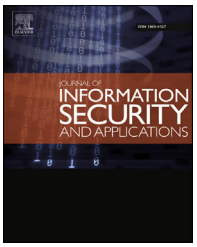
JOURNAL OF INFORMATION SECURITY AND APPLICATIONS XXX (2014) 1–13

Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/jisa



On the privacy of private browsing – A forensic approach

Kiavash Satvat, Matthew Forshaw, Feng Hao*, Ehsan Toreini*

School of Computing Science, Newcastle University, Newcastle upon Tyne, UK

Keywords:
Private browsing
Web security
User privacy
System security

1. Introduction

In 2005, Safari first introduced private browsing, a feature that enables a user to surf the Internet without leaving traces on her local computer, such as history, cookies and temporary files (Aggarwal et al., 2010). Since then, all other mainstream browsers have added the same feature, including Internet Explorer (IE) (Internet Explorer private browsing mode), Chrome (Chrome private browsing mode) and Firefox (Mozilla Firefox private browsing mode).

Although the basic aim of private browsing is the same, the implementations vary greatly across different browsers. This adds significant complexity to the subject. In USENIX Security'10, Aggarwal, Burzstein, Jackson and Boneh first initiated the study of the security of private browsing in modern browsers and discovered several vulnerabilities (Aggarwal et al., 2010). In particular, they studied the dire impact of browser extensions on private browsing in Firefox (v3.6). A year later, Said et al. (2011) continued the study of private browsing. They focused on examining the content in the volatile memory and found that artifacts from the private session remained in memory even after the session had been closed. Recently, in ESORICS'13, Lerner et al. (2013) presented a software tool that allows automatic verification of the browser extensions' compliance with the private mode. The tool was mainly tested on Firefox extensions, although in principle it could be easily extended to other browsers.

Apart from these three papers, the security of private browsing seems to have been almost entirely neglected by the security research community. To date, no study has existed that systematically analyses the security of private browsing across major web browsers and from multiple angles: not just examining the memory, but also the underlying database structure on the disk and web traffic.

We believe this lack of attention is disproportionate to the importance of the subject. Over the past five years since 2008, private browsing has been extensively used by a significant portion of Internet users (19% according to a survey (Aggarwal et al., 2010)) to protect their privacy during web navigation (Lerner et al., 2013). Given the prevalent use of private browsing and the fact that many users are relying on it for privacy, it is important to ensure that private browsing is really as "private" as the browser vendors have claimed.

* *Corresponding authors.*
E-mail addresses: kiavash.satvat@gmail.com (K. Satvat), m.j.forshaw@ncl.ac.uk (M. Forshaw), feng.hao@ncl.ac.uk (F. Hao), ehsan.toreini@ncl.ac.uk (E. Toreini).
http://dx.doi.org/10.1016/j.jisa.2014.02.002

1.1. Contributions

In this paper, we will present an independent and systematic evaluation of the current state of private browsing in popular browsers. Our contributions are summarised below.

1. **Threat model**: We refine a threat model for private browsing based on adjusting a previous model (due to Aggarwal et al. (2010)) in order to capture more realistic threats in practice. This new model provides a concrete definition of security, which allows us to evaluate the security of private browsing in a systematic manner.
2. **Discovery of new attacks**: We have performed a series of concrete experiments and discovered a number of new vulnerabilities across all the web browsers under study. In particular, the attacks based on application crash, cross-mode interference and remote timing measurements are novel and are demonstrated to work in practice for the first time.
3. **Validation of known attacks**: We have tested all previously known vulnerabilities against the latest versions of web browsers and are able to confirm that some still remain unfixed.

Our preliminary research results were presented as a short paper (8 pages) at the ESORICS workshop on Data Privacy Management in September, 2013 (DPM'13) (Satvat et al., 2013). They were based on evaluating the latest versions of the mainstream web browsers as of April, 2013. However, being a short paper, only the main outcomes of the attacks are summarised. This journal paper includes full technical details for each of the attacks, especially the working and quantitative analysis of a novel remote timing attack in Section 5.2. Furthermore, suggestions for countermeasures are added in Section 6. We have informed the relevant browser vendors about the attacks and received useful responses that are also included in this paper. Some of the attacks have been fixed as a result. To inform the reader about the latest situation, we have re-tested all our attacks against the newest versions of browsers as of February 2014 with updates to the previous results included in this paper.

1.2. Outline

The rest of the paper is organised as follows. Section 2 explains the research methodology used for this study. Section 3 defines a threat model for private browsing. The next two sections, 4 and 5, present a series of experiments to expose vulnerabilities of private browsing against local and remote attackers respectively. Section 6 discusses countermeasures for discovered vulnerabilities. Finally, Section 7 concludes our study and suggests future research.

2. Research methodology

In this research work, we took a forensic approach to collect and analyse residual data left on the host computer after the private browsing session. Virtualisation was used to prevent any cross-contamination between experiments. In particular, VMware Player (a free version of VMware) was installed (VMware Player Version 4.0.0). In terms of the operating system, Windows 7 was chosen based on its popularity among the Internet users. The latest versions of the four popular browsers (as in April, 2013 (Most popular web browsers)) were installed: Mozilla Firefox (19.0), Apple Safari (5.1.7), Google Chrome (25.0.1364.97) and IE (10.0.9200.16521).

For each experiment a fresh Windows installation with a single web browser was used. The experiments were carried out for each browser to investigate possible residual data left in memory or disk after private navigation. A set of freely distributed third party tools were chosen (see Table 1), which makes it possible for the reader to replicate the experiments. Finally, all the software tools developed during the course of this research work are released as open source (see Open source code of the software tools). This should help browser vendors to evaluate the security of their products and improve accordingly.

A group of targeted websites were chosen to imitate a real user's behaviour in one browsing session, and to examine a variety of elements involved in web browsing. Table 2 lists the group of targeted websites and their characteristics. In each experiment, the targeted websites were visited in the private mode. The subsequent investigation involved closing the private session and searching for any evidence left on the computer. In most scenarios, this included searching for specific keywords such as URL, cookies, or other content of visited web pages.

3. Threat model

The threat model for private browsing is defined in terms of the attacker's capabilities and their goals. In 2010, Aggarwal et al. defined one threat model for private browsing. Our model is similar to theirs but with some differences, as we will explain. Same as in Aggarwal et al., (2010), we will categorise attackers into two types: local and remote attackers.

3.1. Local attack

A local attacker is someone who has physical access to a user's machine. The threat model defined in Aggarwal et al. (2010) restricts the local attack to "after the fact" forensics. In other words, it is assumed that an attacker cannot have physical access to the user's computer before the private browsing session (otherwise, the attacker may just install a key logger and the attack would be trivial). On the other hand, it is acknowledged in Aggarwal et al. (2010) that the user may

Table 1 – List of third-party software used in each experiment.

Software	Firefox	Chrome	IE	Safari
VMware Player	√	√	√	√
WinHex	√	√	√	√
Index.dat Analyser	N/A	N/A	√	N/A
SQLite browser	√	√	N/A	√
SQLite manager	√	√	N/A	√

Please cite this article in press as: Satvat K, et al., On the privacy of private browsing – A forensic approach, Journal of Information Security and Applications (2014), http://dx.doi.org/10.1016/j.jisa.2014.02.002