Year in Tox

What's been going on?

robinli, sudden6, zoff at ToxCon 2019 11.-13.10.2019

Events - Talks

Grazer Linuxtage - 2019-04-27

Tox, secure open source P2P communication

https://pretalx.linuxtage.at/glt19/talk/38PDHW/

Easterhegg - 2019-04-20

Blinkenwalls, Electronic Windows, and other "magical" portals with Tox

https://conference.c3w.at/eh19/talk/8XZUMW/

Linuxwochen Wien - 2019-05-04

Blinkenwalls, Electronic Windows, and other "magical" portals with Tox

https://cfp.linuxwochen.at/de/LWW19/public/events/933

Events - Faires

Make Munich - 3. + 4. March 2019

https://make-munich.de/programm/

make MUNICH 2. & 3. MÄRZ 2019

Sachsen Maker Faire - 28. + 29. March 2019

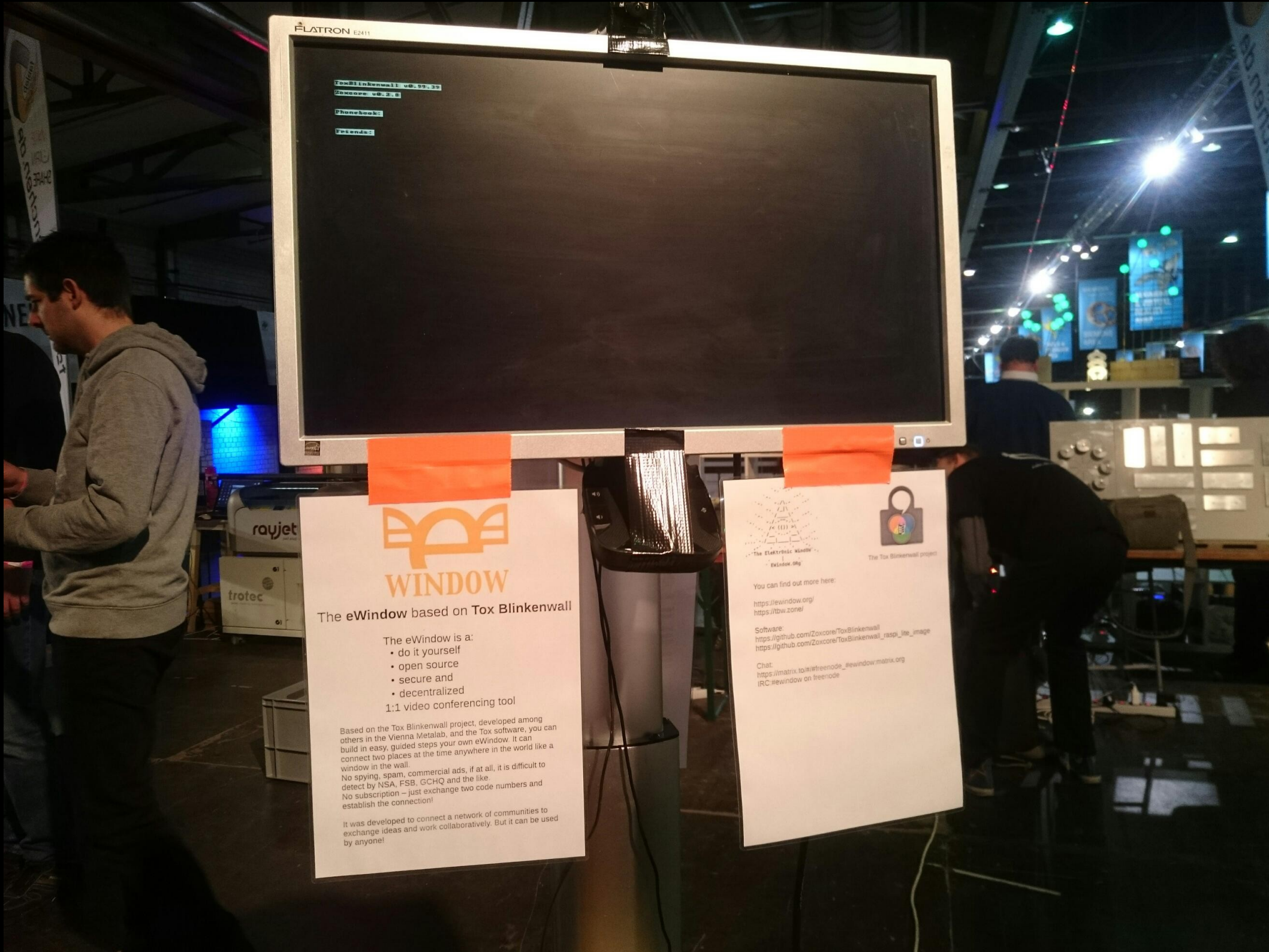
https://www.maker-faire-sachsen.de/

Sachsen Maker Faire®

Maker Faire Vienna - 4. + 5. May 2019

https://www.makerfairevienna.com/maker

04 & 05 MAY 2019 Maker Faire VIENNA


FLATRON E2411
ToxBlinkenwall v0.99.39
Zoxcore v0.2.8
Phonebook:
Friends:
WINDOW
The eWindow based on Tox Blinkenwall
The eWindow is a:
• do it yourself
• open source
• secure and
• decentralized
1:1 video conferencing tool
Based on the Tox Blinkenwall project, developed among others in the Vienna Metalab, and the Tox software, you can build in easy, guided steps your own eWindow. It can connect two places at the time anywhere in the world like a window in the wall.
No spying, spam, commercial ads, if at all, it is difficult to detect by NSA, FSB, GCHQ and the like.
No subscription – just exchange two code numbers and establish the connection!
It was developed to connect a network of communities to exchange ideas and work collaboratively. But it can be used by anyone!
The Elektronic Window
EWindow.ORG
The Tox Blinkenwall project
You can find out more here:
https://ewindow.org/
https://tbw.zone/
Software:
https://github.com/Zoxcore/ToxBlinkenwall
https://github.com/Zoxcore/ToxBlinkenwall_raspi_lite_image
Chat:
https://matrix.to/#/#freenode_#ewindow:matrix.org
IRC:#ewindow on freenode
rayjet
trotec


METALAB
205
Maker Faire Vienna
Reparatur
netzwerk.at
Wir machen's wieder gut.
METALAB
220m² Raum im Herzen Wiens für technologisch-kreative Projekte, Veranstaltungen, Software, Hardware, Essen & mehr...
YOU CAN DO ANYTHING AT METALAB.
THE ONLY LIMIT IS YOURSELF!
Lasercutter, 3D-Drucker, Vinylcutter, CNC-Fräse, Drehbank, Fotolabor stehen für die Realisierung von technologisch-kreativen Projekten zur Verfügung. Küche, Lounge und viel Platz sorgen für eine gemütliche Atmosphäre.
GEMEINSAM UND SELBSTSTÄNDIG HACKEN.
WERDE TEIL DER COMMUNITY!
Egal ob du gerne klassische Werkmaterialien bearbeiten, Roboter bauen, Hardware reparieren oder Software entwickeln und einsetzen möchtest - im Metalab findest du Menschen mit denen du dich über die Materie austauschen kannst.
Schau am besten einfach abends vorbei und frag nach einer Tour durch das Lab!
SPASS MIT MASS
207
Maker Faire Vienna
DO NOT ENTER
METALAB
NOM NOM


Maker Faire
VIENNA
start next level
CONRAD
WILLKOMMEN
WELCOME
FEDERFARBE
119
SOCIAL IMPACT AWARD ÖSTERREICH
120
OPENDRONE
WC


eWindow by
teilWERK
Dresden


Firmware-Hack
Vorgehensweise
1. Firmware der IoT-Geräts organisieren
z. B. Download, Anfordern beim Hersteller, Auslesen vom Flash-Chip, Schwachstelle, ...
2. Firmware entpacken
z. B. Archiv oder Dateisystem extrahieren
3. Dateisystem analysieren, um Backdoor-Möglichkeiten zu finden und einzubauen
4. Firmware, Dateisystem, ... packen
5. Firmware am IoT-Gerät einspielen
z. B. über Update-Mechanismus, Schwachstelle, Flash-Chip flashen, ...
fsfe.org

Master student

Title	Adopting the Noise key exchange in Tox
Company	TokTok Ltd.
Company Website	https://toktok.ltd
Software Repository	https://github.com/TokTok/c-toxcore
Mentor Contact Details	Zoff <tox@zoff.cc>
Type of paper	Master Thesis

Master student

Adopting the Noise key exchange in Tox

Tox is a Messenger Protocol based on a cryptographic network library using Daniel J. Bernstein‘s NaCl crypto library. This means the primitives for key exchange (Curve25519), authentication (Poly1305), and symmetric encryption (XSalsa20) are state of the art peer reviewed algorithms. However, the key exchange itself is a simple transfer of ephemeral public keys encrypted with long term static public keys, authenticated with the long term private keys. This method works but is vulnerable to Key Compromise Impersonation (KCI).

Trevor Perrin‘s Noise is a formally verified authenticated key exchange (AKE) construction which was designed to protect against KCI. The goal of this thesis is to demonstrate the attack on Tox, implement the Noise construction in the toxcore library, and show that KCI is no longer possible.

Master student

Deliverables:
• Create a proof of concept attack program that demonstrates the attack • Describe in detail why the attack works • Implement Noise handshake in toxcore as an alternative to the existing handshake • Show that the attack no longer works when the old handshake is disabled • Update the Tox Protocol Specification

The paper may be written in English or in German

Toxcore

Persistent conferences (merged - #1156)

ToxAV threading fixes (ongoing - #1343, #1346)

New friend finding (ongoing - #1335)

Fuzz-testing (ongoing - #1331)

uTox

Support for persistent conferences

Support for more BSD variants ->
FreeBSD, NetBSD, DragonFlyBSD

Lots of bugfixes

qTox

- multi-language spell checking
- automatic update check
- command line proxy settings (good for Tor-only users)
- desktop integrated notifications
- file history stored across session
- persistent audio groups
- chat history searching
- dark theme
- automatic chat loading on scroll
- tons of bug fixes

TRIfA

- resumable filetransfers
- multidevice / offline messages *

* watch the talk about ToxProxy