

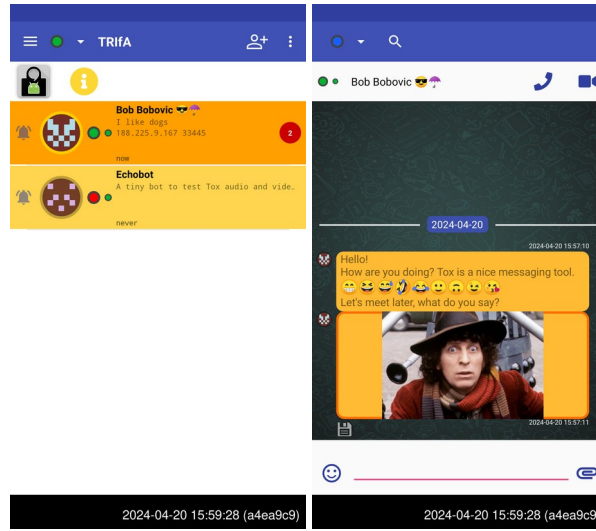
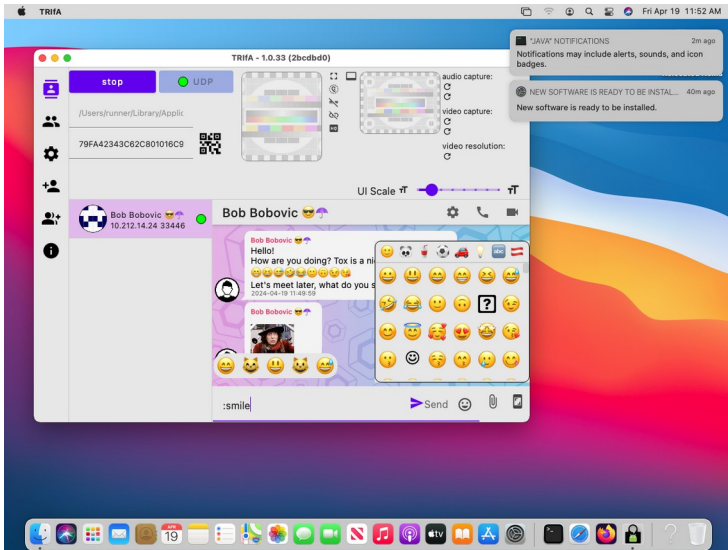


Workshop

Coding and working on security-focused apps, using Tox as example

IT-S NOW 2024

06.06.2024



IT-S NOW

demagic

Adopting the Noise Key Exchange in Tox
Improved security of Tox instant messaging with NoiseIK

Topics ...

Redesign of Tox's cryptographic handshake

Code defensively and use dependencies responsibly

Using GitHub CI and the likes

Make C code safer and better auditable



Redesign of Tox's cryptographic handshake

Adopting the Noise Key Exchange in Tox

Improved security of Tox instant messaging with NoiseIK



Make C code safer and better auditable

```
non_null(5) nullable(1, 2, 4, 6)
static int32_t resolve_bootstrap_node(Tox *tox, const char *host, uint16_t port, const uint8_t *public_key,
                                     IP_Port **root, Tox_Err_Bootstrap *error)
{
    assert(tox != nullptr);
    assert(root != nullptr);

    if (host == nullptr || public_key == nullptr) {
        SET_ERROR_PARAMETER(error, TOX_ERR_BOOTSTRAP_NULL);
        return -1;
    }

    if (port == 0) {
        SET_ERROR_PARAMETER(error, TOX_ERR_BOOTSTRAP_BAD_PORT);
        return -1;
    }

    const int32_t count = net_getipport(host, root, TOX_SOCK_DGRAM);

    if (count < 1) {
        LOGGER_DEBUG(tox->m->log, "could not resolve bootstrap node '%s'", host);
        net_freeipport(*root);
        SET_ERROR_PARAMETER(error, TOX_ERR_BOOTSTRAP_BAD_HOST);
        return -1;
    }

    assert(*root != nullptr);
    return count;
}
```

```
non_null(5) nullable(1, 2, 4, 6)
static int32_t resolve_bootstrap_node(Tox *tox, const char *host, uint16_t port, const uint8_t *public_key,
                                     IP_Port **root, Tox_Err_Bootstrap *error)
{
    assert(tox != nullptr);
    assert(root != nullptr);

    if (host == nullptr || public_key == nullptr) {
        SET_ERROR_PARAMETER(error, TOX_ERR_BOOTSTRAP_NULL);
        return -1;
    }

    if (port == 0) {
        SET_ERROR_PARAMETER(error, TOX_ERR_BOOTSTRAP_BAD_PORT);
        return -1;
    }

    const int32_t count = net_getipport(host, root, TOX_SOCK_DGRAM);

    if (count == -1) {
        LOGGER_DEBUG(tox->m->log, "could not resolve bootstrap node '%s'", host);
        net_freeipport(*root);
        SET_ERROR_PARAMETER(error, TOX_ERR_BOOTSTRAP_BAD_HOST);
        return -1;
    }

    if (*root == nullptr) {
        return -1;
    }

    assert(*root != nullptr);
    return count;
}
```



Make C code safer and better auditable

```
toxcore/network.c
@@ -1791,8 +1791,7 @@ Socket net_socket(const Network *ns, Family domain, int type, int protocol)
1791 1791 uint16_t net_socket_data_recv_buffer(const Network *ns, Socket sock)
1792 1792 {
1793 1793     const int count = ns->funcs->recvbuf(ns->obj, sock.sock);
1794 - assert(count >= 0 && count <= UINT16_MAX);
1795 - return (uint16_t)count;
1794 + return (uint16_t)max_s32(0, min_s32(count, UINT16_MAX));
1796 1795 }
1797 1796
1798 1797 uint32_t net_htonl(uint32_t hostlong)
```



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://code.videolan.org/videolan/x264/-/tree/stable?ref_type=heads

- **libav*** <https://github.com/FFmpeg/FFmpeg>

* **Zoxcore** - toxcore experiment fork (experimental H.264 support and other upgrades)

<https://github.com/zoff99/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://code.videolan.org/videolan/x264/-/tree/stable?ref_type=heads
- libav* <https://github.com/FFmpeg/FFmpeg>
 - 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/zoff99/c-toxcore>



Nice Things (about Toxcore) ...

Easy to compile on almost any platform

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

https://github.com/zoff99/c-toxcore/tree/zoff99/zoxcore_local_fork/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) ...

All checks have passed

13 successful checks

- arm64 build / arm64 Build (push) Successful in 22m
- custom_tests_asan / linux-custom-tests (push) Successful in 11m
- custom_tests_tsan / linux-custom-tests (push) Successful in 12m
- github_build / linux-asan (push) Successful in 1m
- github_tcc / tcc (push) Successful in 21s
- mips build / mips Build (push) Successful in 25m
- riscv64 build / riscv64 Build (push) Successful in 3m
- s390x build / s390x Build (push) Successful in 27m
- github_build / linux-tsan (push) Successful in 1m
- program-analysis Successful in 3m - Workflow: program-analysis

All checks have passed

79 successful checks

- ci / analysis (cppcheck) (pull_request) Successful in 1m
- ci / analysis (doxygen) (pull_request) Successful in 50s
- ci / analysis (goblint) (pull_request) Successful in 22s
- ci / analysis (infer) (pull_request) Successful in 1m
- ci / analysis (freebsd) (pull_request) Successful in 12m
- ci / analysis (misra) (pull_request) Successful in 53s
- ci / analysis (modules) (pull_request) Successful in 51s
- ci / analysis (pkgsrc) (pull_request) Successful in 2m
- ci / analysis (rpm) (pull_request) Successful in 1m
- ci / analysis (slimcc) (pull_request) Successful in 35s

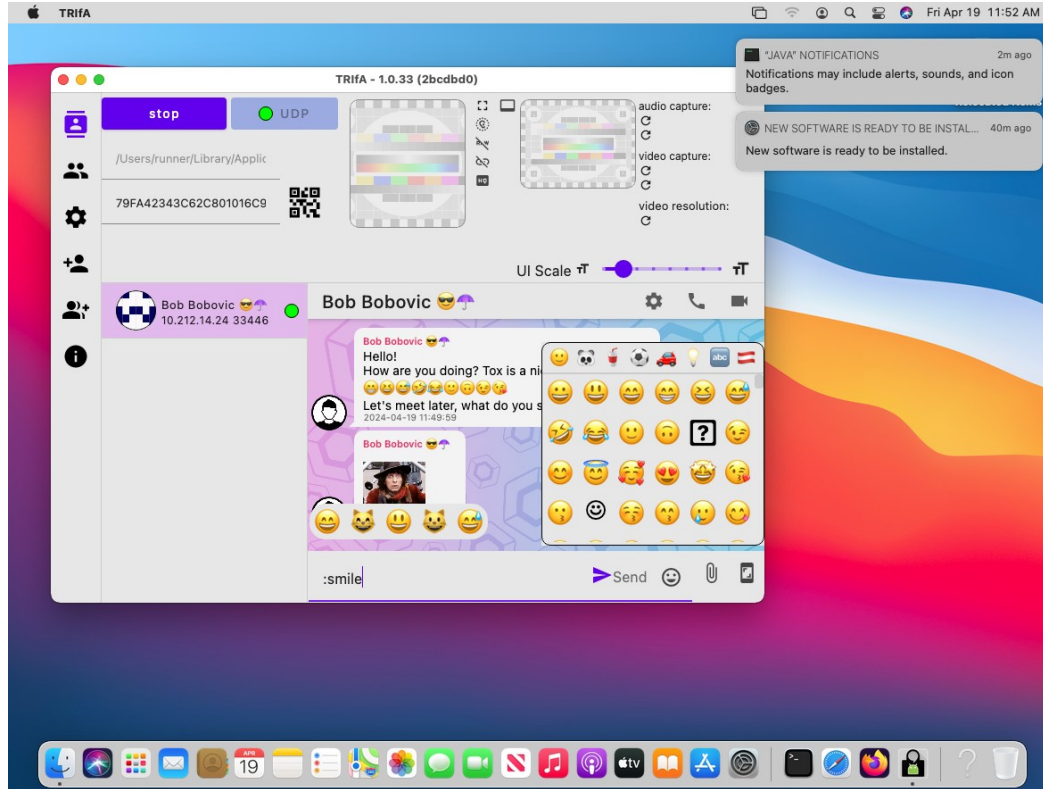
```
657 49/59 Test #52: tox_many_tcp ..... Passed 20.28 sec
658 50/59 Test #41: overflow_recvq ..... Passed 22.17 sec
659 51/59 Test #26: friend_request_spam ..... Passed 23.76 sec
660 52/59 Test #28: group_invite ..... Passed 25.08 sec
661 53/59 Test #21: file_transfer ..... Passed 27.73 sec
662 54/59 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
```



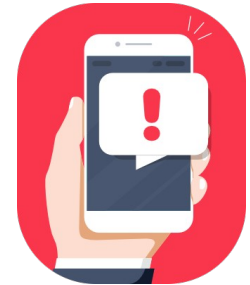
TRiFA Material - Linux, Windows, MacOS ...

GitHub

https://github.com/Zoxcore/trifa_material



triggers Push Notifications



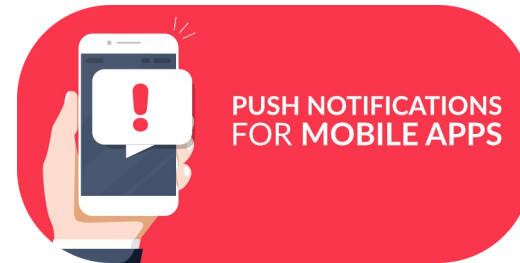
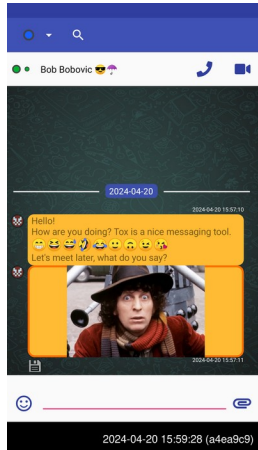
TRiFA - Android



<https://f-droid.org/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



getting in touch ...

- Github

<https://github.com/zoff99/c-toxcore>

- Tox Public Group

[154b3973bd0e66304fd6179a8a54759073649e09e6e368f0334fc6ed666ab762](https://trifagrps.tox.zoff.cc/154b3973bd0e66304fd6179a8a54759073649e09e6e368f0334fc6ed666ab762)

or

<https://trifagrps.tox.zoff.cc/>

or

QR Code ----->



- Matrix

<https://matrix.to/#/#trifa:matrix.org>

- Email

tox@zoff.cc

