Conversations, and more…
- Free and open source implementations:
  - Java (otr4j)
  - C (libotr)
  - Objective-C (OTRKit)

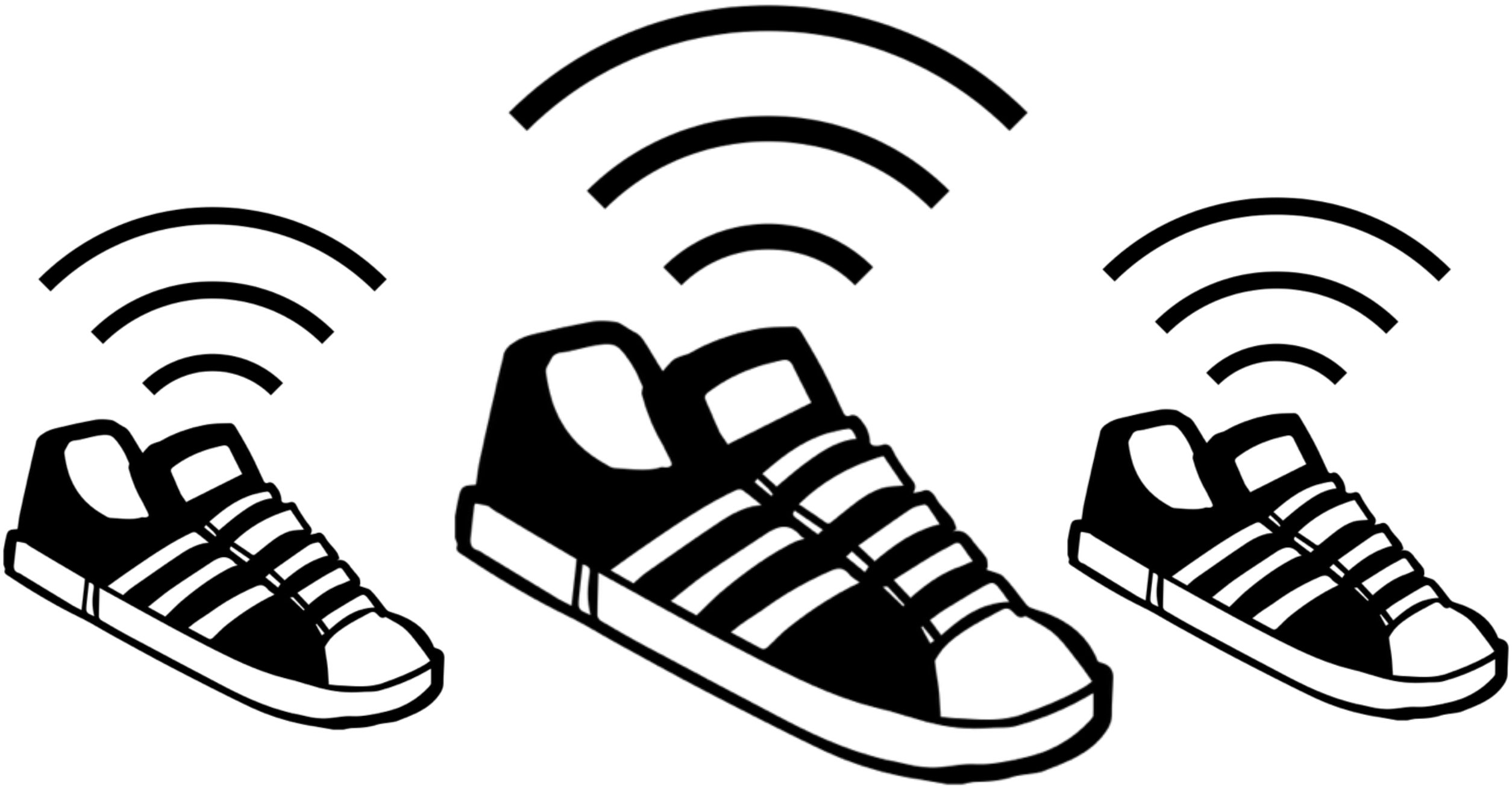
Why not OTR?

- Designed for synchronous communication (desktop)
- No support for group chats
- Not great on multiple devices, even with OTRv3
- Messages can be lost if sent to wrong client
- No way to sync messages across desktop/mobile

What's next?

- Axolotl (used by TextSecure) is a promising successor to OTR for asynchronous communication
- Push messaging
  - We are working on a protocol-agnostic solution
  - Plans for an XMPP server extension

SneakerNet



SneakerNet

- Built in response to situations where internet connectivity is unavailable or has been deliberately blocked
    - Police blocked cell towers during 2011 BART protests
    - Hong Kong protests
    - Large gatherings in the desert
- Unlike FireChat, SneakerNet is open source and *actually* works without internet

SneakerNet

- Built for public broadcast communications
- Uses Bluetooth 4.0 Low Energy, no internet at all!
- Modern crypto (Ed25519) for message authenticity
- Currently in “working prototype” phase for iOS and Android

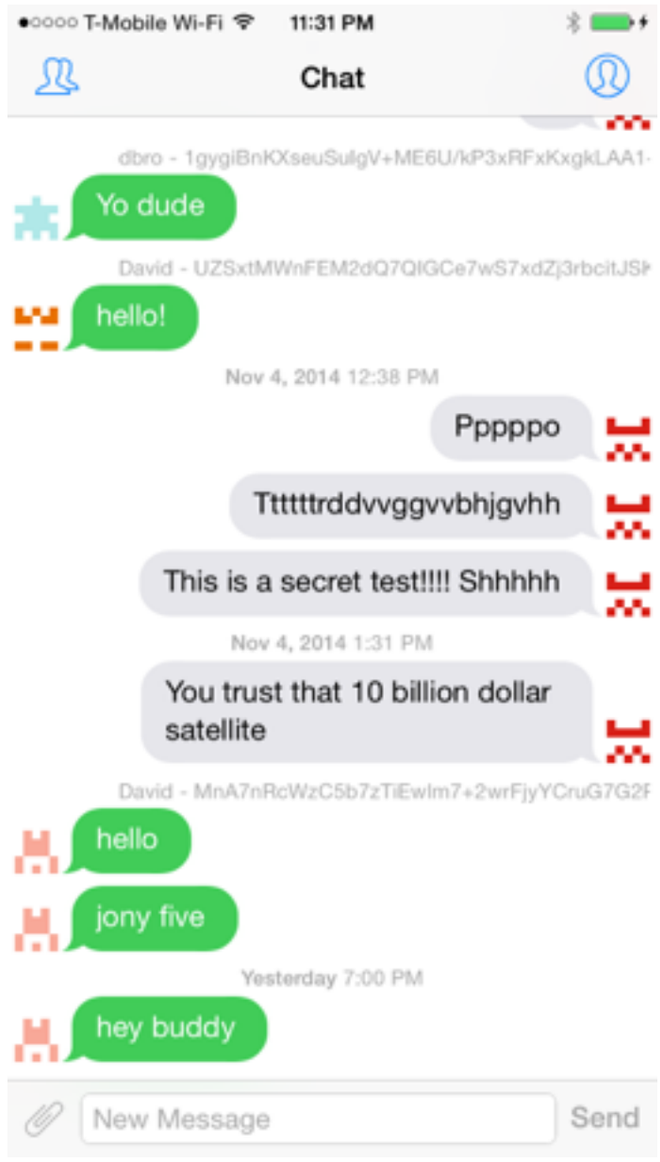
SneakerNet

iOS:

git.io/fhXcRQ

Android:

git.io/GpQAGw



Thank you!

Attribution

- Smartphone by George Agpoon from The Noun Project

- Server by Sergio Luna from The Noun Project