



Alice and Bob are Really Confused

David Huerta - DEF CON 23

Photo credit: Robert Young

A Shiba Inu dog is sitting on a light-colored couch, looking towards the left. The dog has orange and white fur. In the background, there is a wooden shelf with some items, including a framed picture and some pink flowers. The text "much codes" is overlaid in cyan on the left side of the image.

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 noseey.

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.



Macintosh Human Interface Guidelines

by Apple Computer, Inc.



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



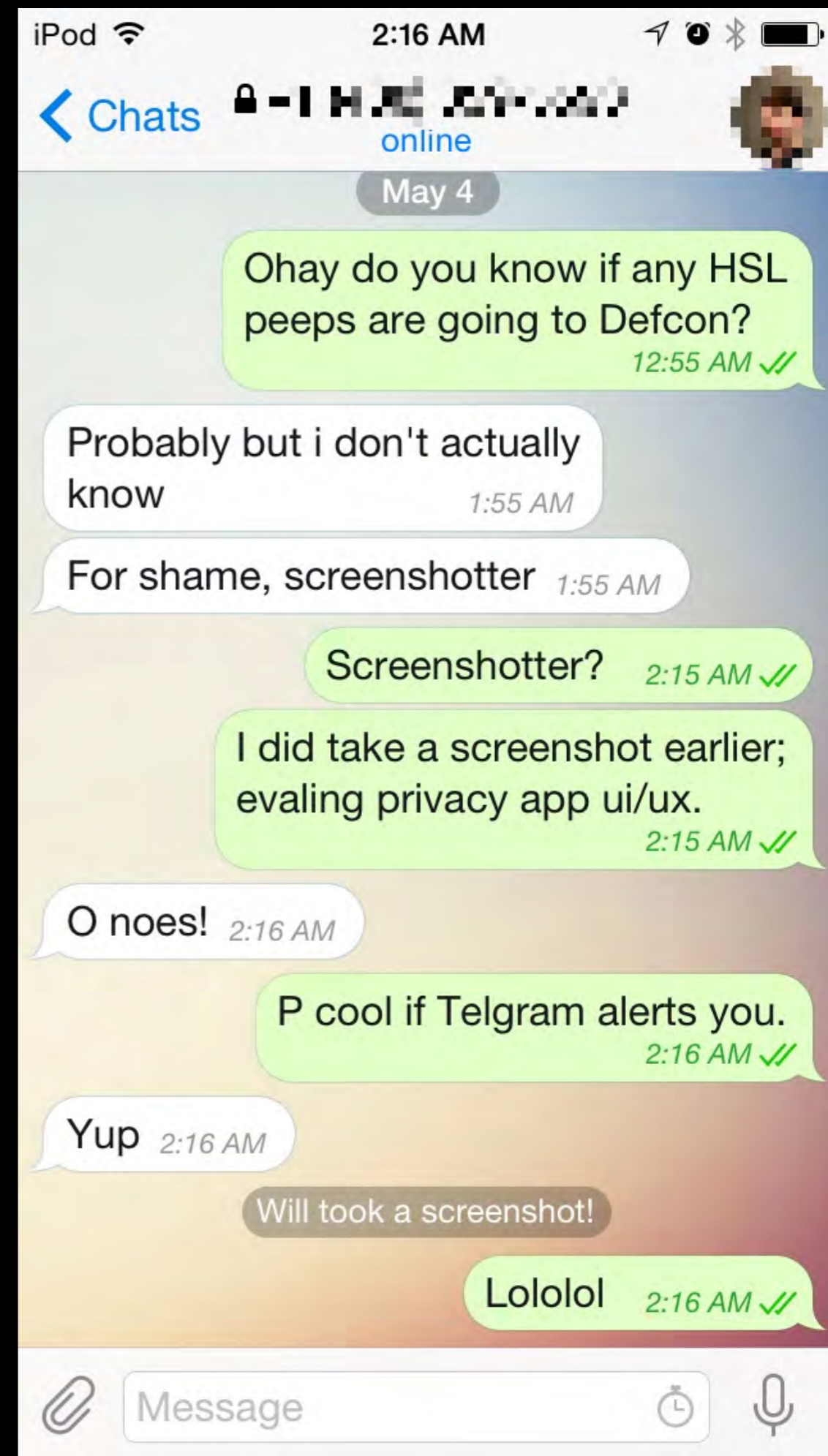
A photograph of two lemurs in a natural setting. One lemur is perched on a dark, textured rock on the right side of the frame, looking towards the left. The second lemur is on the left, reaching out with its right hand towards the first lemur's hand. The background is a soft-focus green field. The text 'Constructive Criticism' is overlaid in white, centered across the middle of the image.

Constructive Criticism

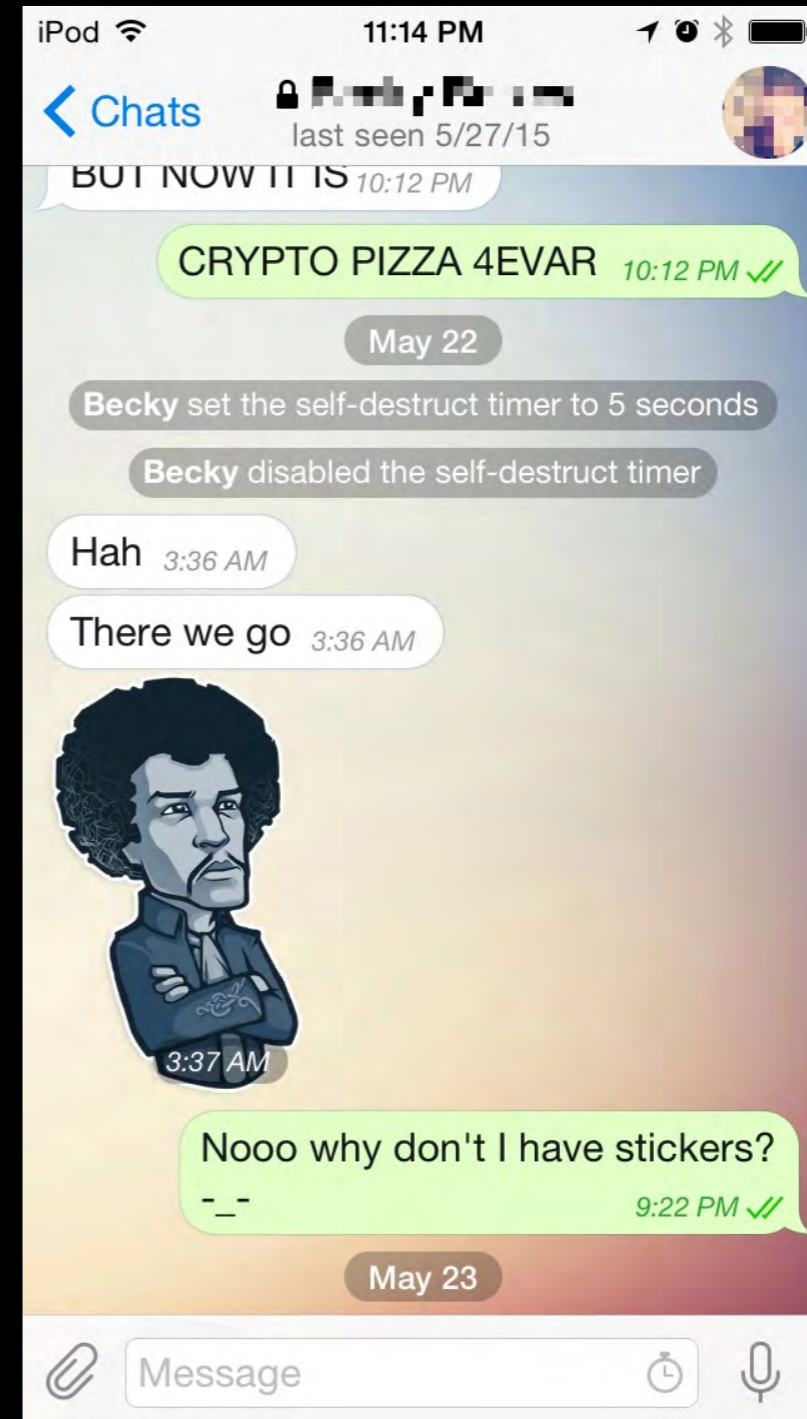
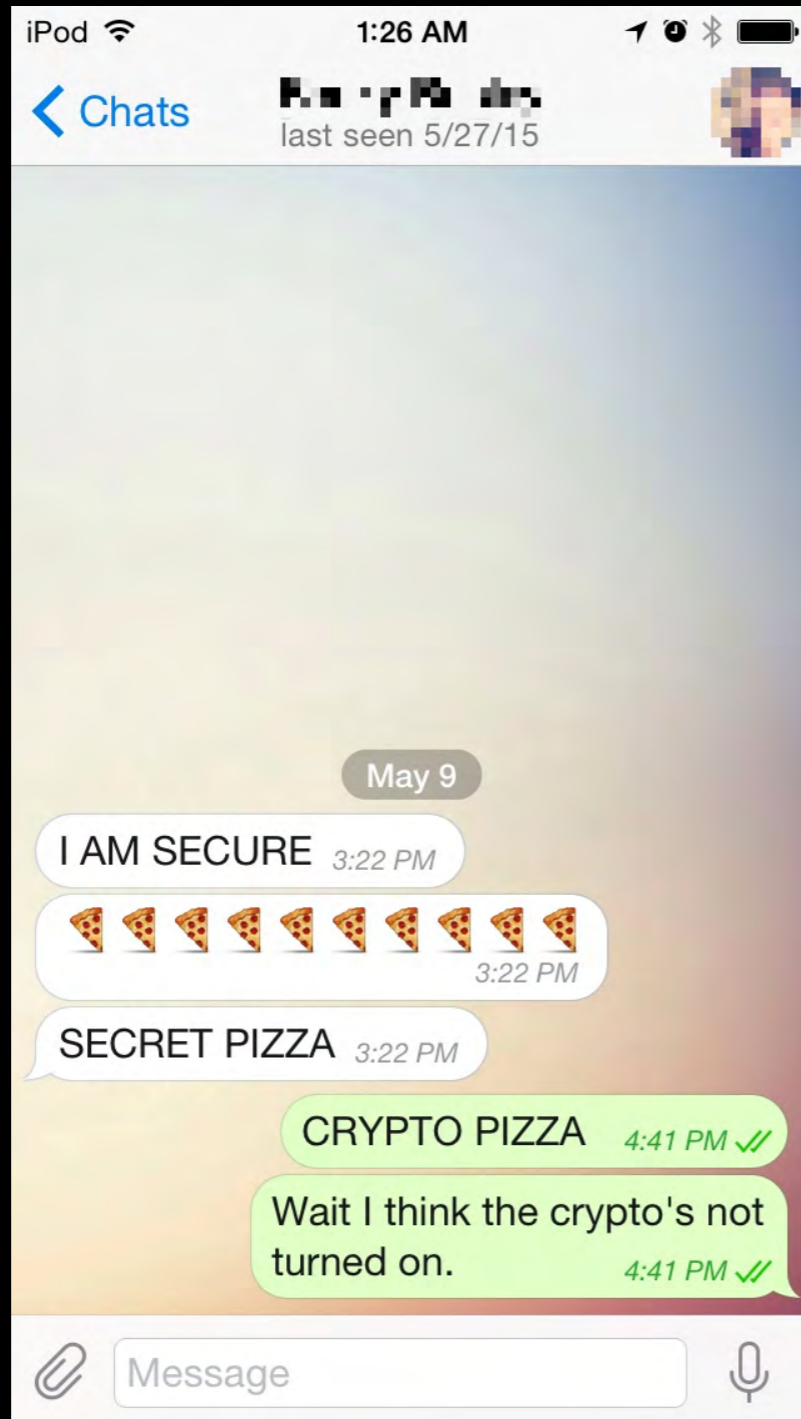
Photo credit: Tambako the Jaguar

Telegram

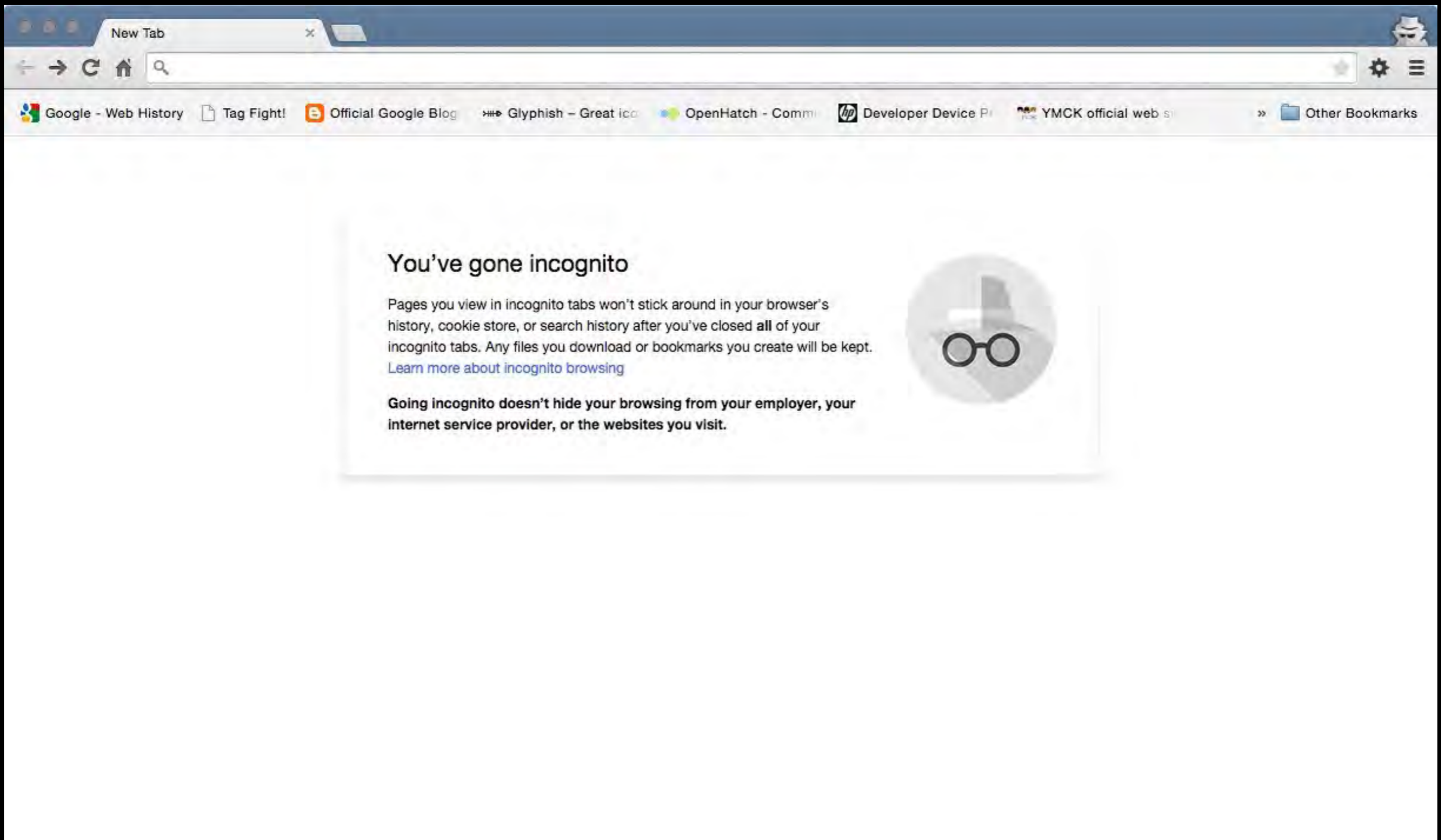
- **DISCLAIMER:** Putin has more money than you. Roll your own phat blunts, but don't roll your own crypto.
- **DISCLAIMER:** No out-of-band verification like in OTR.
- EVERY APP NEEDS THIS THO: Alerts other party when screenshot is taken.
- Hard to tell if your chat is encrypted or not, which is a problem...



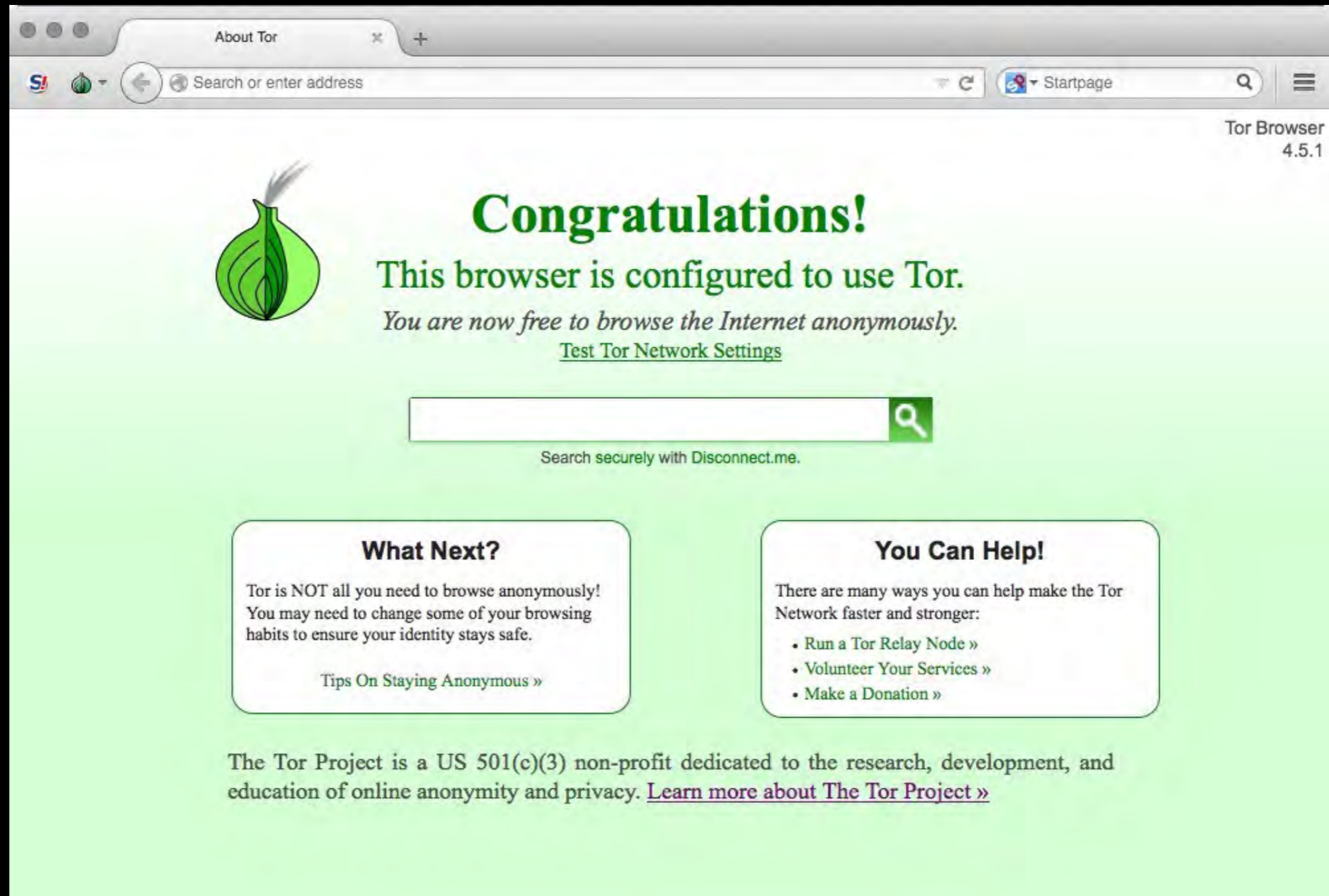
One of these is end-to-end



Mode Made Obvious...ish



Mode Made Obvious...ish




About Tor

Search or enter address

Startpage

Tor Browser 4.5.1



Congratulations!

This browser is configured to use Tor.
You are now free to browse the Internet anonymously.

[Test Tor Network Settings](#)

Search securely with Disconnect.me.

What Next?

Tor is NOT all you need to browse anonymously!
You may need to change some of your browsing habits to ensure your identity stays safe.

[Tips On Staying Anonymous »](#)

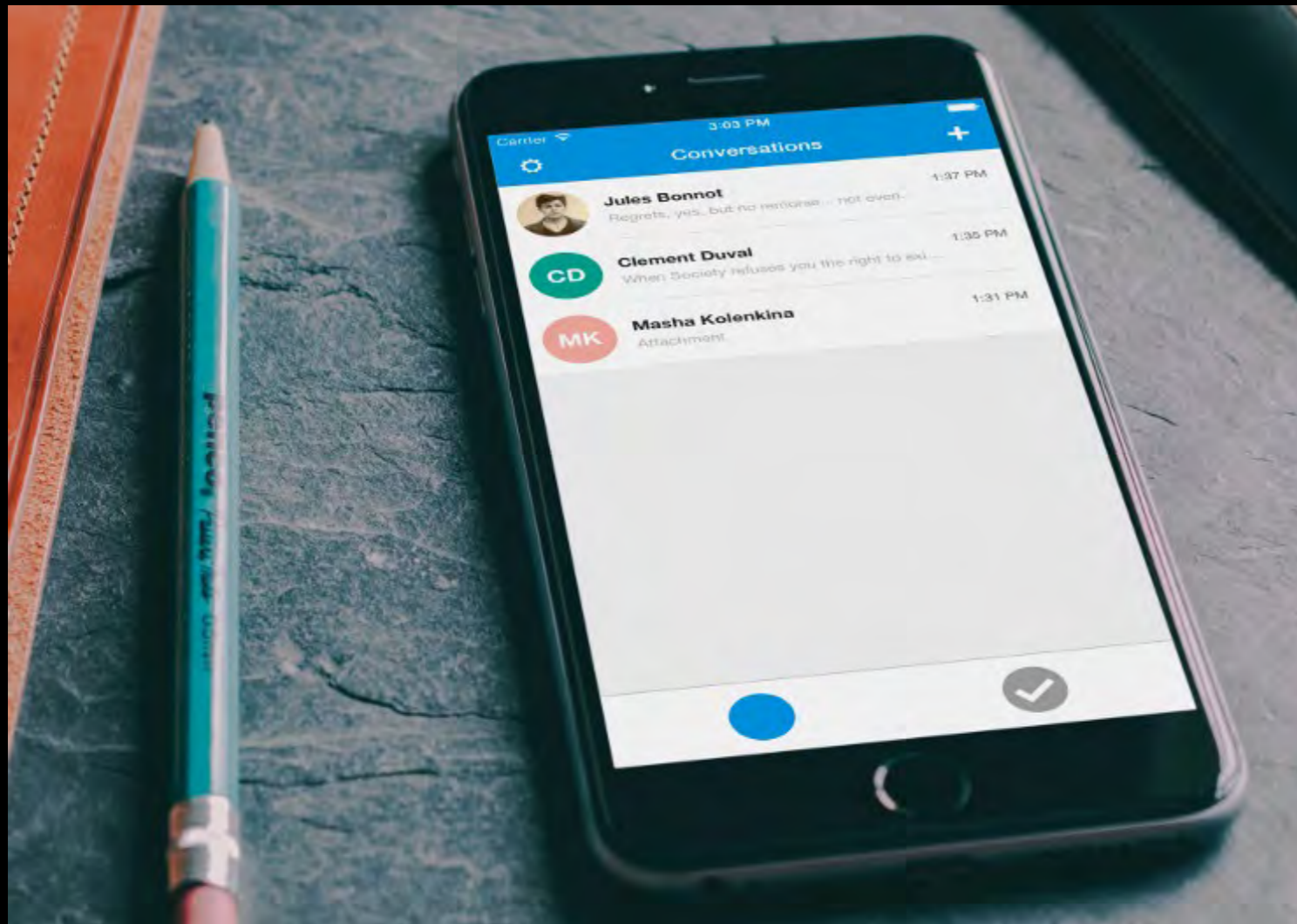
You Can Help!

There are many ways you can help make the Tor Network faster and stronger:

- [Run a Tor Relay Node »](#)
- [Volunteer Your Services »](#)
- [Make a Donation »](#)

The Tor Project is a US 501(c)(3) non-profit dedicated to the research, development, and education of online anonymity and privacy. [Learn more about The Tor Project »](#)

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 Message

Inbox

All Messages

100% New Email



David

To coolpizza

Cool subject



Cool message.

Send

Send

Press Enter to send

Inbox

ENCRYPTED

ENCRYPTED

con workshop
tly be there,
ng to check
[ng-day-pass:](#)

To coolpizza

Cool subject

Cool me

Send

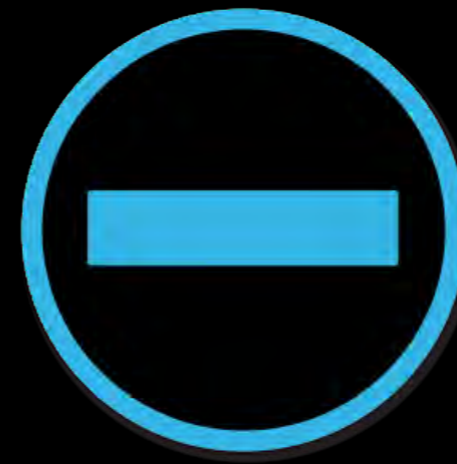
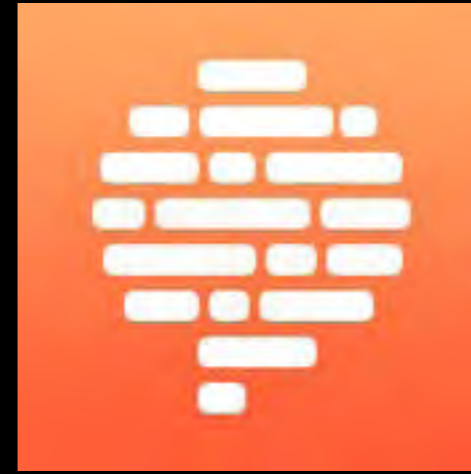


Message has no recipients

Please enter at least one recipient to send your message.

OK

Interoperability :(



Interoperability :(

- Axolotl: Used by Signal.
- Minilock: Used by Peerio.
- OTR: Used by a 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 everyone.

iPod 3:32 PM 102 Results

otr 102 Results

Related: old time radio > the lone ranger > sherlock

Vintage Radio™
Orion Internet Servic...
★★★★★ (638) **\$3.99**
In-App Purchases

OTR Streamer
Arbitrary Software, LLC.
★★★★★ (23) **GET**
In-App Purchases

Vintage Radio Genres Popular More...
Adventure
Anthology
Comedy
Crime-Detective
Drama
History
Horror

Vintage Radio Genres Comedy
Abbott and Costello
79 shows
Abroad with the Lockharts
7 shows
Advs. of Maisie, The
55 shows
Advs. of Topper, The
3 shows
Al Jolson Show, The
10 shows

Featured Top Charts Explore Search Updates



Accept certificate for jabber.ccc.de?

The certificate for jabber.ccc.de could not be validated.

The certificate is not trusted because no certificate that can verify it is currently trusted.

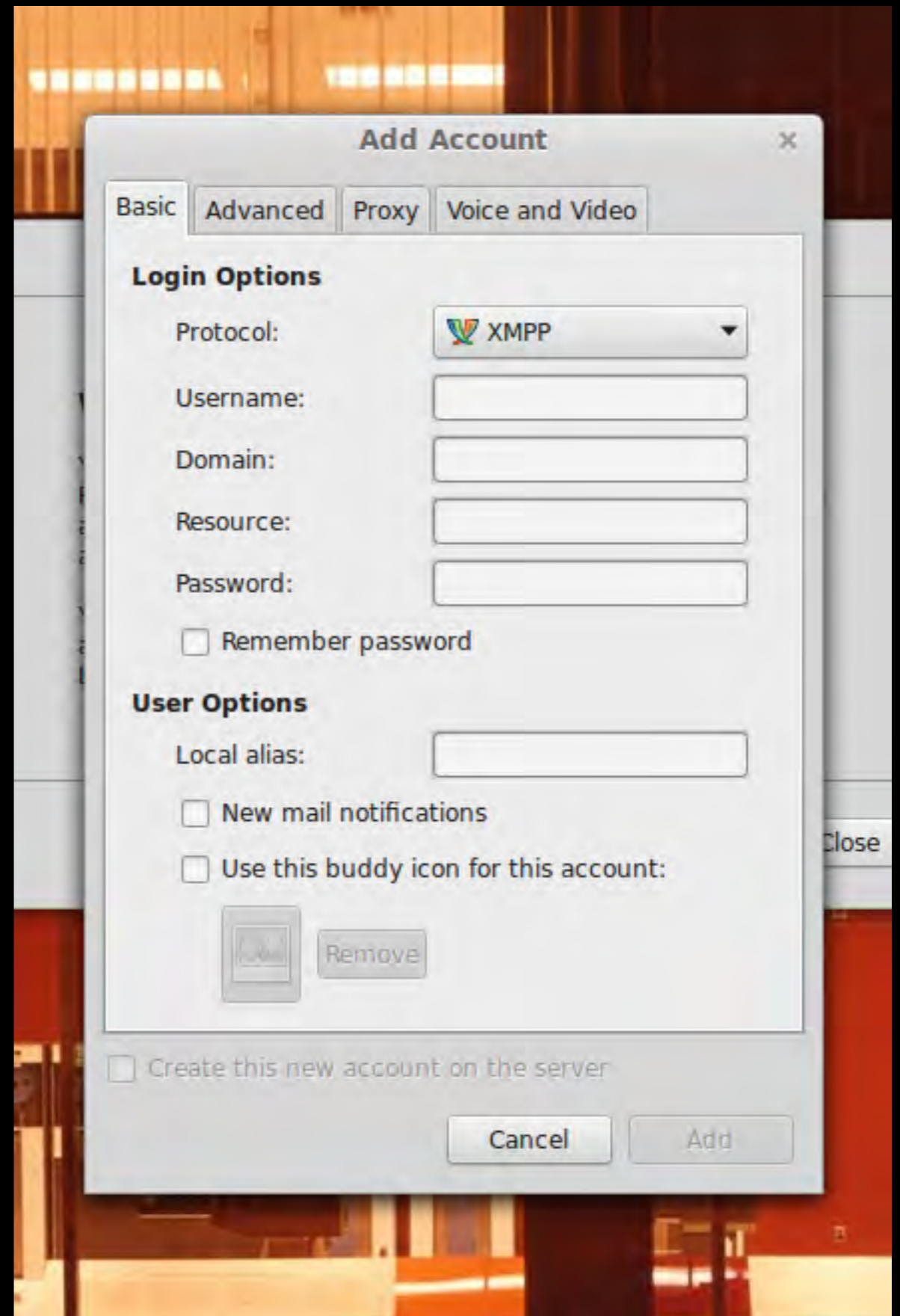
View Certificate...

Reject

Accept

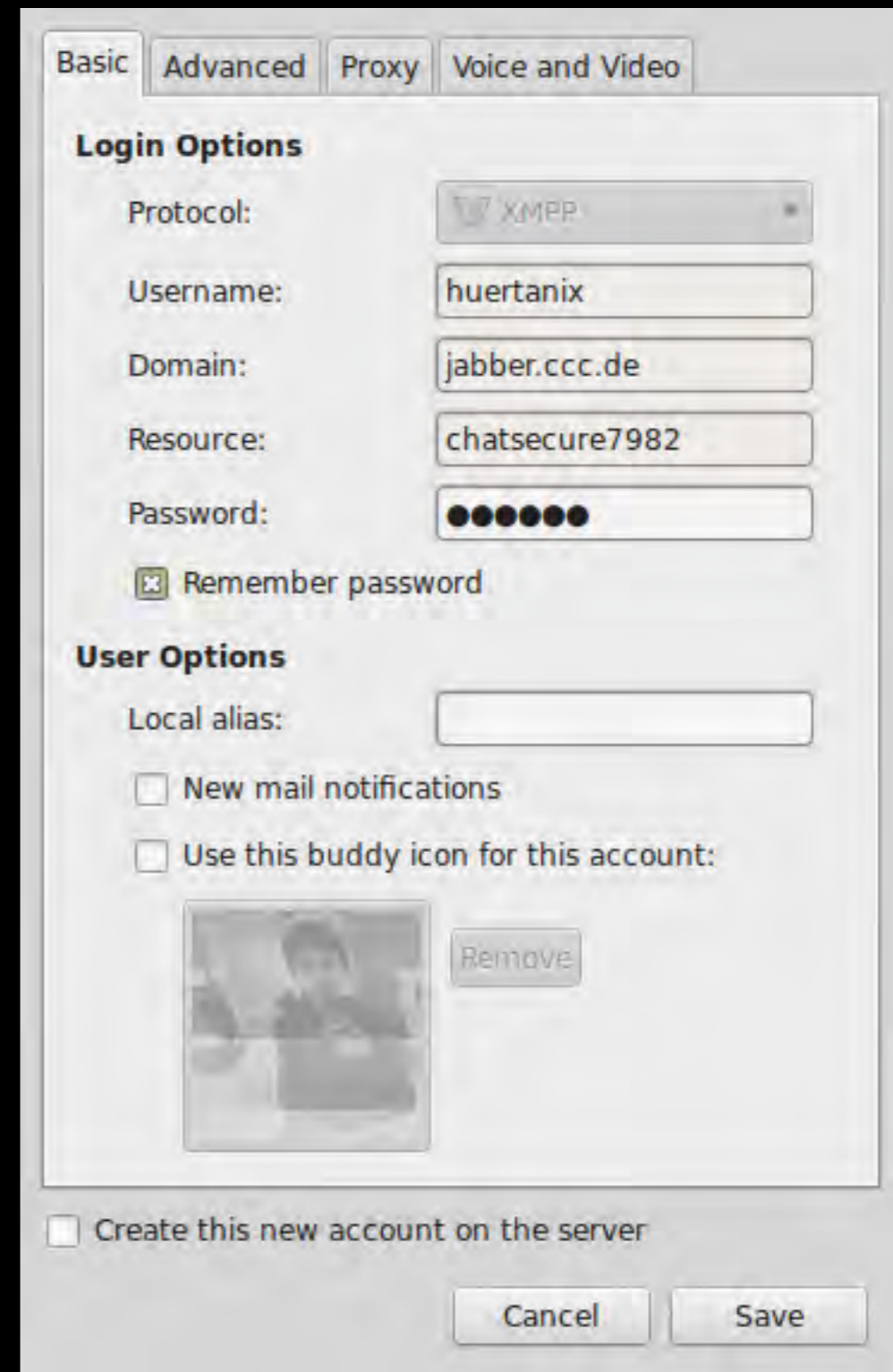
Pidgin

- 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 char) account password.
- “New mail notifications.” At this point, Pidgin knows nothing about my email account.



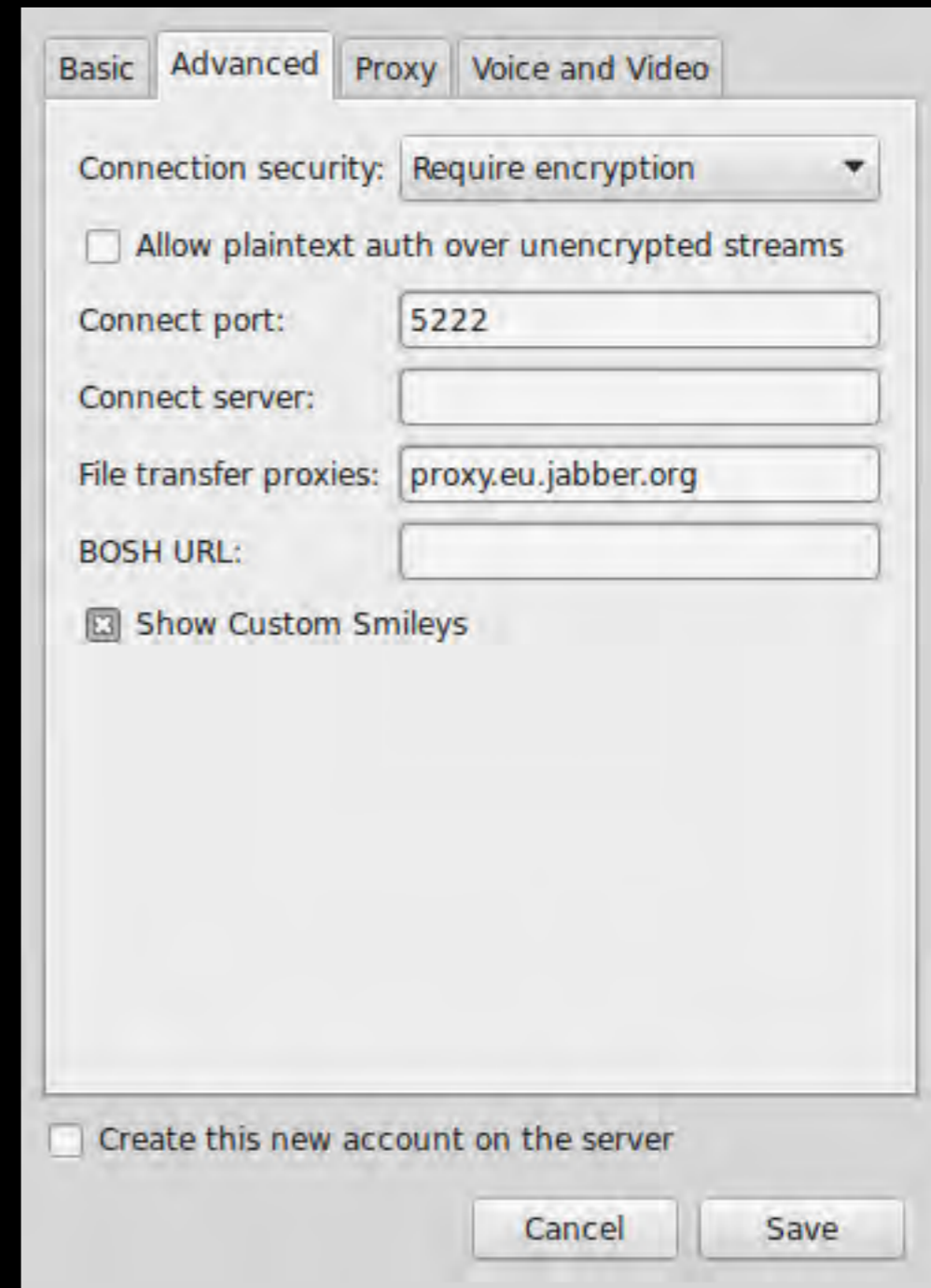
The image shows a screenshot of the Pidgin account configuration dialog box, specifically the 'Basic' tab. The dialog has four tabs: 'Basic', 'Advanced', 'Proxy', and 'Voice and Video'. The 'Basic' tab is selected and contains the following fields and options:

- Login Options:**
 - Protocol: XMP
 - Username: huertanix
 - Domain: jabber.ccc.de
 - Resource: chatsecure7982
 - Password: (masked with six dots)
 - Remember password
- User Options:**
 - Local alias: (empty text box)
 - New mail notifications
 - Use this buddy icon for this account:
 - Icon: A small, faded image of a person's face.
 - Remove button: A button labeled 'Remove' next to the icon.

At the bottom of the dialog, there is a checkbox labeled 'Create this new account on the server' which is currently unchecked. At the very bottom right, there are two buttons: 'Cancel' and 'Save'.

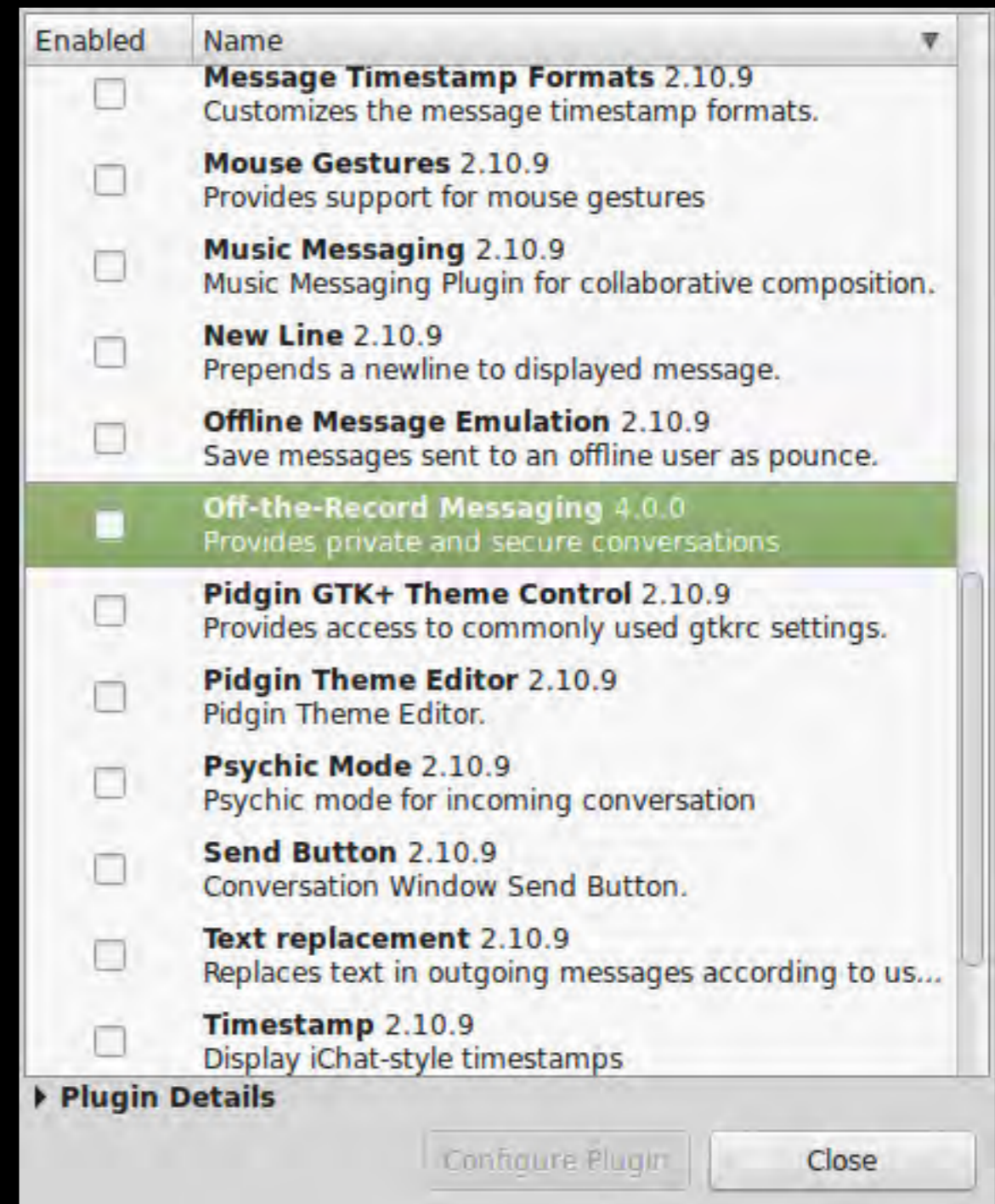
Pidgin

- 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.

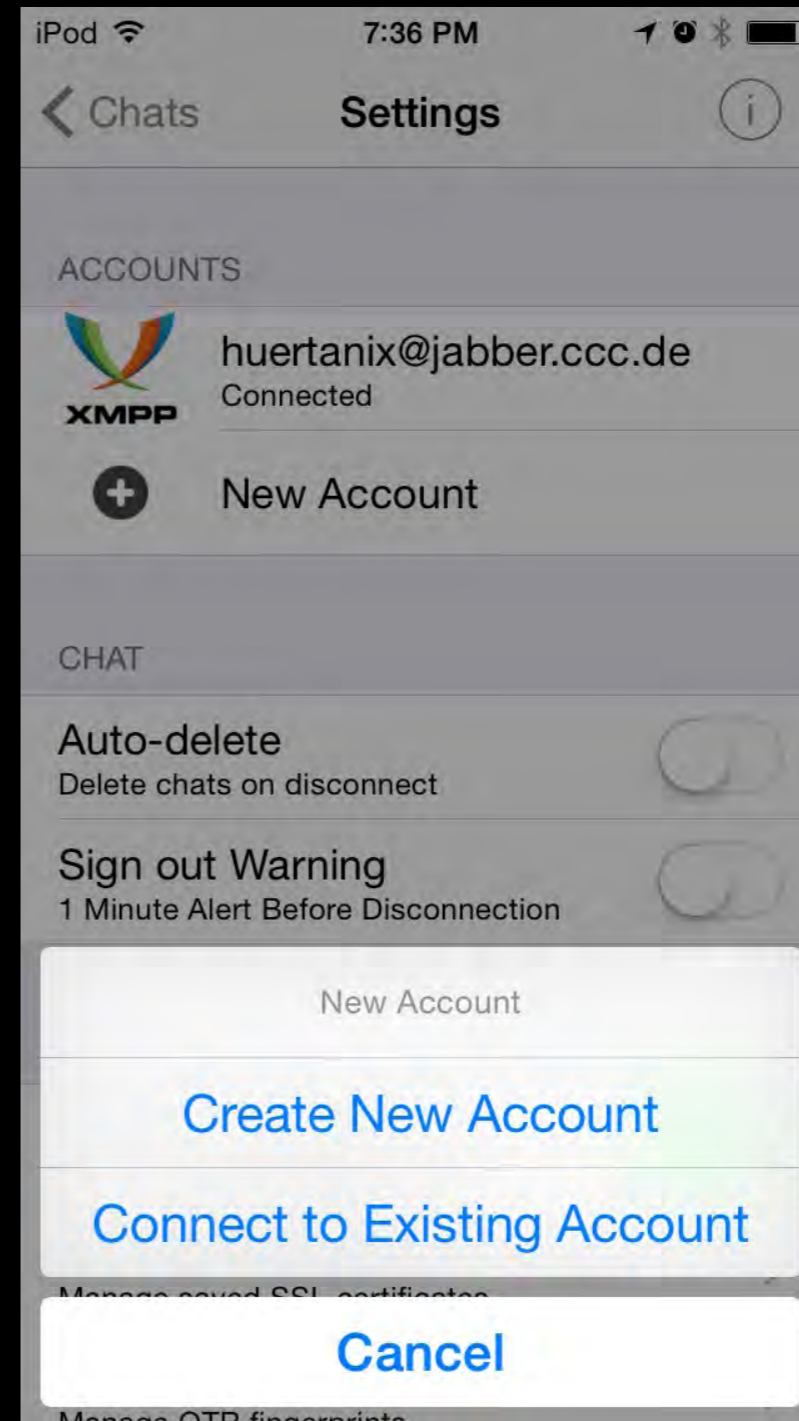


Pidgin

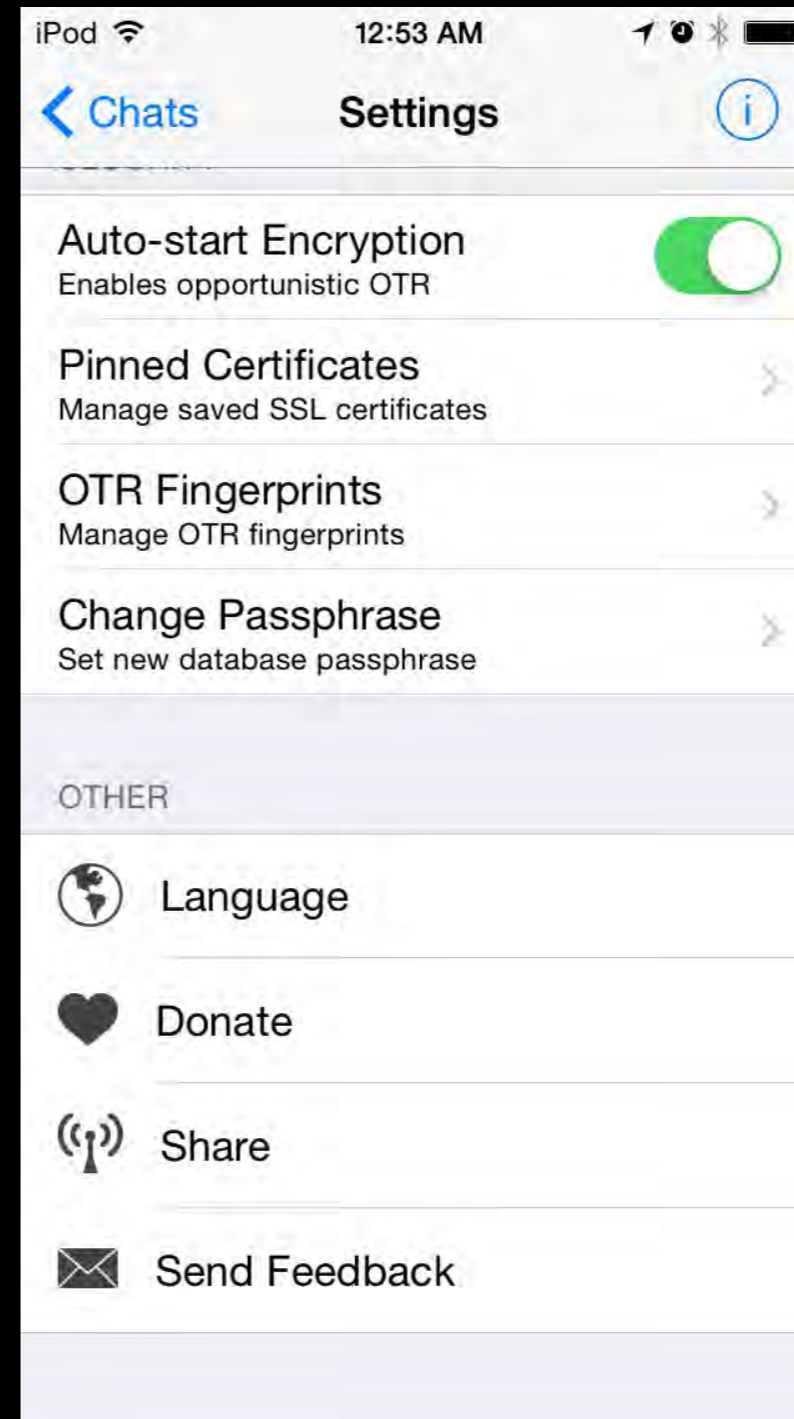
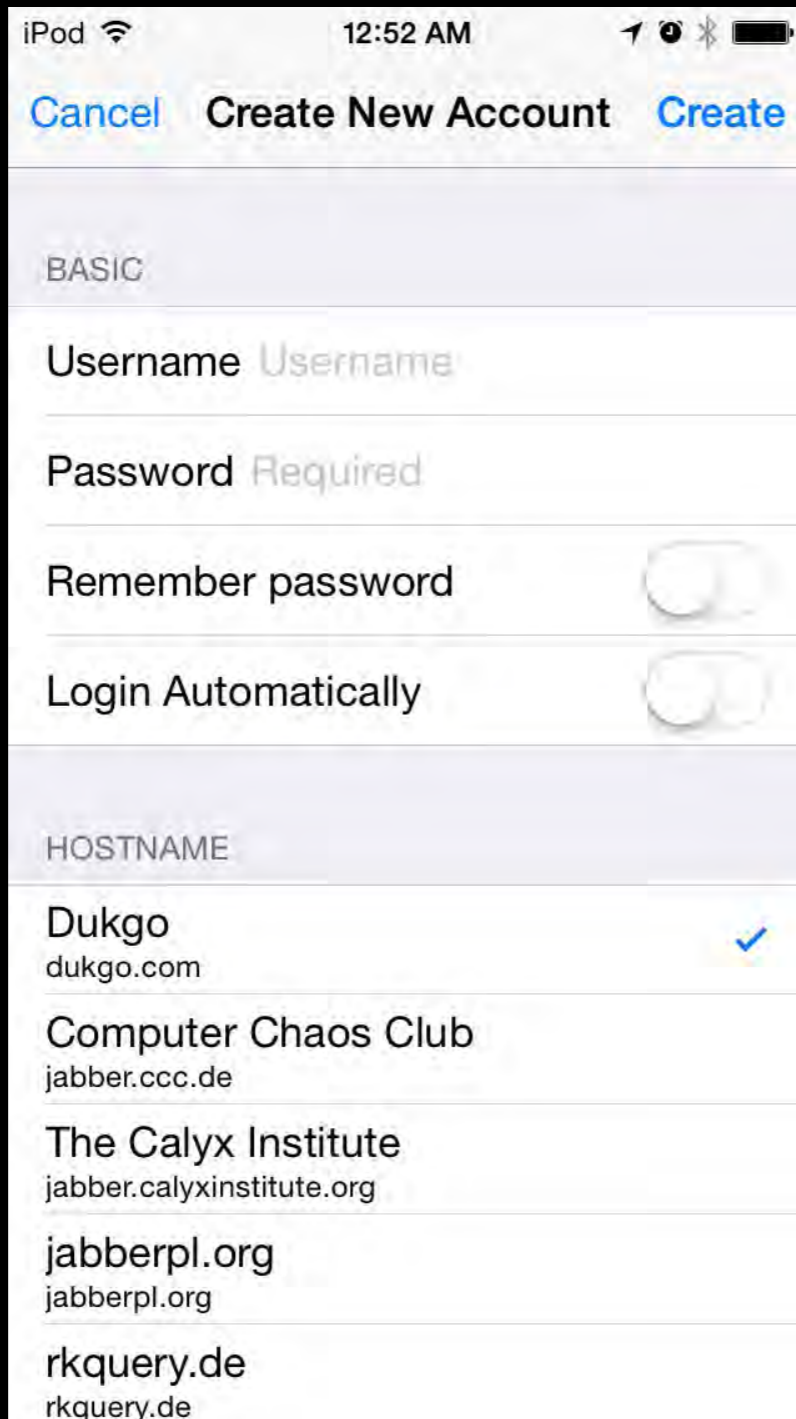
- Process of installing OTR varies between Windows and Linux and between Linux distros (well, package systems).
- Plan to have OTR in Pidgin installed by default began in 2013. Slated as issue for Pidgin 3.0 milestone, 55% of milestone issues complete as of July 2015: <https://developer.pidgin.im/ticket/15513>.



ChatSecure



ChatSecure



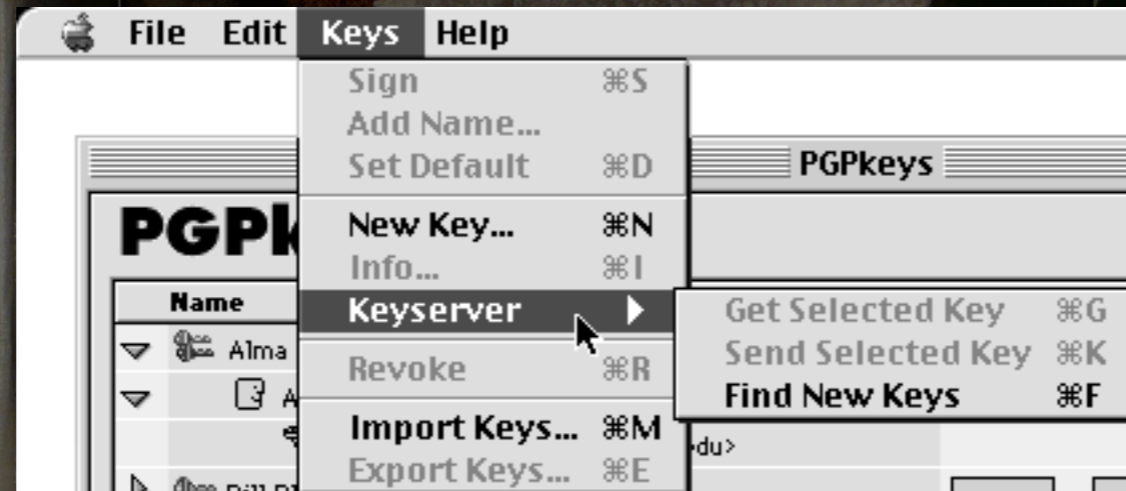
1P 1000570

TIME 63

PROGP

■■■■■■■■■■■■■■■■■■■■
EXD

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

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 encrypted.

huertanix@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
Matthew Coffey and Nick... World Maker Expo New York Times Hall	...	7/13/15, 3:41
		7/13/15, 1:42
		7/13/15, 12:42
		7/12/15, 10:55
		7/12/15, 9:44
		7/12/15, 9:44
		7/12/15, 9:43

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

Send Spelling Attach S/MIME Save

Enigmail: [Icons] Attach My Public Key

From: David Huerta <huertanix@opentil.com>

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

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

Encrypt This Message View or change security settings

Digitally Sign This Message

View Security Info

 david [..dh] huerta
 davidhuerta.me

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

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 most of 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. Please read this whole letter as the process has changed.

Hours and Locations of Speaker Registration:





MORE

DIFFICULT

LESS

DIFFICULT



Photo credit: Sasquatch I

PGP in the Browser

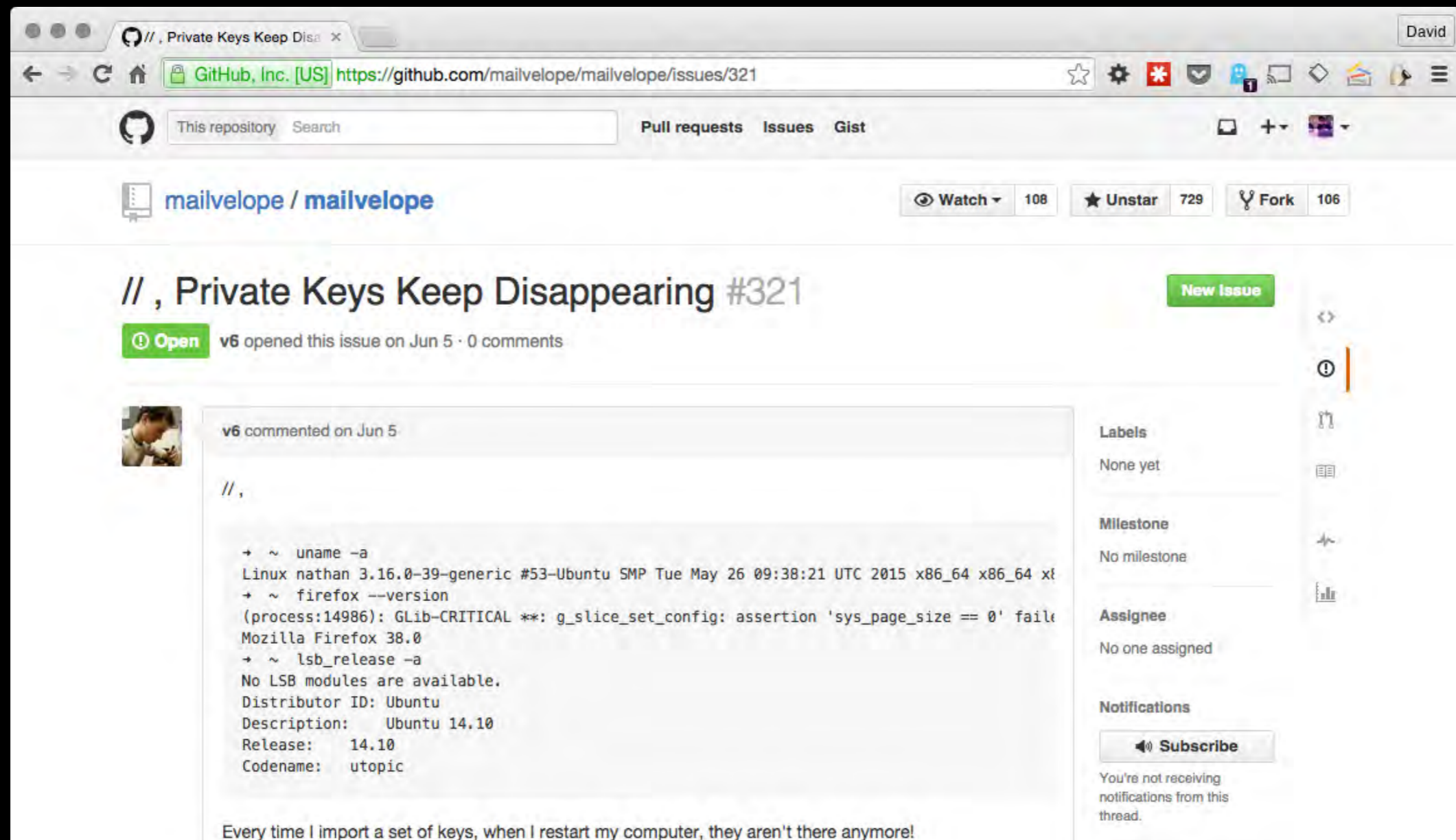
- Yahoo End-to-End: Browser extension, adds PGP functionality on top of webmail.
- Google End-to-End: ^ See above.
- WhiteoutMail: ^ Ditto.
- Mailvelope: ^ Yup.

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



The screenshot shows a GitHub issue page for the repository 'mailvelope / mailvelope'. The issue title is '// , Private Keys Keep Disappearing #321'. The issue is marked as 'Open' and was opened by user 'v6' on June 5. The issue description contains a terminal output snippet:

```
+ ~ uname -a
Linux nathan 3.16.0-39-generic #53-Ubuntu SMP Tue May 26 09:38:21 UTC 2015 x86_64 x86_64 x86_64 GNU/Linux
+ ~ firefox --version
(process:14986): GLib-CRITICAL **: g_slice_set_config: assertion 'sys_page_size == 0' failed
Mozilla Firefox 38.0
+ ~ lsb_release -a
No LSB modules are available.
Distributor ID: Ubuntu
Description:    Ubuntu 14.10
Release:       14.10
Codename:      utopic
```

Below the terminal output, the user 'v6' has written: 'Every time I import a set of keys, when I restart my computer, they aren't there anymore!'

The right sidebar of the issue page includes sections for 'Labels' (None yet), 'Milestone' (No milestone), 'Assignee' (No one assigned), and 'Notifications' (Subscribe button). A 'New Issue' button is visible in the top right corner of the issue content area.

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.

Challenging Design 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 ID (aka fingerprint): 1482 F3BF
3F16 6BD4 3525 D55E 35D7 26BD AE09 F328
- In person at the next NYC cryptoparty!