Mobile Privacy: Tor On The iPhone And Other Unusual Devices

Marco Bonetti - CutAway s.r.l.

CutAway
Only root can do that

whoami

- Marco Bonetti
- Security Consultant @ CutAway s.r.l.
  - mbonetti@cutaway.it
  - http://www.cutaway.it/
- Tor user & researcher @ SLP-IT
  - http://sid77.slackware.it/
  - http://twitter.com/_sid77/
  - http://sid77.soup.io/

Outline

- Mobile Phones (In)Security
- Tor On Mobile Phones And Other Strange Devices
- Tor On The Chumby One
- Tor On Maemo And The Nokia N900
- Orbot: Tor On Android
- Mobile Tor: Tor for iDevices

Mobile Phones (In)Security

Mobile Phones Growth

- Computational power
- High speed data networks
- “Real” operating system

Phones Are Personal

- Raise hand who does not own a mobile phone
- We take them everywhere we go
- Never leave the house without it ;-)

Phones Are Critical

- Call logs
- Address book
- E-mail
- SMS
- GPS data
- Documents
- Calendar events
- Calendar tasks
- Browser history
- Browser cache

Too Much Trust

- Users trust their phone
- Phones trust the operator
- Operators trust themselves
- Users trust operators as well

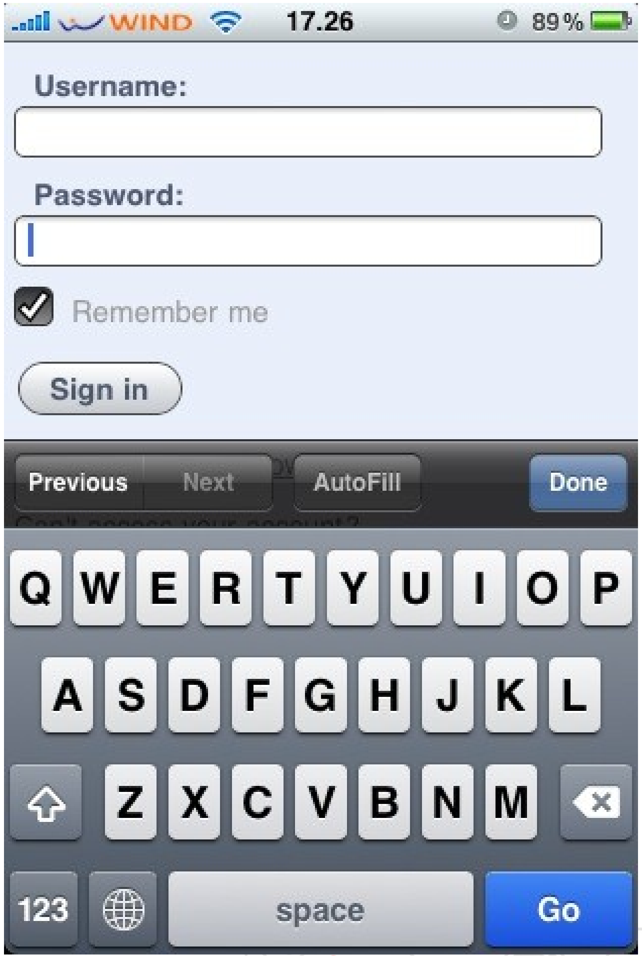
Too Much Trust

Too Much Heterogeneity

- Closed communication protocols
- Heterogeneous networks
- Fragmented hardware landscape
- Many different operating systems

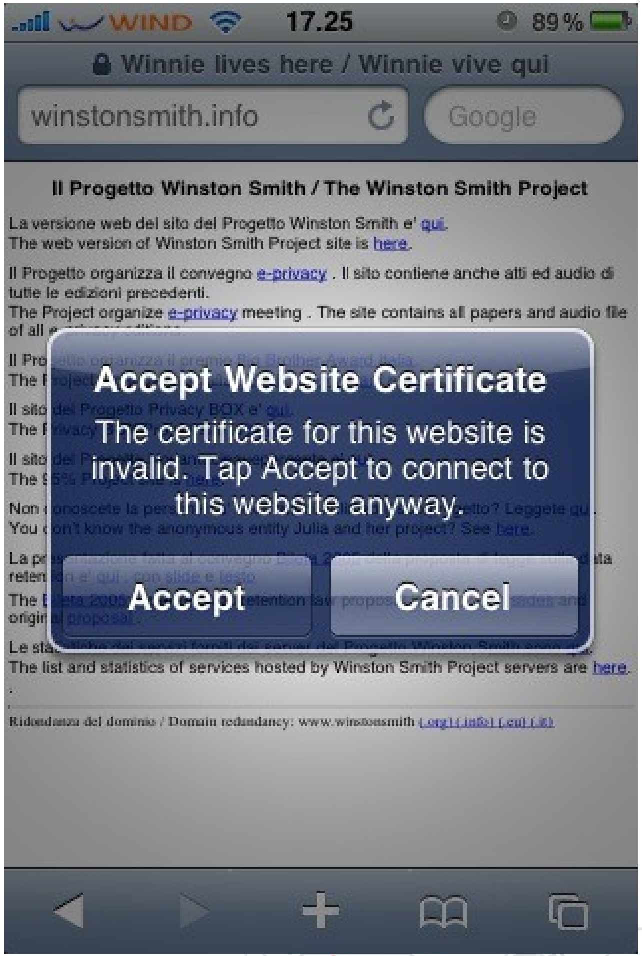
Architectural Issues

- Made for chatting and texting
- Keyboards adopted to the model
- Difficult passwords are... difficult!



Architectural Issues

- Phones are mobile devices
- Screen size is limited
- Checking important stuff is nearly impossible!



Il Progetto Winston Smith / The Winston Smith Project

La versione web del sito del Progetto Winston Smith e' qui.
The web version of Winston Smith Project site is here.

Il Progetto organizza il convegno e-privacy . Il sito contiene anche atti ed audio di tutte le edizioni precedenti.
The Project organize e-privacy meeting . The site contains all papers and audio file of all

You don't know the anonymous entity Julia and her project? See here.

The list and statistics of services hosted by Winston Smith Project servers are here.

Ridondanza del dominio / Domain redundancy: www.winstonsmith (.org) (.info) (.eu) (.it)

Accept Website Certificate

The certificate for this website is invalid. Tap Accept to connect to this website anyway.

Who Own The Device?

- Manufacturer / vendor
  - *“Apple iPhone banned for ministers” (CBS, 2010)*
  - *“Exercising Our Remote Application Removal Feature” (android-developers, 2010)*
- Carrier operator
  - *“BlackBerry update bursting with spyware” (The register, 2009)*
- Application developer
  - *“iPhone Privacy” (BlackHat DC, 2010)*
- End user
  - *We're here!*

Data (In)Security

- Data is stored in cleartext
- Blackberry and Nokia allows some sort of encryption
- Data access is an “all or nothing” approach
- Need permissions fine tuning

Communication (In)Security

- GSM has been broken
- UMTS is not feeling very well
- SMS has been abused
- MMS remote exploit for Windows Mobile, iPhone and many more

Communication (In)Security

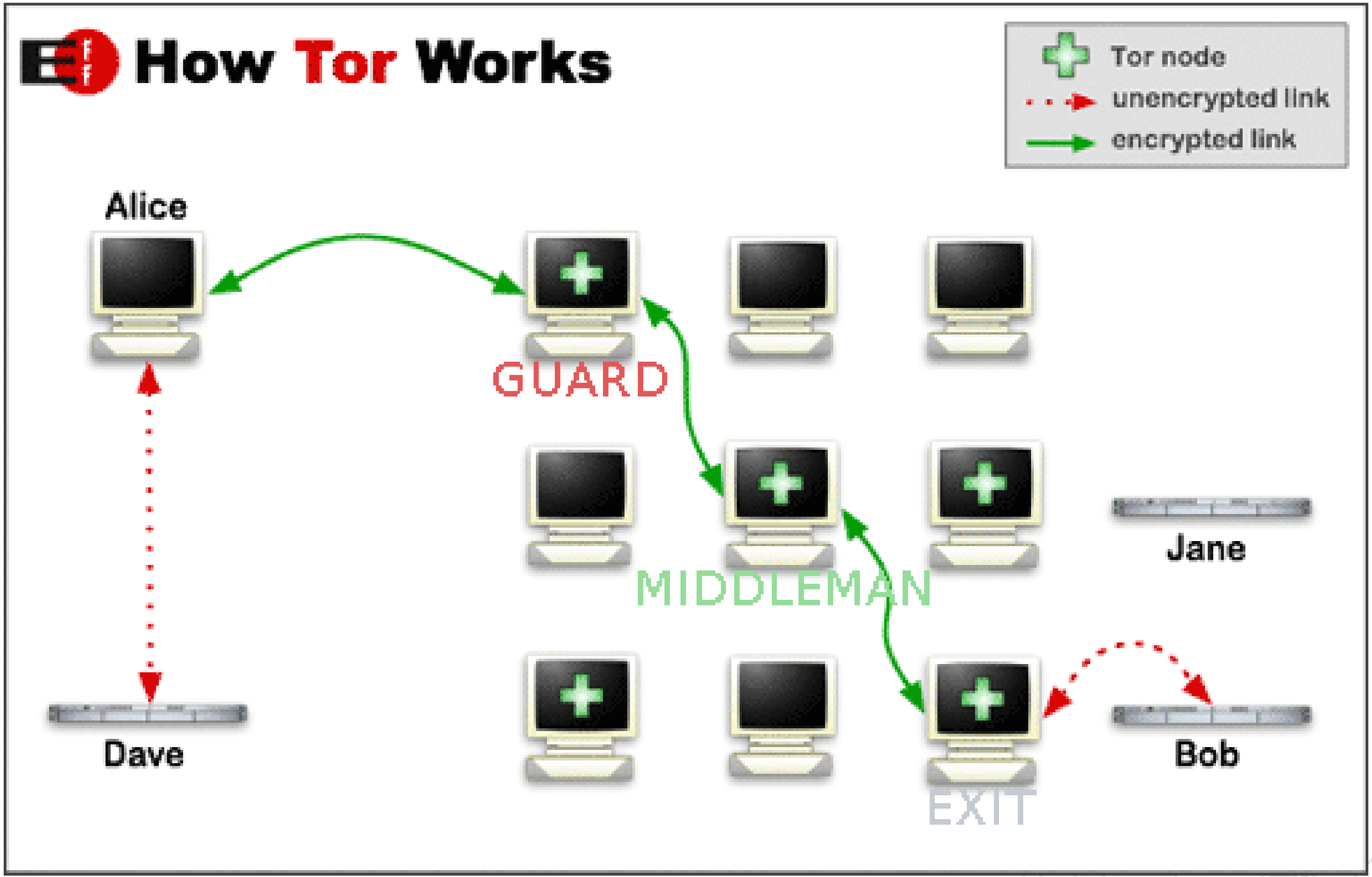
- Bluetooth is dangerous
- WiFi offers a plethora of attacks
- NFC has already been worm-ed
- Operator injected HTTP headers
- SSL/WTSL heavy on lower end phones

To recap

- Mobile phones are everywhere
- Mobile phones are primary designed for making calls and sending text messages
- Stored data can not be easily protected
- Communications need to be secured

Tor On Mobile Phones And Other Strange Devices

Tor Crash Course



Tor On Unusual Devices

- December 2007: iPhone
- December 2009: Chumby One
- February 2010: iPhone, again
- February 2010: Nokia N900
- March 2010: Android

Problems to address

- Available hardware
- Hosting operating system and code rewrite
- Installation process
- Graphical user interface

Tor On The Chumby One

Chumby One

- Hackable Linux device
- ARM CPU
- 64MB of RAM
- Made by bunnie of bunnie:studios and Jacob Appelbaum

Tor
tor.eff.org
Tor bridge relay mod installed, see
http://<chumbyip>/cgi-bin/custom/torlog for stats

Install: the hard way

- Install Chumby cross-toolchain
- Checkout sources
- make
- Unzip build on usb key
- Reboot Chumby with usb key inserted

Install: the easy way

- Unzip build on usb key
- Reboot Chumby with usb key inserted

Running Tor

- Swap file needed
- Configured as a bridge
  - Listening on TCP 443
  - Low consumption of resources
- No upgrade mechanism
- Unofficial support for 3G dongles

Achievements

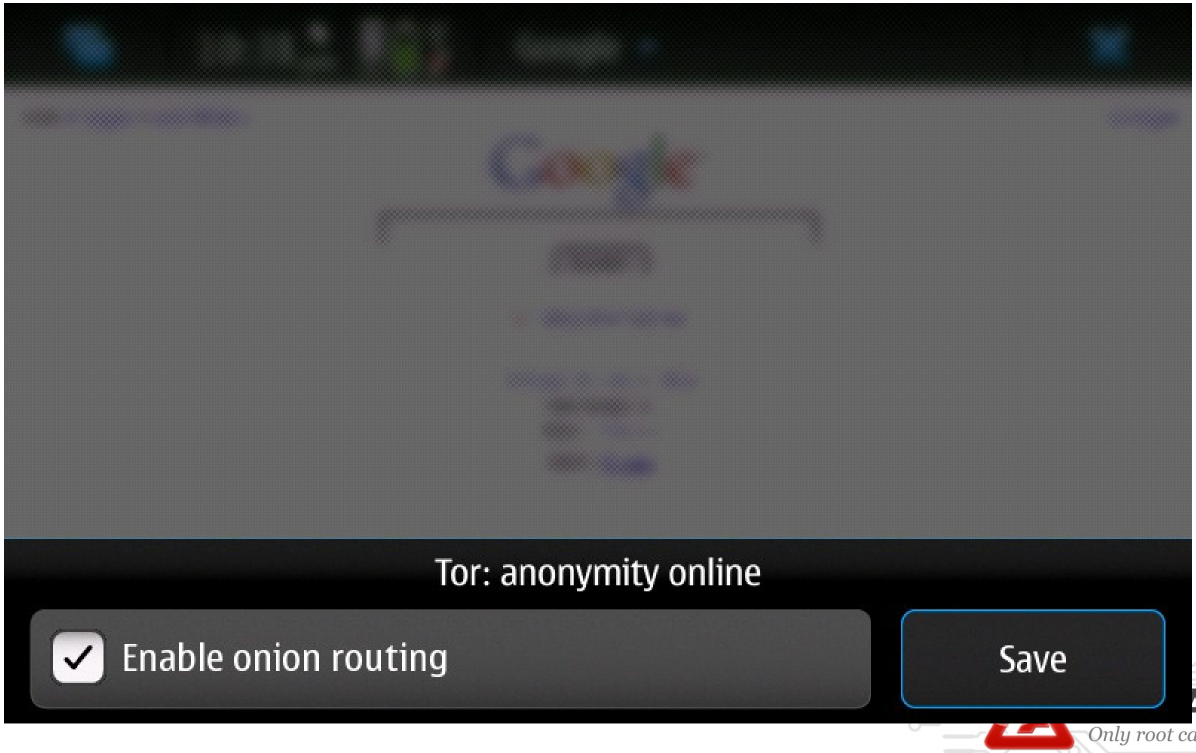
- Running Tor on limited resources
- Easy install method

Tor On Maemo And The Nokia N900

Nokia N900

- Powerful ARM CPU
- 256MB RAM

- Tor in Maemo community



Tor: anonymity online

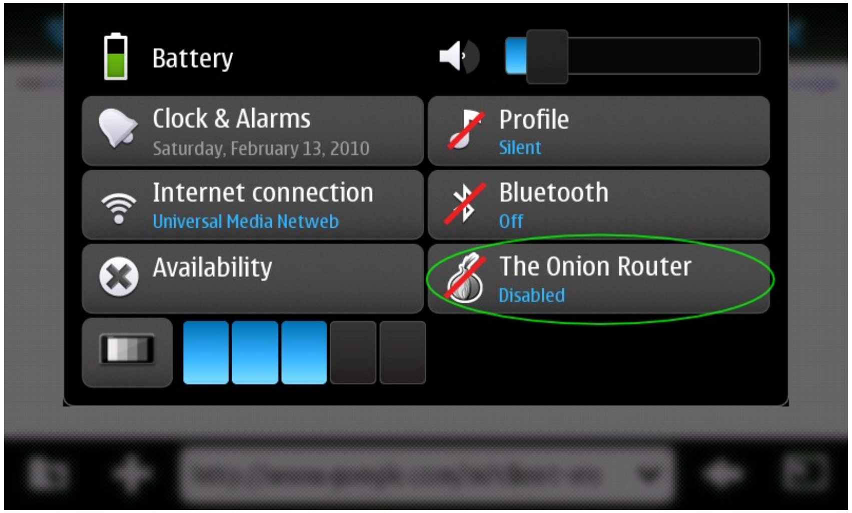
☑ Enable onion routing

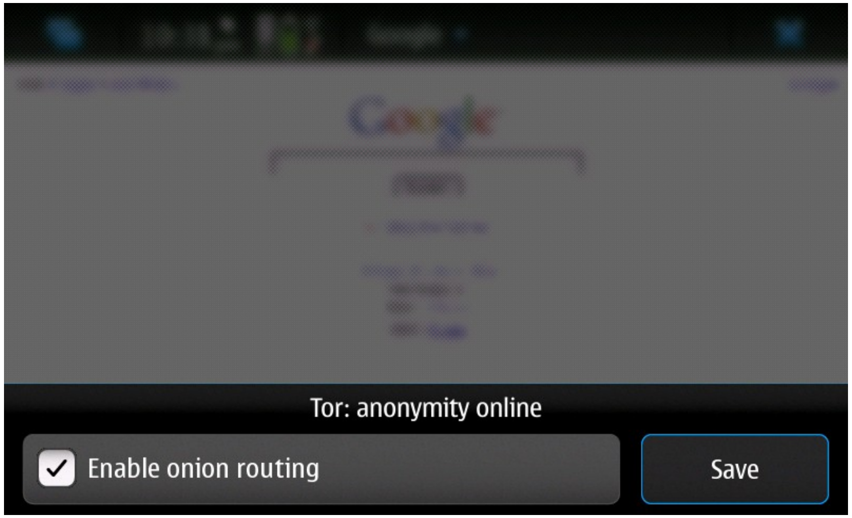
Install

- Enable extras-devel
  - Reported as dangerous!
- Look for Tor in the package manager
- Done!

Running Tor

- Just toggle it!





Tor: anonymity online

☑ Enable onion routing

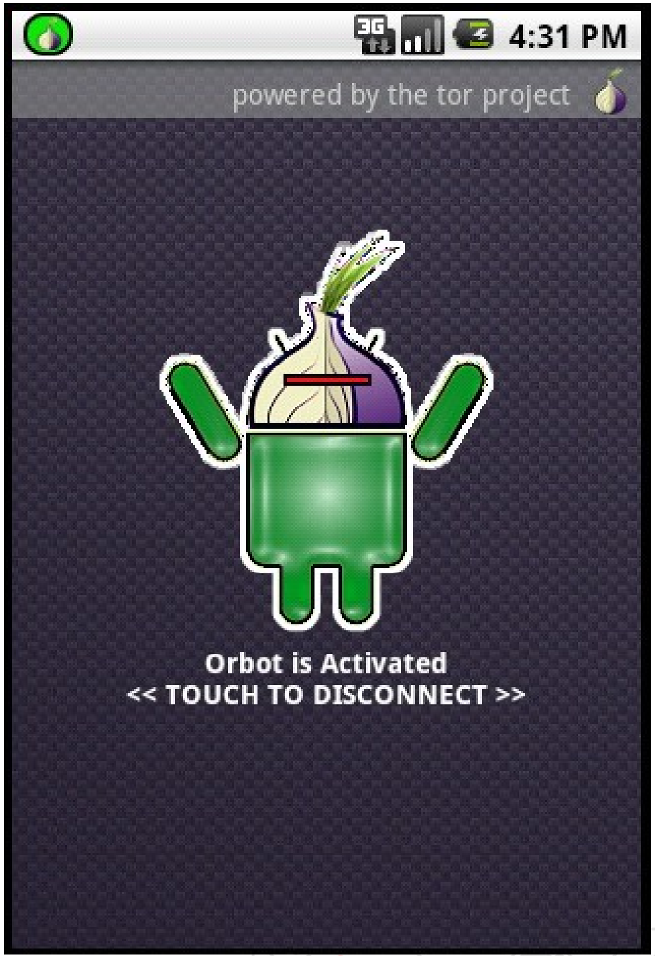
Achievements

- Easy install
- Easy upgrade
- First graphical controller application

Orbot: Tor On Android

Android

- Linux based operating system
- Many different devices
- Orbot built by The Guardian Project



Orbot is Activated
<< TOUCH TO DISCONNECT >>

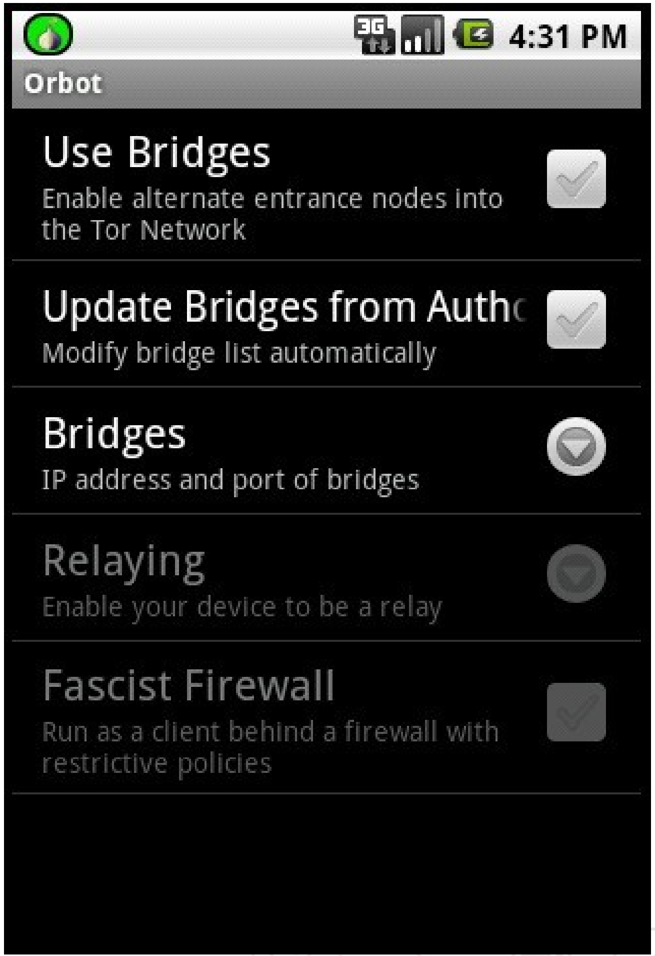
CutAway
Only root can do that

Install

- Scan the QR code!
- Not yet in the Android Market

Running Tor

- Just toggle it!
- Easily configurable
- Runs as transparent proxy for rooted devices



4:31 PM

Orbot

Use Bridges
Enable alternate entrance nodes into the Tor Network ☑

Update Bridges from Autho ☑
Modify bridge list automatically

Bridges
IP address and port of bridges

Relaying
Enable your device to be a relay

Fascist Firewall
Run as a client behind a firewall with restrictive policies ☑

Achievements

- Easy installation
- Highly configurable
- Transparent proxy

Mobile Tor: Tor for iDevices

iDevices

- Hackable Darwin (iOS) devices
- Powerful ARM CPU
- From 128MB to 512MB of RAM

Tor On Unusual Devices

- December 2007: iPhone
- December 2009: Chumby One
- February 2010: iPhone, again
- February 2010: Nokia N900
- March 2010: Android

The Original Port

- Made by *cjacker huang*
- Built for iOS 1.1.1
- Tor sources patched to overcome firmware limitations
- Shipped with a copy of Privoxy
- Shipped with iTor.app controller

The Original Port

- cjacker huang disappeared
- iTor.app disappeared with its author
- Tor patches were still available in the main Tor source tree

Bringing Back Tor On The iPhone

- Open source toolchain
- SDK target: iOS 3.1.2
- Cross-compiling from Slackware 13.1

Bringing Back Tor On The iPhone

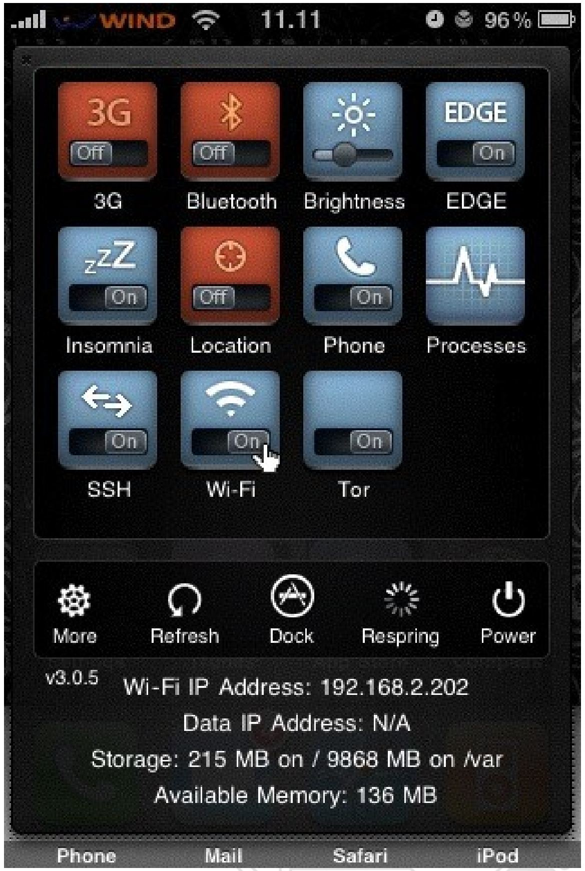
- Built following Jay Freeman's conventions for Cydia packages
- Sources are an overlay for Telesphoreo Tangelo
- http://sid77.slackware.it/iphone/

The New Port

- Made by me :-P
- Built for iOS 3.1.2+
- Old patches no longer needed
- Shipped with a copy of Polipo
- Shipped with an SBSettings plugin

Running Tor

- Add my repository
- Install *Tor Toggle*
- Just toggle it!



Wi-Fi IP Address: 192.168.2.202

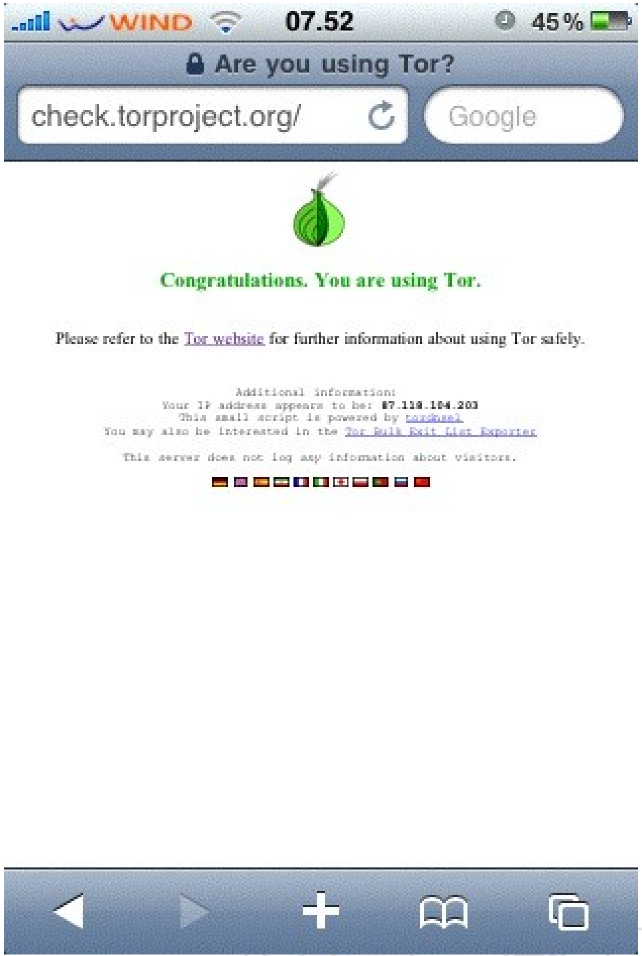
Data IP Address: N/A

Storage: 215 MB on / 9868 MB on /var

Available Memory: 136 MB

Running Tor

- Client
- Relay
- Hidden Services
- Both via wireless and cellular data network
- iOS should do transparent proxy



Congratulations. You are using Tor.

Please refer to the Tor website for further information about using Tor safely.

Additional information:
Your IP address appears to be: 87.118.104.203
This small script is powered by torcheel
You may also be interested in the Tor Bulk Exit List Exporter

This server does not log any information about visitors.

iOS Limitations

- No support for SOCKS proxies
  - Run Polipo!
- No HTTP proxies for cellular data networks
  - VPN trick!
- No Tor-secure browser

Tor Limitations

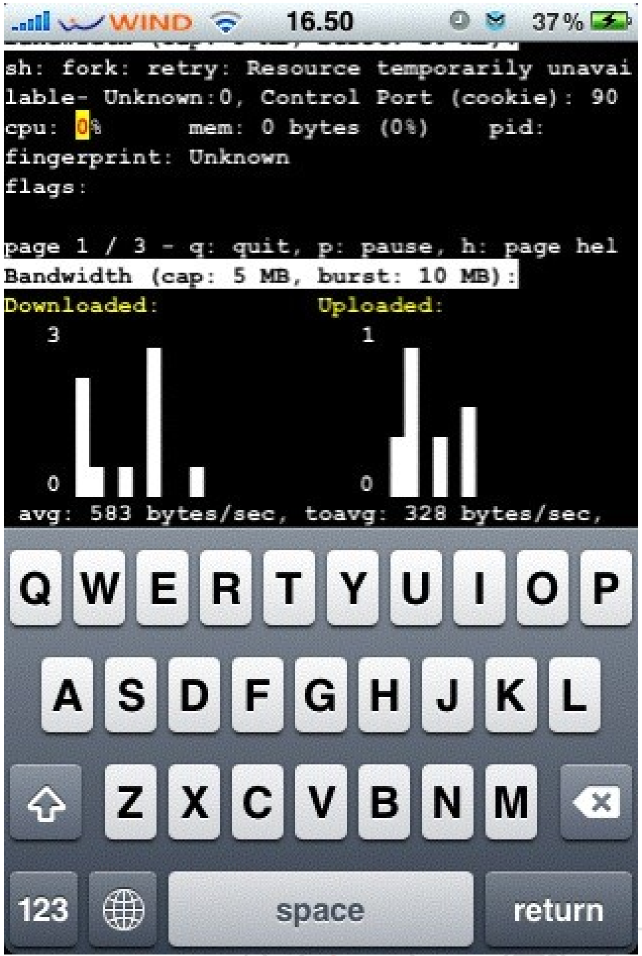
- Cryptographically intense
  - Heavy on battery drain
- Cellular data networks aren't very Tor friendly
  - Rapidly changing IP addresses
  - Spot coverage

Development

- Still too much fiddling with CLI
- Need for a graphical controller, Vidalia style
- Need for a secure browser

Some Crazy Ideas

- Arm is working... somehow
- OnionCat looks promising
- Some work on ttdnsd
- Anything else?



```
sh: fork: retry: Resource temporarily unavai
lable- Unknown:0, Control Port (cookie): 90
cpu: 0%         mem: 0 bytes (0%)      pid:
fingerprint: Unknown
flags:

page 1 / 3 - q: quit, p: pause, h: page hel
Bandwidth (cap: 5 MB, burst: 10 MB):
Downloaded:              Uploaded:
   3                        1



   0                        0
 avg: 583 bytes/sec, toavg: 328 bytes/sec,
```

Questions?

-

http://sid77.slackware.it/
http://twitter.com/_sid77/
http://sid77.soup.io/