2011

Information leakage through second hand USB flash drives within the United Kingdom

Widya Chaerani
University of Plymouth, United Kingdom

Nathan Clarke
Edith Cowan University

Christopher Bolan
Edith Cowan University

DOI: 10.4225/75/57b2ba7e40cea
Originally published in the Proceedings of the 9th Australian Digital Forensics Conference, Edith Cowan University, Perth Western Australia, 5th -7th December 2011

INFORMATION LEAKAGE THROUGH SECOND HAND USB FLASH DRIVES WITHIN THE UNITED KINGDOM

Widya. Chaerani[1], Nathan Clarke[1,2], Christopher Bolan[1,2]
[1]Centre for Security, Communications and Network Research,
University of Plymouth, Plymouth, United Kingdom

[2]secau – Security Research Centre, School of Computer & Security Science
Edith Cowan University, Perth, Western Australia
widya.hc@gmail.com, n.clarke@plymouth.ac.uk, c.bolan@ecu.edu.au

Abstract

The pervasiveness of flash based USB storage alongside increasing capacity and lowering price points has lead to a documented potential for information leakage. Such a potential is significantly raised when employees are able to use personal devices within a business environment with little regard to safe disposal practices. This study purchased a range of USB storage devices from UK based auction sites to determine what if any data was recoverable. The study found a total of 36136 recoverable files including a range of data detailing private information of previous owners, confidential corporate data, with twenty percent of the purchased USB devices securely wiped before sale.

Keywords

Universal Serial Bus, Data Recovery, Data Leakage, Identity Theft, USB Storage

INTRODUCTION

The United Kingdom has a widely documented history of information leakage due to either the loss of or improper disposal of hardware (Kennedy, 2008; Oates, 2008; BBC, 2008; BBC, 2009). With the broad range of well publicised incidents alongside freely available secure erasure tools it may be expected that there should be a reduction in the phenomenon. Therefore the purpose of this research was to investigate a random sample of the second hand portable storage market and quantify whether the increased awareness has lead to any real improvement.

THE SCOPE OF THE PROBLEM

One of the earlier and more influential studies into this area was conducted by Jones (2005) on the disposal of corporate hard disks. It was found that only 16% of the imaged disks were completely erased, with a further 48% showing signs of superficial data removal. Even with such attempts 51% of the imaged disks contained personal information, 20% financial information, 8% network information and 4% contained illicit material.

This research was expanded in 2006 in a joint study (Jones, 2006). In this attempt 42% were found to be totally blank, 28% contained commercial data and a further 29% individual data. This was an improvement on the previous year but still an unacceptable level. The 2007 results were similarly decreased with a 37% finding of personal data.

In the following year the InfoWatch (2008) research enumerated the victims of information leakage into commercial entities (50%), educational and non-governmental organizations (31%) and governmental bodies (18%). When further quantified, it was revealed that 95% of the leakage could be classified as personal data with portable storage accounting for most of these. The results were supported by Hoffman (2008) who found that over 25% of employees admitted to storing sensitive data from there organization on portable storage devices. Despite such findings the BERR (2008) survey detailed that over 67% of the companies in their study did nothing to prevent confidential data being transported on unsecured USB sticks and other removable media. This was followed again in 2009 with a survey which found that 52% of the disks contain organizational information, 51% personal information, and only 31% of the disks were wiped (Jones, 2009).

WHY TARGET USB STORAGE

USB flash storage has gradually become synonymous with portable data storage since its commercial introduction in 2000 (ENISA, 2008). A study conducted by Gartner (2005) enumerated the market for USB flash drives in 2004 as $1.47 billion forecasts growth to reach $3.47 billion in 2010. This growth in sales has been alongside an increase in the average capacity of these devices. According to Crisp (2009) the average capacity of drives sold in 2005 was only 462.3MB which has grown to around 4.8GB in 2009.

The portability and low price point of these devices has not been accompanied by the use of appropriate encryption. A 2007 study found that of the USB drives sold to corporate entities, as little as 10% claimed to mandate the use of encryption to protect the data (Chapman, 2007). This is despite research which detailed that over 77% of USB drives may be used by users at work and of these users only 21% demonstrated awareness of information leakage threats (ENISA, 2008). This usage was further enumerated into the type of data stored on USB devices as detailed in the figure below

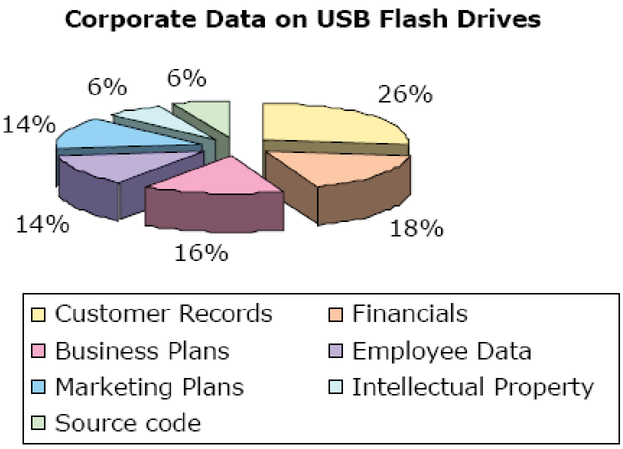

Figure 1. Corporate Data on USB Keys (ENISA, 2008)

These worrying trends are compounded by the research conducted by the Ponemon Institute (2009) into downsized employees. They found that over 59% of their sample reported keeping company data after leaving employment. The type of data kept included email lists (65%), non-financial business information (45%), and customer information including contact lists (39%). Of the respondents that admitted to removing data, 42% utilised USB flash drives in the transfer. Despite this the research showed that 89% of companies in the study failed to audit USB devices for data leakage even though a majority did not require the return of flash storage on cessation of employment.

SAMPLE ACQUISITION AND METHOD

For the purposes of this research it was decided to target USB storage devices that were as widely available as possible, thus the UK version of eBay website was used in the acquisition of the sample. Only USB flash drives that were clearly marked by the seller as used were purchased and efforts were undertaken to ensure that each purchase was from a different seller and that no identifying features were present on the device. A range of capacities were purchased and are enumerated in the table below:

Size	128Mb	256Mb	512Mb	1Gb	2Gb	4Gb
Number of devices	2	1	4	8	3	2

Table 1. Capacity of USB Drives used in sample

Upon receipt of the devices, each was handled in accordance with correct forensic procedures. Once imaged the analysis was conducted using the following software:

- Encase 5
- Forensic Tool Kit 1.81.3.

- Recuva
- Zero Assumption Image Recovery

Every image within the study was subjected to a full range of recovery procedures as afforded by the aforementioned software packages.

RESULTS

In all 36,136 files were recovered from the secondhand USB devices. As detailed in the figure below the majority of files were Microsoft Word Documents, followed by images, then emails/html files.

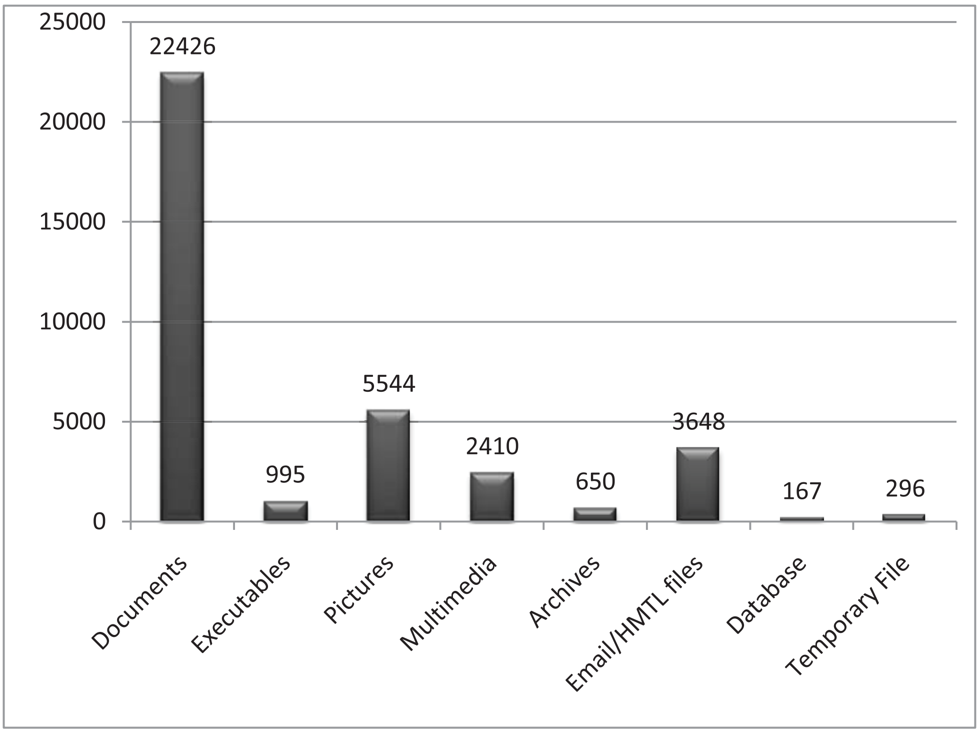

Figure 2 Total Files Recovered

Post recovery the files were investigated and classified according to type individual or corporate. Individual files where determined to be any file that could not be identified as belonging or related to a business. Files were then further separated into the likely sensitivity of the information between high and low sensitivity. This data is enumerated in the following table. The four USB key devices that were determined to be empty, contained no recoverable files or folders and were also free of data within their unallocated clusters.

Category		Number of Keys		Percentage	
Empty		4		20%	
Individual	Low Sensitivity	14	11	70%	55%
	High Sensitivity		14		70%
Corporate	Low Sensitivity	6	2	30%	10%
	High Sensitivity		6		30%

Table 2. Breakdown of Information Types Discovered

Of the keys that were categorized as containing individual data over 92% contained enough information to identify the owner of the USB storage device prior to sale. The extent of this information is illustrated in the figure 3. It is noteworthy that the inclusion of mothers maiden name and the date of birth would be significant in the likelihood of identity theft should the information be gathered for nefarious purposes. In addition to the personal identification a range of the devices contained banking and/or login information of the previous owner as detailed in figure 4.

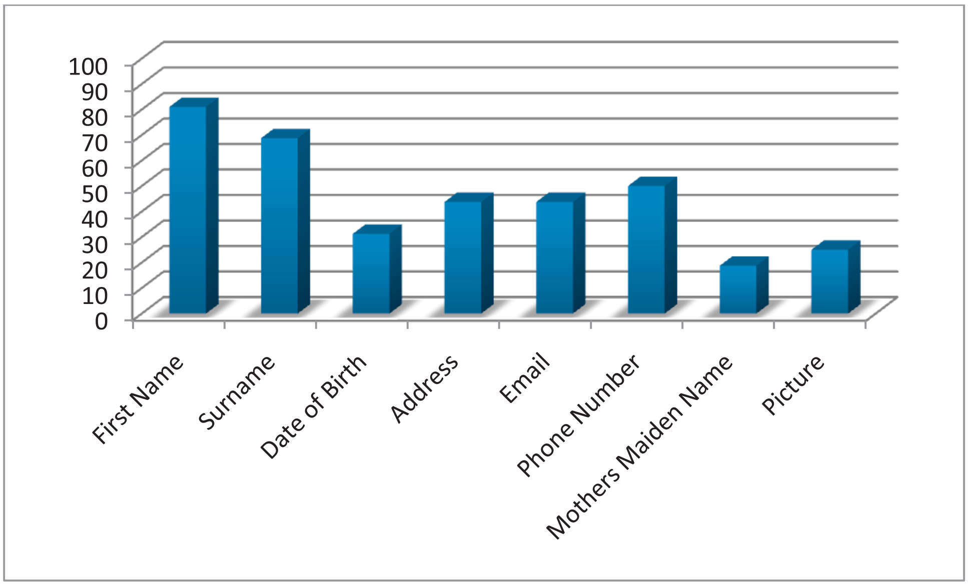

Figure 3. Type of Personal Identifier

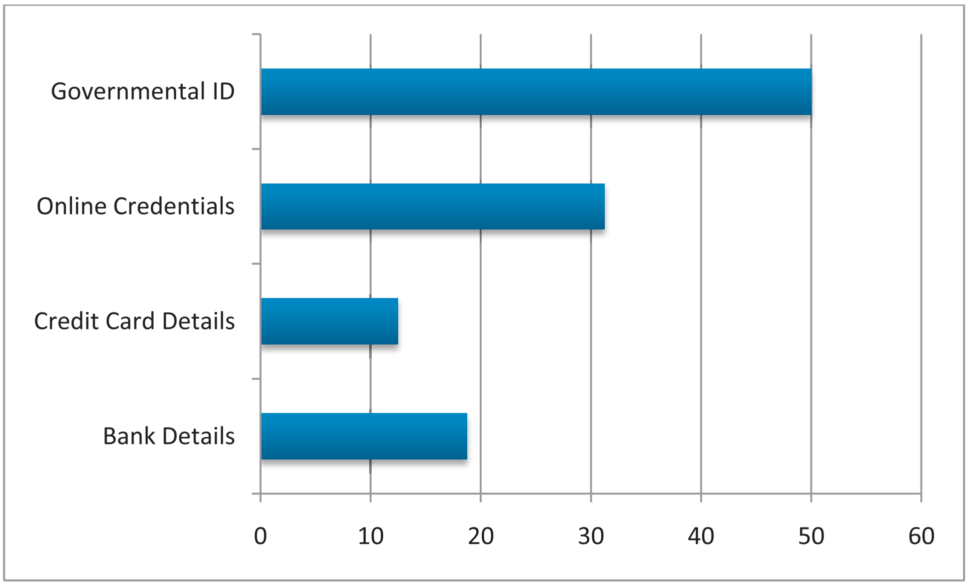

Figure 4. Percentage of Devices Containing Bank or Login Details

In addition to the above findings, 15% of the devices contained the CV of either the owner or a third party. When this statistic is expanded to include keys that contained personal details of any third party this number increased significantly to 60%. These details included full names, passport details and third party banking information. Of the devices containing corporate data, there were found company logos, form letter templates, meeting notes, financial reports, list of board members along with their personal information, turnover analysis, sales forecasts, signature scans and companies' bank details. Such information would allow direct targeting of these companies for a range of fraudulent activities.

With the cataloguing of this information it was possible to delineate the type of threats that might be carried out against either the owners or the included third parties. The identified data (detailed in the table below) would facilitate over 32 criminal acts including direct removal of funds from an identified individuals account.

Threats	Identity Theft	Fraud	Industrial Espionage	Blackmail	Hacking / Network Intrusion	Robbery
Number of devices	11	9	2	5	4	1

Table 3. Direct Threats Possible from Included Data

CONCLUSION

When the findings of this research is viewed in the light of the previously discussed studies a worry trend emerges. Whilst the breadth of collection is indicative of this work as a pilot study, the low rate (20%) of securely wiped devices is lower than that found in the HDD based research. This may be attributable to the fact that the previous studies were from corporate environments, whereas it is more likely that the sellers and previous owners of these devices were individuals. The range and seriousness of the information leakage represented by the data found on the devices was directly inline with other studies discussed.

Without exception every study of this type has documented findings of threats to both corporates and individuals and this work is no exception. Of concern is that whilst the previous studies have typically dealt with corporate disposals, in this study the sellers are exclusively private individuals. Thus whilst the corporate problem may be reduced by awareness of liability and institutional education, it may be that the only viable solution to this sort of leakage by individuals may be the banning of sales of second-hand storage devices. The scope of this problem is barely known and definitely in need of further exploration. To this end similar studies are to be undertaken worldwide to gain a true understanding of the true impact of second-hand USB storage disposal.

REFERENCES

BBC, 2008. More secret files found on train. [Online] Available at: http://news.bbc.co.uk/1/hi/uk/7455084.stm [Accessed 13 August 2009].

BBC, 2009. Previous cases of missing data. [Online] Available at: http://news.bbc.co.uk/1/hi/uk/7449927.stm [Accessed 13 August 2009].

BERR , 2008. BERR Information Security Breaches Survey. [Online] Available at: www.security-survey.gov.uk [Accessed 15 November 2008].

Chapman, M., 2007. Data Breaches are 'Everyday Incidents'. [Online] Available at: http://www.v3.co.uk/vnunet/news/2203540/security-breaches-everyday [Accessed 30 August 2009].

Crisp, S., 2009. Kingston Launches "World's First" 128Gb USB Flash Drives. For The Price Of A Laptop. [Online] Available at: http://gizmodo.com/5292392/kingston-launches-worlds-first-128gb-usb-flash-drive-for-the-price-of-a-laptop [Accessed 30 august 2009].

ENISA, 2008. Secure USB Flash Drives. [Online] Available at: http://www.enisa.europa.eu/doc/pdf/publications/Secure%20USB%20drives_180608.pdf [Accessed 30 August 2009].

Gartner, 2005. Market Trends: USB Flash Drives, Worldwide, 2001 - 2010 (Executive Summary). [Online] Available at: http://www3.villanova.edu/gartner/research/130800/130851/130851.pdf [Accessed 30 August 2009].

Hoffman, S., 2008. Cisco Survey Designated 10 Riskiest Data Loss Behavior. [Online] Available at: http://www.crn.com/security/210604893?cid=ChannelWebBreakingNews [Accessed 1 February 2009].

InfoWatch, 2008. InfoWatch research for the 1st half – 2008: personal data leak is in the spotlight. [Online] Available at: http://www.infowatch.com/about?chapter=148834537&id=207784846 [Accessed 3 December 2008].

Oates, J., 2008. Million bank details sold on eBay and a few more gone AWOL. [Online] Available at: http://www.theregister.co.uk/2008/08/26/more_details_lost/ [Accessed 14 July 2009].

Kennedy, J., 2008. Alarm as four laptops stolen from Bank of Ireland. [Online] Available at: http://www.siliconrepublic.com/news/news.nv?storyid=single10808 [Accessed 16 September 2009].

Jones, A., 2005. How much information do organizations throw away? Computer Fraud & Security, 2005(3), pp.4-9. DOI: 10.1016/S1361-3723(05)70170-6 [Accessed 31 July

Jones, A., 2006. Cradle to grave - security failure to the very end. Computer Fraud & Security, 2006(9), pp.4-8. DOI: 10.1016/S1361-3723(06)70418-3 [Accessed: 13 August 2009].

Jones, A., 2009. Lessons not learned on data disposal. Digital Investigation, pp.1-5. DOI: 10.1016/j.diin.2009.06.017 [Accessed 15 July 2009].