Surviving Your Phone: Protecting Mobile Communications With Tor

Marco Bonetti - CutAway s.r.l.

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://www.slackware.it/
  - http://twitter.com/_sid77/

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 On The iPhone

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

Phones Are Critical

- 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 Heterogeneity

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

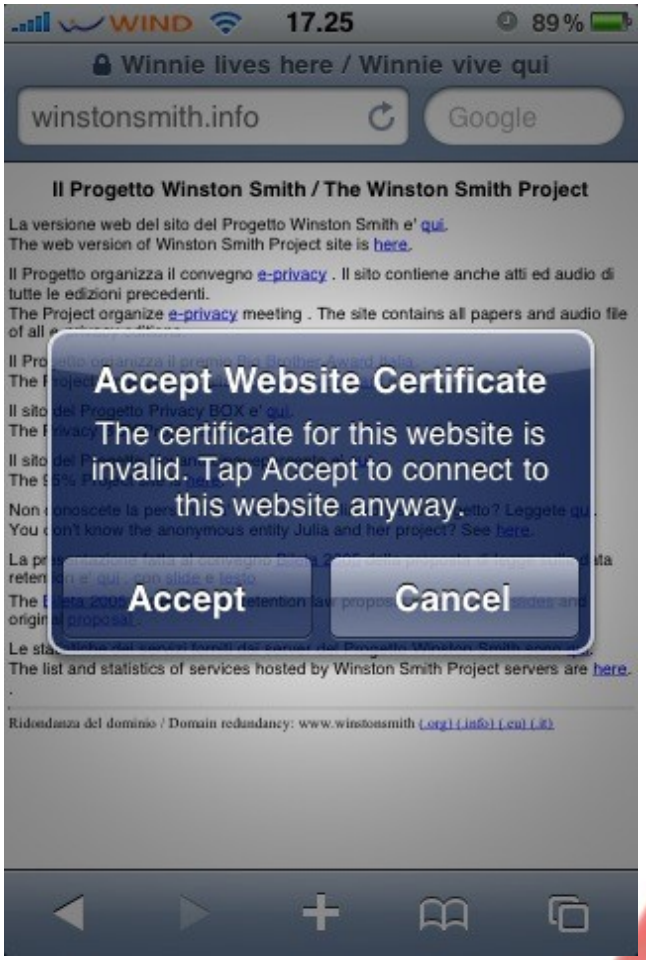
Architectural Issues

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

CutAway

Architectural Issues

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

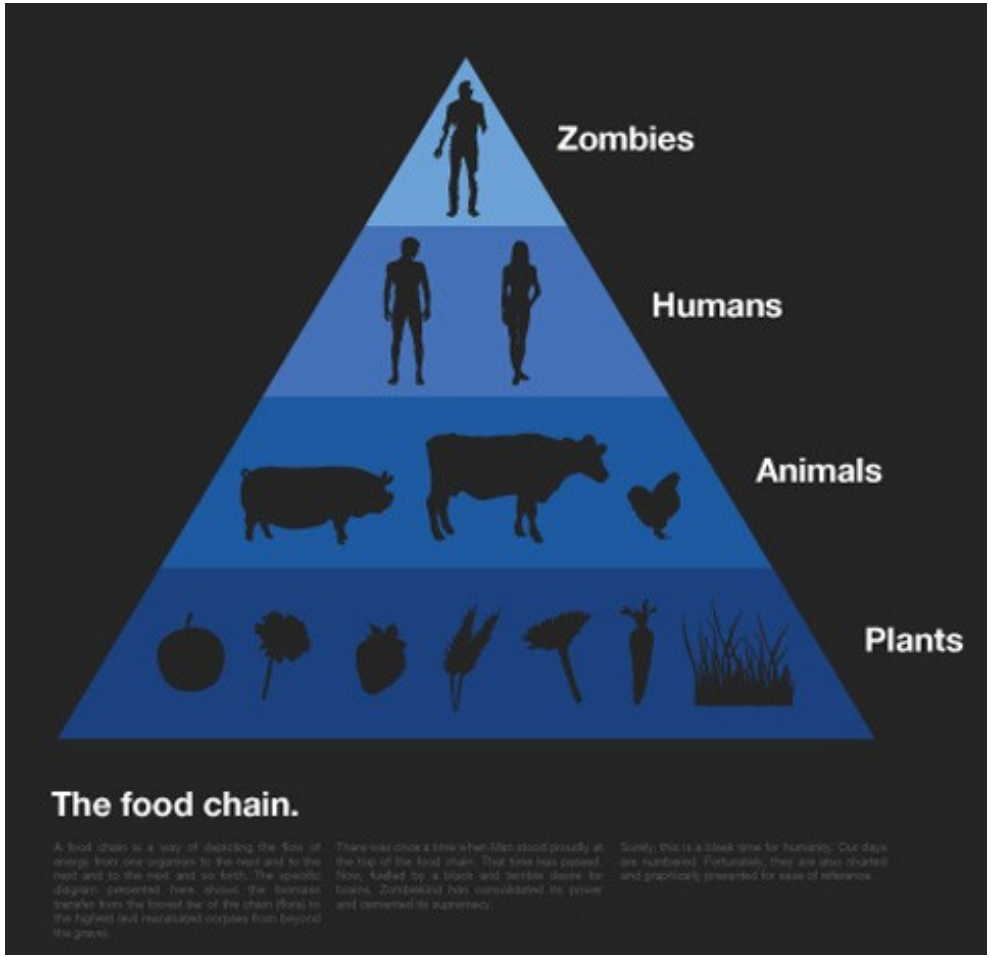


CutAway

Who Own The Device?

- Manufacturer / vendor
  - *“Blackberry ban for French elite” (BBC, 2007)*
- Carrier operator
  - *“BlackBerry update bursting with spyware” (The register, 2009)*
- Application developer
  - *“iPhone Privacy” (BlackHat DC, 2010)*
- End user
  - *We're here!*

Who Own The Device?



Data (In)Security

- Data is stored in cleartext
- Blackberry 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 been already worm-ed
- Operator injected HTTP headers
- SSL/WTSL heavy on lower end phones

Tor On Mobile Phones And Other Strange Devices

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

CutAway

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

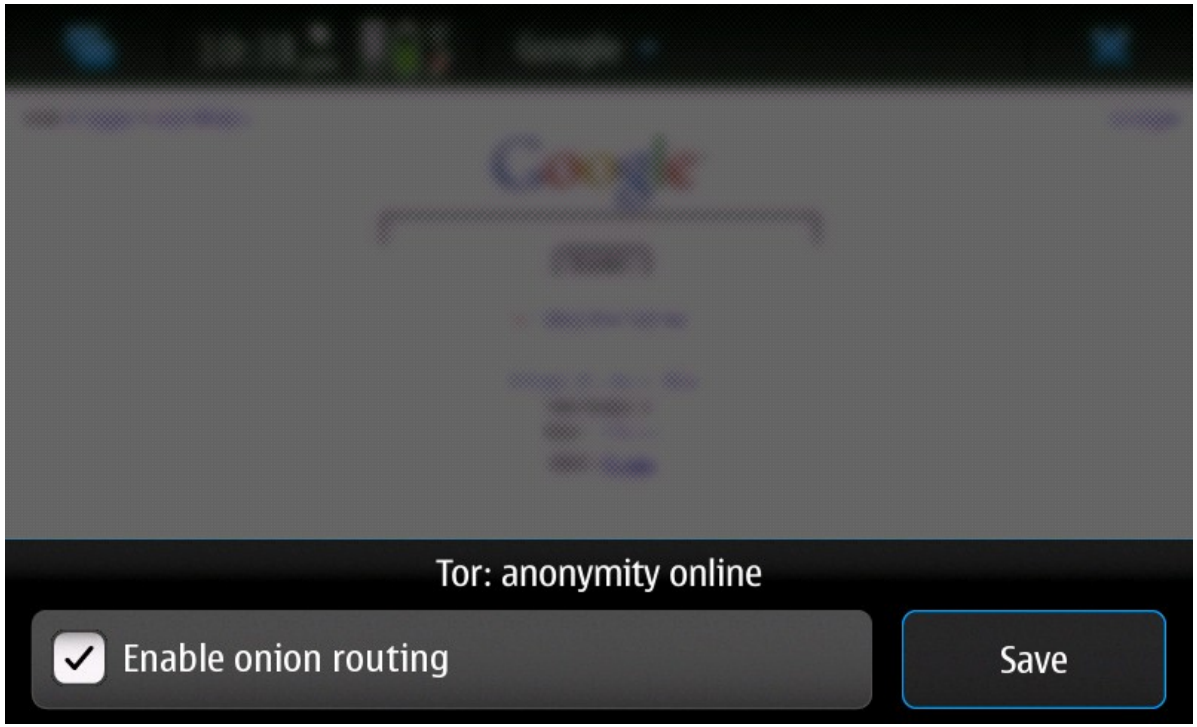
Achievements

- 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



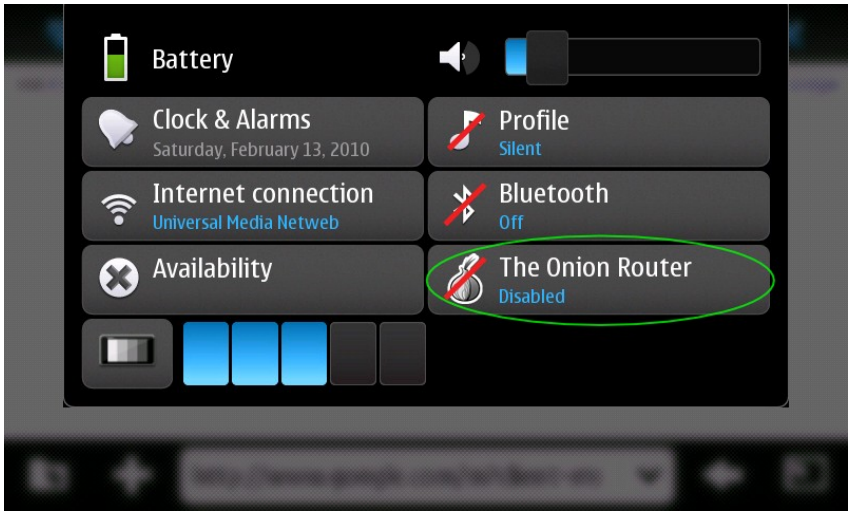
CutAway

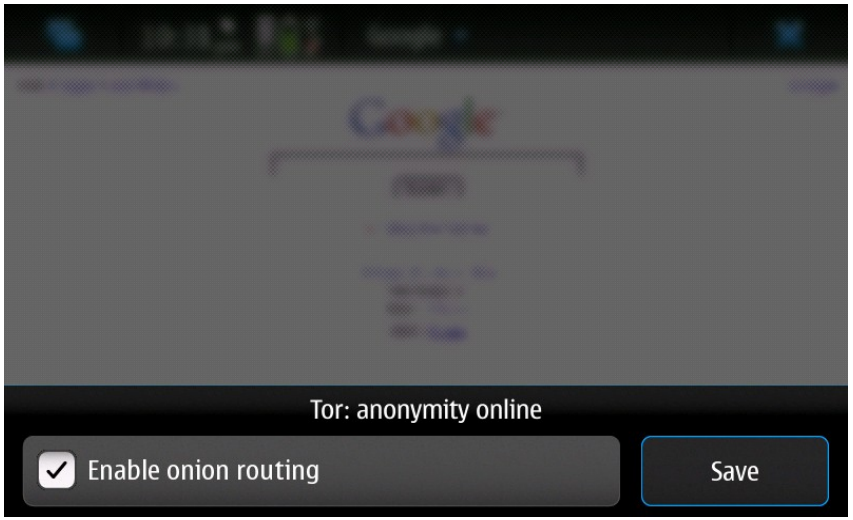
Install

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

Running Tor

- Just toggle it!





CutAway

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

CutAway

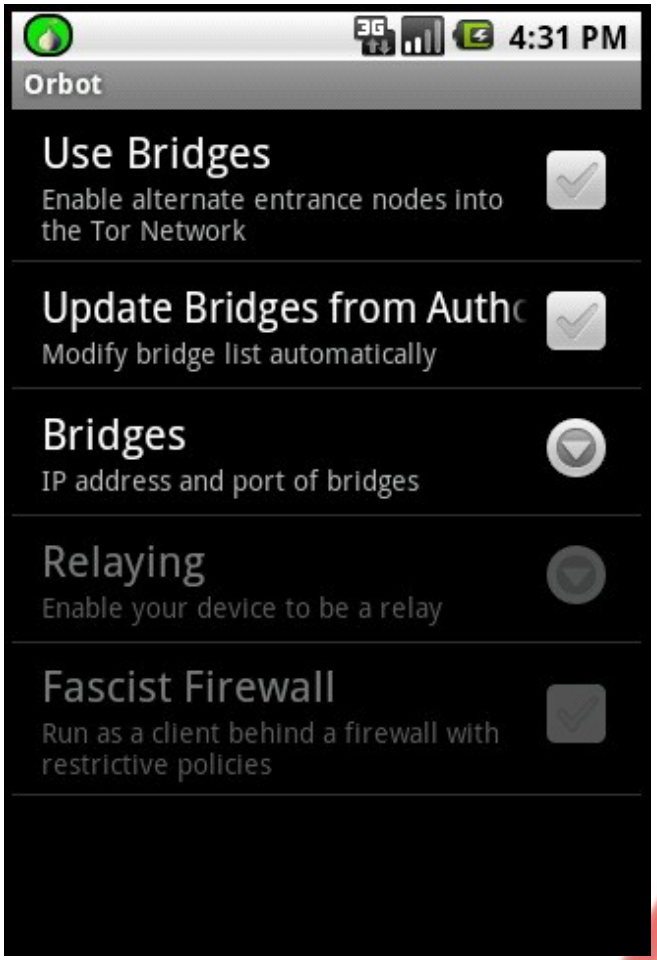
Install

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

CutAway

Running Tor

- Just toggle it!
- Easily configurable
- Transparent proxying for rooted devices



CutAway

Achievements

- Easy installation
- Highly configurable
- Transparent proxying

Mobile Tor: Tor On The iPhone

iPhone / iPod Touch

- Hackable Darwin (iPhone OS) devices
- Powerful ARM CPU
- 256MB RAM

CutAway

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 iPhone OS 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: iPhone OS 3.1.2
- Cross-compiling from Slackware64 13.0

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 iPhone OS 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*
- Copy or modify configuration samples
- Just toggle it!

CutAway

Running Tor

- Client
- Relay
- Hidden Services
- Both via wireless and cellular data network

CutAway

•iPhone OS Limitations

- No support for SOCKS proxies
  - Run Polipo! :)
- No HTTP proxies for cellular data networks
  - VPN trick! :)
- No transparent proxying
  - Missing KEXTs :(

Tor Limitations

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

CutAway

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
- TunEmu could be worth a look
- Do you have a spare iPad?

CutAway

Questions?

CutAway

Released under Creative Commons
Attribution Share-Alike 3.0 Unported
http://creativecommons.org/licenses/by-sa/3.0/
-
http://www.cutway.it/
http://sid77.slackware.it/