The Privacy of Private Browsing

Ashley Hedberg*
ashley.hedberg@tufts.edu

Abstract

Most modern web browsers have a "private browsing" mode that supposedly allows a user to surf the internet without leaving any traces of his or her activity on his or her machine. However, the notion of "private browsing" offers users a false sense of security, as browsing information is often left behind when a private browsing session terminates. Several researchers have already demonstrated methods of detecting this information. These include the analysis of virtual and browser memory and the pagefile on Windows machines. The existence of private browsing artifacts on a users machine raises many questions: how much privacy do web browser developers actually aim to provide with "private browsing" modes? Are these goals accurately conveyed to the end user? And, if the users browsing session can be reconstructed from these artifacts, how might this be exploited by digital forensics professionals? This paper seeks to answer these questions and to prove that such artifacts can be used to determine, at least in part, what a user was doing during his or her "private browsing" session—thereby rendering it not very private at all.

1 Introduction

1.1 Browser Overview

Currently, the most popular browsers for the Windows and Linux families of operating systems are Mozilla Firefox, Google Chrome, and Microsoft Internet Explorer. (Internet Explorer runs only on the Windows family of operating systems, whereas Firefox and Chrome run on both Windows and Linux.) All three of these browsers have built-in private browsing modes. The features and protections provided by each of these private browsing modes are summarized below.[1][2][3]

Mentor: Ming Chow, Tufts University

	Firefox Private Browsing	Chrome Incognito Mode	Internet Explorer InPrivate Browsng
Browser history	X	X	X
Form data	X		X
Search bar data	X		X
Passwords	X		X
Downloads	X	X	
Cookies	X	X	X
Cached files	X		X
Simulataneous sessions with different privacy settings	X	X	X

The private browsing modes of Firefox, Chrome, and Internet Explorer are designed with the intent of preventing users of the same computer from determining what someone was doing on that computer. They do not attempt to keep a user's internet activities hidden from that user's internet service provider (ISP), and they do not prevent websites from identifying that user.[1][2][3]

Users seeking this kind of anonymity should use the Tor browser, which employs onion routing to connect a user to a destination server. In this type of routing, a random path from the user to the destination is constructed, and content is encrypted at each point in the path. Furthermore, each point (known as a relay or node) only knows from which relay any given piece of network traffic immediately came and the next relay to which it is going. It does not know the original source of the network traffic or its final destination. This is what allows users to keep themselves and their activities anonymous using Tor in a way that the traditional web browsers cannot.[4]

The specifics of the Tor network and how it can be used (and abused) will not be considered here. It is mentioned because the Tor browser, like the more common web browsers, can leave artifacts of web browsing sessions on an individual's computer.

1.2 Known Issues with Private Browsing

Prior research in this area indicates that web browsers, even when used in their respective private browsing modes, can leave artifacts on a user's machine that can reveal their internet

activities.

2 To the Community

3 Applications

4 Conclusion

References

[1] Verdi, Michael et al. "Private Browsing." *Mozilla Support*. Mozilla Foundation, 29 Mar. 2013. Web. 10 Dec. 2013. <http://support.mozilla.org/en-US/kb/private-browsing-browse-web-without-saving-info>.

[2] "Chrome Browser." *Chrome*. Google, 18 Nov. 2013. Web. 10 Dec. 2013. <http://www.google.com/intl/en/chrome/browser/features.html#privacy>.

[3] "InPrivate Browsing." *Microsoft Windows*. Microsoft, 10 Dec. 2013. Web. 10 Dec. 2013. <http://windows.microsoft.com/en-us/internet-explorer/products/ie-9/features/in-private>.

[4] "Tor Project: Overview." *Tor*. Tor, 7 Dec. 2013. Web. 10 Dec. 2013. <http://www.torproject.org/about/overview.html.en>.