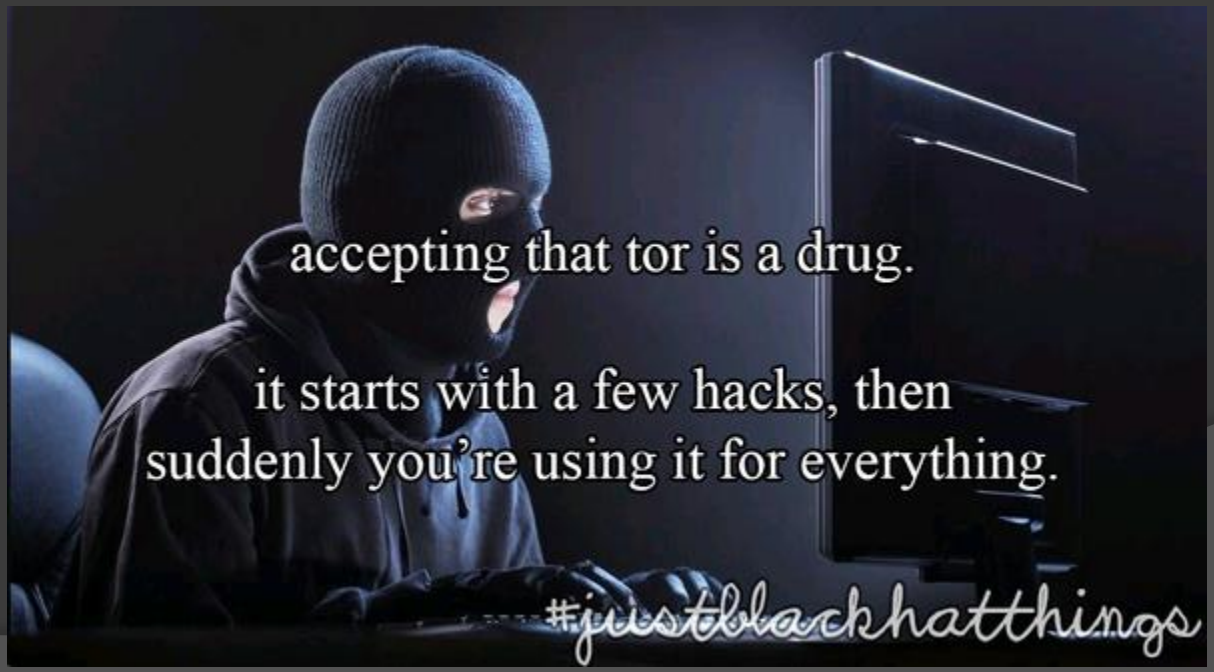
Fun and mayhem for less than 20 €

GUERRILLA TOR

Let's hide our IP address...

- A VPN/proxy implies trust in a third party
  - Passive adversary can still learn your IP
- Tor implies trust in the exit nodes
  - Setting up your own exit nodes fixes this



Seattle police raid home of privacy activists who maintain Tor anonymity network node

By Mary-Ann Russon

March 31, 2016 19:02 BST

techdirt

Techdirt | Wireless News | Innovation | Case Studies | Startups | Net Neutrality | Techdirt Deals!

Main | Submit a Story | RSS

PODCAST Techdirt – The Link Between Credit And Surveillance SOUNDCLOUD

<< Citizens On Terrorist Watchlist - Including A... | Sony Finally Releases PS4 Remote Play For PC... >>

Law Enforcement Raids Another Tor Exit Node Because It Still Believes An IP Address Is A Person

from the *TASE-THAT-ROUTER* dept

An IP address is **not a person**, even less so if said IP address traces back to a Tor exit relay. But
…s" from subjecting people with no knowledge at all of alleged
… to raids and searches.

…eized a bunch of **computer equipment** from a residence
…moving forward with nothing more than an IP address -- seized
…was ***also* running** a Tor exit relay.

…ed ICE's "upon information and belief" affidavit statements
…*e* "information" and recommended law enforcement check
…s before conducting raids based on IP addresses. ICE,
…same mistake, no matter what information was brought to its

…predicated on nothing more than an IP address -- at least not
…formed by Seattle PD conducting a child porn investigation.
…d the activity back to an IP address, which was all the probable
cause it needed to **show up at privacy activist David Robinson's home at 6 a.m. and demand access to his computers**

the grugq

@thegrugq

Following

Ran Tor exit node out of residence. Police showed up with a warrant. Sad this still happens, but that's police logic twitter.com/SeattlePrivacy …

Our idea

- Set up **disposable** Tor exit nodes:
  - It's our own node, not someone else's box
  - Only used a few times, then never again (good OPSEC)
  - Cannot be traced back to you (no hosting)
  - Must be cheap
    - If we were rich we wouldn't be here, folks!
  - Must use public internet infrastructure
    - We don't want to break the law…

Can we trust Tor?

- Ehrm… no. But we don't need to:
  - We control the exit nodes ☺
  - Using OpenVPN we can thwart (some) existing crypto & traffic analysis attacks against Tor
  - Time is our ally here
  - But nothing replaces good OPSEC!

Our first prototype: TL-WR703N

Problems

- Somewhat bulky, difficult to hide in public places
- Requires external power
- 32 Mb of RAM, 4 Mb of ROM
  - You can fit a minimal build of OpenWrt with Tor, but little else
- Requires a USB stick for additional storage

Here comes the ZSUN

Here comes the ZSUN

- Even cheaper than the TP-LINK!
- Much, much, much smaller
- 64 Mb RAM, 16 Mb ROM
- External storage can be a MicroSD card
- Hardware is (relatively) easy to change
- Powered from the USB port itself
- Already researched at ***hackerspace.pl***


zsun
4GB
CD4G CHINA
1605PY27336
Kingston
SDC4-4GB 154 FC T


TRAVELADAPTER
Адаптер питания
MODEL NO./МОДЕЛЬ:ART-U90EWE
INPUT/TEG LISTRIK/ВХОД:
100-240V~FREKUENSI 50-60Hz 0.35A
OUTPUT/ВЫХОД : 5.0V ⎓ 2.0A
SIN, Серийный номер: RT1C915CS/B-E
Дата производства: 27.03.2014Z
MADE IN CHINA/ СДЕЛАНО В КИТАЕ
AB10 KZO.02.0072
zsun

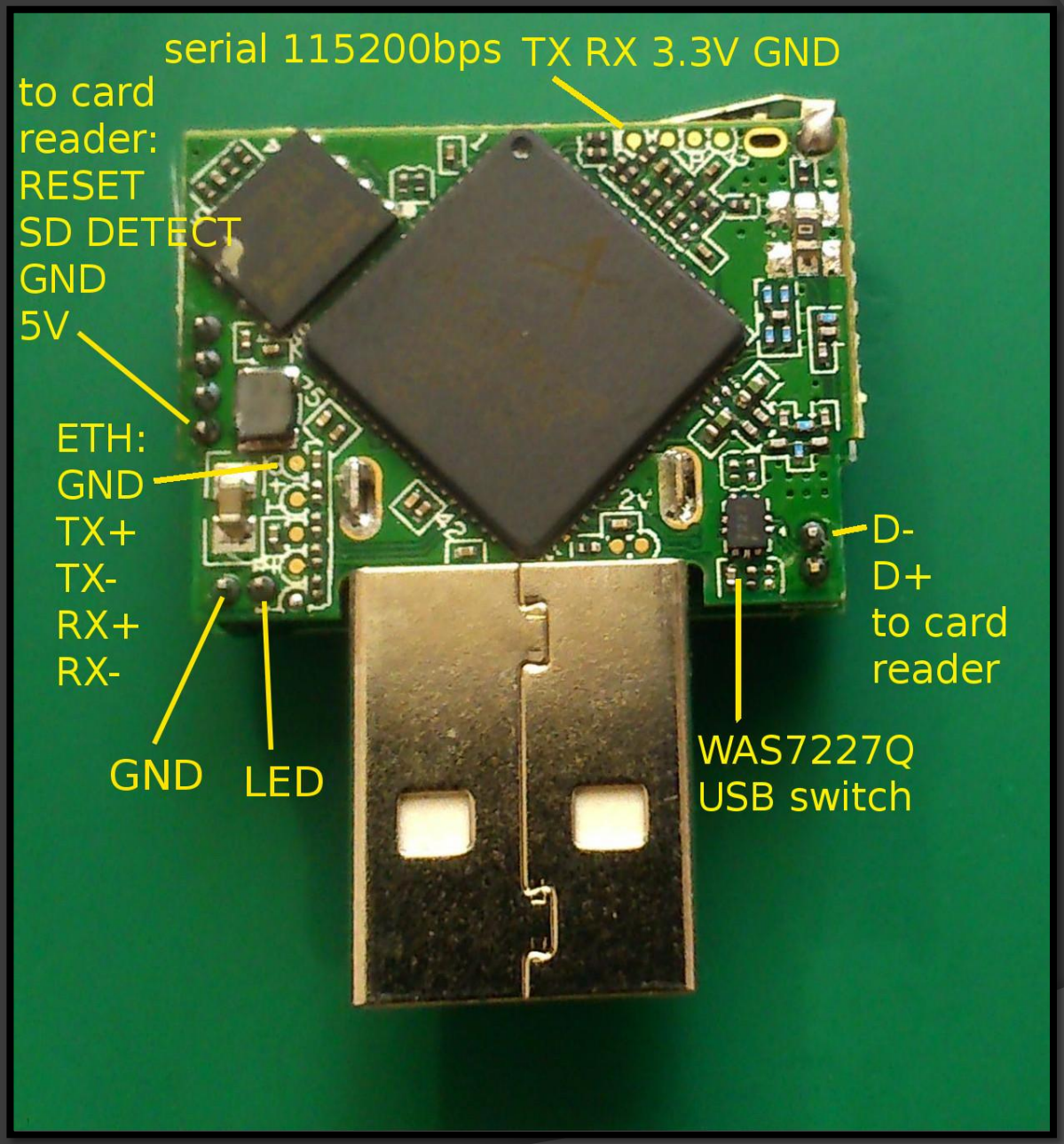


Image credit: https://wiki.hackerspace.pl/projects:zsun-wifi-card-reader

Getting the hardware

- We ordered our prototype devices from DealExtreme
  - This won't do in real life, cash is better
  - For bulk purchasing go to the manufacturer
- Prices (individual / bulk):
  - 10 € / 7 € – ZSUN WiFi SD Card Reader
  - 9 € / 8 € – Waterproof Solar Power Bank
  - 3 € / 2.50 € – MicroSD & USB Charger

Getting the hardware

- http://www.dx.com/p/genuine-sandisk-microsd-transflash-tf-memory-card-4gb-34531
- http://www.dx.com/p/sungzu-5000mah-waterproof-solar-power-bank-blue-black-430794
- http://www.dx.com/p/zsun-wi-fi-usb-2-0-card-reader-for-tablet-pc-ipad-iphone-android-mobile-phone-black-379018

Let’s change the firmware

- We’ll miss this beautiful banner though!

```
$ socat - TCP4:10.168.168.1:11880
??????!????
(none) login: root
root
Password: zsun1188

Welcome to
          -------      |            /    /--/         ___       |
           /           |           /|     \/         _____    --|--|
          /_____\      |---       --|--   //--/      /         /  |
           __|__       |           /|\    / \/      /___\     /   |
          ___|___   ___|____      / | \     /                /   \|
                          深圳至上移动科技有限公司
                          Shenzhen Zsun Cloud Technology Co., LTD.
                          www.zsuncloud.com

BusyBox v1.01 (2014.12.27-02:50+0000) Built-in shell (ash)
Enter 'help' for a list of built-in commands.

~ #
```

Building OpenWrt

- The folks at Hackerspace.pl already wrote a kernel patch for this hardware
  - It's for an old kernel now, but we ported it to more versions (3.18.29, 4.1, 4.4)
  - Hopefully soon official in OpenWrt!
- The OpenWrt sources have to be compiled on Ubuntu
  - We prefer real Linux, thank you :P
  - Solution: Vagrant or Docker

Building OpenWrt

- We started by using Vagrant to set up an Ubuntu VM
  - Downloads all dependencies and sources automatically
  - Very easy to do!
- Recently we added Docker support too
  - Better resource management
  - We can have a proper build server now

Building OpenWrt

- From the user's point of view, it's the same
- A Makefile takes care of automating the process of parallel building multiple images
  - Support for adding patches and additional software and configuration files
  - SSL/SSH/VPN/Tor certificates generated automatically on each build
- Just git clone and you're good to go: https://github.com/OpenWrt-HappyHacker/vagrant-happyhacker

Building OpenWrt

```
~/happyhacker/vagrant-happyhacker$ make help

To build all targets just type:
    make all

To list the available targets:
    make list

To build a specific target:
    make bin/<target>

To clean the build files (but not the VM or output files):
    make clean

To completely clean up everything (including the VM and output files):
    make dirclean

To begin preparing a new firmware image from scratch:
    make menuconfig

To modify the configuration for an existing target firmware image:
    make menuconfig CONFIG=<target>

Vagrant VM control:
    make up
    make suspend
    make destroy

~/happyhacker/vagrant-happyhacker$
```

Building OpenWrt

```
~/happyhacker/vagrant-happyhacker$ ls
bin  config  Makefile  patches  README.md  script  src  TODO.md  Vagrantfile
~/happyhacker/vagrant-happyhacker$ make list

The following targets are available:

$ make bin/x86-torrorist
$ make bin/zsun-debug
$ make bin/zsun-extboot
$ make bin/zsun-torrorist

~/happyhacker/vagrant-happyhacker$ make bin/zsun-debug
Bringing machine 'openwrt-happyhacker-build-vm' up with 'virtualbox' provider...
==> openwrt-happyhacker-build-vm: VirtualBox VM is already running.
--------------------------------------------------------------------
BUILDING FIRMWARE IMAGE FOR TARGET: zsun-debug
--------------------------------------------------------------------
‘/vagrant/src/common/files/’ -> ‘./files/’
‘/vagrant/src/common/files/etc’ -> ‘./files/etc’
‘/vagrant/src/common/files/etc/banner’ -> ‘./files/etc/banner’
/vagrant/patches/zsun-openwrt-chaos-calmer.diff:280: space before tab in indent.
        {"w25x10"},     {"w25x20"},     {"w25x40"},     {"w25x80"},
/vagrant/patches/zsun-openwrt-chaos-calmer.diff:281: space before tab in indent.
        {"w25x16"},     {"w25x32"},     {"w25q32"},     {"w25q32dw"},
/vagrant/patches/zsun-openwrt-chaos-calmer.diff:282: space before tab in indent.
```

Building OpenWrt

```
Applied patch target/linux/ar71xx/files/arch/mips/ath79/mach-zsun-sdreader.c cleanly.
Applied patch target/linux/ar71xx/generic/profiles/zsun.mk cleanly.
Applied patch target/linux/ar71xx/image/Makefile cleanly.
Applied patch target/linux/ar71xx/patches-3.18/415-mtd-m25p80-add-w25q128fw.patch cleanly.
Applied patch target/linux/ar71xx/patches-3.18/610-MIPS-ath79-openwrt-machines.patch cleanly.
warning: squelched 7 whitespace errors
warning: 12 lines add whitespace errors.
Generating new SSH keypair...
Tor hidden service keys created for: ydw5ifukbsegmt3c.onion
Added new Tor hidden service on port 443.
Root certificate found at: /vagrant/script/ca.crt
Generating new SSL certificate...
New SSL certificate created for domain: ydw5ifukbsegmt3c.onion
Collecting package info: done
Collecting target info: done
#
# configuration written to .config
#
Checking 'mkisofs'... ok.
Checking 'mkisofs'... ok.
 make[1] world
 make[2] tools/install
 make[3] -C tools/patch compile
```

Building OpenWrt

```
bin/{target}/*                  This is where the output files will be written

config/{target}/config          OpenWRT makefile configuration, this is mandatory
config/{target}/sources         List of components to be included in this target
config/{target}/patches         List of patches to be applied on this target

config/{target}/files/*         Files to be included directly in the device filesystem
config/{target}/initialize.sh   Initialization script for this target
config/{target}/finish.sh       Post build customization script for this target

src/{component}/files/*         Files to be included directly in the device filesystem
src/{component}/initialize.sh   Initialization script for this component
src/{component}/finish.sh       Post build customization script for this component

patches/{patch}.diff            Diff-style patch for the OpenWRT source code to be applied
```

Our setup: ph33r the “torrorist”

- Tor with hidden services
  - OpenVPN for masking our own traffic, better than a conventional exit node
- Optional applications can be added
  - A file sharing application to act as an anonymous dead drop for files
  - More fun stuff can be added too:
    - IRC/XMPP servers for secure chat
    - Murmur server for voice (Mumble)
  - Could be used as dead man’s switch

Our setup: ph33r the “torrorist”

- New SSH keys generated for each build
- New Tor hidden service keys as well
- New SSL certificates, signed by a common root certificate
  - Easier to set up
  - Root cert is created on first build
  - Certificate pinning is recommended, though
- No hard-coded credentials anywhere

Connecting to the Internet

- This proved to be the most difficult part
- Our first idea: 4G modems
  - They provide a reasonable speed
  - Can be deployed almost anywhere
  - Some countries (like Ireland) don't ask for ID when buying a SIM card
- Problem: 4G modems are expensive!
  - Still doable if you've got the cash

Connecting to the Internet

- Our evil scheme: public Internet access
  - Many cities in the world have public Wi-Fi infrastructure
  - Depending on local legislation, you may get away with using Wi-Fi connections from bars and other publically accessible locations
  - Technical problem is solved, human problems begin ☹
  - Consult your local tech lawyer!

Connecting to the Internet

Using the Wi-Fi Manager

- We developed our own Wi-Fi manager
  - Can connect to multiple Wi-Fi networks at the same time
  - Each connection has a different “identity”, with random ***realistic*** hostnames and MAC addresses
  - Integrates with UCI, the OpenWrt configuration system
  - Modular and very configurable
    - But works directly out of the box too

Using the Wi-Fi Manager

Lucass-MacBook	18:ff:0f:30:34:aa	100.100.100.104	2 days, 17 hours, 10 minutes, 13 seconds
android-047h6319764j0yaw	00:25:9e:da:b8:74	100.100.100.105	2 days, 17 hours, 43 minutes, 39 seconds
Annas-MacBook	18:ff:0f:2b:21:61	100.100.100.106	2 days, 17 hours, 55 minutes, 17 seconds
hostname	0c:82:68:ee:7f:3e	100.100.100.107	2 days, 21 hours, 46 minutes, 5 seconds
android-02feqr1uw2j7jq9j	58:3f:54:b5:30:55	100.100.100.109	2 days, 19 hours, 18 minutes, 45 seconds
android-qn23oj1i48f9m567	f8:3d:ff:89:5b:e3	100.100.100.110	2 days, 19 hours, 27 minutes, 12 seconds
android-p091n709kqi90om6	ac:e2:15:7a:8a:7e	100.100.100.111	2 days, 19 hours, 43 minutes, 51 seconds
Islas-iPhone	00:f4:b9:44:4a:c7	100.100.100.112	2 days, 19 hours, 55 minutes, 17 seconds
Jazmin-Notebook	00:10:18:b4:cb:09	100.100.100.113	2 days, 20 hours, 45 minutes, 55 seconds
Kaspars-MacBook	18:ff:0f:8a:c1:53	100.100.100.114	2 days, 20 hours, 53 minutes, 26 seconds
android-e1tlq04mo8411ae4	00:25:9e:81:61:50	100.100.100.115	2 days, 21 hours, 23 minutes, 33 seconds
android-5d2pfrgim3dj8u0b	58:3f:54:ac:ad:a1	100.100.100.116	2 days, 21 hours, 41 minutes, 57 seconds
William-Laptop	5c:51:4f:75:54:55	100.100.100.117	2 days, 21 hours, 47 minutes, 28 seconds
android-0474pg35t6th3hj7	f8:95:c7:d9:41:07	100.100.100.118	2 days, 21 hours, 54 minutes, 28 seconds
Harry-Computer	00:10:18:8b:85:6c	100.100.100.119	2 days, 21 hours, 56 minutes, 22 seconds
Maksims-MacBook	18:ff:0f:88:c9:4e	100.100.100.120	2 days, 23 hours, 51 minutes, 33 seconds
Emilys-iPhone	00:f4:b9:3c:c2:5e	100.100.100.121	2 days, 23 hours, 58 minutes, 7 seconds

It’s demo time!

Future work

- More security improvements are needed
  - OpenWrt is clearly not designed as a secure environment…
  - Defaults to building with ALL exploit mitigations turned off
  - By default everything runs as root

Future work

- We’re working on a way to boot OpenWrt directly from the SD card
  - Not as easy as it seems! We don’t have a helpful BIOS here like we do in x86 ☹
  - We need to patch uboot to support the SD card used by the ZSUN
  - The advantage for the end user: no need to flash a new image, just change the SD card

Future work

- Another evil plan: using LXC
  - Containers are handy for isolating the different services running on the device
  - Deploying containers remotely over Tor is also a possibility
    - Everything would be volatile – shutting down the device would destroy all data
    - Think of a guerrilla cloud environment ☺

Thanks for all the fish!