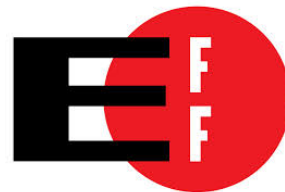


# Why aren't all comms end-to-end encrypted in 2015?



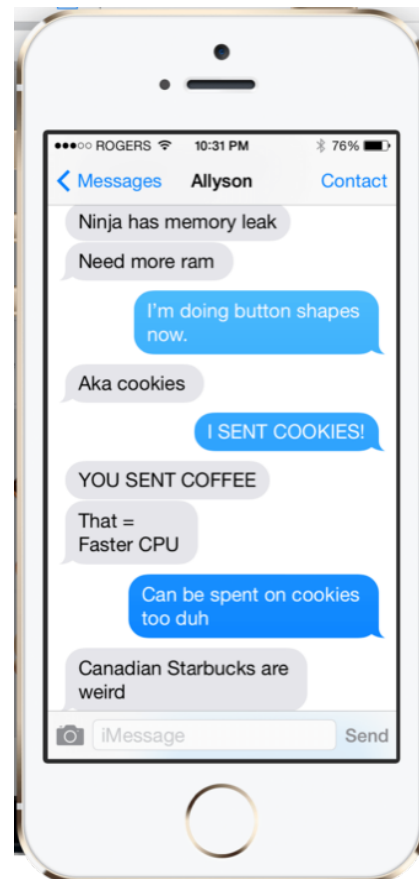
**Joseph Bonneau**  
Stanford University  
& Electronic Frontier Foundation



CONIKS is joint work with Marcela Melara, Aaron Blankstein, Ed Felten and Mike Freedmen,  
Princeton University

# Email vs. “chat”

- Asynchronous
- Federated/open
- Threaded
- Searchable
- Archived
- Public addressing



- Asynchronous
- Walled gardens
- Two-party
- Not searchable
- Ephemeral
- No spam (yet)

# End-to-end encrypted chat is here



1 billion+ users!

Central key servers

No security UI/fingerprints (yet)

# Pain points for encrypted email

- Search
- Spam
- Federation
- Group messaging/threading

# Potential future strategies

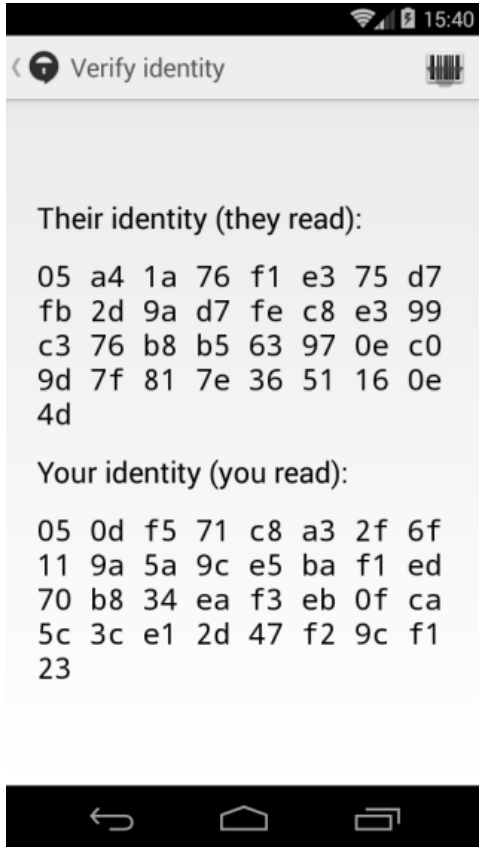
- Fix encrypted email
- Two systems, different security profiles



# Pain points for all systems

- Trust establishment
  - ~~key management~~

# Manual key verification in TextSecure



BdY73Lfk12kv9iTVUTGIL6VZrpbG+6V1q+ZsZMrpu2p3

# Key changes are a major pain point...

## Complete key exchange

The signature on this key exchange is different than what you've previously received from this contact. This could either mean that someone is trying to intercept your communication, or that this contact simply re-installed TextSecure and now has a new identity key. [You may wish to verify this contact.](#)

Cancel

Complete

## Rough estimate:

1% of users change keys each day

Median key age < 6 months



# In practice: trust your provider



iMessage



TextSecure



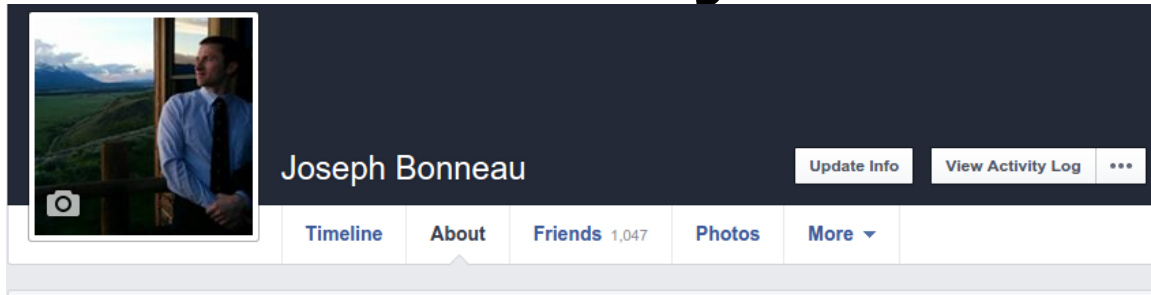
**Threema.**

Seriously secure mobile messaging.



Telegram

# Facebook is now a key server!



**Problem:** what if Facebook is malicious/coerced/compromised?

Family and Relationships	Website	<a href="http://www.jbonneau.com">http://www.jbonneau.com</a> <a href="http://picasaweb.google.com/jbonneau">http://picasaweb.google.com/jbonneau</a>
Details About You	Email	<a href="mailto:jbonneau@facebook.com">jbonneau@facebook.com</a> 4 emails hidden from Timeline
Life Events	Facebook	<a href="http://facebook.com/jbonneau">http://facebook.com/jbonneau</a>
	PGP Public Key	7418 4405 F45F FDA9 B172 D845 58F8 D41E 8CA3 A9E8

# What if Facebook is coerced/malicious?

- Use multiple social identity providers

or

- Ensure Facebook is *globally consistent*

# Using multiple providers (KeyBase)



Max Krohn

Keybase.io co-founder and developer;  
PhD MIT CSAIL 2008; OkCupid CTO  
& co-founder; SparkNotes CTO & co-  
founder. Creator of IcedCoffeeScript,  
OKWS, and OneShallPass.com  
New York, NY

keybase.io/**max**

6052 B2AD 31A6 631C

maxtaco tweet

maxtaco gist

maxtaco post

coinbase/maxtaco post

maxtaco profile

oneshallpass.com https dns

keybase.io https

nutflex.com dns

maxk.org dns

1BYzrCvfbn81dfiksmD1Bdgt8pgLi1SD7Z



Max Krohn

@maxtaco

Follow

Verifying myself: I am max on Keybase.io.  
ZnBizHMA8RKSB598TaDtjIPILKSEu1WuaT  
59 / keybase.io/max/signs/ZnBiz...



maxtaco / keybase.md

Created on Feb 6, 2014

keybase.md

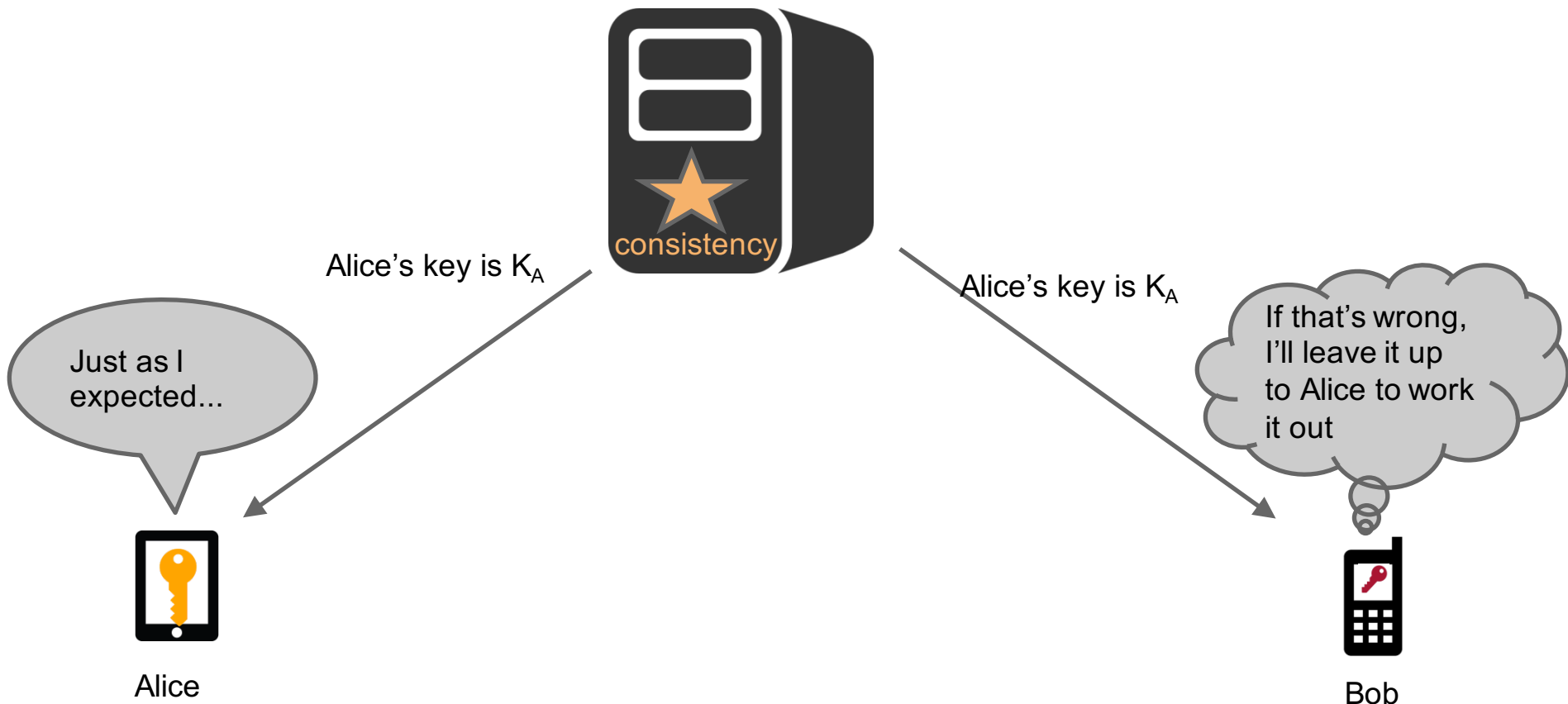
Raw

Verifying myself: I am <https://keybase.io/max>

As part of this verification process, I am signing this object and posting as a gist as github user  
maxtaco

```
{
  "body": {
    "key": {
      "fingerprint": "8efbe2e4dd56b35273634e8f6952b2ad31a6631c",
      "host": "keybase.io",
```

# Globally consistent key server (CONIKS)



# Error UI with consistent key servers

## Complete key exchange

The signature on this key exchange is different than what you've previously received from this contact. This could either mean that someone is trying to intercept your communication, or that this contact simply re-installed TextSecure and now has a new identity key. [You may wish to verify this contact.](#)

Cancel

Complete

## Key change detected

The server has published an unexpected key for you. If you haven't re-installed this app recently, this may mean somebody is trying to intercept your communications.

[Check list of devices and keys](#)

Cancel

Complete

# Cryptographic append-only logs

Invariant: can only add data, not delete

More formally:  $\mathbf{v}_i = \mathbf{v}_{i-1} \parallel \mathbf{X}_i$

Current  
version

Previous  
version

New  
data



# Questions & concerns

**Bystander effect:** Why check when others will?

**Too-big-to-fail:** Equivocation is detected. Now what?

**My word vs. yours:** Users claim misbehavior. Now what?

**Trust:** I know my company is honest. Why prove it?



# Thanks!

Feedback: [jbonneau@cs.stanford.edu](mailto:jbonneau@cs.stanford.edu)

EFF Crypto prize: [cryptoprize@eff.org](mailto:cryptoprize@eff.org)

Discussion list: [messaging@moderncrypto.org](mailto:messaging@moderncrypto.org)