Alice and Bob are Really Confused

David Huerta - DEF CON 23

Photo credit: Robert Young


much codes
such crypto parties
very google trolling
so cypherpunks
wow nyc
many credits: Atsuko Sato

Alice wants to talk to Bob,
but Eve is being nosey.


Alice hears about crypto,
goes to a crypto party to
learn how to crypto.

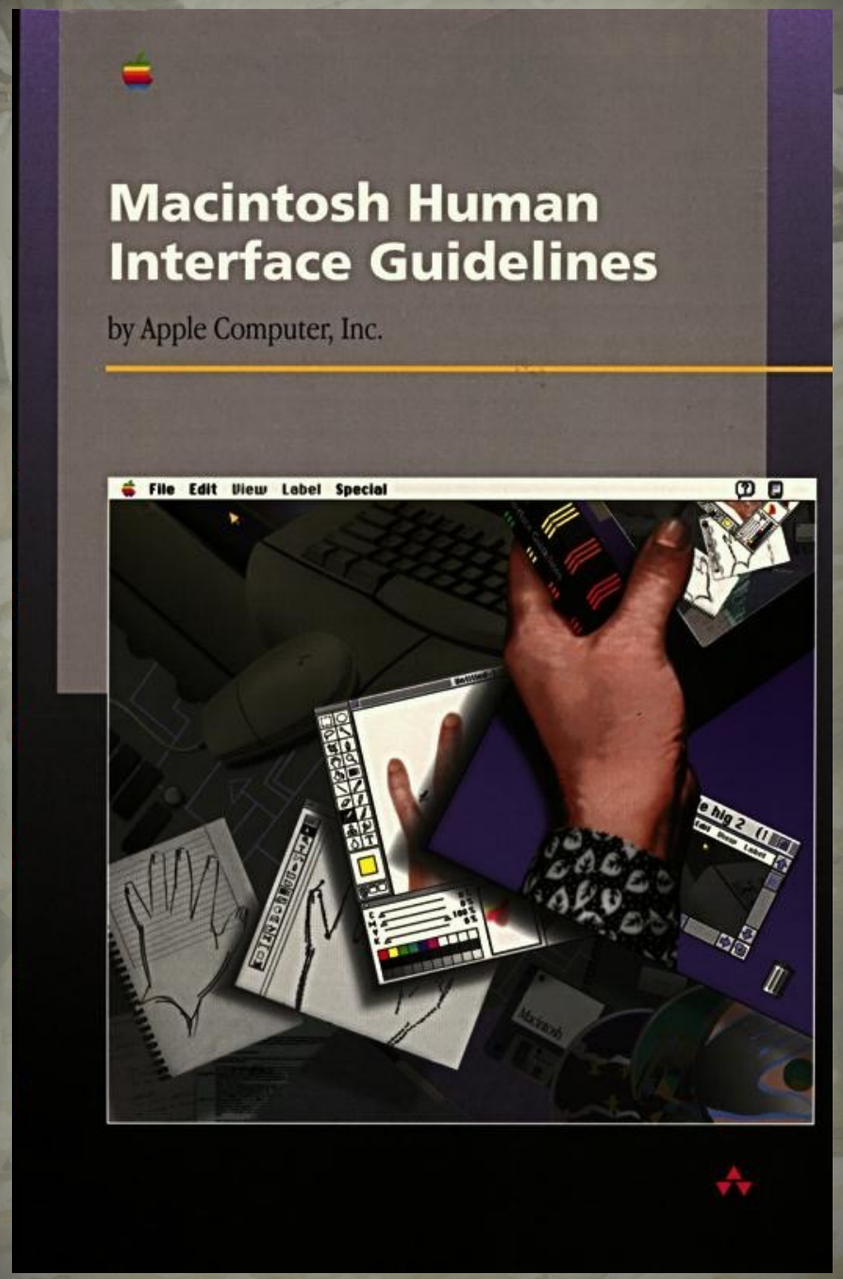
Sec in the City

- 24+ Cryptoparties as of July 2015
- Varying communities with varying skill levels
  - Hackerspaces (Alpha One Labs, Fat Cat Fab Lab, NYC Resistor)
  - Libraries (Brooklyn Public Library, Verso Books)
  - Art Galleries (Calyx Institute, Babycastles)
  - Co-working spaces (Harlem Creative Space)
  - Universities (CUNY Graduate Center, Columbia)

Photo credit: Roman Kruglov

This is Your New Bible

This is canon, everything that came after it is slash fanfic.



Key Lessons from 1992

- Modelessness: This is why CAD software is always awful; You want to limit the modes a user has to remember they're in. BUT with a private/un-private set of situations that can't always be avoided and should be handled carefully.

- Perceived Stability: Your back-end might be solid but if the front-end isn't, people will assume the whole thing is broken and Seal Team 6 is on their way to bust down your door.

- User Testing: Prototype your software and ask people to try it out, change design accordingly.

- Metaphors: No one uses a key to unlock a key in the real world.

Key Lessons from 2015

- Forgive[less]ness: UX tends to focus on allowing people to undo things or bring things back to an original state. Mistakes in crypto are not usually forgivable.

- Too many tools: If a chain of tools has to be installed in a particular order people will not do that. If too many steps involved in downloading/verifying/install, multiply by number of tools and you have a problem.

- False hope: If there's any chance something could go wrong or some feature might not be available, warn the user.

- Confusion through curiosity: Even if you perfectly illustrate a mental model of how something works, the internet will fuck it up.

OMG RTFM!!!!111

OMGWTFBBQ RTFHIG!...

.tumblr.com

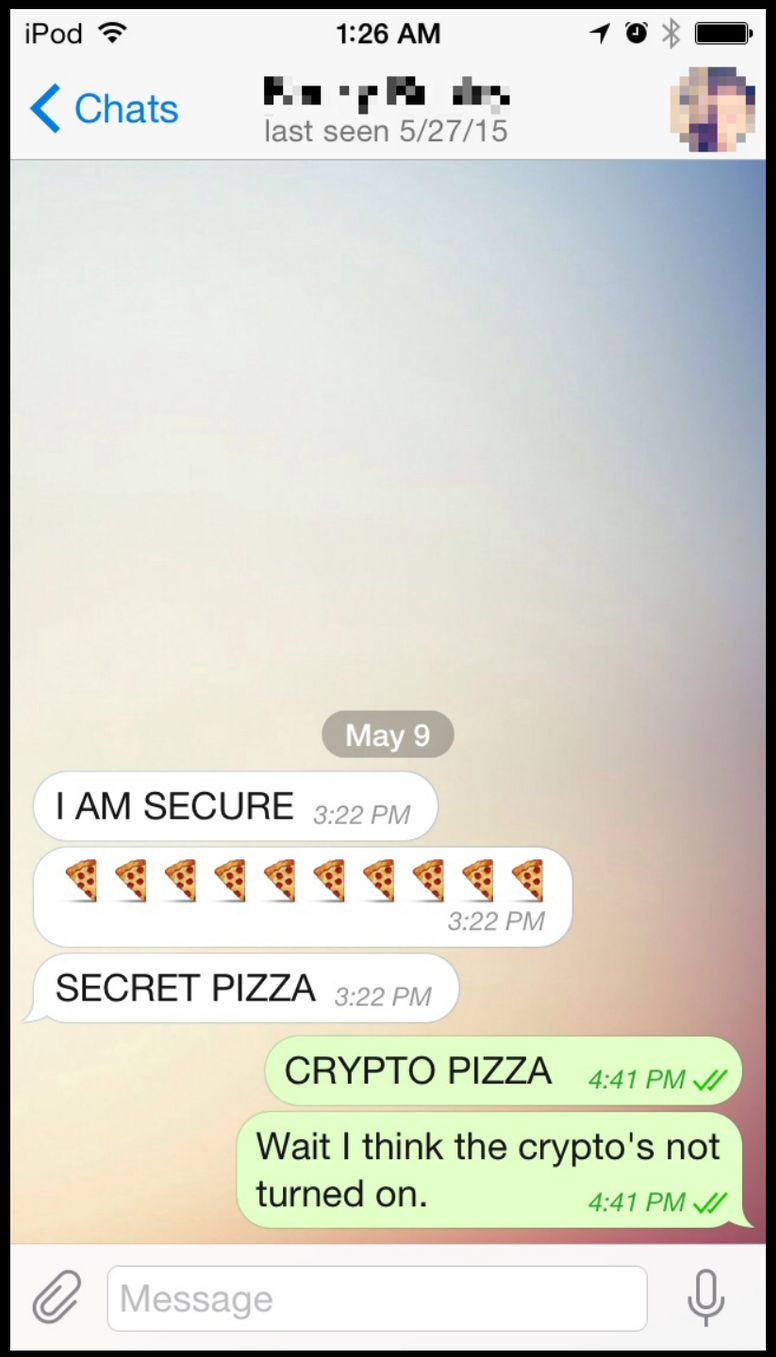
Constructive Criticism

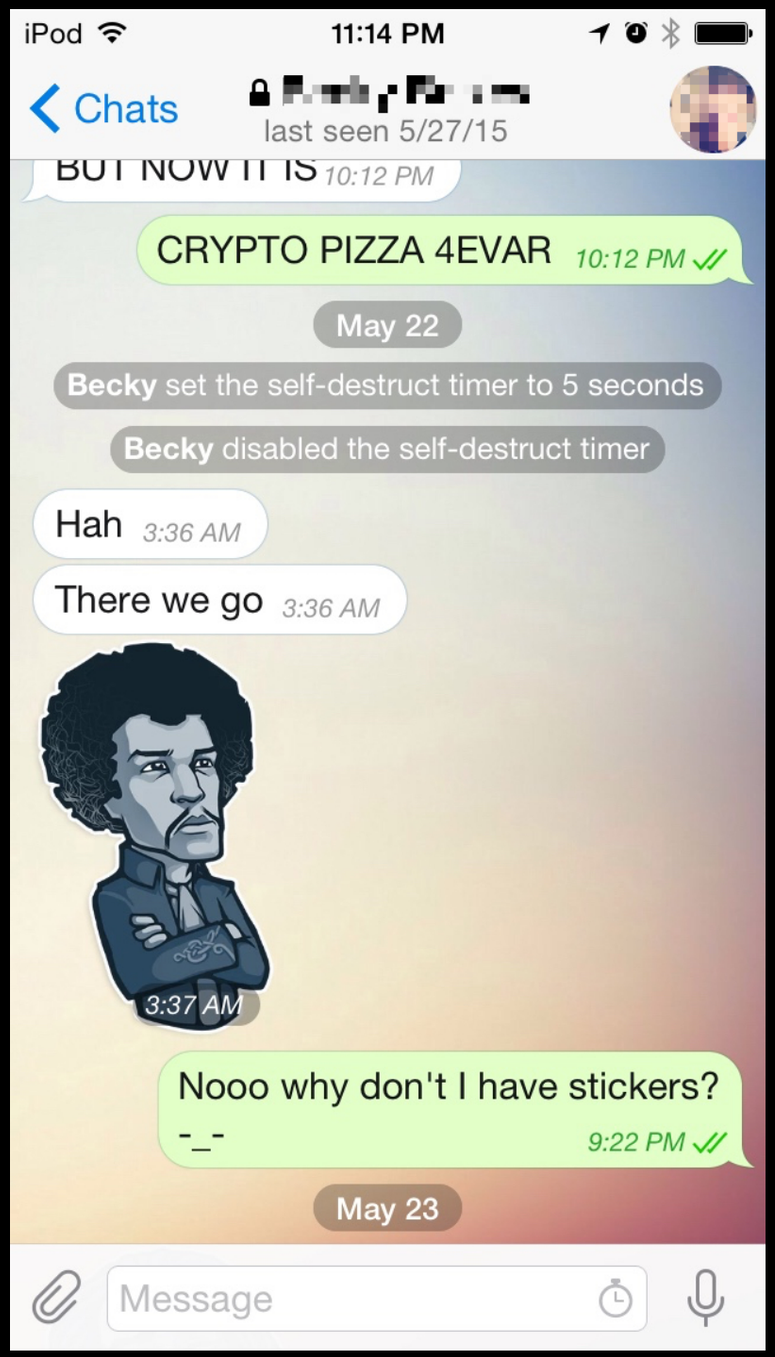
Photo credit: Tambako the Jaguar

Telegram

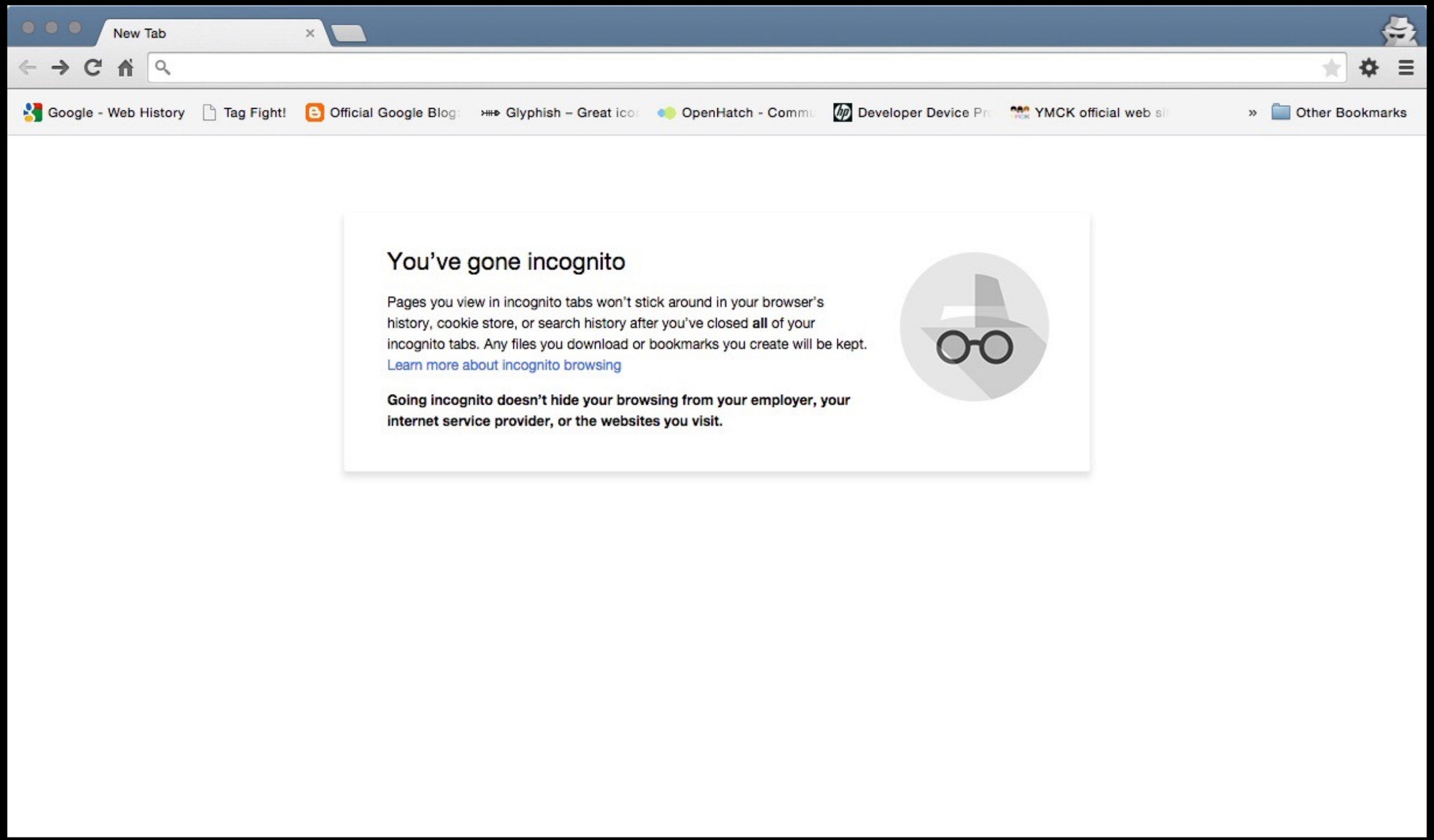
- **DISCLAIMER**: Putin has more money than you. Roll your own phat blunts, but don’t roll your own crypto.
- **DISCLAIMER**: No out-of-band verification like in OTR.
- EVERY APP NEEDS THIS THO: Alerts other party when screenshot is taken.
- Hard to tell if your chat is encrypted or not, which is a problem…

One of these is end-to-end

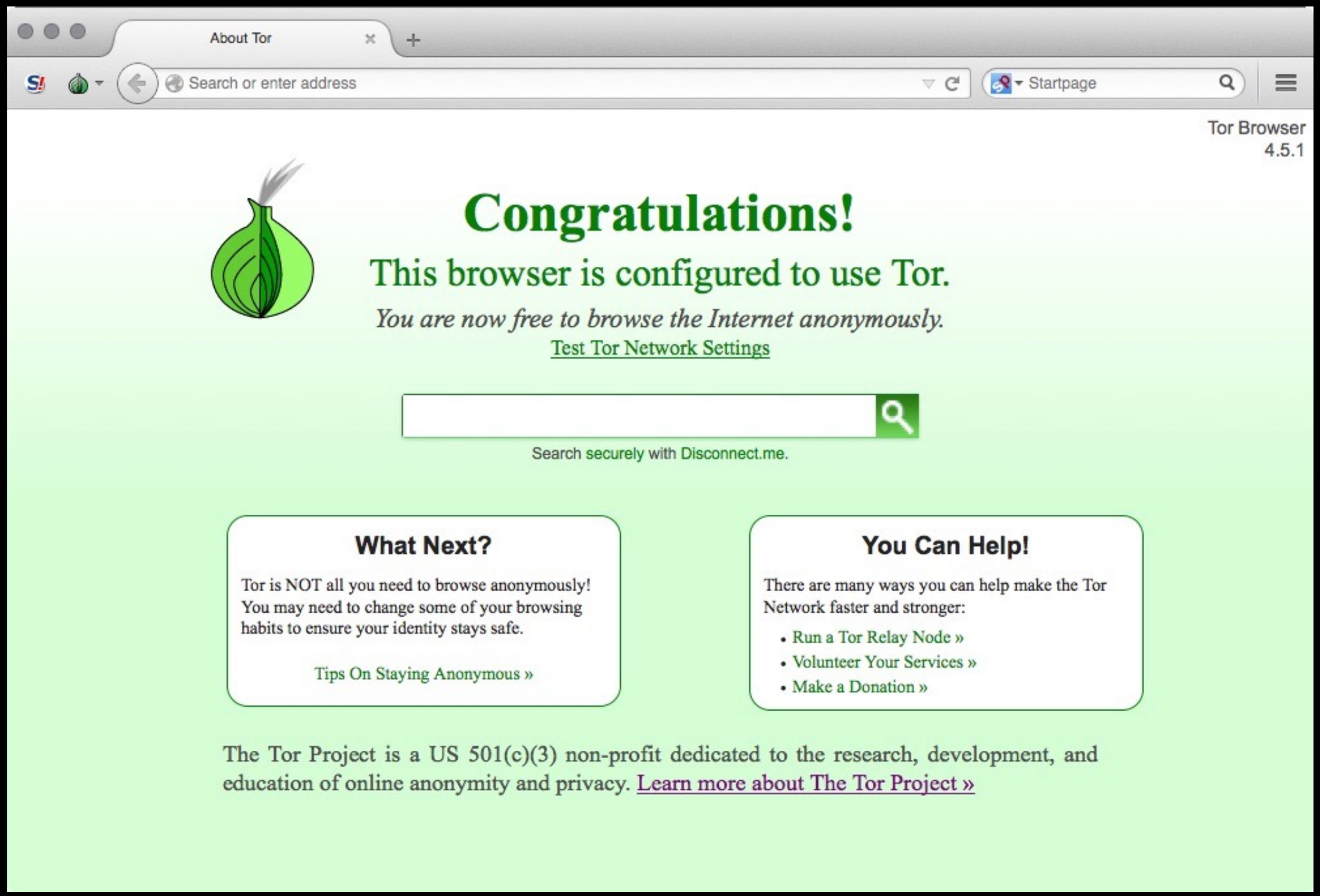




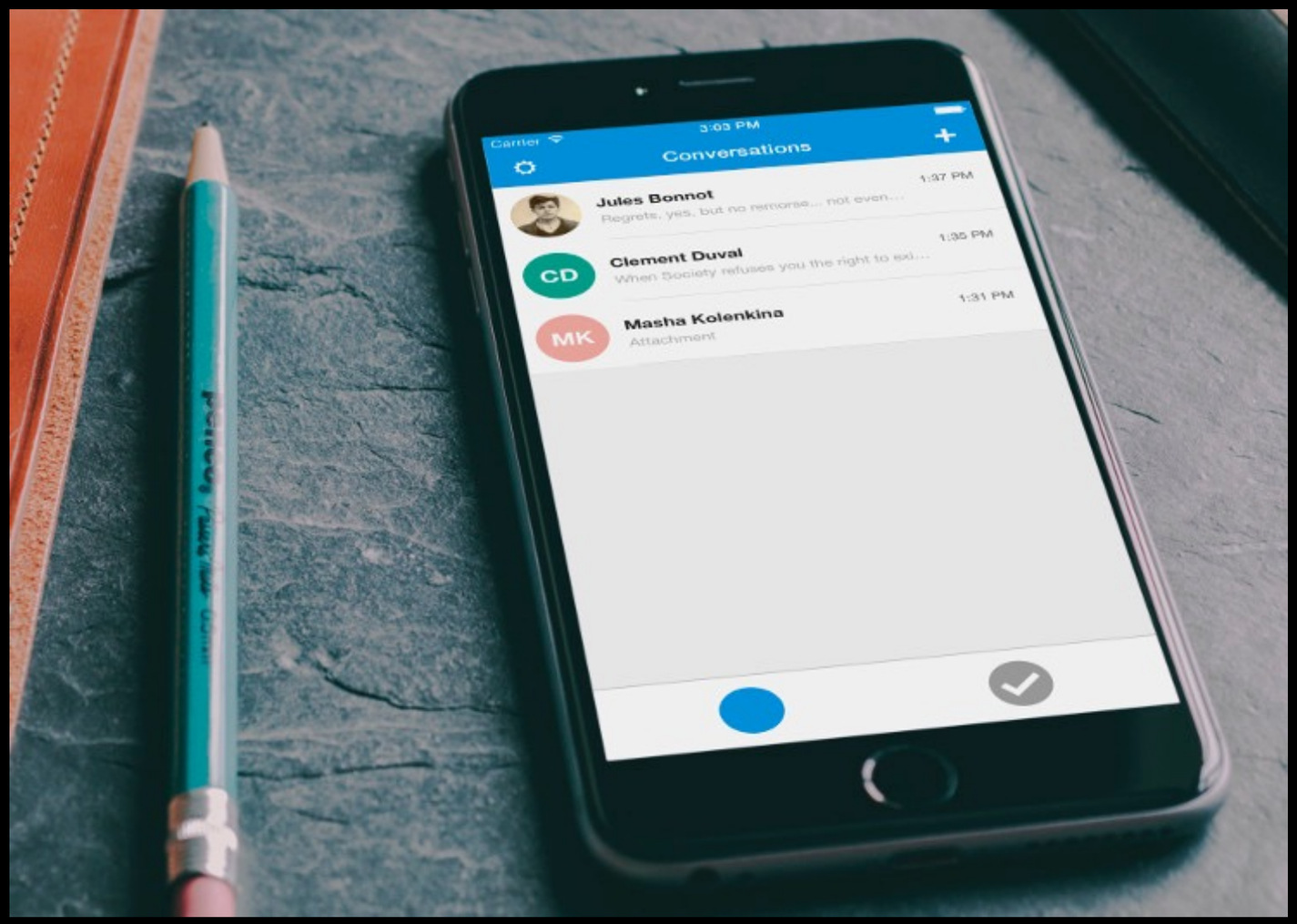
Mode Made Obvious…ish



Mode Made Obvious…ish



Signal

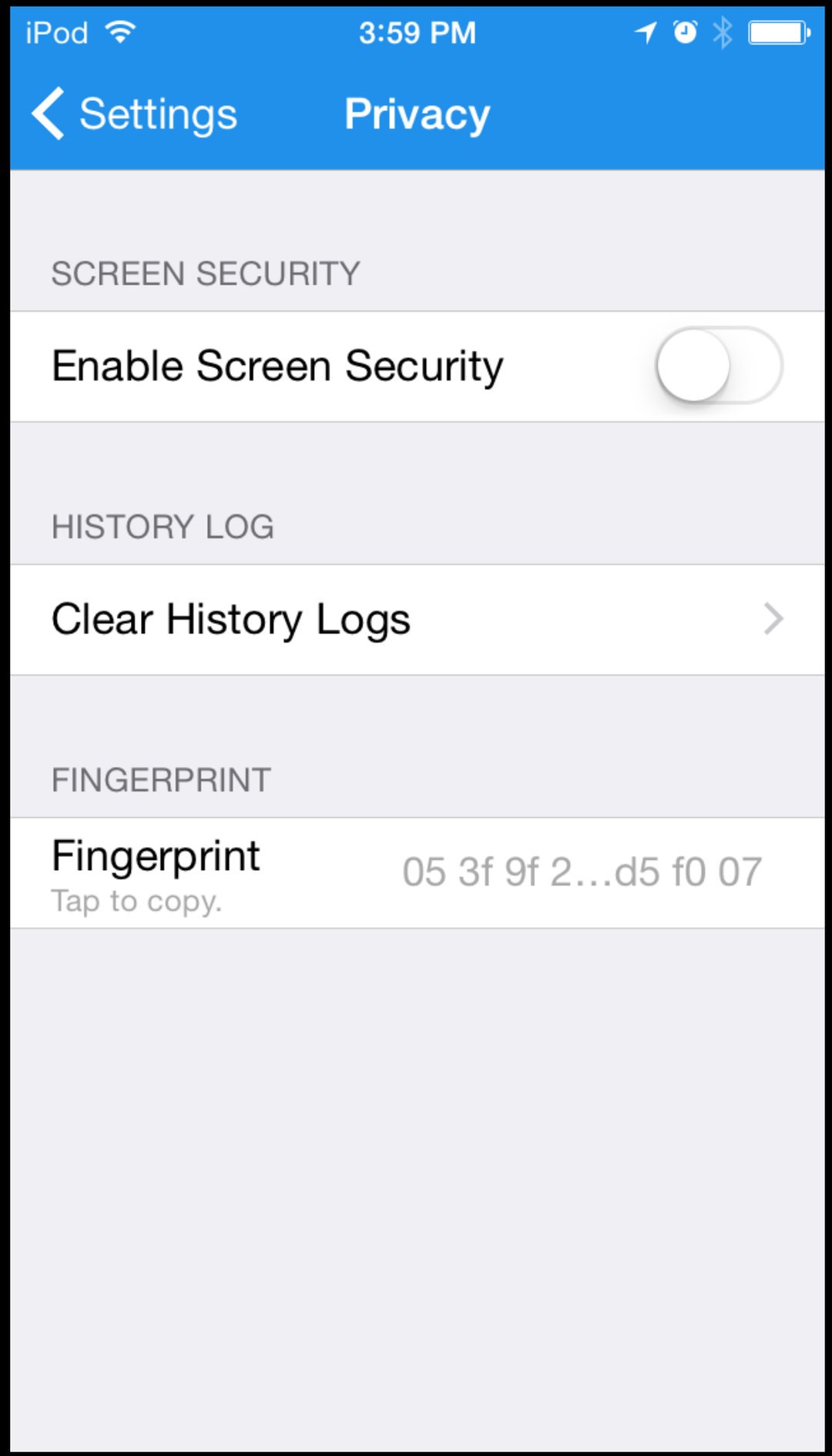


- Mystery blue button (FIXED).
- Selecting a contact immediately calls them (FIXED).
- Non-functional on iPod Touch despite lack of need for phone bits (FIXED).

Signal

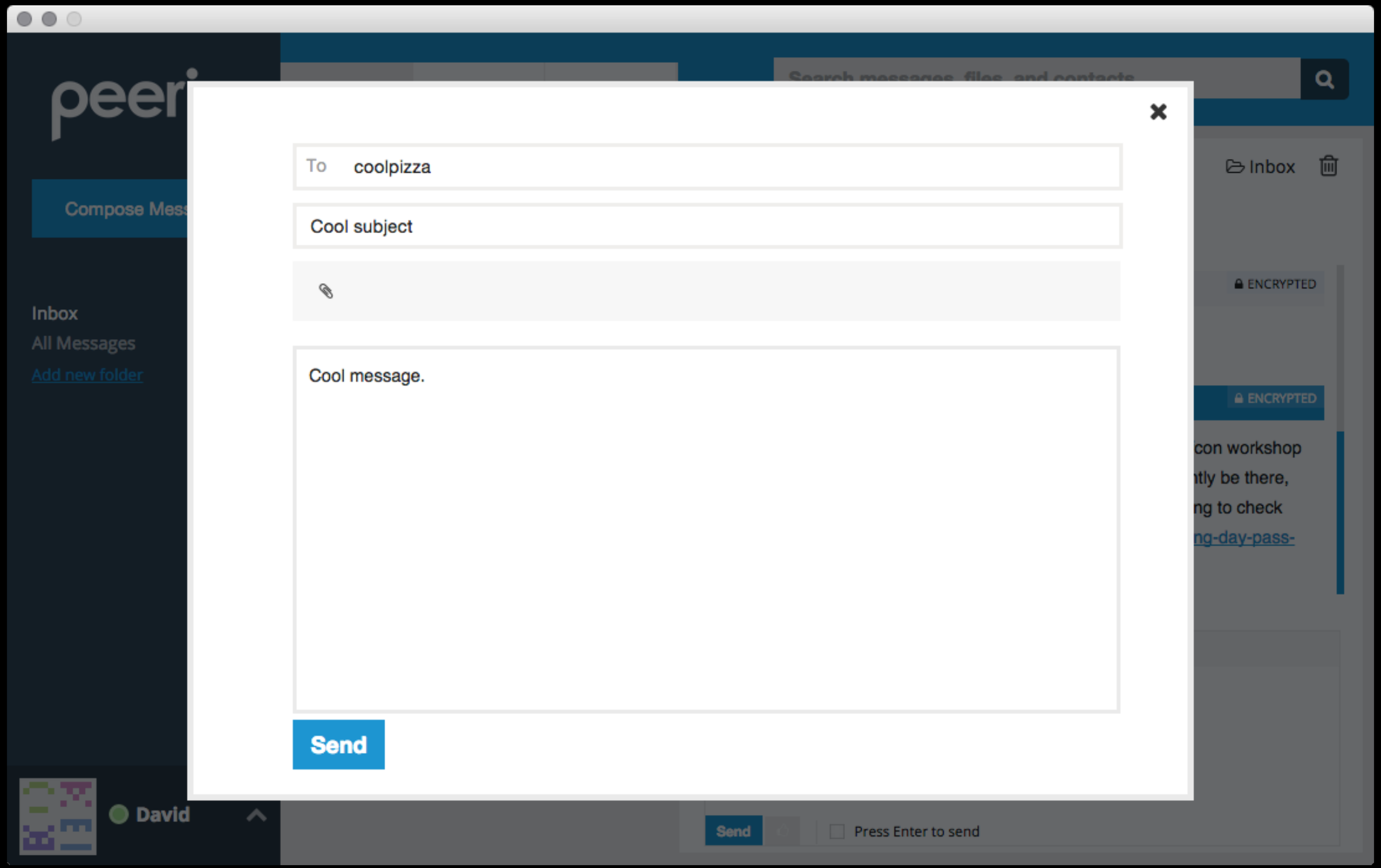
- Call button (corded phone handset icon) still unlabeled, might be a generational issue post-Snake People.

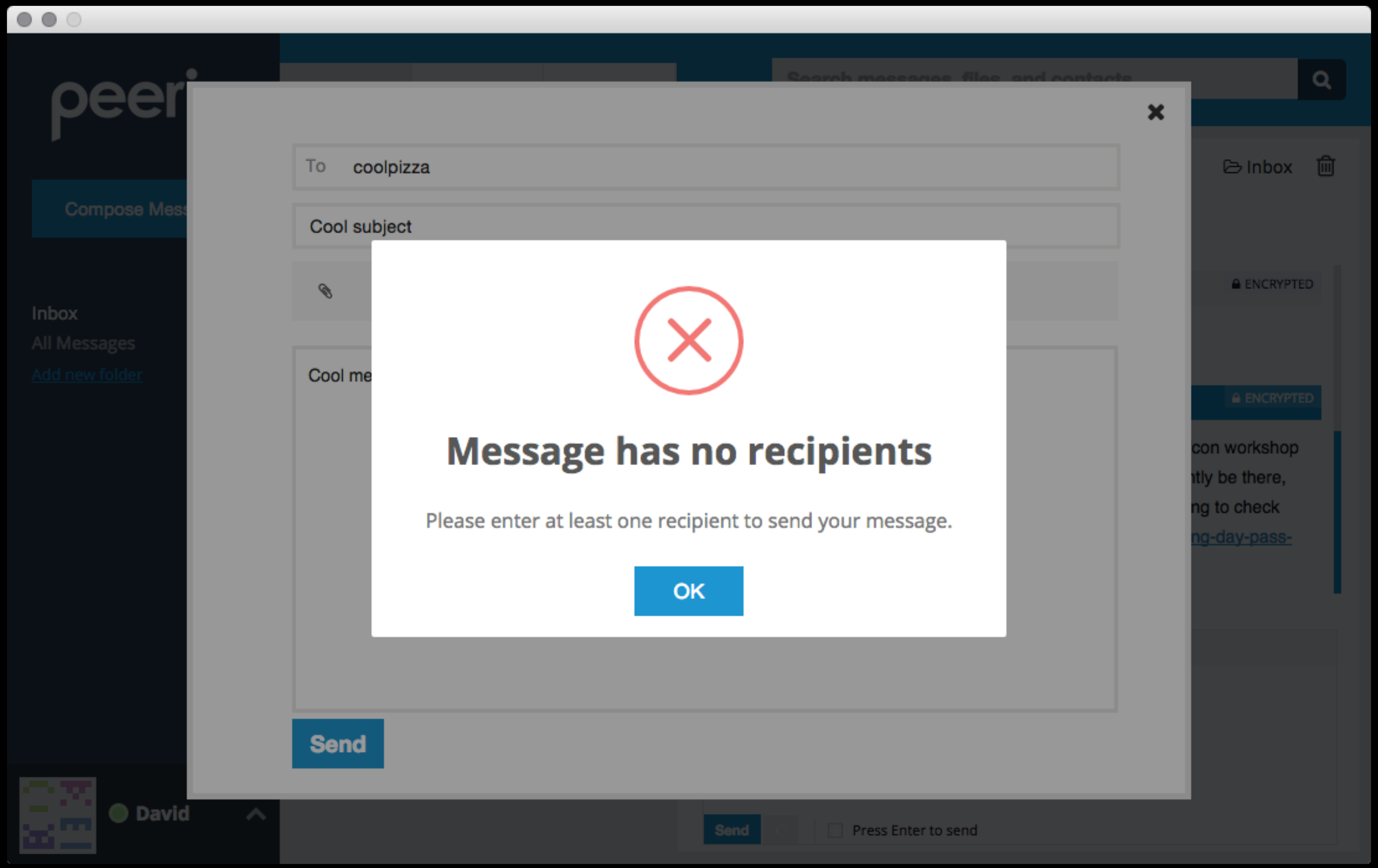
- Privacy Settings screen leaves more mysteries:
  - “Screen security”
  - I can’t see the whole fingerprint (and can we stop calling it that in devices with fingerprint readers)?



Peerio

- Designed to only work end-to-end encrypted, no other insecure modes to accidentally end up in.
- Human memory is great at memorizing strings of words, but not if they only type them once and use a short PIN instead.
- Requires anyone you try to contact to approve your ability to contact them; UI doesn’t communicate this (yet; this is being worked on).


peer
Compose Mess
Inbox
All Messages
Add new folder
David
Search messages, files, and contacts
Inbox
ENCRYPTED
ENCRYPTED
con workshop
tly be there,
ng to check
ng-day-pass-
To coolpizza
Cool subject
Cool message.
Send
Send
Press Enter to send


To coolpizza
Cool subject
Cool me
Send
Message has no recipients
Please enter at least one recipient to send your message.
OK
Inbox
All Messages
Add new folder
ENCRYPTED
ENCRYPTED
con workshop
tly be there,
ng to check
ng-day-pass-
David
Send
Press Enter to send

Interoperability :(








Interoperability :(

- Axolotl: Used by Signal.
- Minilock: Used by Peerio.
- OTR: Used by some things.
- PGP: Used by some other things.

“OTR”

- Really “Pidgin or Adium for desktops, with the OTR add-on or plugin but ChatSecure if you’re on Android and also you need a Jabber or mid-90s startup IM account from somewhere unspecified. Also it’ll be called XMPP instead of Jabber in Pidgin.”

- XMPP accounts end up coming from the CCC and their unsigned certificate. Unsigned certificates scare people.

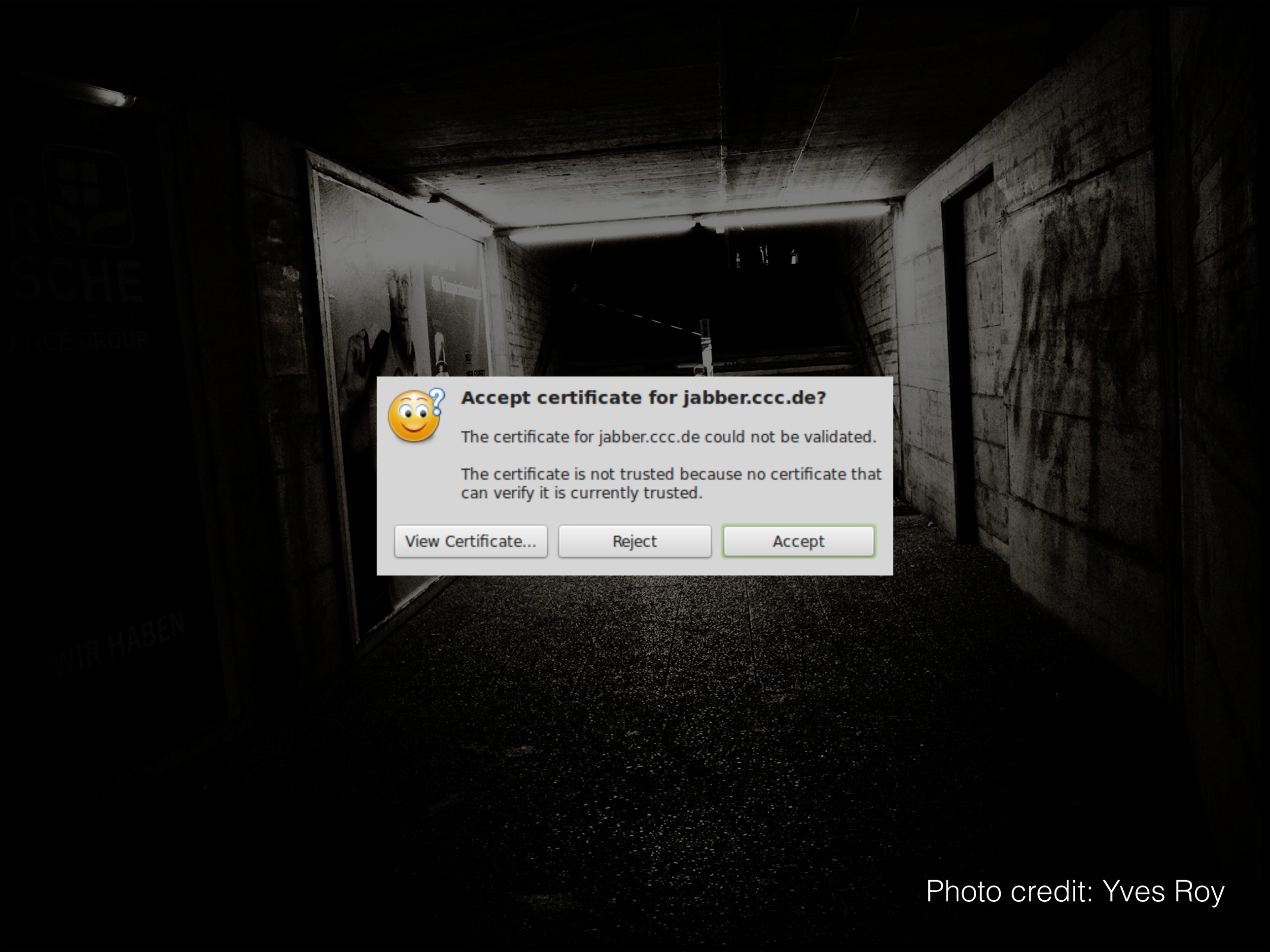
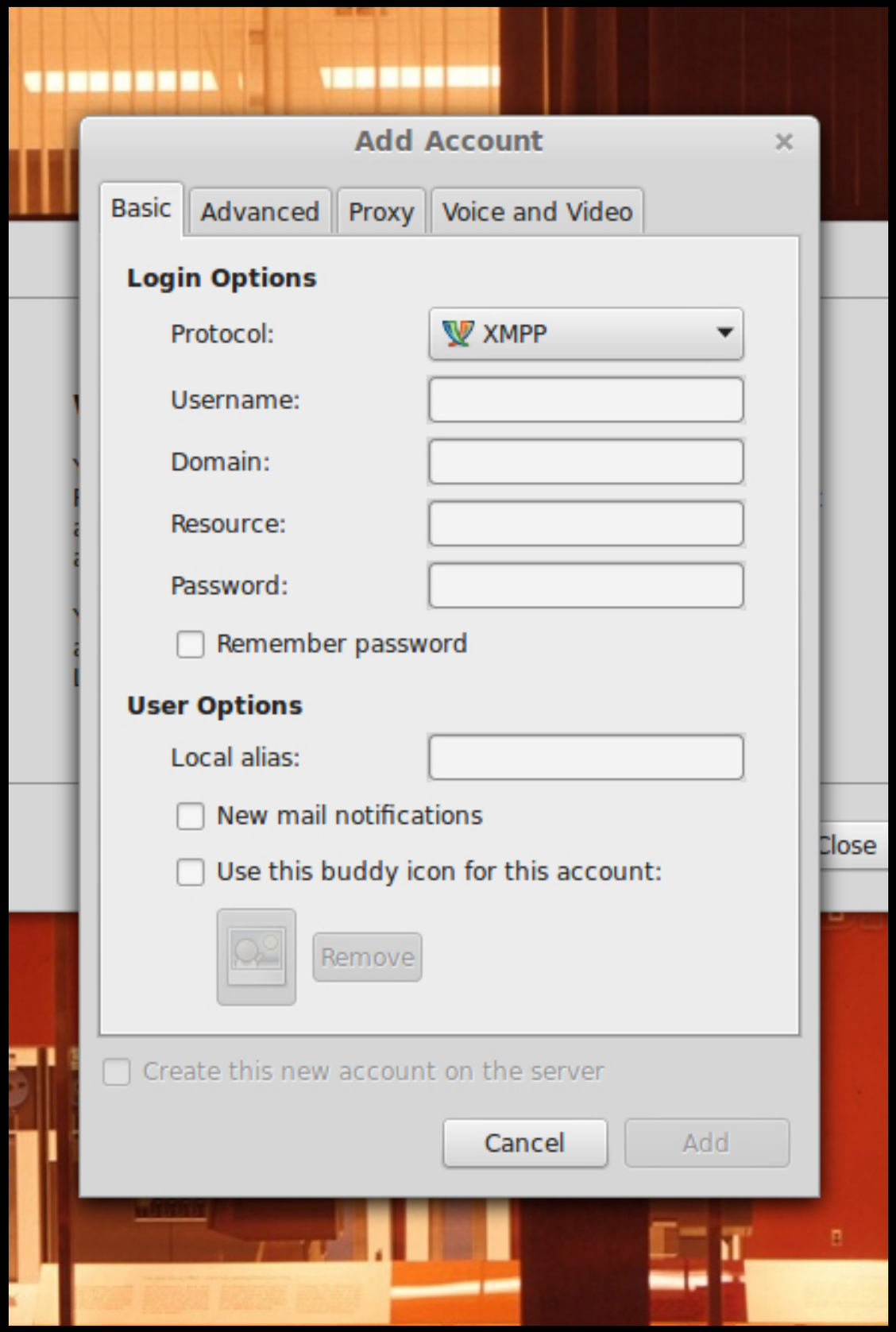


Photo credit: Yves Roy

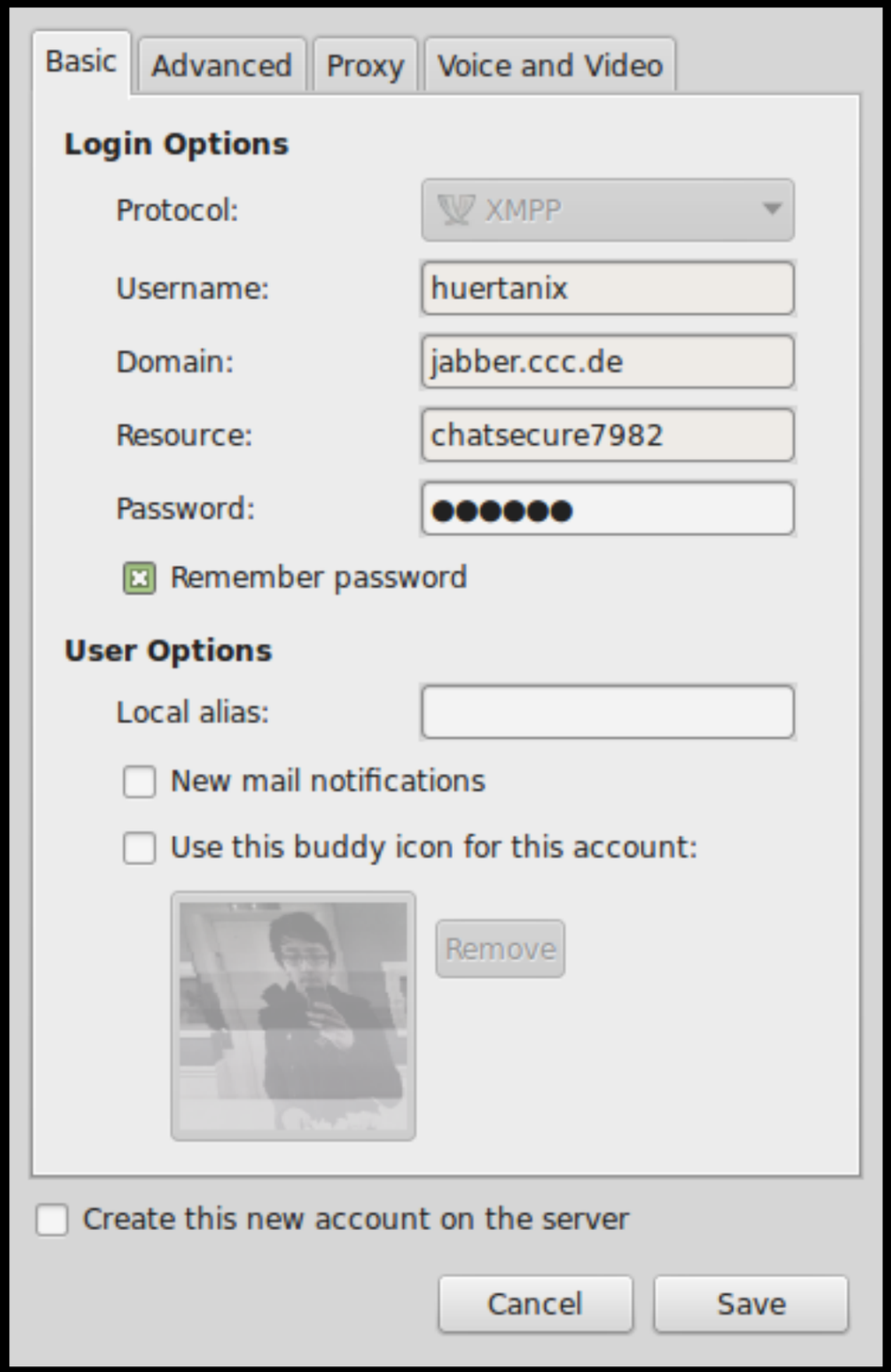
Pidgin

- Unlike Thunderbird w/ gandi.net, Pidgin lacks an on-boarding process for creating an account, just the ability to add a pre-existing account.
- People will call it Jabber, Pidgin will call it XMPP.
- Weird “Create this new account” checkbox always needs explanation.



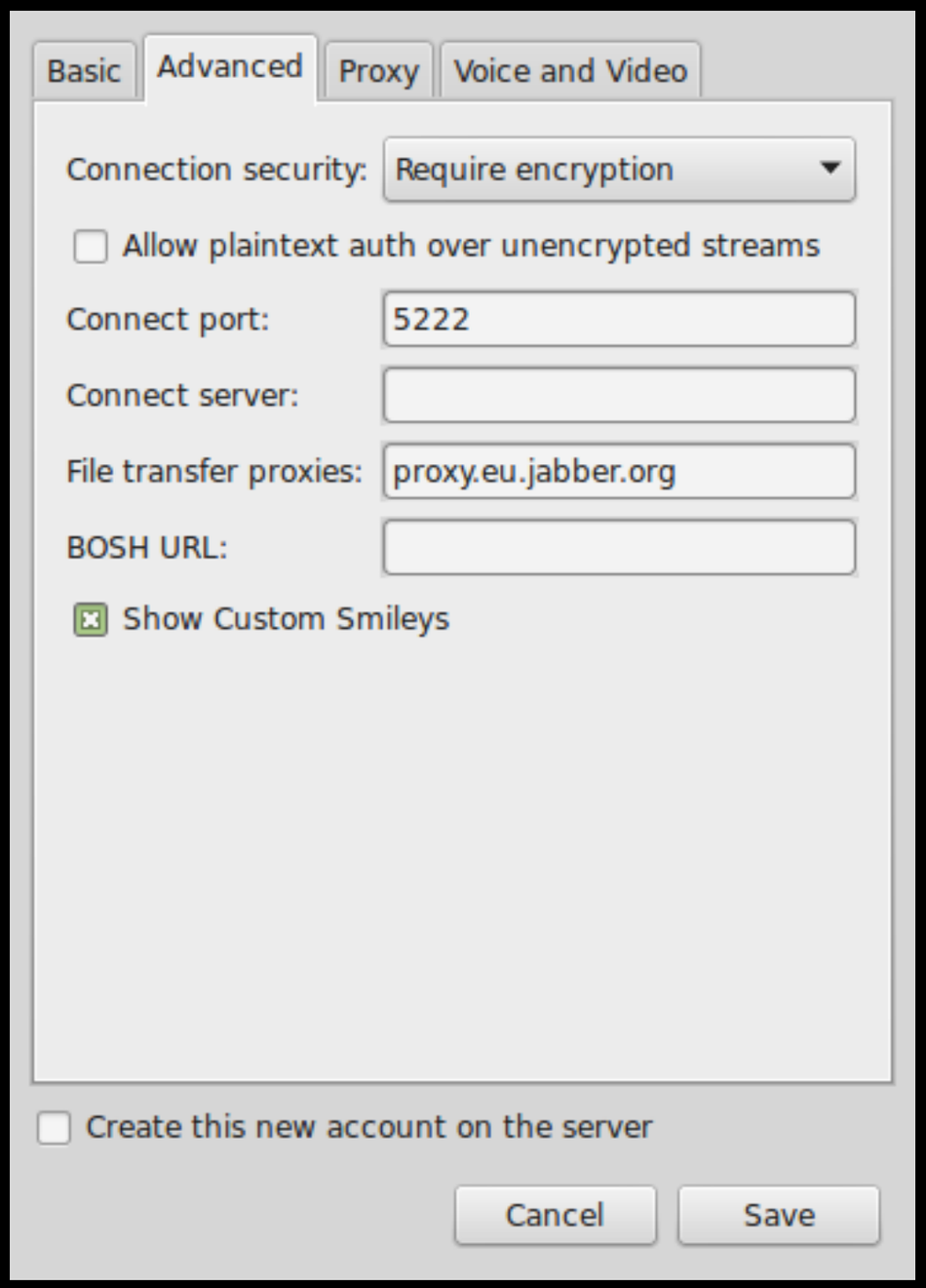
Pidgin

- After creating an account using text box, the option is still there for some reason.
- No noticeable way to change existing (lol six chars) account password.
- “New mail notifications.” At this point, Pidgin knows nothing about my email account.



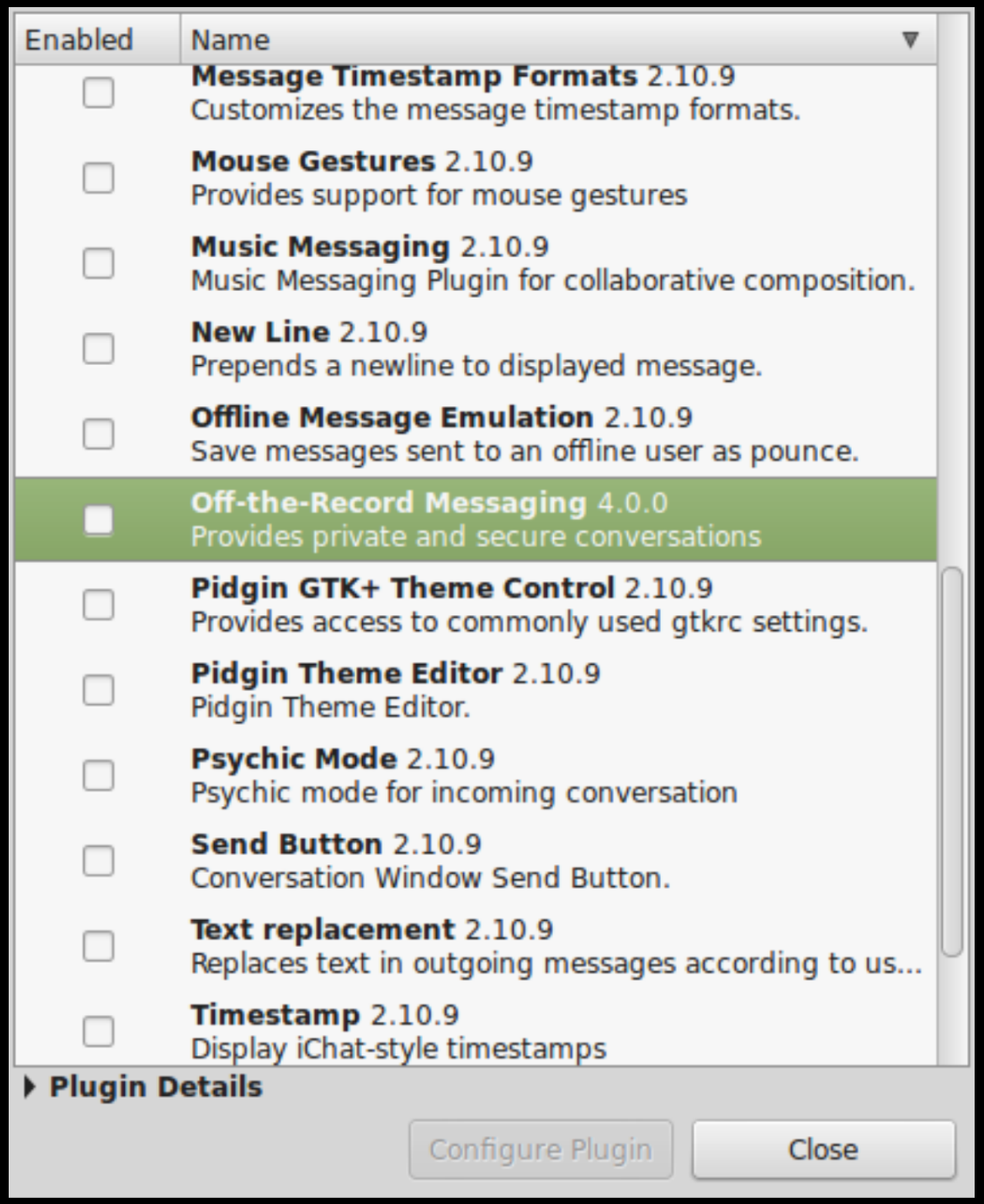
Pidgin

- SSL/TLS encryption not differentiated from OTR encryption in UI.
- OTR settings are buried in plugin config options.
- Seriously though, axe the Create the new account checkbox.

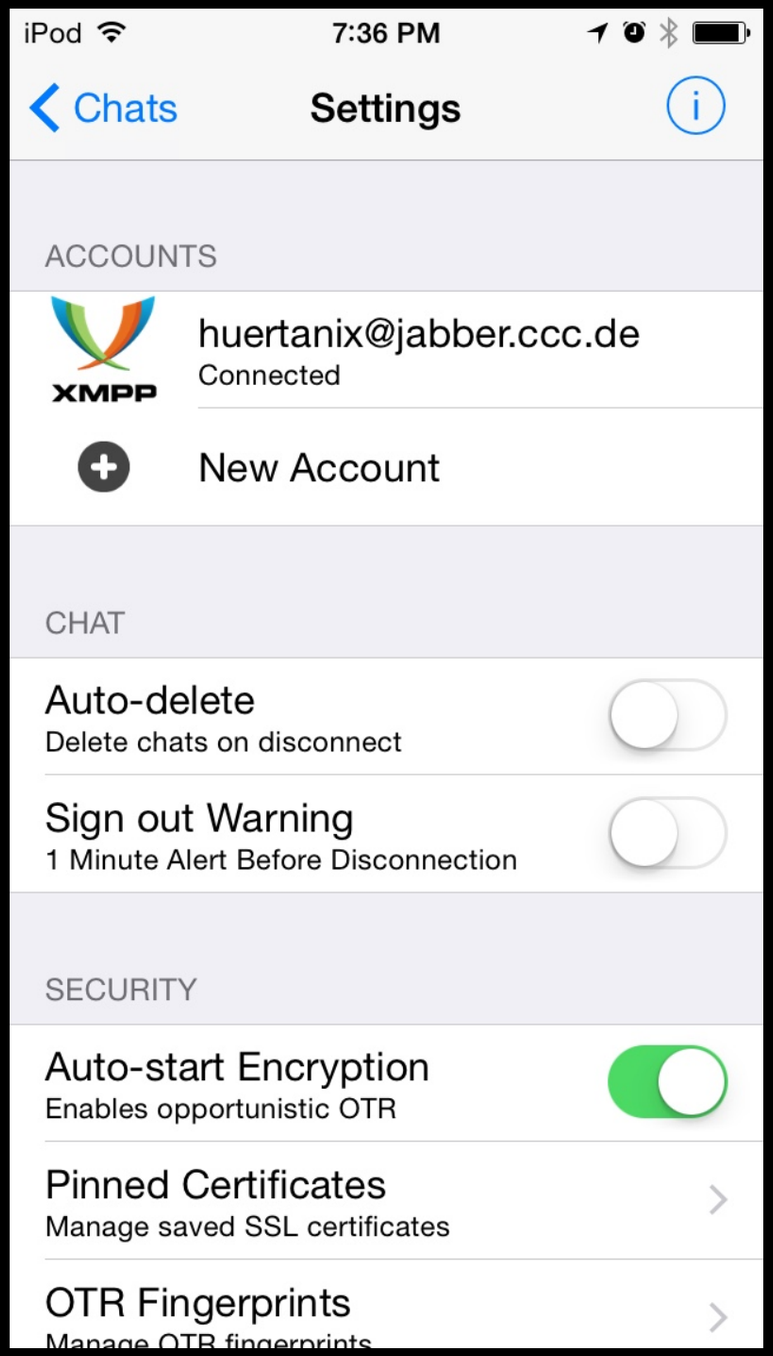


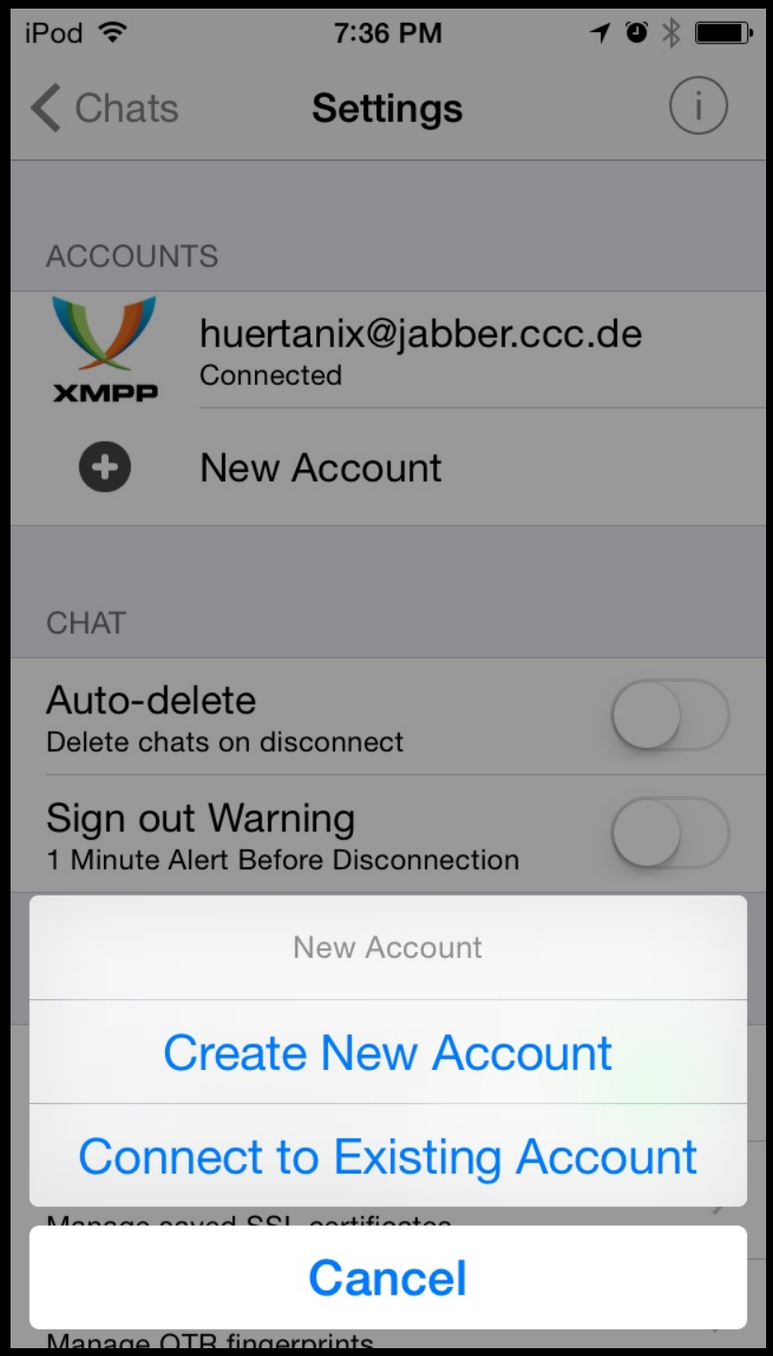
Pidgin

- Process of installing OTR varies between Windows and Linux and between Linux distros (well, package systems).
- Plan to have OTR in Pidgin installed by default began in 2013. Slated as issue for Pidgin 3.0 milestone, 55% of milestone issues complete as of July 2015: https://developer.pidgin.im/ticket/15513.

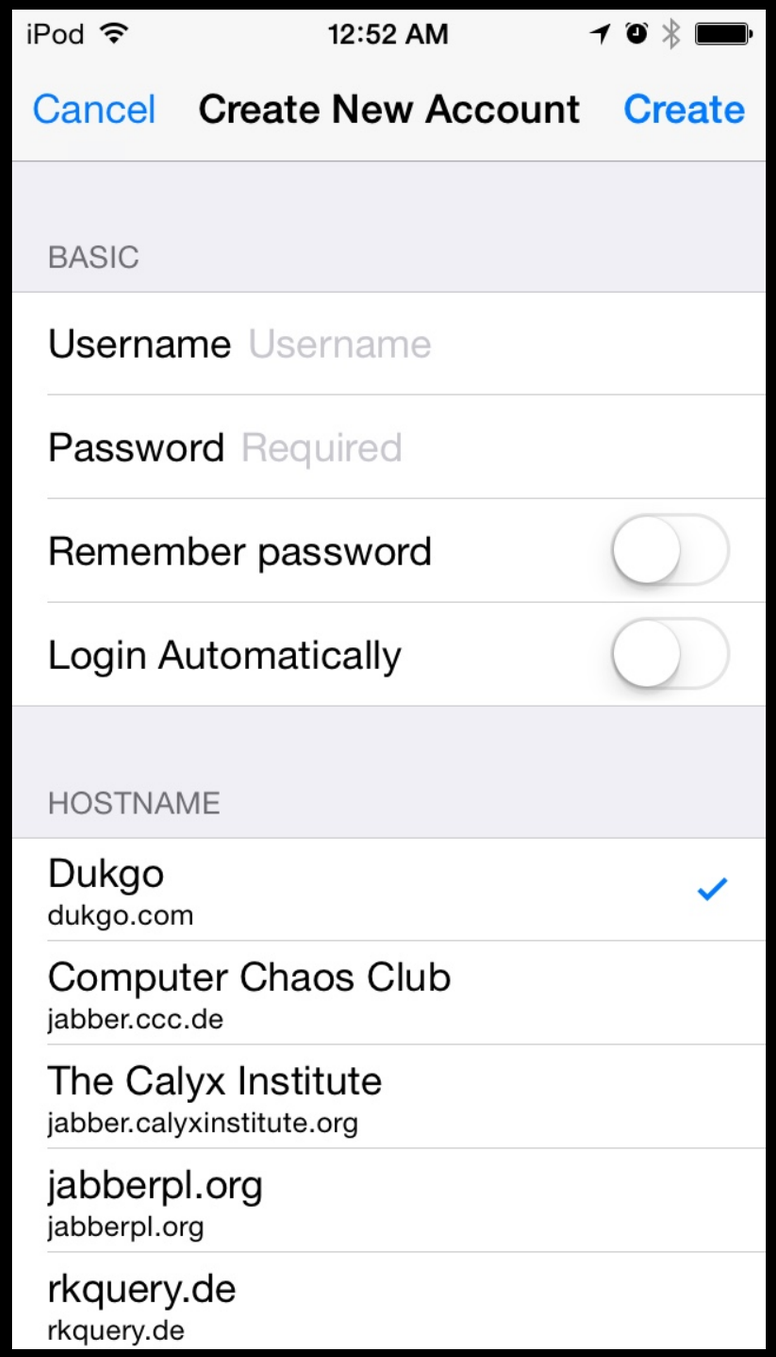


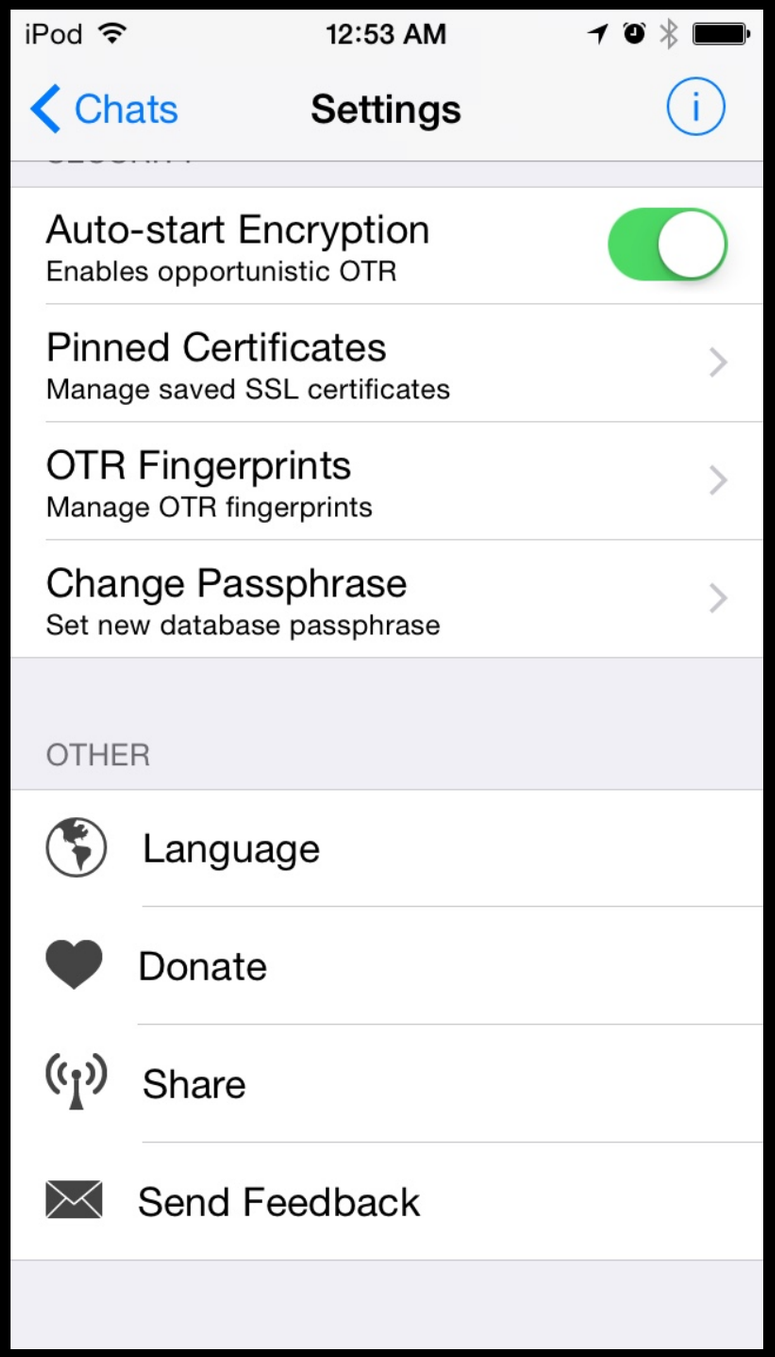
ChatSecure


iPod
7:36 PM
Chats
Settings
ACCOUNTS
XMPP
huertanix@jabber.ccc.de
Connected
New Account
CHAT
Auto-delete
Delete chats on disconnect
Sign out Warning
1 Minute Alert Before Disconnection
SECURITY
Auto-start Encryption
Enables opportunistic OTR
Pinned Certificates
Manage saved SSL certificates
OTR Fingerprints


iPod
7:36 PM
Chats
Settings
ACCOUNTS
XMPP
huertanix@jabber.ccc.de
Connected
New Account
CHAT
Auto-delete
Delete chats on disconnect
Sign out Warning
1 Minute Alert Before Disconnection
New Account
Create New Account
Connect to Existing Account
Cancel

ChatSecure


iPod
12:52 AM
Cancel
Create New Account
Create
BASIC
Username Username
Password Required
Remember password
Login Automatically
HOSTNAME
Dukgo
dukgo.com
Computer Chaos Club
jabber.ccc.de
The Calyx Institute
jabber.calyxinstitute.org
jabberpl.org
jabberpl.org
rkquery.de
rkquery.de


iPod
12:53 AM
Chats
Settings
Auto-start Encryption
Enables opportunistic OTR
Pinned Certificates
Manage saved SSL certificates
OTR Fingerprints
Manage OTR fingerprints
Change Passphrase
Set new database passphrase
OTHER
Language
Donate
Share
Send Feedback

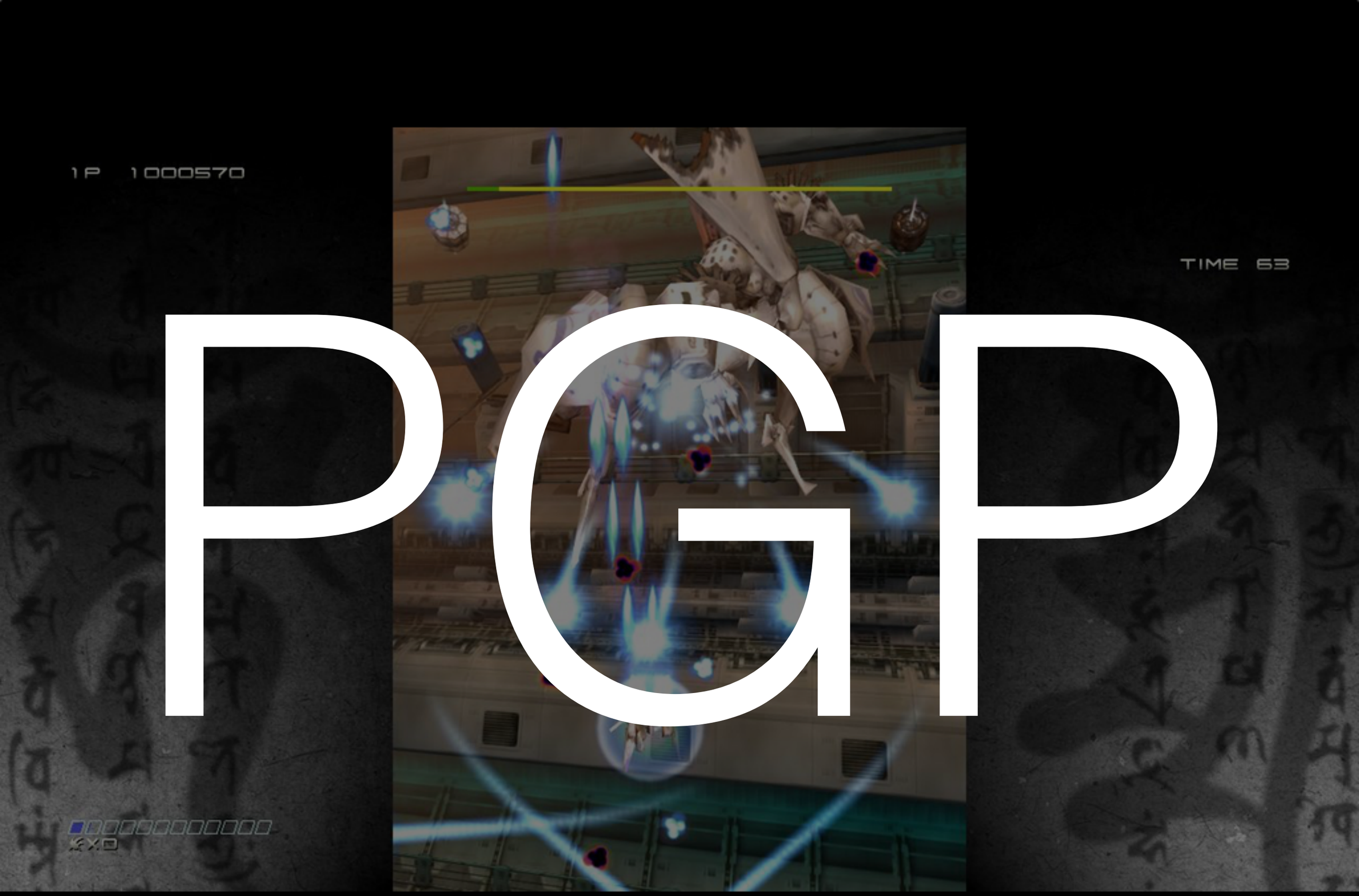


Photo credit: Gamerscore Blog

Lessons from 1999

- Add to your reading list: *Why Johnny Can't Encrypt* by Alma Whitten, J.D. Tiger

- Users in 1999 user testing ran into some of the same problems at Cryptoparties in 2015

Photo credit: K W Reinsch

Implementation Problems

- Too Many Tools: Fully open-source install on OS X cocktail is GPG Tools, Thunderbird, Enigmail.
- Too Many Different Tools: In [NYC] Cryptoparties, more people know about running PGP in OpenBSD than using pgp4win for Windows.
- Order of installation has to be explained explicitly.

Implementation Problems

- New (after Hotmail/Yahoo/Gmail) Internet users have never used email outside a website.
- People have decades+ old email accounts now, Thunderbird chokes on loading email via IMAP, slowing down everything to postpone-to-never point.
- The way POP mail works in the age of multiple devices scares everyone.

Implementation Problems

- Latest Thunderbird updates are mostly bug fixes, basically abandonware from a design perspective.
- Tiny Thunderbird text is tiny and getting tinier as hi-res screens grow.
- PGP and S/MIME settings both using the same verbs to describe what each do in the same window.
- Nothing to indicate the subject line is *not* encrypted.

rbird File Edit View Options Enigmail Tools Window Help 99% Wed 1:21 A

Inbox - huertanix@opentil.com

ertanix@opentil.com

Write Chat Address Book Tag Quick Filter Search… <⌘K>

Subject	From	Date
Re: [tor-relays] IANA running Tor relays?	nusenu	7/13/15, 6:19
New gTLD Update for the Week of July 13, 2015	101domain, Inc.	7/13/15, 6:16
Re: [tor-dev] Proposal: Merging Hidden Service Directories and Introduction Points	John Brooks	7/13/15, 2:10
[illegible]	[illegible]	7/13/15, 3:41
[illegible]	[illegible]	7/13/15, 1:42
[illegible]	[illegible]	7/13/15, 12:42
[illegible]	[illegible]	7/12/15, 10:59
[illegible]	[illegible]	7/12/15, 9:44
[illegible]	[illegible]	7/12/15, 9:44
[illegible]	[illegible]	7/12/15, 9:43

Write: Hey did you know this subject line is unencrypted?

Send Spelling Attach S/MIME Save

Enigmail: Attach My Public Key

Encrypt Th… View or change security settings
Digitally Sign This Message
View Security Info

From: David Huerta <huertanix@open…

To: Stephanie Hyland <steph.hyland@gmail.com>

Subject: Hey did you know this subject line is unencrypted?

--
david [.dh] huerta
davidhuerta.me

pgp public key: https://keybase.io/huertanix
pgp fingerprint: 35D7 26BD AE09 F328

Archive

when you arr
ave any ques

Dear Speakers,

Congratulations on being selected to present at DEF CON 23. Below you will find some instructions that will assist you in making the m
your speaking experience at DEF CON. Please be aware that the DEF CON speaker process is a high volume, low drag affair. Every year we
refine this process, please respect it by adhering to it. Every year we make small changes to the plan, even if you have spoken before
this whole letter as the process has changed.

Hours and Locations of Speaker Registration:

ntil.com is up to date

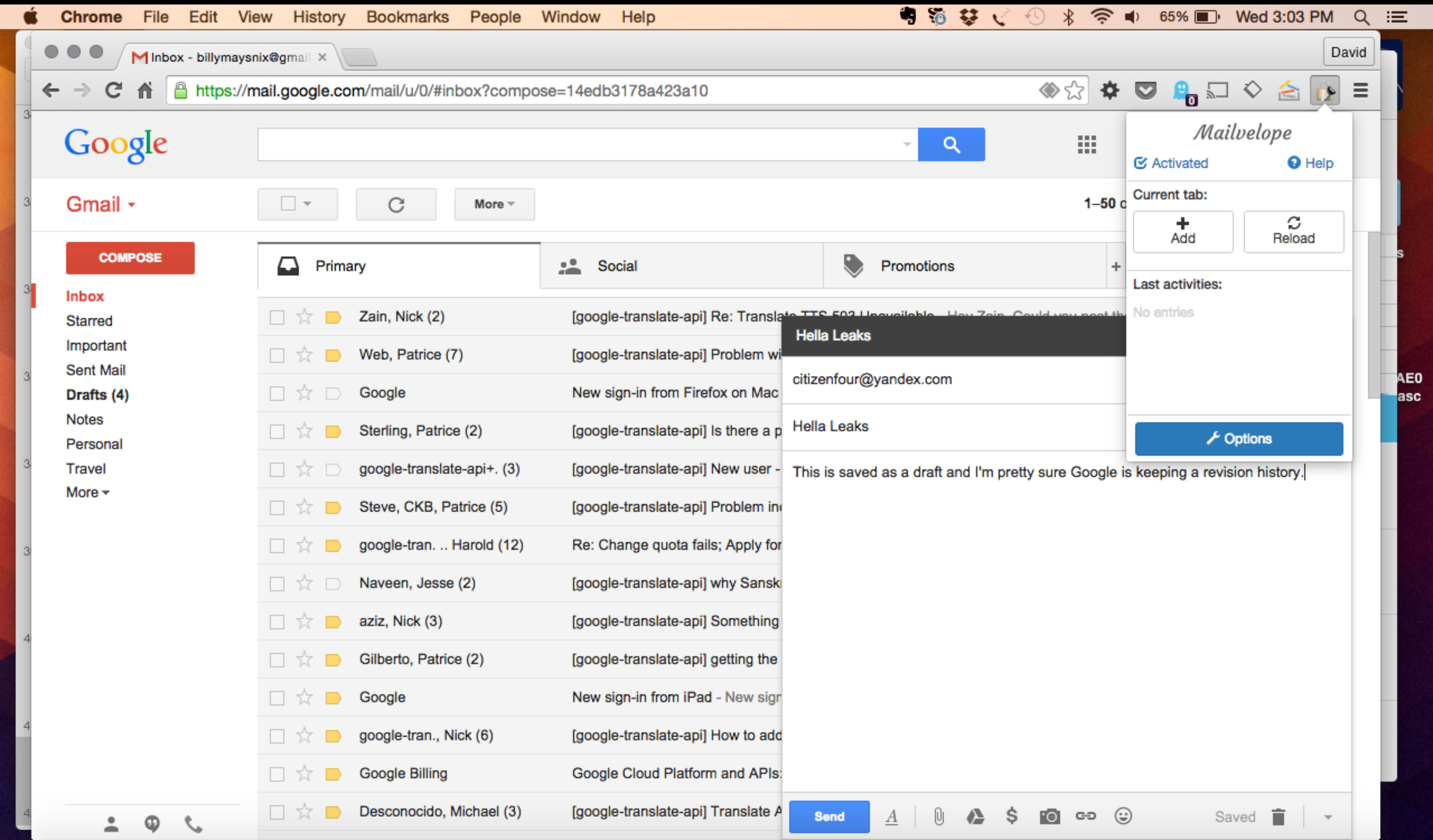
Unread: 0

Photo credit: Sasquatch I

PGP in the Browser

- Yahoo End-to-End: Browser extension, adds PGP functionality on top of webmail.
- Google End-to-End: ^ See above.
- WhiteoutMail: ^ Ditto.
- Mailvelope: ^ Yup.

Migrating UI/UX Issues to JS



In-browser PGP Advantages

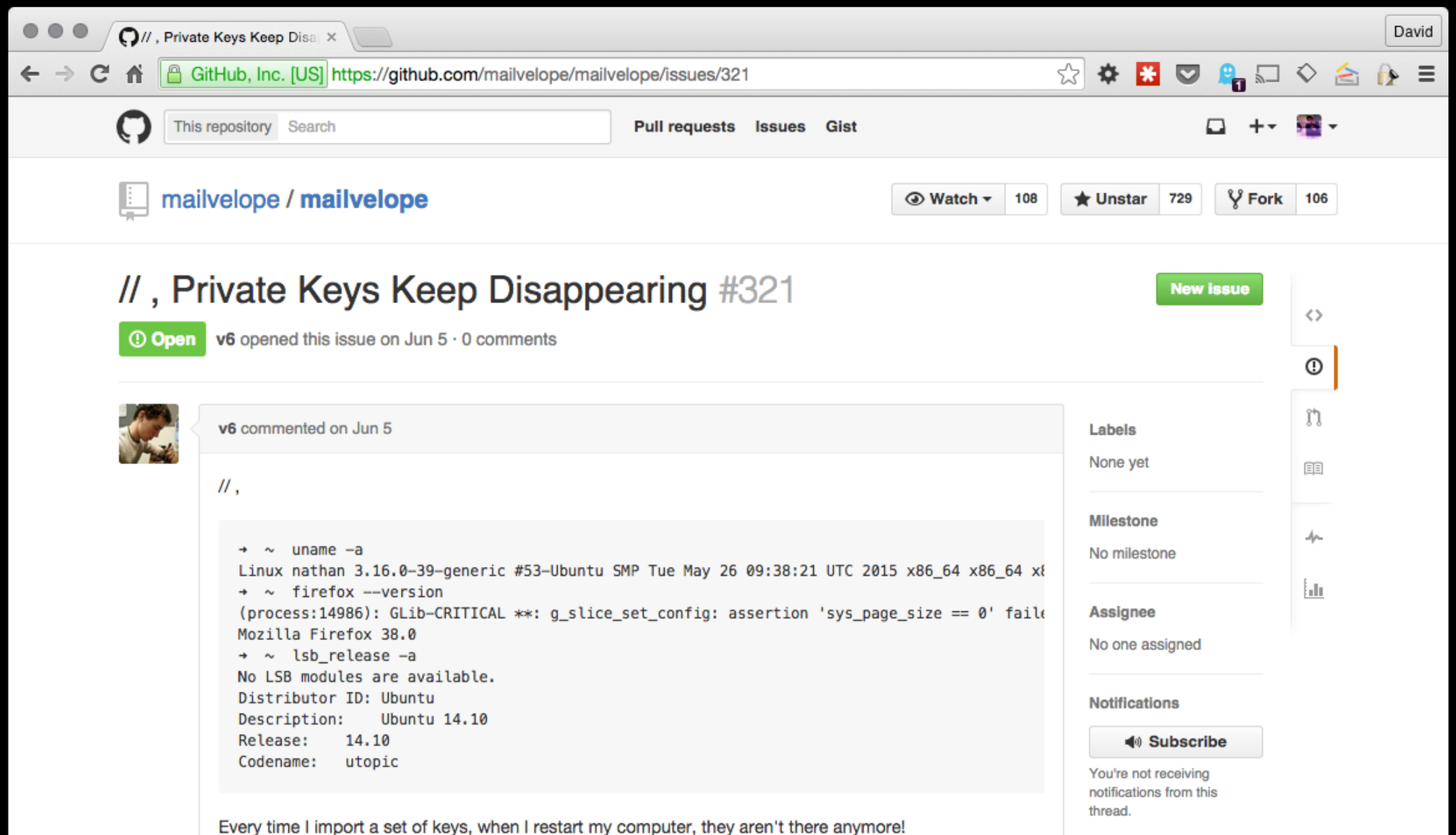
- User is already working in a familiar interface and workflow.

- Everyone has a web browser installed already.

- *Chromebooks now the fastest-growing segment of PC market*, The Register - http://www.theregister.co.uk/2013/07/11/chromebooks_fastest_growing_pc_market/

In-browser PGP Disadvantages

- PGP



Sensible Design for 1991

- Private keys as files: One user, one computer, inside a locked house. No automatic cloud backup software. No constant/fast internet connection between attacker and OS.

- Key servers: No https-encrypted sites to post public key to. No variety of https-encrypted social media to transmit public key. No other encrypted communication basically at all.

- RSA-based keys: Public keys long enough to pass tl;dr threshold, fingerprints—err, key IDs used for verification. Encryption ran slowly, but bearably in C. ECC still experimental, unvetted.

Design Challenges for 2015

- Private keys as files: Backup software means your private key may accidentally get copied to cloud. Laptops get lost/stolen. Migrating keys from one machine to the next is not a thought-out process. Browser plugins holding private keys is concerning.

- Key servers: Many use cases for PGP now involve sending email to a person only known by a Twitter/social media account, w/o the possibility of in-person signing. Directories like Keybase provide a contemporary use case for verifying identity.

- RSA-based keys: In-browser PGP means JavaScript PGP. Performance is significantly lower than ECC-based alternatives like NaCL, because math, idk. Slowness == users rage quit.

Following Up

- Twitters: @huertanix and @cryptopartynyc
- Web: http://www.davidhuerta.me
- Peerio: huertanix
- PGP Public Key “fingerprint”: 1482 F3BF 3F16 6BD4 3525 D55E 35D7 26BD AE09 F328
- **BONUS**: Bookmark http://www.simplysecure.org, listen to @kayteenesmith’s HOPE talk on user testing: http://hope.net/schedule.html#diyusabili