



An Analysis of Private Browsing Modes in Modern Browsers

Gaurav Aggarwal, Elie Bursztein, Collin Jackson,
Dan Boneh



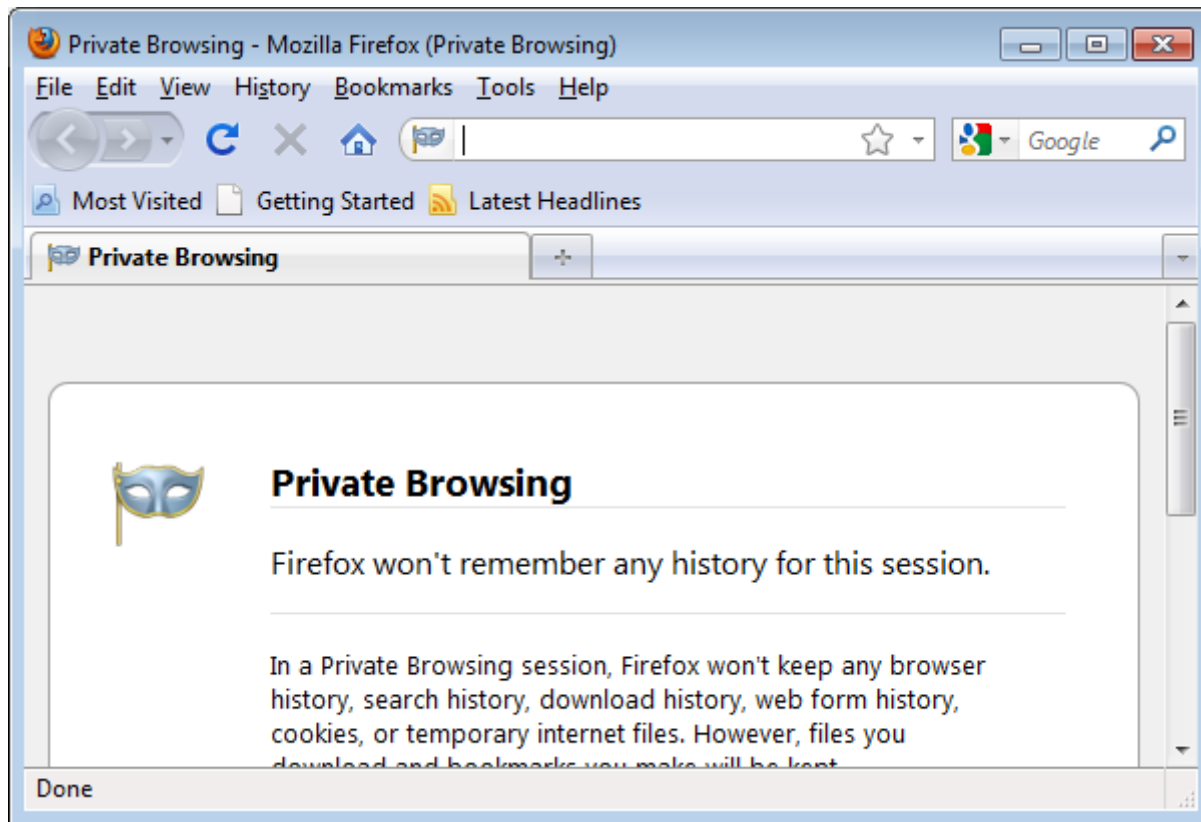
Private Browsing ?

Browse **without** leaving trace
of visited URLs

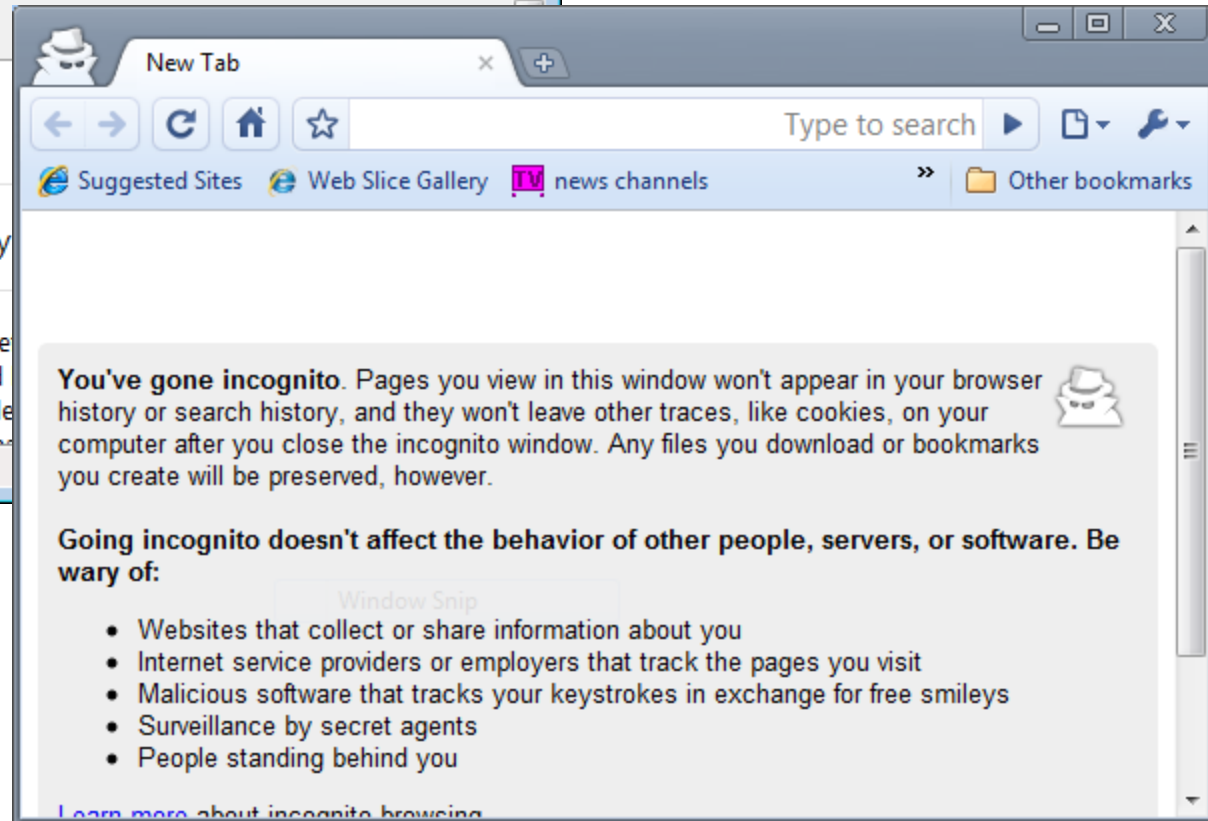
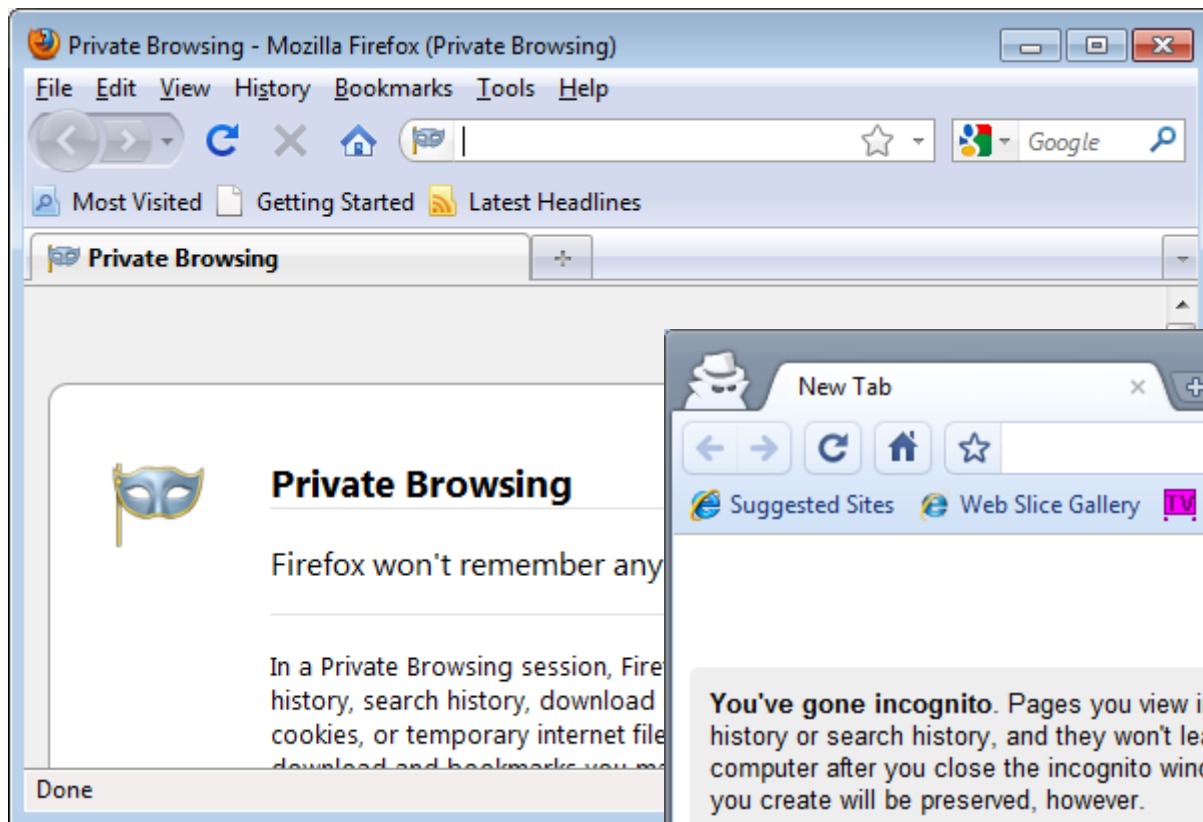
Now in all major browsers



Private browsing UI



Private browsing UI



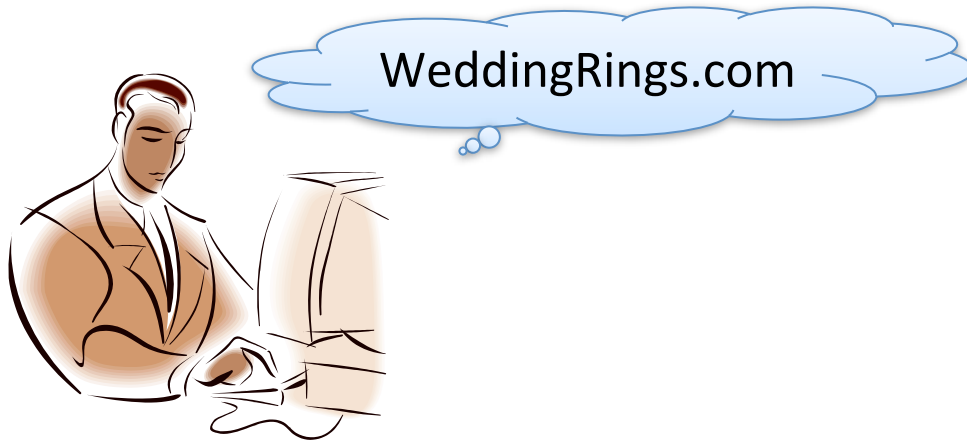
Threat Model

Home Computer or Internet Kiosk



Threat Model

Home Computer or Internet Kiosk



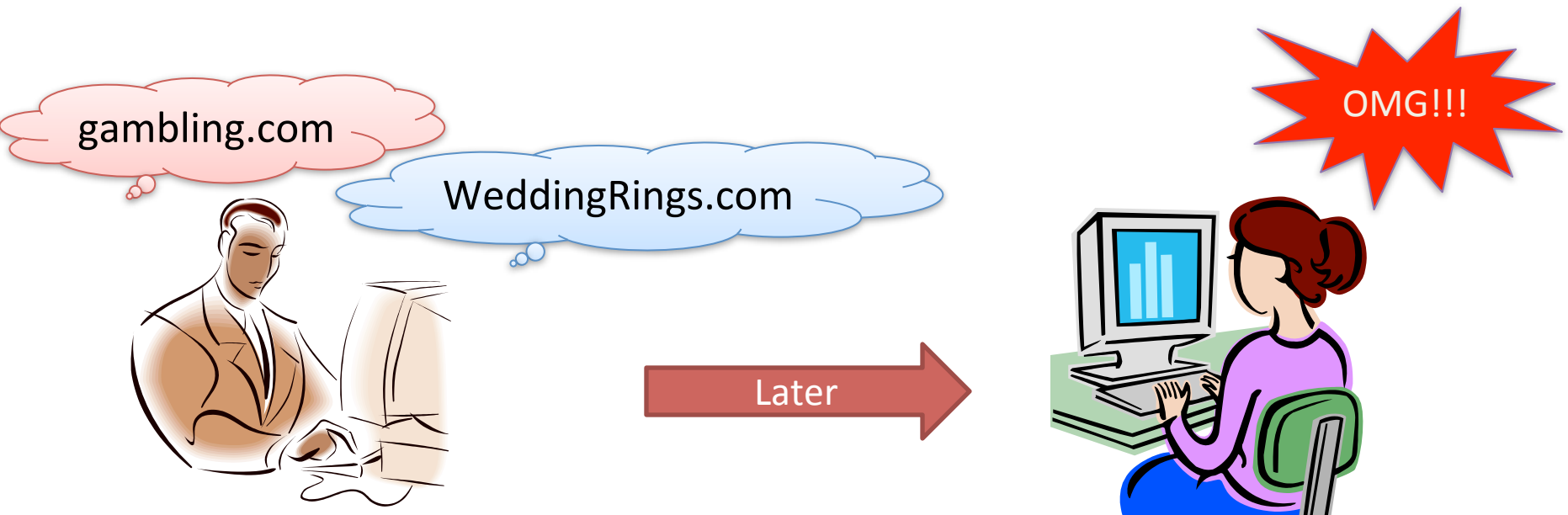
Threat Model

Home Computer or Internet Kiosk



Threat Model

Home Computer or Internet Kiosk



Marketed for surprise gifts ...

People Really care about this !

The image shows a Google search for "browser privacy mode" and a Google News page. The search results page on the left shows about 728,000 results in 0.26 seconds, with a filter for "Past 3 days". The Google News page on the right displays several articles related to private browsing, including "Private browsing is not as secure as users think, says study", "Private browsing tools still leave data trail", and "Web Browser Privacy Settings Flawed - Browser Security".

Google search results for "browser privacy mode":

- About 728,000 results (0.26 seconds)
- Past 3 days
- News for browser privacy mode**
- [Don't Trust Private Browsing Modes for True Privacy](#) - Lifehacker - 89 related articles »
- [Reviewing the "Privacy Mode" Browser Debate | thech](#) - 1 day ago - We've got to step back and look at this from a different angle. All a good reminder that while there are ways to browse the internet, we're leaking data about ourselves all over the place. [www.thechsource.com/reviewing-the-privacy-mode-browser-debate](#)
- [Google Chrome - Wikipedia, the free encyclopedia](#) - 2 days ago - Incognito mode is similar to the private browsing feature. The Under the Hood tab allows changing network, privacy, download settings. [en.wikipedia.org/wiki/Google_Chrome](#) - Similar
- [Private browsing: it's not so private](#) - 2 days ago - Internet Explorer and Chrome both disable browser extensions in private mode; Firefox, however, does not, and this provides yet another security hole. [arstechnica.com/security/news/.../private-browsing-not-so-private-and-why-not](#)
- [Web Browser Privacy Settings Flawed - Browser Security](#) - 1 day ago - Do you believe that your browser's privacy settings hide your browsing history? In short, "privacy" mode can be anything but, at least against a determined attacker. [www.informationweek.com/news/security/.../showArticle.jhtml?...&cid=27828](#)
- [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, you shouldn't count on your browser's privacy mode to do much more than make you feel safe. [lifehacker.com/.../dont-trust-private-browsing-modes-for-true-privacy](#)
- [Web Browser Privacy Settings Flawed - Techzonez](#) - 1 post - 1 author - Last post: yesterday - Do you believe that your browser's privacy settings hide your browsing history? Ever study of the privacy mode in browsers found multiple flaws. [www.techzonez.com/forums/showthread.php?t=27828](#) - Cached
- [Your browser's 'private mode' may still leave tracks | The Verge](#) - 2 days ago - All modern browsers now offer some feature that allows you to browse "privately", in which no trace of your activities are left on the local hard drive. [blogs.chron.com/.../your_browsers_private_mode_may_still_leave_tracks](#) - Cached

Google News page:

- Full coverage**
- Top Stories**
- More sections**
- Search this story** (private brow) (Go)
- All news**
- Articles**
- Images**
- Blog**
- Sorted by relevance**
- Sorted by date**
- Reset options**
- [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 Espiner - Aug 9, 2010 - The private browsing features in Internet Explorer, Firefox, Chrome and Safari are not as protective as they ...
- [Private browsing mode leaves data trail, says research](#) - FierceCIO - Paul Mah - 22 hours ago - New research at Stanford University's Computer Science Security Lab has revealed that the private browsing modes of the major web browsers are not as ...
- [Web add-ons 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 ...
- [Private web browser modes not as anonymous as you might think](#) - Infosecurity Magazine - Aug 9, 2010 - The paper observes that "current private browsing implementations provide privacy against some local and Web attackers, but can be defeated by determined ...
- ['Porn mode' not necessarily anonymous](#) - CNET (blog) - Seth Rosenblatt - Aug 7, 2010 - The private browsing options provided by the four major Web browser publishers aren't as anonymous and secure as most users might think, ...
- [Private browsing: it's not so private](#) - Ars Technica - Peter Bright - Aug 8, 2010 - Research by Stanford University to investigate the privacy of the "private browsing" feature of many ...
- [Private browsing modes leak data](#) - BBC News - Mark Ward - Aug 6, 2010 - Many extras 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 Neal - 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:
``

Web Attacker: an IE example

- The attack works as follows:
 1. Embedded an smb link on attacker's page:
``
 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:
``
 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:
``
 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

```
linux:~# ruby ./smb.rb
Windows SMB Deanonymizer
(c) 2010 Elie Bursztein web@elie.im
Based on Hernan Ochoa (hernan@gmail.com) poc for smb weak challenge
waiting for connections from victim
1
neg proto request received
neg proto response sent
session setup and request received!
session setup and access denied sent!
session setup andx request with creds received!
ansi 0000000000000000000000000000000000000000000000000000000000000000
NTLM v2 auth
unicode 195ccaab0ede1dcd2f61ec1a82ddb64c010100000000000000000000000000
cd7fe447439cb01d4436d39988bfaa90000000002000000000000000000000000000
user: Elie
domain: Jade
os:
```

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”

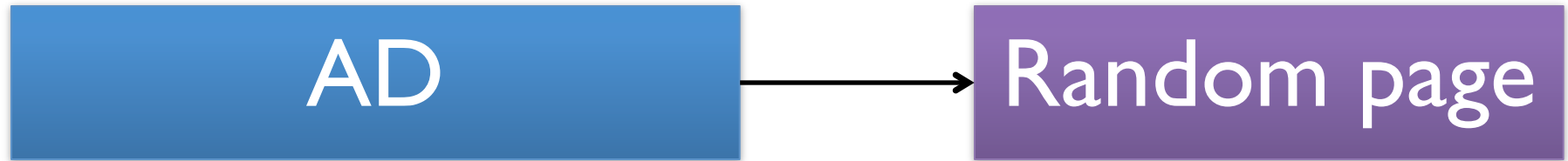
Behavior in Regular Mode

AD



Random page

Behavior in Regular Mode



Random page



Random page

```
If ( getComputedStyle(link).color == RGB(51,102,160) )
```

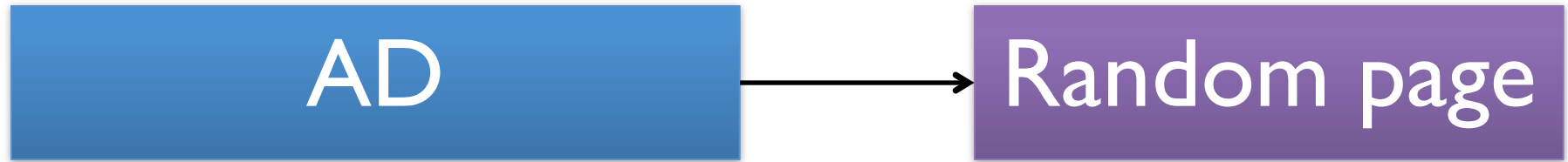
Behavior in Private Mode

AD



Random page

Behavior in Private Mode

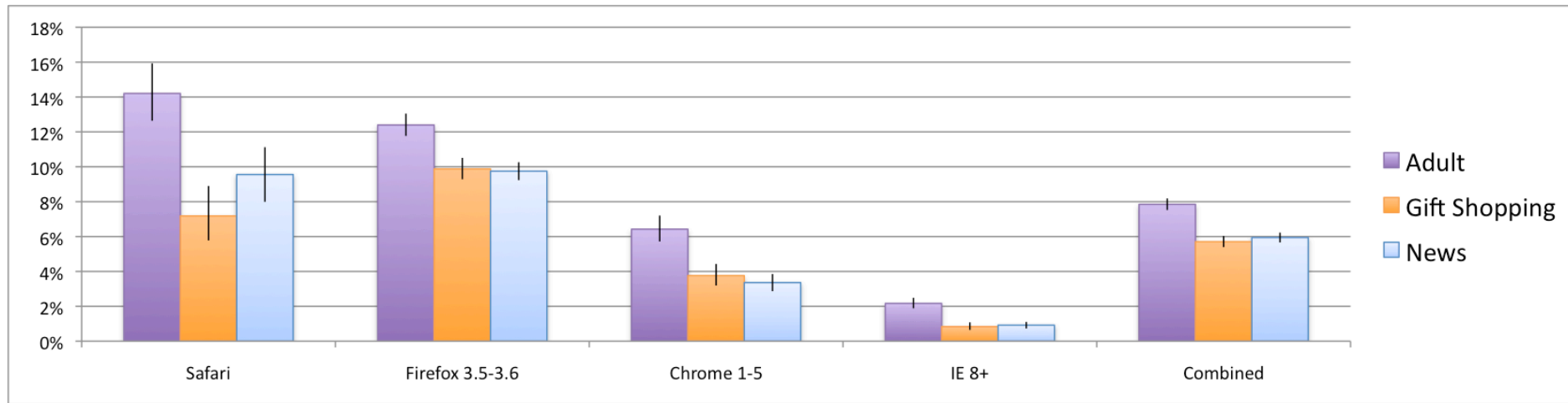


Random page



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



Safari in private

The screenshot shows a Safari browser window with the address bar displaying `http://seclab.stanford.edu/`. The browser's interface includes a search bar with the text "PRIVATE" and a Google search button. The website content is for the Stanford Security Laboratory, featuring a red header with the text "Stanford Security Laboratory" and "Added in Safari 5". The main content area is divided into sections: Overview, Courses, and Seminars. The Overview section describes the lab as part of the Computer Science Department at Stanford University. The Courses section lists several courses with links: CS142, CS155, CS255, CS259, CS355, CS99J, and CS55N. The Seminars section describes the Stanford Security Seminar and the Security Lunch. On the right side, there is a sidebar with a Stanford University logo and lists of Faculty, Ph.D. Students, and Post-docs. An orange arrow points from the "Added in Safari 5" text to the "PRIVATE" button in the browser's search bar.

Stanford Security Laboratory

Added in Safari 5

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 with between students in the security lab and stuents in related research groups. Typically a student gives a technical presentation about

Faculty

- [Alex Aiken](#)
- [Dan Boneh](#)
- [David Dill](#)
- [Dawson Engler](#)
- [Hector Garcia-Molina](#)
- [Monica Lam](#)
- [David Mazieres](#)
- [Nick McKeown](#)
- [John Mitchell](#)
- [Mendel Rosenblum](#)

Ph.D. Students

- [Andrew Bortz](#)
- [Hristo Bujinov](#)
- [Tal Garfinkel](#)
- [Mike Hamburg](#)
- [Peifung Eric Lam](#)
- [Hart Montgomery](#)
- [Arnab Roy](#)
- [Stephan Hyeonjun Stiller](#)
- [Mukund Sundararajan](#)
- [Ankur Taly](#)

Post-docs

- [Elie Bursztein](#)
- [David Freeman](#)
- [Arvind Narayanan](#)

... 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

Firefox: a detailed analysis

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

Firefox: a detailed analysis

Method 2: automated testing

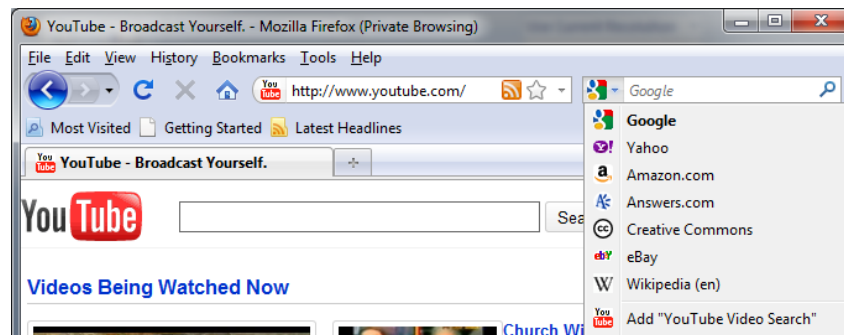
- Leverage existing browser unit tests
- MozMill test framework
 - User interface test automation tool
 - 196 tests currently
 - ... and we added a few additional tests

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)

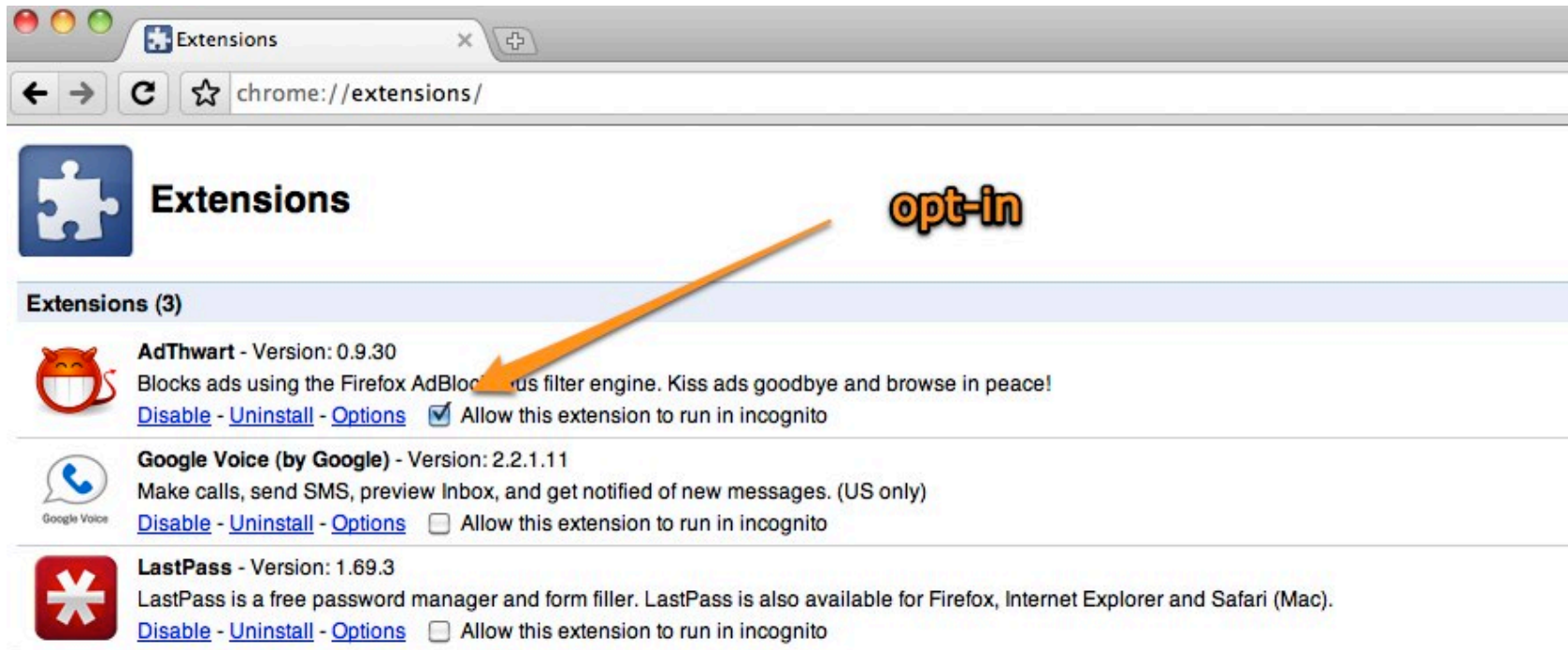
Firefox:

- Extensions and plug-ins work normally

Safari:

- No supported extension API

Chrome Extensions



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](#)