An introduction to Tox

What is Tox?

Tox Devs at ToxCon 2019 11.-13.10.2019

About

robinli

- Tox Project Leader
- Engineer person who loves low-level programming
- I work on robots and AI and stuff

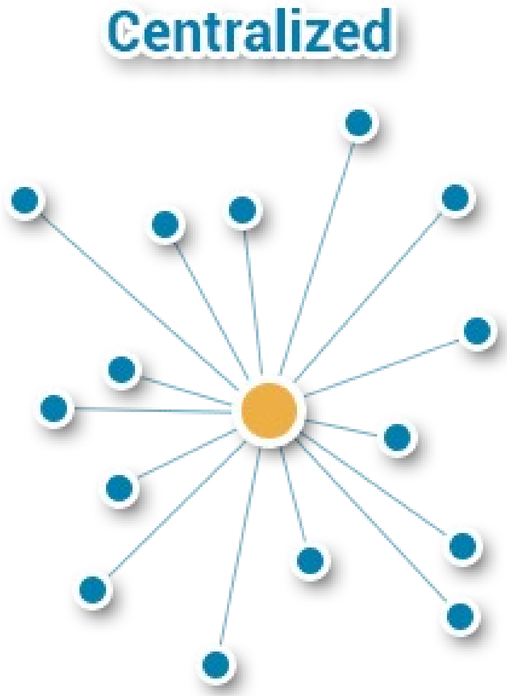
Federated - Matrix

most users are on 1 central server

source:
https://www.hello-matrix.net/public_servers.php

Public Aliases shows the number of published aliases in that homeserver's public room directory and is based on the `total_room_count_estimate` returned by the servers' APIs. We update this number once a day.

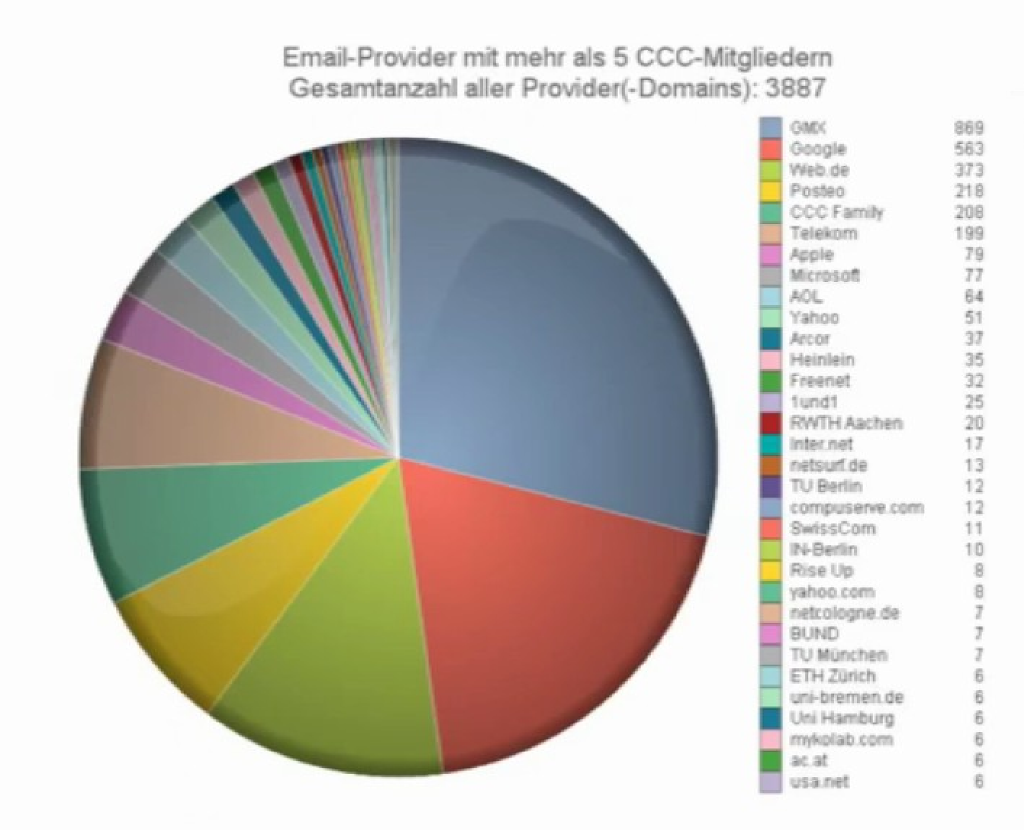
* October 2018

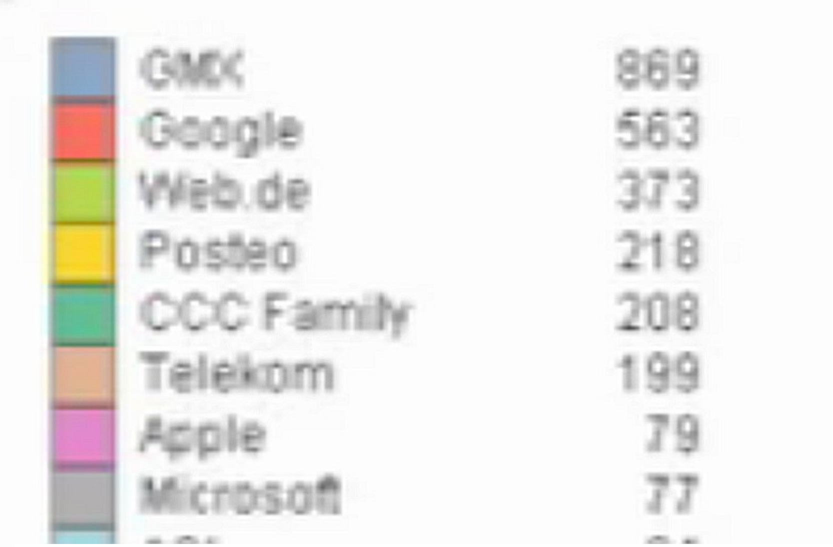


Office CCC - EMail providers

most users are on a few providers

source:
https://media.ccc.de/v/eh16-68-how_to_ccc_office



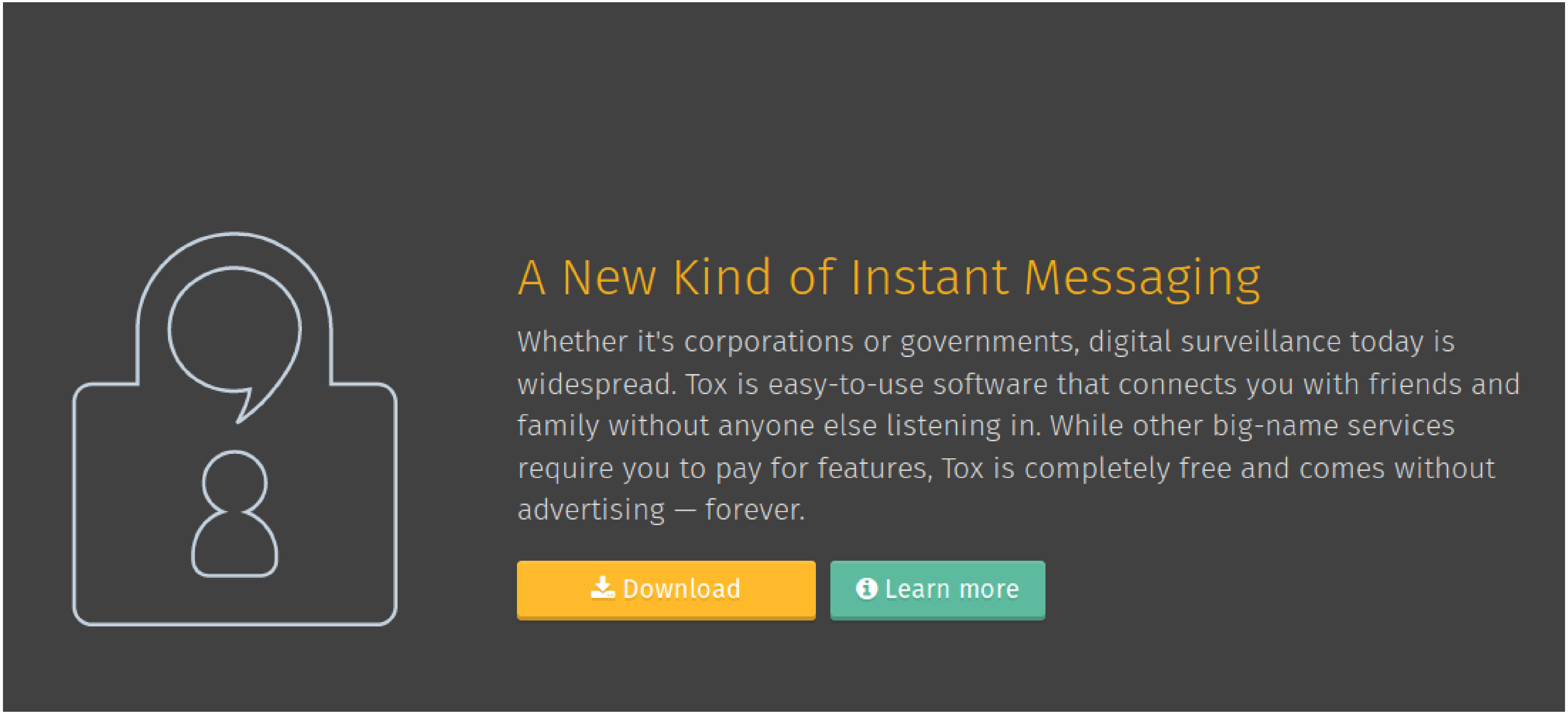


Can we do better?

Can we do some things better?

with less effort, fewer dependencies?

Tox?



A New Kind of Instant Messaging

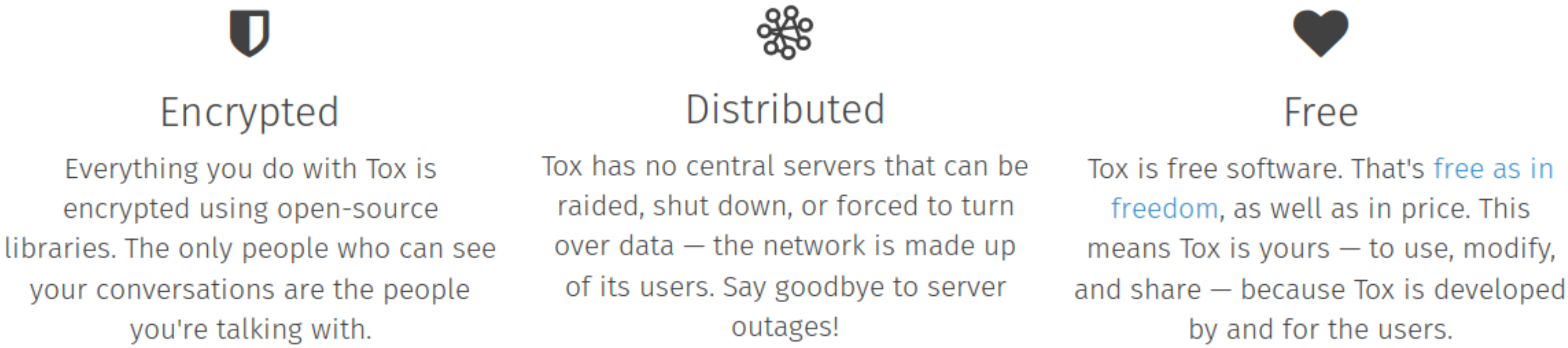
Whether it's corporations or governments, digital surveillance today is widespread. Tox is easy-to-use software that connects you with friends and family without anyone else listening in. While other big-name services require you to pay for features, Tox is completely free and comes without advertising — forever.

What is Tox?

Tox began in the wake of Edward Snowden's leaks regarding NSA spying activity.

The idea was to create an instant messaging application that ran without requiring the use of central servers, with no way to disable any of the encryption features.
The application would be easily usable by the layperson with no practical knowledge of cryptography or distributed systems.

During the Summer of 2013 a small group of developers from all around the globe formed and began working on a library implementing the Tox protocol.



Encrypted

Everything you do with Tox is encrypted using open-source libraries. The only people who can see your conversations are the people you're talking with.

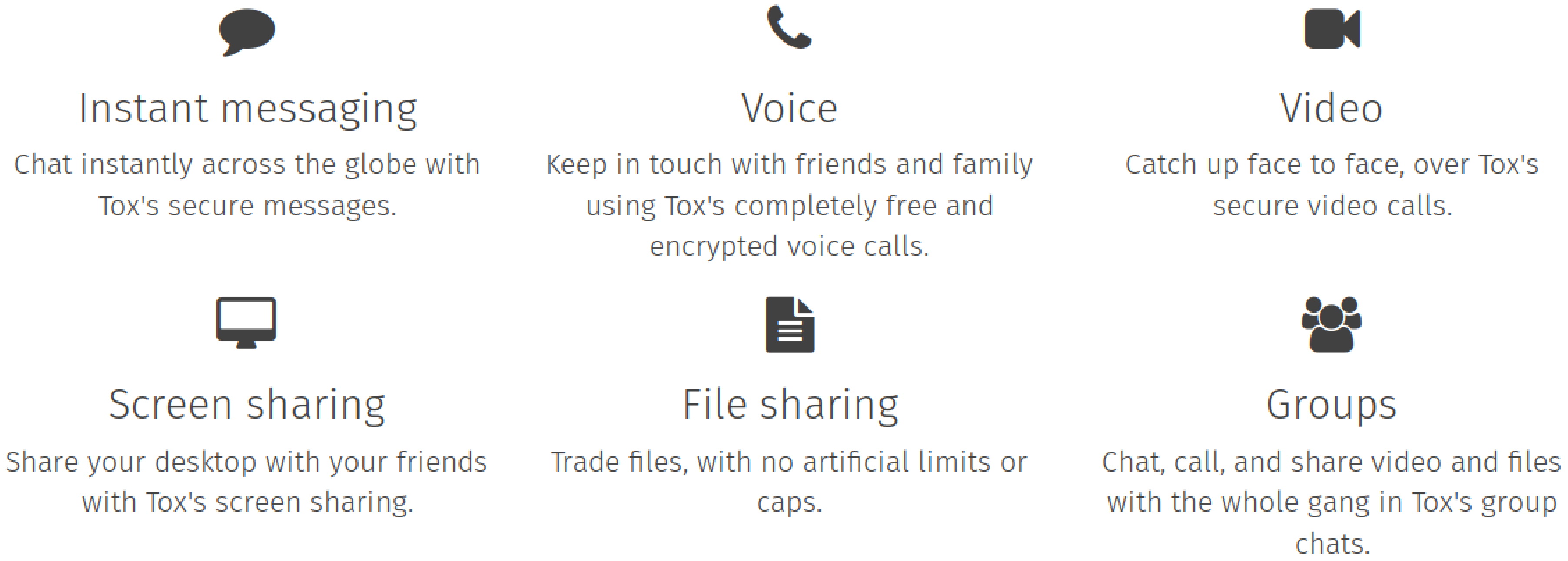
Distributed

Tox has no central servers that can be raided, shut down, or forced to turn over data — the network is made up of its users. Say goodbye to server outages!

Free

Tox is free software. That's free as in freedom, as well as in price. This means Tox is yours — to use, modify, and share — because Tox is developed by and for the users.

Basic features of Tox?



Instant messaging

Chat instantly across the globe with Tox's secure messages.

Voice

Keep in touch with friends and family using Tox's completely free and encrypted voice calls.

Video

Catch up face to face, over Tox's secure video calls.

Screen sharing

Share your desktop with your friends with Tox's screen sharing.

File sharing

Trade files, with no artificial limits or caps.

Groups

Chat, call, and share video and files with the whole gang in Tox's group chats.

Tox protocol

Tox is a distributed system for establishing authenticated encrypted direct network connections between peers.

If Alice and Bob know each other’s public keys, they can find each other and establish a secure connection, punching through any firewalls.

Toxcore

The Tox core is a networking library implementing the Tox protocol.

The reference implementation c-toxcore is 32,546 SLOC of C, licensed under GPLv3.

Cryptography

- building upon existing cryptography
- using libsodium, which is a portable fork of NaCl (Salt)
- curve25519 for Key exchange
- xsalsa20 for encryption
- poly1305 for message authentication

Tox clients

Tox is also a secure chat system.

Once we have an authenticated
encrypted network connection, we can push text, audio, video etc along it.

Tox clients wrap the tox core in a UI.
Since the core is GPL, all clients are free software.

Key features

Distributed

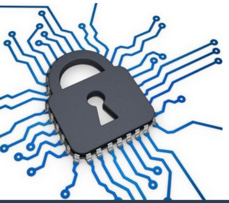
No single point of failure.
No single point of metadata collection.
Volunteer-run publically listed bootstrap nodes are used to introduce new users to the network, only on first run.

Encrypted

All cryptographical operations performed using NaCl/libsodium.
Has per-session perfect forward secrecy.
Communications are authenticated but not signed, and are deniable.

Pseudonymous

Tox users are identified only by their Tox ID.
A Tox ID is simply a public key created by the user.



Key features

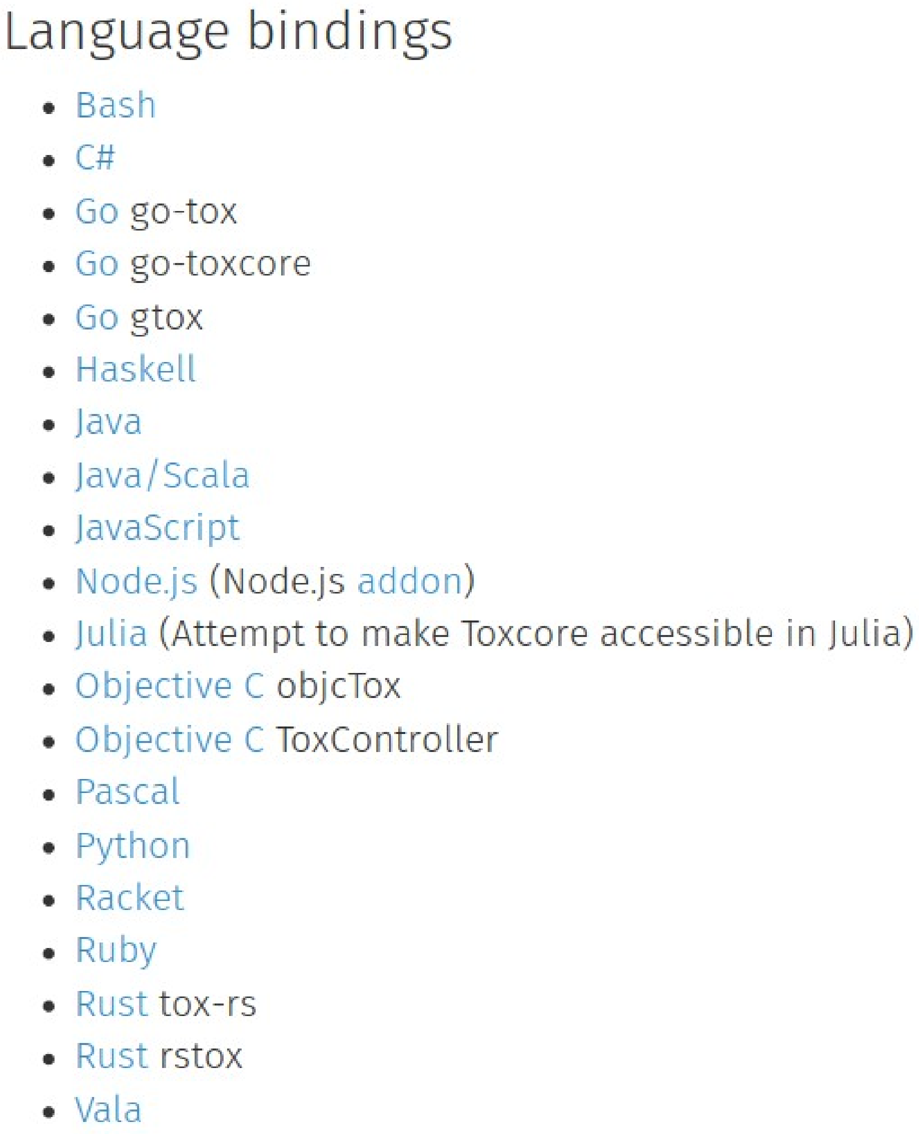
Direct

Tox aims to form direct IP-to-IP UDP connections where possible.
This makes high-bandwidth applications like video feasible.
Volunteer-run TCP relays exist as a back-up, automatically used when a direct connection fails.
Tox is not designed for anonymous communications. However, it is possible to connect via Tor, using TCP relays.

Groups

Private groups (“conferences”) for multi-user text/audio chats are implemented.
There are plans for public groups.

Tox in your language …



Language bindings

- Bash
- C#
- Go go-tox
- Go go-toxcore
- Go gtox
- Haskell
- Java
- Java/Scala
- JavaScript
- Node.js (Node.js addon)
- Julia (Attempt to make Toxcore accessible in Julia)
- Objective C objcTox
- Objective C ToxController
- Pascal
- Python
- Racket
- Ruby
- Rust tox-rs
- Rust rstox
- Vala

Fun things with Tox ...

some very fun things to check out:

- VPN over Tox
  https://github.com/cleverca22/toxvpn
  https://github.com/gjedeer/tuntox/blob/master/VPN.md

- SSH over Tox
  https://github.com/gjedeer/tuntox

- VNC over Tox
  https://github.com/gjedeer/tuntox

Source and compiling

A Look at the source code and dependencies for compiling.

Can video chat be done without WebRTC?

Can we reduce the dependencies to a minimum?

Toxcore - Source Stats

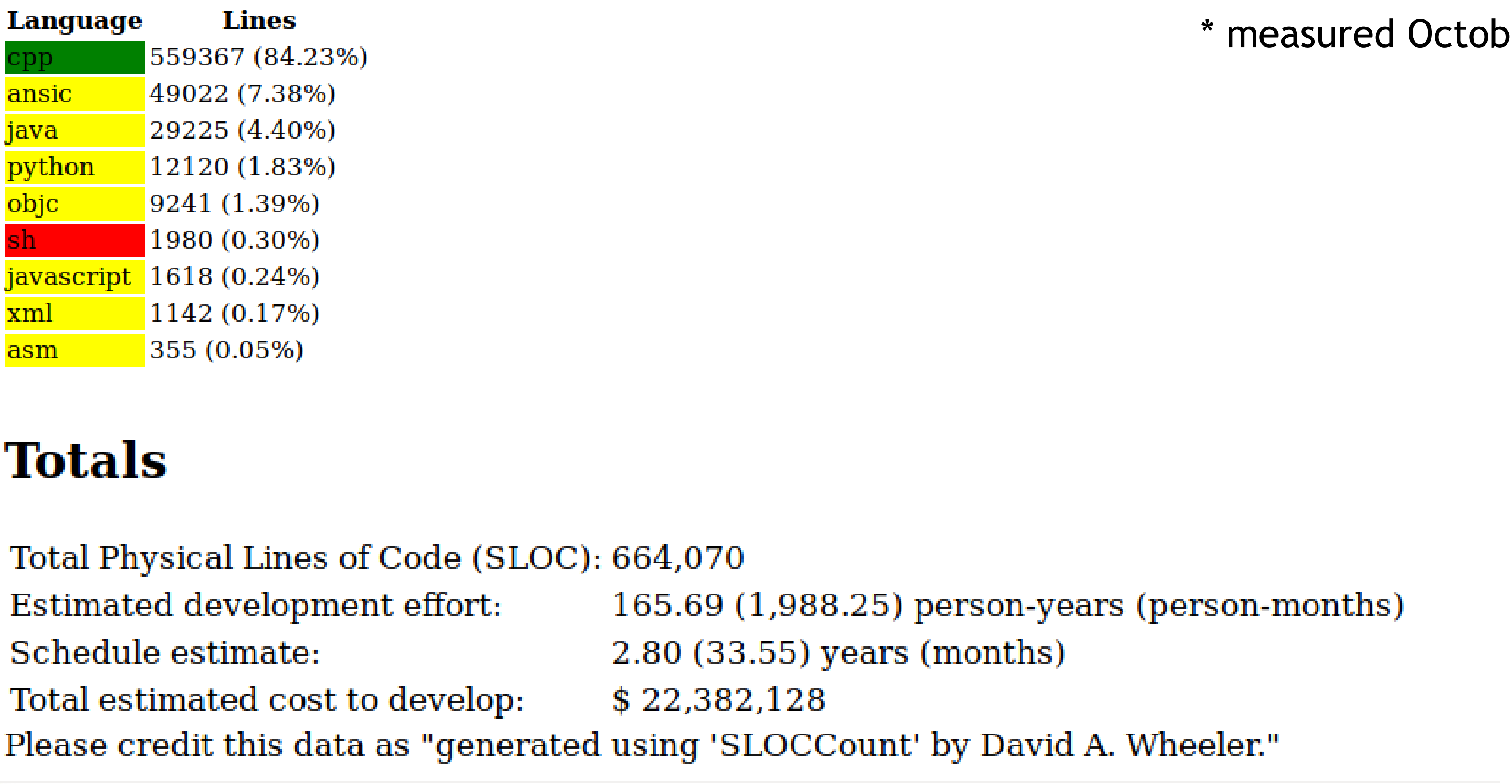
toxcore	files: 61	C: 25	SLOC: 21.333
toxav	files: 38	C: 16	SLOC: 8.512
toxencryptsave	files: 24	C: 8	SLOC: 1.696
toxutil	files: 4	C: 1	SLOC: 1.005
Total	**files: 127**	**C: 50**	**SLOC: 32.546***

* measured October 2018

Web-RTC

- Total C++: 2150 SLOC: 664.070*
- cmp. c-toxcore ~ x43 ~ x20

* measured October 2018



Language	Lines
cpp	559367 (84.23%)
ansic	49022 (7.38%)
java	29225 (4.40%)
python	12120 (1.83%)
objc	9241 (1.39%)
sh	1980 (0.30%)
javascript	1618 (0.24%)
xml	1142 (0.17%)
asm	355 (0.05%)

Totals

```
Total Physical Lines of Code (SLOC): 664,070
Estimated development effort:        165.69 (1,988.25) person-years (person-months)
Schedule estimate:                   2.80 (33.55) years (months)
Total estimated cost to develop:     $ 22,382,128
Please credit this data as "generated using 'SLOCCount' by David A. Wheeler."
```

Toxcore - Dependencies

- toxcore + toxencryptsave
  - libsodium
    https://github.com/jedisct1/libsodium
    Libsodium v1.0.12 and v1.0.13 Security Assessment in 2017
    https://www.privateinternetaccess.com/blog/2017/08/libsodium-v1-0-12-and-v1-0-13-security-assessment/

Cryptography Engineering

- toxav
  - libvpx https://github.com/webmproject/libvpx
  - libopus https://github.com/xiph/opus
  - x264* https://git.videolan.org/?p=x264.git;a=shortlog;h=refs/heads/stable
  - libav* https://github.com/libav/libav

* Zoxcore - toxcore experiment fork (experimental H.264 support and other upgrades)
https://github.com/Zoxcore/c-toxcore

Toxcore - Dependencies (2)

- libvpx https://github.com/webmproject/libvpx
- libopus https://github.com/xiph/opus
  - yasm https://github.com/yasm/yasm

- x264* https://git.videolan.org/?p=x264.git;a=shortlog;h=refs/heads/stable
- libav* https://github.com/libav/libav
  - nasm https://www.nasm.us/pub/nasm/releasebuilds/2.13.02/nasm-2.13.02.tar.bz2
  - yasm https://github.com/yasm/yasm

* Zoxcore - toxcore experiment fork (experimental H.264 support and other upgrades)
https://github.com/Zoxcore/c-toxcore

Toxcore - Plaform Support

- Windows (32bit, 64bit) H.264 HW Acceleration*
- Linux (Debian, Ubuntu, Suse, Alpine, ...) H.264 HW Acceleration*
- BSD (open BSD, free BSD)
- OSX
- IOS (IPhone)
- ARM (Android, Raspberry PI) H.264 HW Acceleration*
- Solaris (open Solaris)

* toxcore expermient fork
https://github.com/Zoxcore/c-toxcore
* as of October 2018

Comparison

Comparable systems

Centralised (Signal, Telegram, etc) and federated (Matrix) systems are different beasts entirely.

Comparable distributed systems

- Jami (formerly known as GNU Ring)
- Ricochet
- Briar

Tox vs. Jami

Jami uses TLS, ICE (STUN/TURN), and OpenDHT on top of a SIP softphone to achieve much the same goals as Tox.

Tox meanwhile is a compact integrated system, essentially depending only on NaCl.

Jami does not seriously try to ensure metadata privacy, while Tox aims to.

Tox vs. Ricochet and Briar

Ricochet uses Tor’s hidden services mechanism to provide fully anonymous chat with full metadata privacy: snoopers can not determine even the IP addresses of your friends (assuming Tor works).

Tox meanwhile only aims (and fails) to prevent snoopers determining friends’ Tox IDs.

Ricochet is text-only; Tor isn’t designed for very-low-latency communications.

Briar uses Tor in a similar way to Ricochet when connecting over the internet.

Tox TODO list

Tox is very much a work in progress, though it is already useable and used.

New **C developers** to help with c-toxcore are particularly in need!

Talk to us if you might be interested.

We need your help

We are looking for help with these:

- general cleanup of c-toxcore
- multi-device
- metadata privacy
- traffic taming
- UPnP support
- DoS resistance
- Support post-quantum cryptography
- offline messaging

talk to us on Tox:

A571A6C77225C4081BA4D7AC268B9659B78704037959817E6ED56C4E6BD84B7E3E3EDB624583

or Email:

dev@robinlinden.eu or zoff@zoff.cc

Want to get involved?

for more information about Tox please visit these links:

https://tox.chat/faq.html

https://toktok.ltd/integrations.html

Tox is global (TRIfA - on the „north pole“)

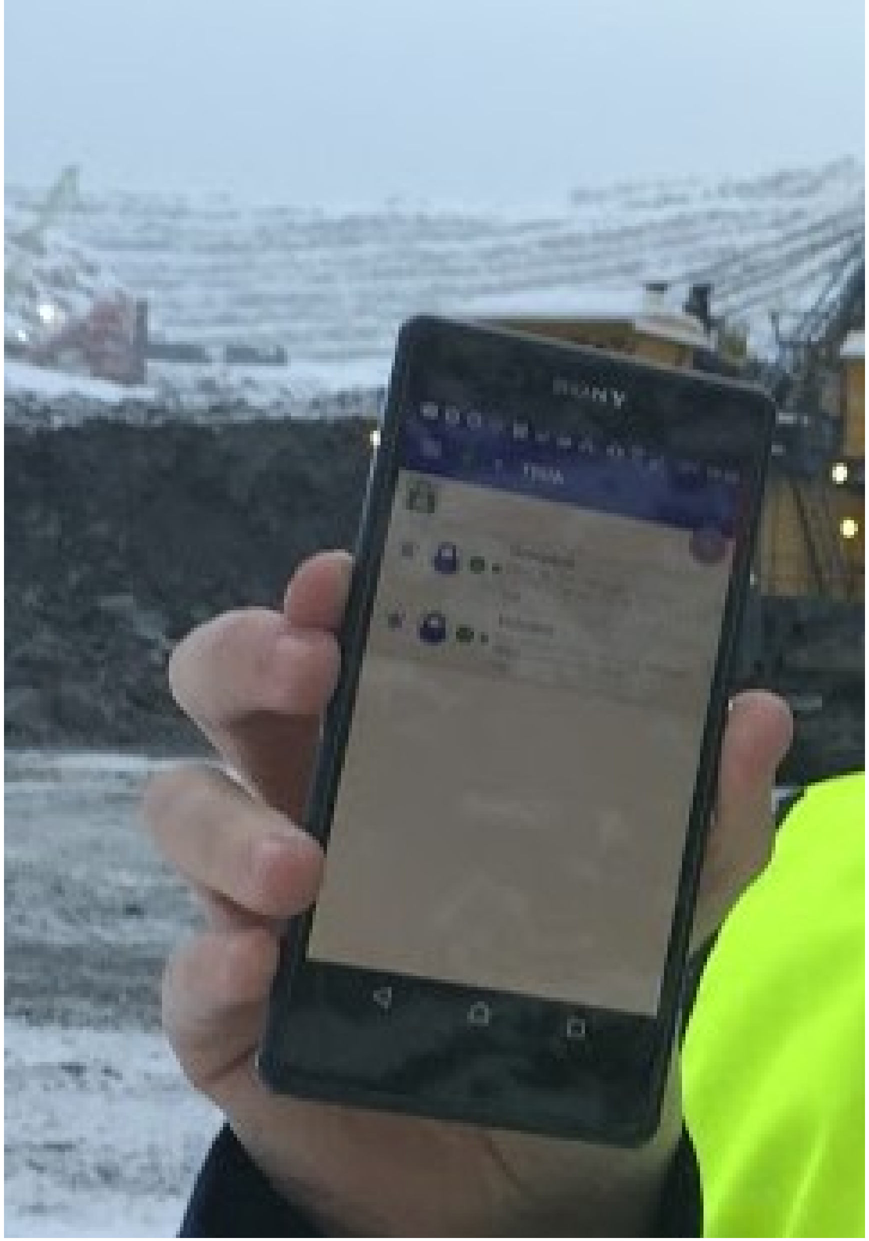


Photo credit: <a href="https://s3.amazonaws.com/lowres.cartoonstock.com/weather-smartphone-cold_weather-wintry_condition-cold-blizzard-amrn839_low.jpg">Amazonaws.com</a>

getting in touch ...

- Github
  https://github.com/TokTok/c-toxcore
- Tox
  A571A6C77225C4081BA4D7AC268B9659B78704037959817E6ED56C4E6BD84B7E3E3EDB624583
- IRC
  #toktok on freenode
- Matrix
  https://matrix.to/#/#freenode_#toktok:matrix.org
- Email
  dev@robinlinden.eu or zoff@zoff.cc