12-4-2013

The Effectiveness of Internet Activity Erasure Tools to Protect Privacy

Brian Cusack
Auckland University of Technology

Andrew Woodward
Edith Cowan University

Scott Butson
Edith Cowan University

Benjamin Leber
Edith Cowan University

DOI: 10.4225/75/57b56364cd8e2
11th Australian Information Security Management Conference, Edith Cowan University, Perth, Western Australia, 2nd-4th December, 2013
This Conference Proceeding is posted at Research Online.
https://ro.ecu.edu.au/ism/154

THE EFFECTIVENESS OF INTERNET ACTIVITY ERASURE TOOLS TO PROTECT PRIVACY

Brian Cusack[1,2], Andrew Woodward[2,3], Scott Butson[3], Benjamin Leber[3],
Auckland University of Technology, Auckland, New Zealand[1],
School of Computer and Security Science [3], Security Research Institute[2],
Edith Cowan University, Perth, Australia
brian.cusack@aut.ac.nz, a.woodward@ecu.edu.au, sbutson0@our.ecu.edu.au, bleber@our.ecu.edu.au

Abstract

When most people go to the trouble of getting erasure tools to remove data from their hard drives they expect the job is done correctly. Using erasure tools is a step to protect privacy by assuming the applied tools erase data rather than simply delete data that may be recovered using forensic tools. In this research we tested the performance of the delete function on three web browsers against the performance of eight erasure tools with alarming results. It was found that the erasure tools had almost the same capability to delete data as the web browsers delete function; and that no tool actually erased data. The implications for people using these tools to protect sensitive data are profound. People and organisations as they retire, sell or dispose of their hardware containing information assets require assurance they will not be impacted by the adverse effects of unintended disclosure of sensitive information. Better software solutions are required and better software certification measures require implementation.

Keywords

Delete, Erase, Software, Tools, Performance

INTRODUCTION

There are ten years of studies reporting what people throw away in their old computers. In the US and Australia over 50% of the hard drives recovered were readable and statistics obtained. In the UK, France and Germany the readable rate was 25-30%. Of these between 18% and 41% had been wiped of all data. The purposes in the various studies was to identify the percentage of readable data and then to analyse it in terms of privacy sensitivity. This included personal information and corporate information. Of the readable information in France, Germany and Australia up to 25% identified the Organisation or the Individual with sufficient clarity they could be traced through a telephone book. In The US and the UK the percentage was 45%. The studies highlighted the risk of unwanted disclosures and the need for better education on retiring hardware, software and data (Valli, 2004; Jones, Mee, Meyler & Gooch, 2005; Valli, & Woodward, 2007; Jones, Valli & Sutherland, 2008; Medlin & Cazier, 2010; Sansurooah & Szewezyk, 2012). Our study targeted the tools people use to do the right thing and to erase their information resources before release. Data erasure tools may be used for legitimate privacy protection but also illegal activity to destroy evidence. For example an employee of an organisation may wish to remove evidence of access to files that are not permitted or other activity such as copying, distributing or destroying files. The logical action would be to erase recent document histories. These histories include sessions, web browser logs, chat files and specific actions such as download, delete or broadcast. Poorly performing erasure tools leave not only useful data but also evidence of their use. Each tool leaves its own footprint for identification. An alert digital forensic investigator will pick up these signs when analysing forensic images of cloned media and make a full disclosure in the report (Gutmann, 1996; Garfinkle & Shelat, 2003; Carrier, 2011).

We examined a range of browser delete functions and Internet activity erasure tools to determine how well they actually erase or delete data (Oh, Lee & Lee, 2011). A selection of freeware and licensed erasure tools were chosen for a more complete snapshot of the choices currently available for use. All tools were used in their default configuration. A base image was created in a virtual environment, and then cloned for installation of each tool, ensuring that no remnant data remained from previous tests. Most of the tools did not delete what they claimed to delete in the original descriptions. Further, a common trend throughout the entire testing phase was that the Internet data is only deleted, and not erased. Many of the tested tools did not target the default download folder which would likely be an indicator of basic Internet activity. Additionally, the erasure of indicative peer-to-peer activity was largely un-catered for and left un-touched unless directly specified by the user. A common theme throughout deletion application tests was that none of the vendors managed to erase DOM cookies. Such cookies are a new form of cookie and are far more extensible than conventional cookies, which has raised some concern from the test results. In comparison with the delete function on each of the web browsers used the erasure tools added little value.

BACKGROUND

The recovery and inadvertent release of sensitive information is a serious risk for individuals and organisations (Valli et al., 2007; Sansurooah et al., 2012). Incidents of fraud, identity theft, corporate espionage and other aspects of technology crime are over represented in the literature (Wang, Yuan, & Archer, 2006; Wall, 2013). As computer and network security increases attackers and malicious users are now looking for easier alternatives to compromising systems. One potential attack vector is examining discarded or re-used hard drives for information which could be exploited for financial gain. The single home user or organisation might think that their sensitive data and information contained on these devices has been deleted but an attacker with even the most basic computer forensic skills would easily be able to recover such deleted data (Jones et al., 2008). As a response to this issue, there are now many varying hard drive erasure tools that have been developed for this market. These tools range from catering to simple web browser history deletion to entire hard drive erasure. There are a number of tools available on the market that claim to remove evidence of, amongst other things, Internet activity such as web browsing, downloaded files and chat logs. Organisations and home users must be able to trust that an erasure tool performs as advertised, and the user will subsequently dispose of a hard disk, remaining confident that their sensitive data has been adequately erased to prevent an attacker or even a casual browser from capturing sensitive material (Triton & Woodward, 2010).

There have been notable incidents of organisations selling their used computer equipment only to realise that they had also inadvertently released (secret) company data (Sansurooah et al., 2012). There are also a multitude of examples where confidential medical records have also been left on a hard drive which had been disposed of. One report detailed the discovery of a guided missile launch system document being found a on a second hand drive (Jones, Valli, Sutherland & Thomas, 2008). The disk also contained information including security policies, facility blueprints and employee social security numbers. There are many file system level locations on a hard drive to search for data and information (Olazak, 2006; Medlin et al., 2010). It is possible to monitor these varying locations to ascertain the effectiveness of the selected programs to securely delete information. Locations include personal folders, caches, temporary files, emails, browsing histories, registry settings, bad sectors, and slack space. Our project tested the hypothesis that internet browsing tools do not erase user history. This was done to both determine the efficacy of erasure as stated by the manufacturer, as well as to classify the tools in terms of the usefulness to an end user.

THE RESEARCH METHODS

The tests were limited to the erasure of internet artefacts as both a feasible study area and a sensitive focus area of common user activity. To test the capability of a sample of three web browsers and eight erasure tools to perform delete and erasure tasks we set up a testbed and applied standard test procedures. The following list is the erasure tools which were tested. Also indicated is the license state and version for each tool:

- CCleaner (3.22.1823, Freeware)
- History Sweeper (3.34, Free 14-day trial)
- R-Wipe and Clean (9.7, Free 15-day trial)
- Privacy Shredder (3.2 Free 14-day trial)
- Cyber Scrub Privacy Suite (5.1 Trial Version)
- Wash N' Go (2.4.3.1, Freeware)
- Eusing Internet Window Washer (3.1 Freeware)
- Ultra Sentry (6.10 Freeware)

The testing environment consisted of avirtual host, mounted OS and Autopsy forensic software. The specific details of the virtual machine test environment are as follows.

A VMware workstation 9.0 was used as the virtual software environment. CAINE was the OS for the investigation purposes, with the help of Autopsy. The CAINE 2.5.1 ISO, a virtual machine (VM) was created with the following settings: RAM: 512 MB, HDD: 10GB, Network Adapter: Bridged Connection, and Defaults are default settings. Name: CAINE. A baseline VM disk was established using a Microsoft Windows 7 Professional 32 bit Service Pack 1 ISO file. The VM was created within the VMware GUI with the following details to be included within the VM creation stage: RAM: 512 MB, HDD:10GB, Network Adapter: Bridged Connection, Defaults: Remaining options will be default. Name: Windows 7 VM. After creation of the Windows 7 VM, the following three web browsers, each with their default configurations, were installed: Internet Explorer (Version 8.0.6001), Firefox (Version – 14.01), Google Chrome (Version - 21.0.1180.83). The Process Monitor tool was installed to aid in the forensic procedure and filters were applied so that only relevant information from the relevant process was recorded. Once all browsers and PROCMON.exe were installed, all programs were closed and a snapshot taken of the VM, named as "baseline.vmsn" - the base-line for the testing. This VM image was then shutdown. Using HashCalc, an md5 hash was recorded of the snapshot file baseline.vmsn to ensure the integrity of the image, and the VM disk itself labelled as "Windows 7 VM.vmdk.

The following procedure was followed in order to test the efficacy of the erasure tools. This procedure was used for each instance of erasing software located in the third party erasing tools section.

- Prior to running of the Windows 7 VM, ensure that hash value of the correct snapshot file (baseline.vmsn) and VM file (Windows 7 VM.vmdk) are calculated and compared against the original values.
- Revert the VM to the correct snapshot file (baseline with Chrome, IE, Firefox etc.vmsn), create a clone of the windows 7 vmdk file and name it as the name of the tool being tested, install the default configuration of the erasing software from the list, if torrent activity erasing is supported, then proceed with the installing the UTorrent application, and select and download one torrent file; begin download and wait until finished.

- Turn on Process Monitor, and update the flag to the IE, Chrome, and Firefox processes; run the prescribed Internet activity on all the browsers supported by the erasing software tool, and visit a predetermined list of websites
- Update the Process Monitor with the erasing tool's process ID; run the erasure tool, and prepare for the selection of configuration, which was to delete all browser history, cookies, and temporary internet files and begin erasing
- Once finished, shutdown the VM; boot up the CAINE VM OS, and mount the cloned VMware disk specifically with the (ro) flag.
- Use the "dd" utility convert to an image.
- Once completed run the Autopsy application within the CAINE VM, and load up the relevant VM image.
- Record the md5 digest of the image; begin forensic examination, and record results.
- Run a scalpel command on the disk (jpeg and gif only); compare hash values of VM image.
- Shutdown Autopsy and the CAINE VM.

THE RESULTS

The results showed the delete function and the erasure tool performance against four browser artefacts; History, Cookies, Temporary Internet files, and stored password deletion. The most comprehensive tool was CCleaner, which had support for all three browsers tested, and deleted all categories of data. However, this tool only deleted data from each of the targeted locations on all browsers implying that the data was not erased and thus was recoverable. No one tool clearly fell to the bottom of stack but all tools failed to live up to the shrink-wrap claim of "erasing" internet activity. The majority did deletion only of limited information, no erasure, and had limited browser support. Only two of the tools had the ability to detect BitTorrent activity, and only one deleted the test activity. Table 1 shows the performance of each tool.

Tool name	Browser Score[1]			Torrent erased?
	Internet Explorer	Chrome	Firefox	
CCleaner	4/4 (delete only)	4/4 (delete only)	4/4 (delete only)	Yes (delete only)
History Sweeper	1/4 (delete only)	2/4 (delete only)	1/4 (delete only)	Not supported
R-Wipe and Clean	2/4 (delete only)	Not supported	2/4 (delete only)	Not supported
Privacy Shredder	1/4 (delete only)	Not supported	Not supported	Not supported
Cyber Scrub Privacy Suite	2/4 (delete only)	0/4	1/4 (delete only)	No
Wash N' Go	2/4 (delete only)	Not supported	Not supported	Not supported
Eusing Internet Window Washer	2/4 (delete only)	2/4 (delete only)	2/4 (delete only)	Not supported
Ultra Sentry	2/4 (delete only)	0/4	0/4	Not supported

Table 1. Ability of software based activity erasure tools to meet erasure specification when used with three browsers

The testing of the effectiveness of three Web Browser deletion capabilities showed the same result for each. Each browser deleted the Histories, the Cookies, the Temporary Internet files and the Saved/Stored passwords. This was deletion – not erasure; and a range of images, bookmarks, directory information, files and so on were easily recovered.

DISCUSSION

What the tests have shown from our initial hypothesis is that running Internet cleaning applications such as those used in the testing phase will not entirely erase user data, and hence what ultimately will occur is that those who are relying on these tools to erase data will need to take a different approach for removing online footprints. As Jones & Meyler (2004) state “legitimate motives for removing data could include the deletion of classified or sensitive material, such as personal, governmental, military, or medical data”. Therefore corporate and government users need to ensure that sensitive information is erased securely and efficiently.

If after performing the erasure tasks the user was to dispose of the machine, and there was sensitive information that can be retrieved, it can have adverse effects on the organisation and or the owner of the hard disk. After retrieving data such as cache, history, cookies, and download lists from a user’s computer, it is possible to analyse this evidence for Web sites visited, time and frequency of access, and search engine keywords used by the user. Obtaining such data should be extremely difficult for the forensic examiner, but is in fact trivial if data has only been deleted and not erased. This research has demonstrated that adequate erasure of activity cannot be achieved with the tools or browser deletion methods evaluated in this research.

Of the eight tools tested, the Ultra Sentry & Privacy Suite by Cyber S were the lowest performers from a perspective of erasing data. This was due to the nature in which the tools declared what was possible and what was not possible to be deleted. Ultra Sentry did indicate multiple browser support, yet was unable to securely erase the claimed files and directories. User data in both Firefox and Chrome was effectively untouched by this tool, as evidenced by cookies, cache, and history that were still detectable. Counter to this finding, Piriform’s CCleaner performed highly, in that the tool claimed to support multiple browsers and alternative applications such as UTorrent, and did delete what was declared. However, this was only deleted and not erased; the implication being that all data has effectively not been removed and can be recovered until such time as that sector of the disk is overwritten. This suggests that a user would be able to achieve the same level of performance by using built in browser privacy options as opposed to using third party tools.

A common theme throughout the tests conducted on the third party erasing tools, was the inability for such applications to delete dominant object model (DOM) cookies. DOM storage items can be substantially larger than conventional cookies and can contain more information. Users of these applications will need to implement a far more secure approach since almost all applications failed this test. The selected list of browsers and erasure based applications which claimed to remove Internet history and their associated logs did not in fact do so as data was recoverable. Hence it is suggested that such methods for deleting Internet based logs are an inefficient and insecure approach, and therefore the use of a proven secure erasing application would be needed. If a user is truly concerned about their privacy, then they would be better advised to use an encrypted hidden partition, such as TrueCrypts “plausible deniability” tool to protect their privacy than to rely on one of these tools (Miao, 2010). The other alternative is to erase or destroy the drive before disposal.

CONCLUSION

Our findings suggest that erasure tools do not function as promoted. Organisations and individuals who have used erasure tools to legitimately protect privacy should not have to worry about the tool performance. Similarly they should not have to go through laborious laboratory testing to assure the tool performance before use. However, there are grounds for not trusting the full erasure of data and the requirement for tool certification by independent experts. It has been shown that in most cases erasure tools leave residual data. This may come from storage principles applied, magnetic properties, the algorithms used or the tool capability. Data can be written on any part of the media as they are created, re-written and deleted. Some tools only erase by proportion leaving related artifacts in other portions. This includes slack space, hidden sectors, virtual memories and other abnormalities outside of the erasure algorithm. Until universal certification criteria are applied every device once erased by a tool ought to be checked by another tool such as Encase, FTK, Autopsy or other open source tools to assure no data remains.

This research determined that most tools deleted some data and very few of the tools as tested successfully erased data. This is significant as many individuals and organisations rely on such tools when they dispose of information assets, or as highlighted in previous research, not at all. There is already significant risk associated with disposal of information assets, and an organisation which doesn’t have the resources to audit or conduct secure disposal procedures may find themselves a victim of information theft. We plan to contact consumer advocacy groups and highlight this issue with the aim of bringing it to the attention of the public. Future research will widen the scope to examine other tools, and will also look to examine whole-of-disk erasure tools.

REFERENCES

Carrier, B. (2011). The Sleuth Kit. Retrieved from http://www.sleuthkit.org/autopsy/download.php.

Garfinkle, S, & Shelat, A. (2003). Rememberance of Data Passed: A Study of Disk Sanitization Practices. *IEEE Transactions in Security & Privacy*, Vol. 1, 1.

Gutmann, P. (1996). Secure Deletion of Data from Magnetic and Solid State Memory. *Proceedings of the USENIX Security Symposium*, San Jose, July 22-25, pp. 77-89.

Jones, A., Mee, V., Meyler, C., & Gooch, J. (2005). Analysis of Data recovered from Computer Disks Released for Sale by Organisations. *Journal of Information Warfare*, 4(2), 45-53.

Jones, A, Valli, C., Sutherland, I, & Thomas, G (2008). The 2007 Analysis of Information Remaining on Disks Offered for Sale on Second Hand Markets. *International Journal of Liability and Scientific Enquiry*, 2(1), 53-68.

Medlin, B., & Cazier, J. (2010). A Study of Hard Drive Forensics on Consumer’s PCs: Data recovery and exploitation. *Journal of Management Policy and Practice*, 12(1), 27-35.

Miao, Q. (2010). Research and analysis on encryption principle of truecrypt software system. *Proceedings of the 2nd International Conference on Information Science and Engineering (ICISE),*IEEE, Boston.

Oh, J., Lee, S., & Lee, S. (2011). Advances in Evidence Collection and Analysis of Web Browser Activity. *Digital Investigation*, 8: S62-S70.

Olazak, T. (2006). Fundamentals of Storage Media Sanitation. Retrieved from http://www.usenix.org/events/sec01/full_papers/gutmann_html.

Sansurooah, K. & Szewezyk, P. (2012). A Study of Remnant Data found on USB Storage Devices Offered for Sale on the Australian Second Hand Market. *Proceedings of the 10th Australian Information Security Management Conference*, Perth.

Triton, C. and Woodward, A. (2010). An Investigation into the Efficacy of Three Erasure Tools under Windows 7. *Proceedings of the 8th Australian Digital Forensics Conference,* Perth, WA.

Valli, C. (2004). Throwing Out the Enterprise with the Hard disk. *Proceedings of the Second Australian Computer, Information and Network Forensics Conference*, Freemantle, WA .

Valli, C. and A. Woodward. Oops they did it again: The 2007 Australian study of remnant data contained on 2nd hand hard disks. *Proceedings of theAustralian Digital Forensics Conference, Perth, WA.*

Wall, D.S. (2013). Policing identity crimes. *Policing and Society*, 3(1), 1-24.

Wang, W., Yuan, Y. and Archer, N. (2006). A contextual framework for combating identity theft. *IEEE Transactions in Security & Privacy*, 4(2), 30-38.