Tox Workshop

Install a Tox Client and have some fun with it

IT-S NOW 2023 02.06.2023

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.

Goals?

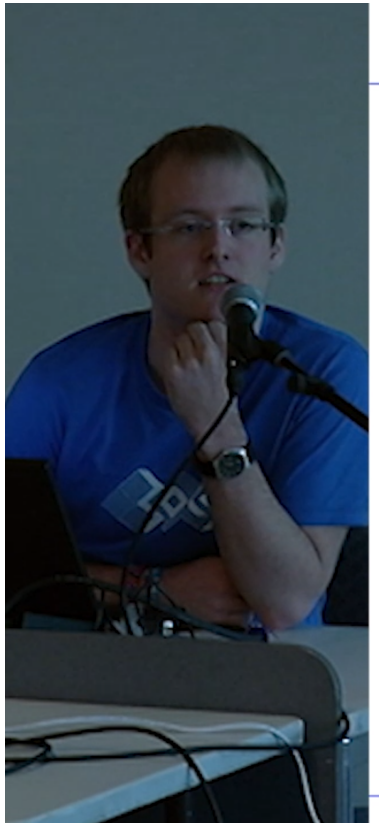
What are your goals with Tox?

We want Tox to be as simple as possible while remaining as secure as possible.

Why are you doing this?

There are already a bunch of free Skype alternatives.
The goal of this project is to create a configuration-free P2P Skype replacement. “Configuration-free” means that the user will simply have to open the program and will be capable of adding people and communicating with them without having to set up an account. There are many so-called Skype replacements, but all of them are either hard to configure for the normal user or suffer from being way too centralized.

from (~2014):
https://github.com/irungentoo/toxcore#qa



The why

Goals?

TOX

Why are we doing this?

- We want a free(as in Freedom) and secure alternative for Skype
- *"We don't want to be the next secure chatting program, we want to be the next secure chatting program that people actually use."* - Someone on IRC
- Current secure chat programs aren't easy to use, at least not for ~~our parents and grandparents~~ normal people

from (28. Dec. 2013): Talk on the Tox project at the 30c3

https://www.youtube.com/watch?v=WfHgkLoRAE8

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

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.

* measured October 2018

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

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/

- 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)

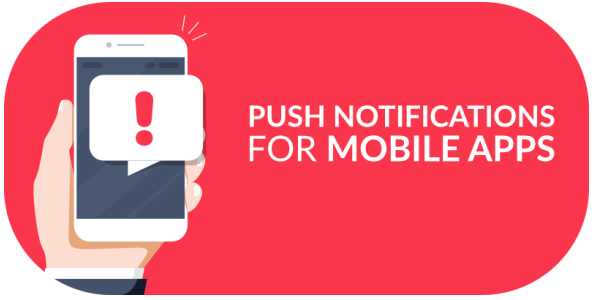
- libvpx https://github.com/webmproject/libvpx
- libopus https://github.com/xiph/opus
  - yasm https://github.com/yasm/yasm

- 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 - Platform 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

Nice Things (about Toxcore) ...

Easy to compile on almost any platform

use make or cmake or just use the single file toxcore amalgamation

No Access to Storage / Disk

Toxcore itself does not read / write or access any storage itself

Does not do Anything on it's own

a client application needs to trigger actions (iterate) in Toxcore

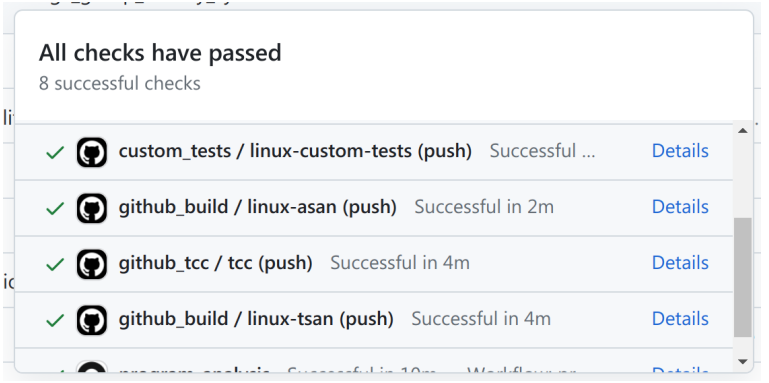
No internal Threads are created

Toxcore runs on the Thread(s) given to by a client application

Nice Things (about Toxcore) ...

Every commit and pull request tested for issues

tested with many automated testcases with ASAN, TSAN, MSAN, UBSAN and static code analyzers, on linux and other platforms




```
657  49/59 Test #52: tox_many_tcp .....................   Passed   20.28 sec
658  50/59 Test #41: overflow_recvq ...................   Passed   22.17 sec
659  51/59 Test #26: friend_request_spam ..............   Passed   23.76 sec
660  52/59 Test #28: group_invite .....................   Passed   25.08 sec
661  53/59 Test #21: file_transfer ....................   Passed   27.73 sec
662  54/59 Test #40: onion ............................   Passed   27.55 sec
663  55/59 Test #51: tox_many .........................   Passed   28.70 sec
664  56/59 Test #13: conference .......................   Passed   31.19 sec
665  57/59 Test #34: invalid_tcp_proxy ................   Passed   30.91 sec
666  58/59 Test #35: invalid_udp_proxy ................   Passed   30.88 sec
667  59/59 Test #57: conference_av ....................   Passed   31.20 sec
668
669  100% tests passed, 0 tests failed out of 59
670
671  Total Test time (real) =  32.40 sec
```

What's new ...

NGC - New Groupchats https://github.com/TokTok/c-toxcore/pull/2269

NGC has similar features to IRC
Admin / Moderators, kick, silence
public and private groups

Redesign of Tox's Cryptographic Handshake

Tobi (goldroom on GitHub) wrote his master's thesis ("Adopting the Noise Key Exchange in Tox")
on the KCI issue in Tox ...
... applied for funding at NLnet foundation and their NGI Assure fund to continue his work on Tox
https://blog.tox.chat/2023/03/redesign-of-toxs-cryptographic-handshake/

History sync in public groups

Some Clients have history sync for public groups **[Beta]**

Group images in NGC groups

send and receive group images in NGC groups **[Beta]**

What's new right now!

25. May 2023 - 0day ?

https://twitter.com/3xp0rtblog/status/1661826845791117314

https://twitter.com/vxunderground/status/1661789069670780934

using qTox v1.17.6, c-toxcore 0.2.13
and Qt 5.12.12 or Qt 5.7.1 on Windows Platform

vx-underground
@vxunderground

A TOX 1.17.6 (current version) RCE 0day is for sale.

It would give nerds the ability to pwn literally every ransomware group, and major Threat Actor, on the planet. All it requests is sending a friend request, and the other person accepting it.

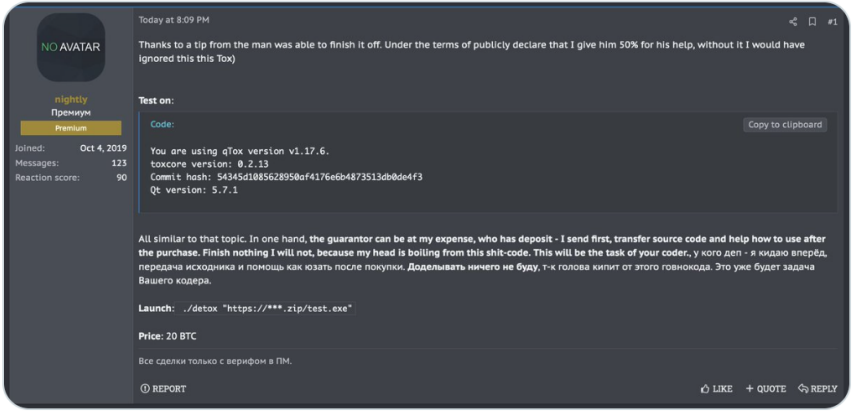
It is being sold for $500,000

7:39 PM · May 25, 2023 · **155.9K** Views

149 Retweets **22** Quotes **715** Likes **61** Bookmarks

3xp0rt @3xp0rtblog · 16h

The same guy who related to the Fortinet incident posted this on XSS forum for 20 BTC. Gif with proof shows launching Putty after adding a friend. Judging by the gif, it uses a buffer overflow in the qTox client.



vx-underground @vxunderground · 19h

A TOX 1.17.6 (current version) RCE 0day is for sale.

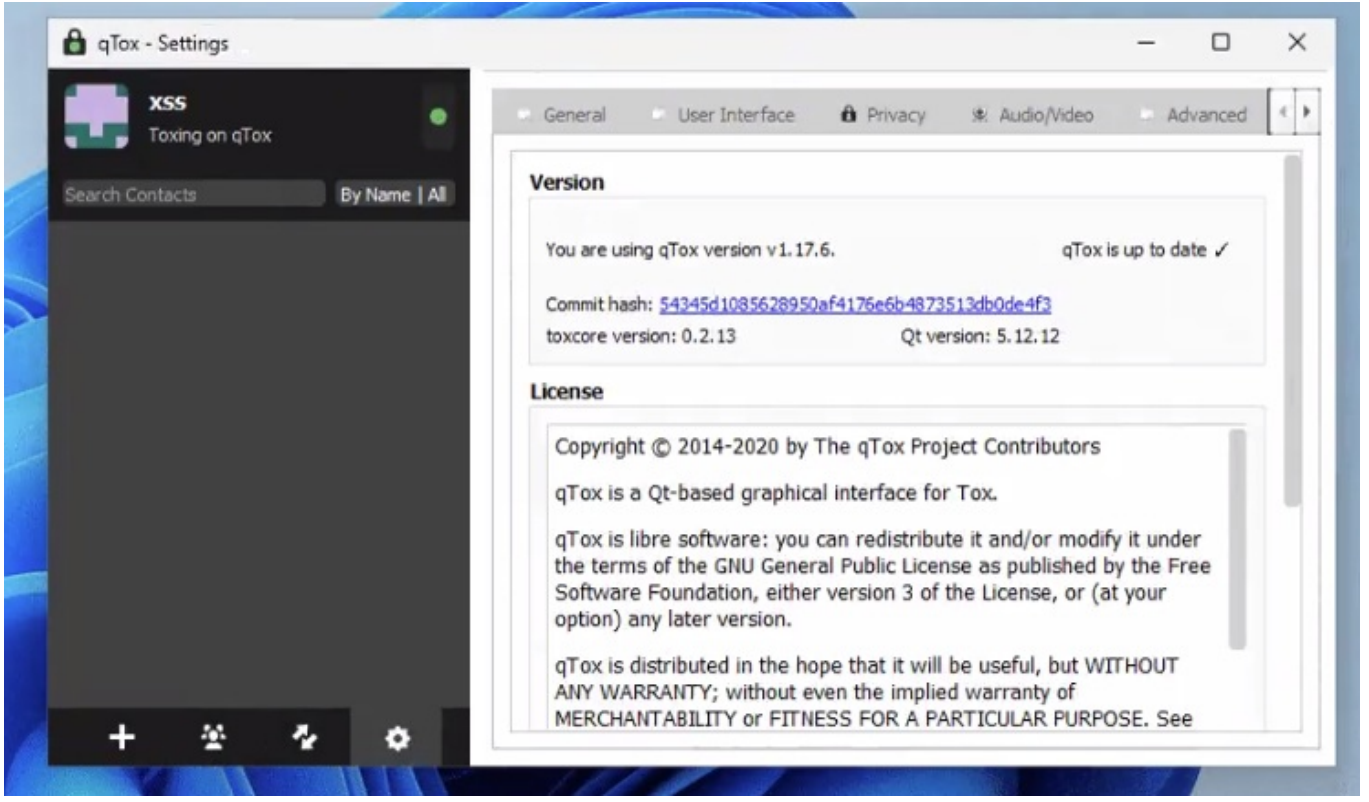
It would give nerds the ability to pwn literally every ransomware group, and major Threat Actor, on the planet. All it requests is sending a friend request, and the other person accepting it....

Show this thread

What's new right now!

25. May 2023 - 0day ?

- download your updates
- use ASAN builds if possible
- avoid Windows if you can



What's new right now!

fixed ?

https://github.com/Zoxcore/qTox_enhanced/pull/7

- sanitize notification strings

It seems there is a vulnerability in Snorenotify on Windows. It gives strings to SnoreToast.exe on the commandline, most likely unsanitized. As a countermeasure all notification strings now only allow characters on a whilelist: a-z A-Z 0-9 _ <space> :

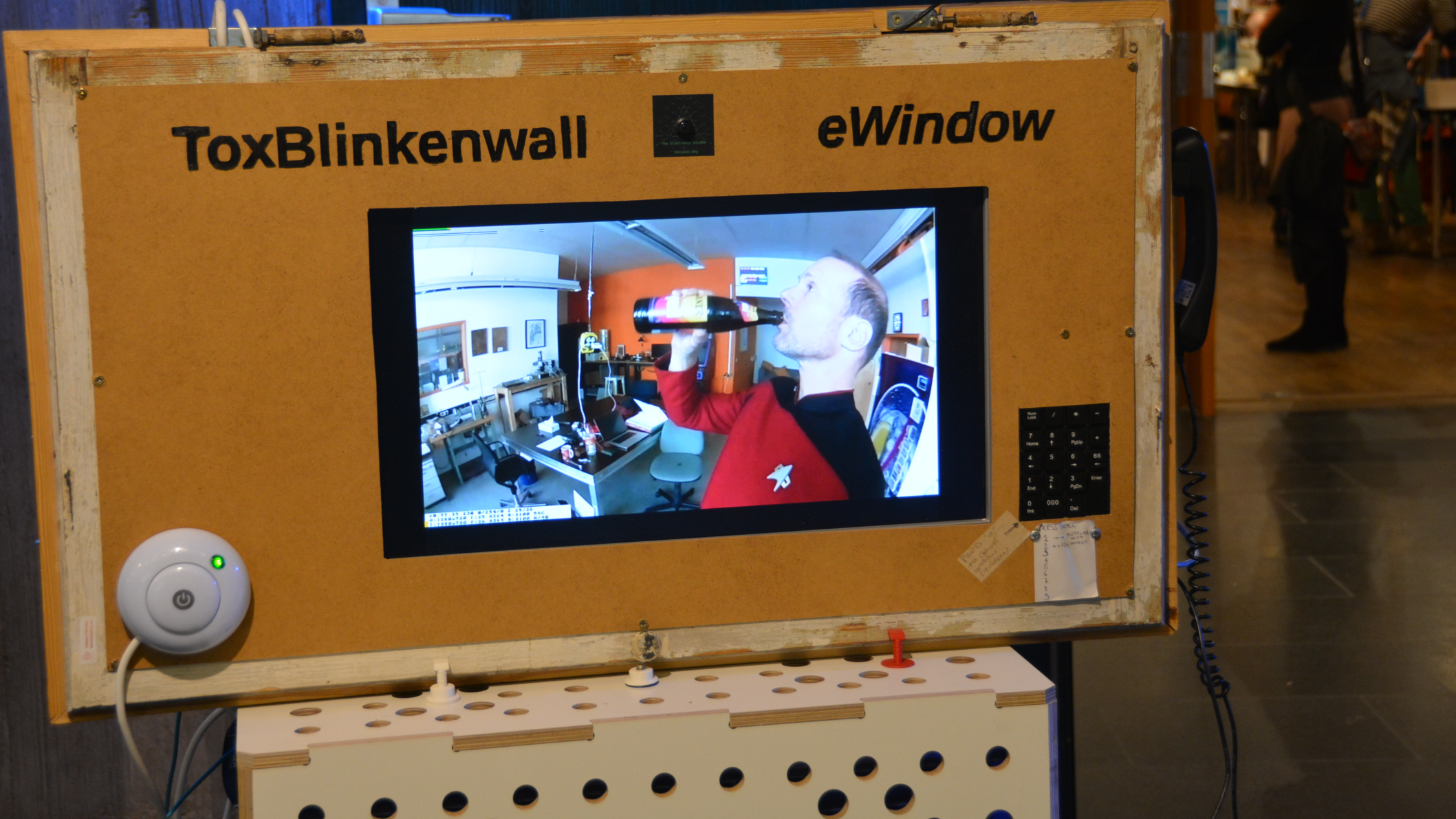
```
QString DesktopNotify::sanitizeTextForNotifications(const QString& input_text)
{
    QString output_text = QString(input_text);
    output_text.replace(QRegularExpression("[^a-zA-Z0-9 _:]"), "_"); // allow only a A-Z and 0-9 and "_" and " " and ":" chars
    // qDebug() << "sanitizeTextForNotifications: input:" << input_text << "output:" << output_text;
    return output_text;
}
```

Blinkenwall


CYBER
ATTENTION!

Blinkenwall

ToxBlinkenwall


ToxBlinkenwall
eWindow


USB
USB Handset
FC CE
1 2 3
4 5 6
7 8 9
* 0 #
MFV
SCHRACK


USB
FC CE
SCHRACK


USB Handset
ToxBlinkenwall

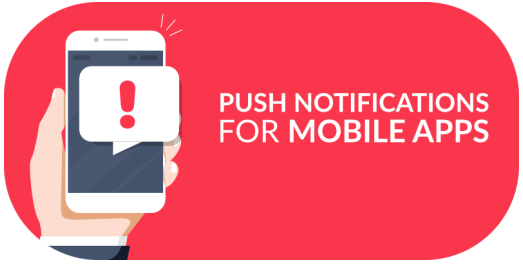

TRIBE


ToxBlinkenwall
IP:
CPU Load: 1.41
Mem: 28/432 MB
40.1'C+
New Bee

TRIfA - Android

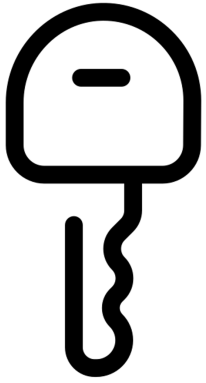
https://f-droid.org/en/packages/com.zoffcc.applications.trifa/

https://play.google.com/store/apps/details?id=com.zoffcc.applications.trifa



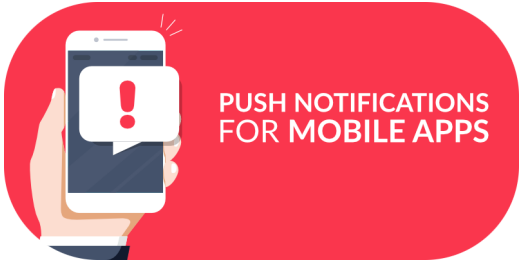
https://zoff99.github.io/ToxAndroidRefImpl/PUSH_NOTIFICATION.html

Antidote - iOS



Download on the App Store

https://apps.apple.com/app/antidote-tox-client/id1592895292



qTox - Linux (Windows, MacOS)

GitHub

https://github.com/Zoxcore/qTox_enhanced/releases/

Get it from the Snap Store

https://snapcraft.io/qtox-enhanced

triggers Push Notifications

Want to get involved?

for more information about Tox please visit these links:

https://toktok.ltd/integrations.html

getting in touch ...

- Github
  https://github.com/TokTok/c-toxcore
- Tox Public Group
  154b3973bd0e66304fd6179a8a54759073649e09e6e368f0334fc6ed666ab762
- Matrix
  https://matrix.to/#/#trifa:matrix.org

Your devices? Your use cases?...

What devices do you want to install Tox on?

What is your use case for Tox?

interactive part ...