We live in a world where digital privacy doesn't exist anymore, where journalists couldn't securely do their work, where companies and individuals are spyed upon by various entities with no real reason, and where Human Rights are cynically disregarded.

So, there is an urgent need for an easy-to-use tool to restore digital privacy, designed for non-tech people.

This autonomous device is designed to protect online privacy, using powerful softwares, but keeping it simple and practical with its easy to use touch interface and convenient features.

It is autonomous and small enough to be transported, making it the perfect companion for our digital devices.

It uses the available connectivity to build a secure access-point and bypasses internet filters to connect to a remote network, use a secured internet or even browse anonymously.

It's easy to connect laptop/smartphone to the device's secured wifi access-point : no additional setup is needed, except connecting to the wireless access-point.

It could connect the internet via a public wifi access-point, 3G internet via phone usb/wifi tethering, corporate cable network, or even your own router/ADSL box.

Details

Basically, this device acts as a wifi / ethernet router and access point. It could connect to the internet using some random wifi, a wired network, or a tethered android phone (wifi or usb). On the secured side, it acts as a wireless access point with internet forwarding so it works with every kind of device : PC, laptop, smartphone, using Windows, GNU/Linux, Android or even Mac-OSX.

The wireless access-point is also hardened with a random key feature. The access-point security key and SSID could be modified on-demand and at boot-time with some random one.

From the touch screen interface, TOR or an OpenVPN tunnel could be enabled. This custom interface could be used for complete operation, full setup and device monitoring.

It requires no setup on the endpoint device (computer, smartphone...) to work. The user interface is also very easy to use with on/off buttons, so it is very easy to operate by non tech people.

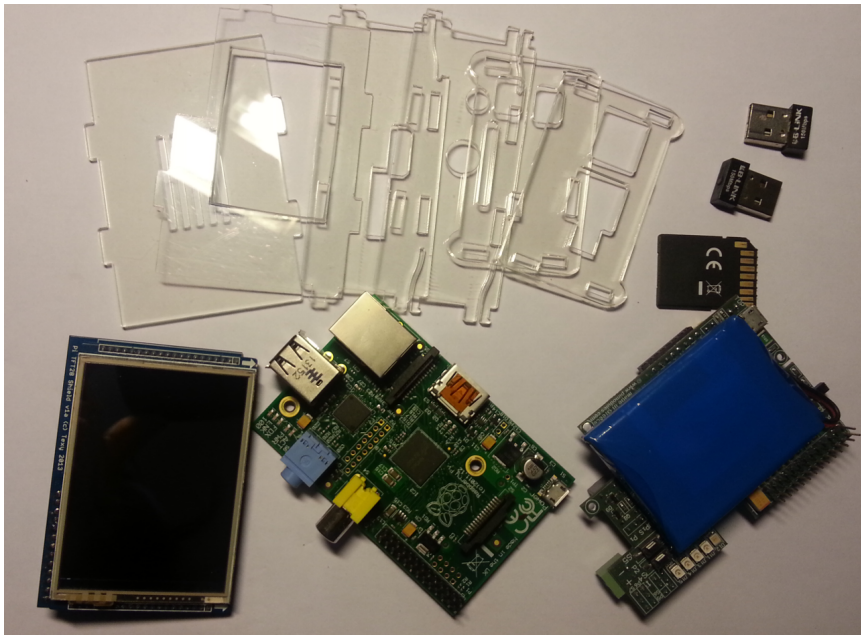
There is no configuration web interface, like routers. Everything is done using the touch interface, so a physical access is needed to use the device.

In sensitive situations, the complete software and operating system could be installed in a few minutes from a preconfigured and encrypted image. The SD-card could also be removed from the device or even destroyed in a few seconds, causing no harm to the device, but makes it completely empty and useless. This way, sensitive data such as SSH private keys are secure.

The device hardware is open source, and uses only Libre software. This way, it could be improved by the community when it needs to, and it also helps defend digital freedom and Human Rights.

It also makes a perfect device to fight planned obscolescence : the software is built to be cross-compatible with different boards, offering different features, to adapt to various situations and evolve over time.

The device could be built at home using some easily sourceable parts and laser cut / 3D printed enclosure, would be available in a ready-to-build kit, but could also be easily customized and adapted for specifical needs.



Ready-to-build kit

Key features

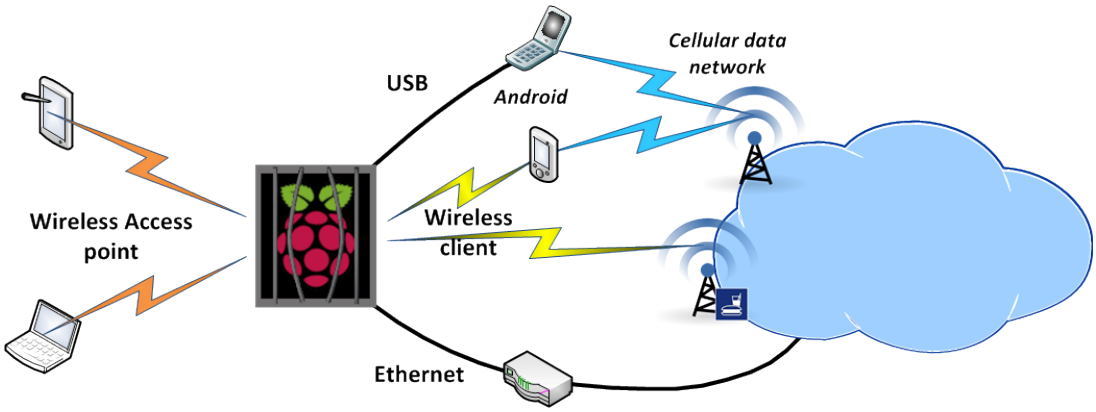
- Secure wireless access point :
    - Random security key and SSID generation features
    - Quick connect to Android using QR code
    - Locked AP security settings
- On-demand OpenVPN transparent tunnelling to a remote trusted network/server (hosted on a second similar device or a computer) :
    - Point to point tunneling with internet forwarding
    - Very stable and fast over wireless, cellular and other non reliable networks
    - Keeps connected over a roaming connection
    - Capable of traversing NATs and firewalls
- On-demand Tor transparent proxy :
    - Anonymous browsing
    - Access forbidden websites / services based on location
    - Force or block relay nodes based on their location, from the main interface
- Hardware firewall with dynamically and automatically addressed rules
- Ad-blocker / DNS filter feature with quick custom rules
- Touch display control interface
- Very low power consumption : ~5 Watts, runs on a phone charger
- Onboard 2600 mAh battery : ~4h running time
- Optional external 10000 mAh battery : adds ~8h and charges onboard battery
- Very easy to operate, install and deploy

Raspberry Pi type B prototype

Wireless Access-Point

Android QR-code easy connection

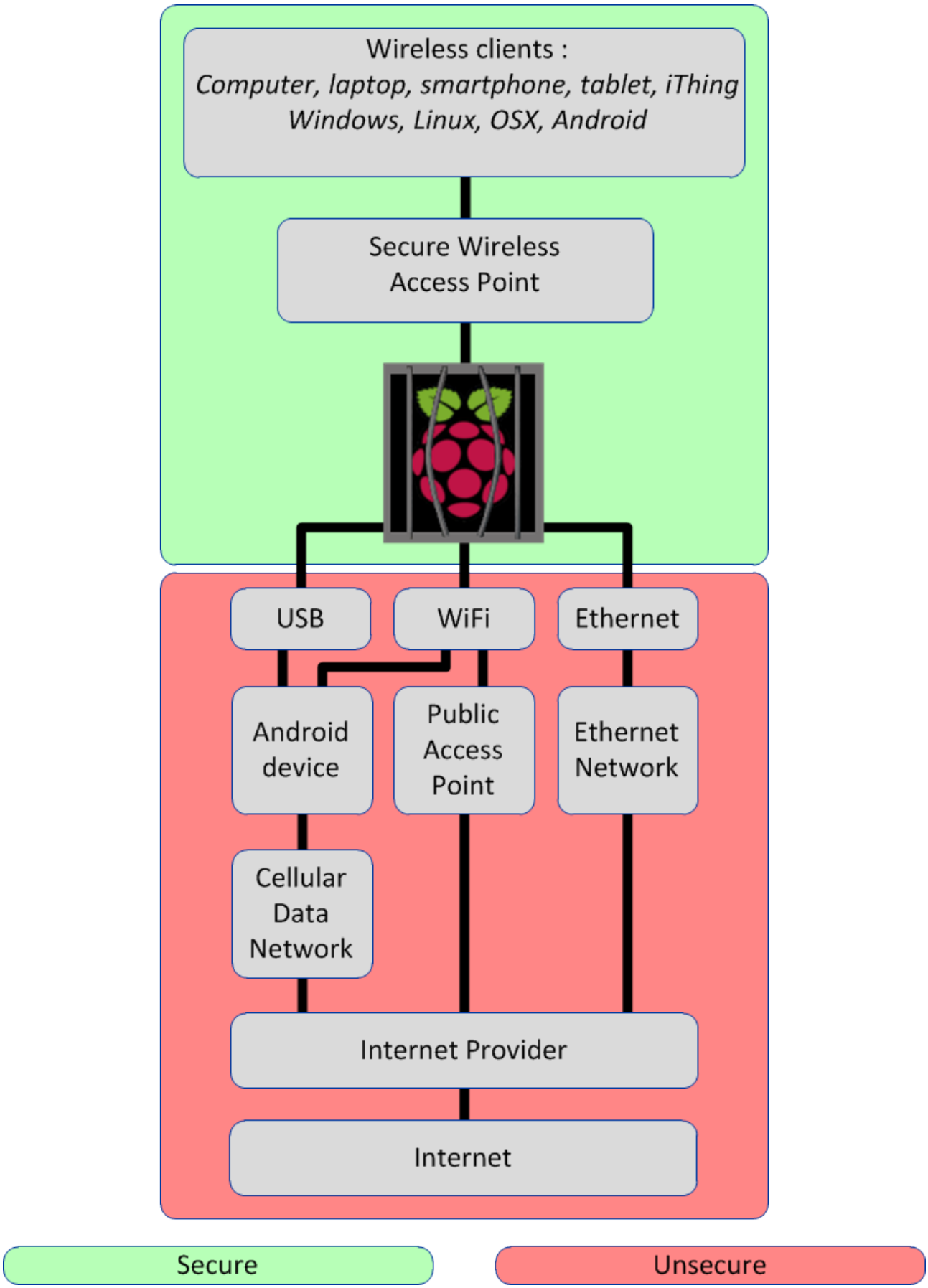
- Random SSID and passphrase generator : each time the Wireless AP is restarted, a new random SSID and passphrase combo is generated. It could be enabled on boot (*default enabled*).
- Quick connect : when the Wireless AP is restarted (or SSID / passphrase combo changed), a screen shows these informations (for PC users) along a QR code for quick Android connection.
- Important settings are hardcoded using highest security available (WPA2-PSK).
- Ad-blocker / DNS filter feature with quick custom rules
- Could use any outgoing connection : cable ethernet, public wifi (using a second optional WiFi USB adapter), cellular network using USB/WiFi android tethering



User settings

- Security key lenght (32-64-96-128-196-256 bits, *defaults 128*),
- AP Channel (1 to 13),
- random SSID (*defaults on*),
- random SSID / passphrase on boot (*defaults on*),
- request new random SSID/passphrase

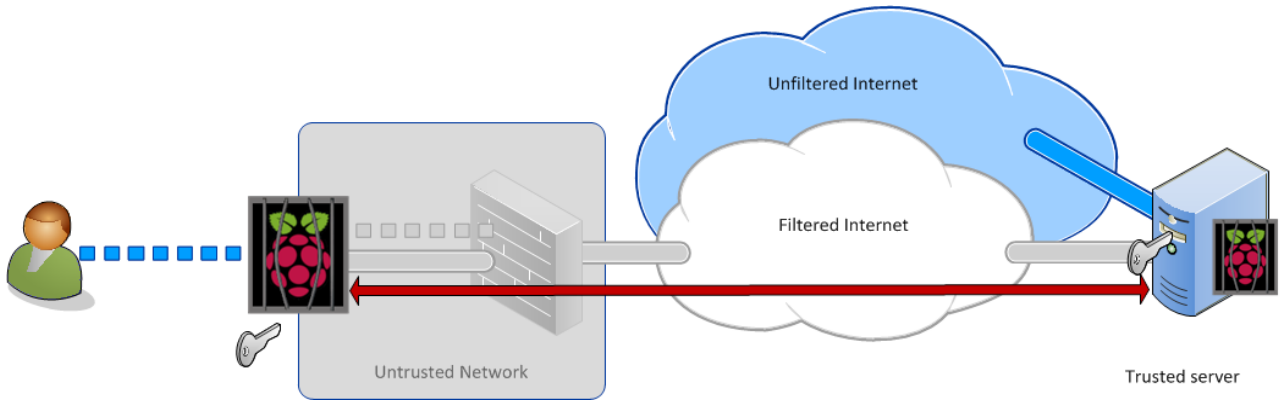
Connection diagram



OpenVPN transparent proxy

OpenVPN transparent proxy offers a security layer over an unsecure connection, routing the internet traffic to a secure location using an encrypted tunnel.

- Point to point tunneling with internet forwarding : securely access a remote network and use it's internet connection
- Capable of traversing NATs, firewalls, and various web filters
- Very stable and fast over wireless, cellular and other non reliable networks, works over a roaming connection
- No major vulnerabilities and considered extremely secure, as opposed to PPTP/L2TP/Ipsec
- Designed for use with a companion server device hosted in a secure location
- No additional setup needed on the end device



Use OpenVPN to bypass common internet filters

Protocol : OpenVPN

Authentication : self-generated pre-shared SSL certificate

Encryption : AES-256

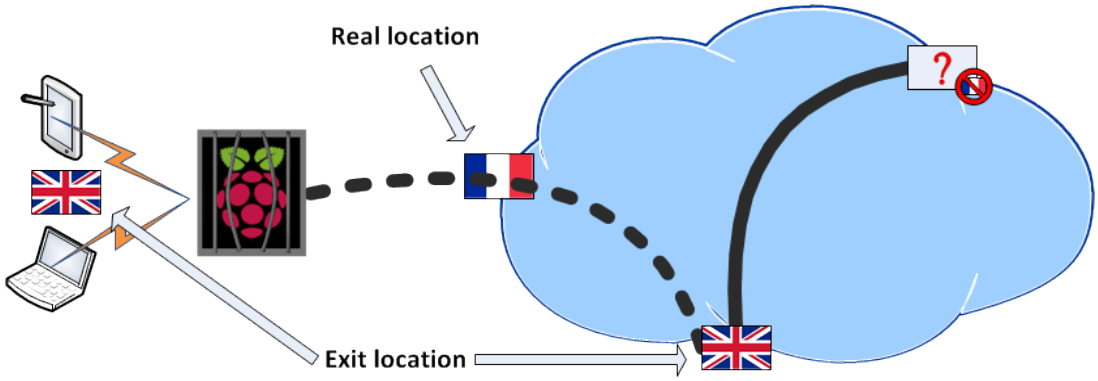
Tor transparent proxy

Tor transparent proxy offers a anonymity layer over an internet connection, using random encrypted circuits. Real IP address is hidden, internet traffic seems to originate from a remote location.

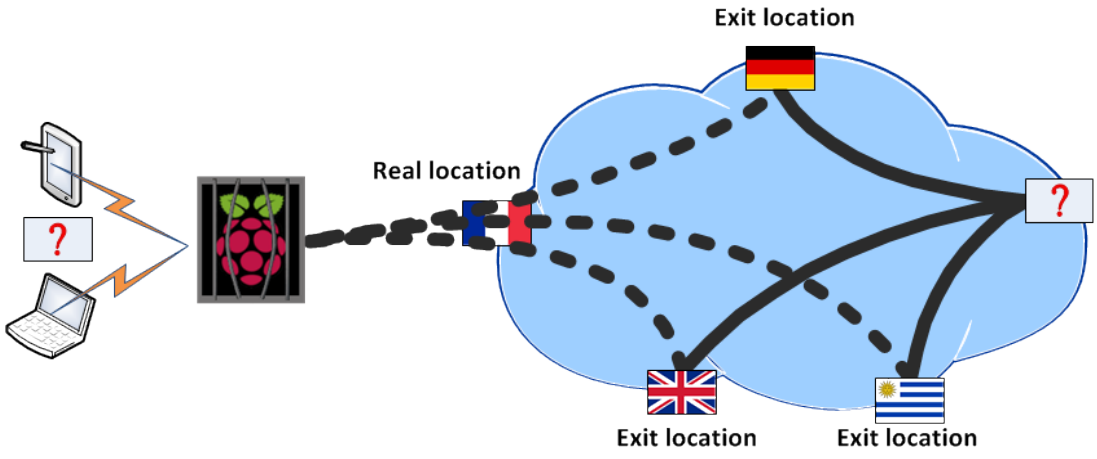
Tor transparent proxy also allows to use blocked internet services based on user location or IP.

Tor is a very powerful software, and could cause more harm than good if misused. Please use it only when needed.

- Prevents people from learning your physical location or browsing habits
- Ability to use a random encrypted circuit
- Force / blocks circuits based on location (246 countries listed)
- Locked to only allow predefined allowed services : using it for torrent downloading, for instance, would cause harm to the entire Tor network and would also be a risky use. Using HTTP without encryption on Tor network could also be unsecure. That's why only predefined services like HTTPS are allowed
- No additional setup needed on the end device



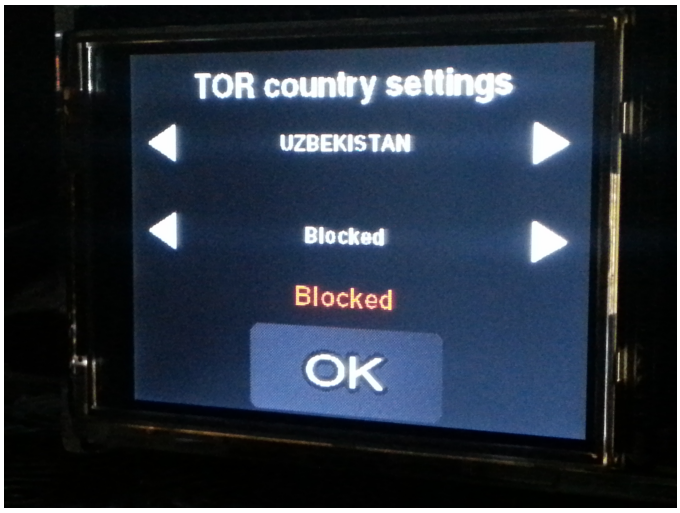
Access forbidden websites / services based on location



Real IP is hidden using random encrypted circuits

Tor user setting

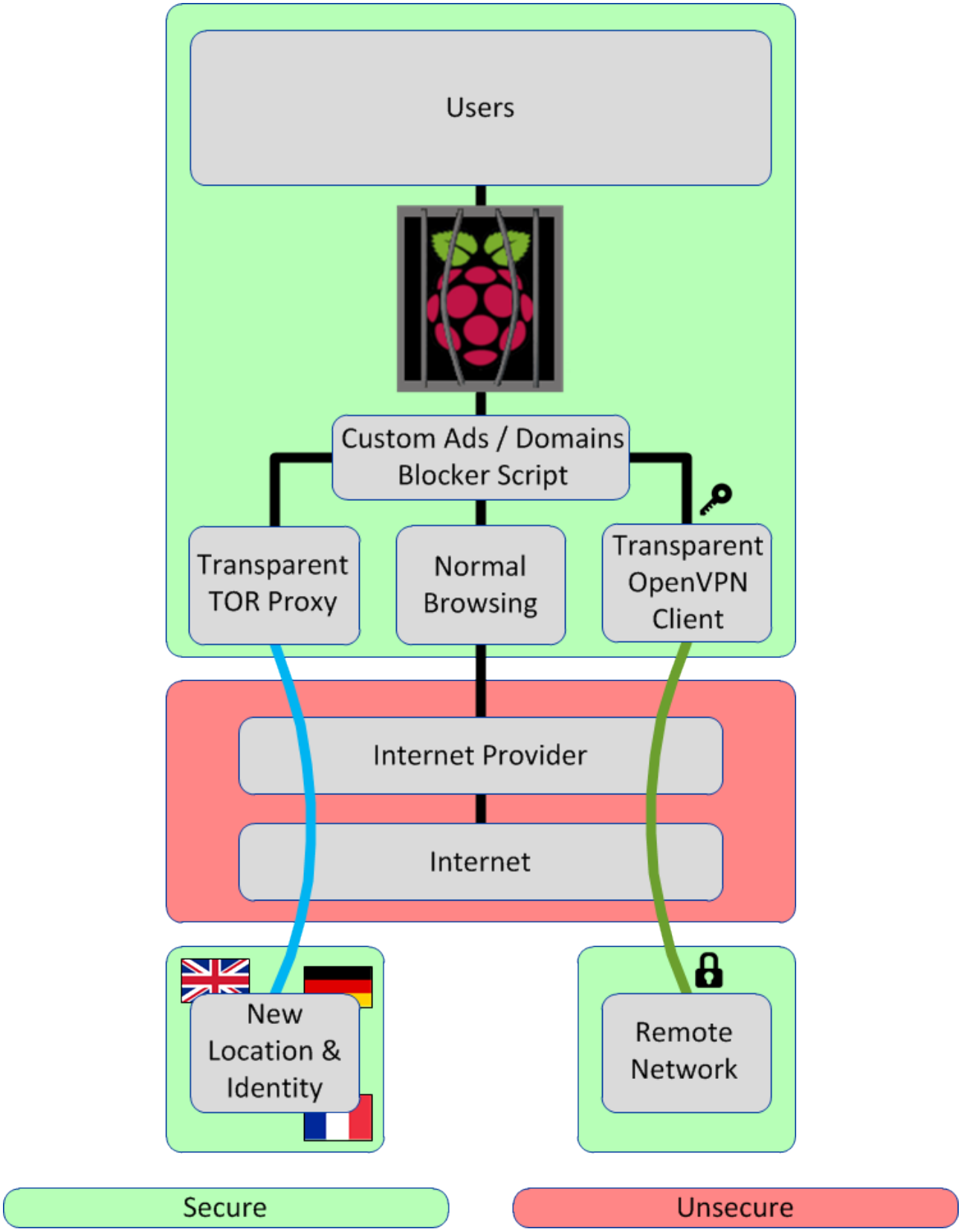
- Block or force individual nodes based on their location



Tor target uses

- Helps defend individuals against traffic analysis
- Helps people to use online services blocked by their local Internet providers
- Helps businesses to keep their strategies confidential
- Helps activists to anonymously report abuses or corruption
- Helps journalists to protect their research and sources online

Main features diagram



Additional features

- Touch display + control software
- Easy to use : designed for non experts people
- Software and OS on accessible SD-card : easy and economical to maintain, repair, replace or even destroy
- Very low power consumption : ~4 Watts, runs on a phone charger (1 Amp mini)
- Power monitoring and energy saving features
- Onboard battery : ~ 4h running time
- Optional external battery : adds ~ 8h running time and charges onboard battery
- Very easy to clone, deploy, and customize to various uses
- Designed to be built using easy sourceable parts or ready-to-build kit

Actually under development

Software

- Improved firewall profiles system
- Improved web filter
- Device installation / update functions

Hardware

- Device porting to a more powerful and compact mainboard with onboard wifi
- Device porting to a mainboard with 5x ethernet switch
- New, more consumer ready touch display
- Overall cost reduction

Planned features

- Filesystem encryption
- Kill switch
- Transparent SSH tunnel

References

Project page

http://hardware-libre.fr/category/hacks-hwl/unjailpi/

Project page on HackaDay

http://hackaday.io/project/2040

HackaDay coverage article

http://hackaday.com/2014/09/06/secure-your-internets-with-web-security-everywhere/

Contact email

unjailpi@arcadia-labs.com