3-12-2009

The 2009 Analysis of Information Remaining on USB Storage Devices Offered forSale on the Second Hand Market

Andy Jones
Khalifa University of Science

Craig Valli
Edith Cowan University

G. Dabibi
Security Research Centre

The 2009 Analysis of Information Remaining on USB Storage Devices Offered for Sale on the Second Hand Market

Andy Jones[1,2,3]
Craig Valli[2]
G Dabibi[3]

[1]Khalifa University of Science, Technology and Research
[2] Edith Cowan University
[3]Security Research Centre, BT

andrew.28.jones@bt.com
Phone: +9716-5043501
Fax: +9716-5611789

Abstract

The use of the USB storage device, also known as the USB drive, a thumb drive, a keychain drive and a flash drive has, for the most part, replaced the floppy disk and to some extent the Compact Disk (CD), the DVD (Digital Video Disk or Digital Versatile Disk) and the external hard disk. Their robustness, size and weight make them easy to transport, but also to lose or misplace. They are inexpensive and are often given away as promotional items by organisations. Over the last few years there has been a dramatic increase in the storage capacity of these devices, going from a few tens of megabytes to a current capacity of around 64 gigabytes (equal to around 13 DVDs). The larger capacity and continued low cost has vastly increased the potential uses of the devices and also the volumes and types of data that they may contain.

There have been four annual studies carried out by the same research group to look at the level of data remaining on second hand computer hard disks and one study looking at data remaining on hand held mobile devices such as mobile (cell) phones and RIM Blackberry devices. With the increasingly common use of the USB Storage device as a means of transferring and transporting data, coupled with the increasing storage capacity and decreasing cost, it was felt that the research should be extended to include the examination of USB storage devices to determine the level of threat they may pose.

The purpose of the research has been to gain an understanding of the information that remains on the USB storage devices and to determine the level of damage that could, potentially, be caused if that information fell into the wrong hands. The study examined USB storage devices that had been obtained in the UK to determine whether the way that the disposal of USB storage devices is addressed achieved the desired result, to determine the level of information remaining on the devices and the level of risk that this may create.

The study was conducted by the British Telecommunications (BT) in the UK, Khalifa University of Science, Technology and research (KUTAR) in the UAE and Edith Cowan University in Australia. The basis of the research was to acquire a number of second hand USB storage devices from a range of sources and to determine whether they still contained information or whether it had been effectively erased. If they still contained information, the research looked to see if it was in a sufficient volume and of enough sensitivity to the original owner to be of value to anyone with malicious intent that had obtained it, whether a competitor or a criminal. The results of the research were that in most cases, the USB storage devices contained a significant volume of information. As with the findings of the second hand disk studies, where the USB storage devices had originally been owned by organisations, they had failed to meet their statutory, regulatory or legal obligations.

Keywords

Digital forensics, USB Storage, analysis, data recovery, data disposal, electronic data destruction, privacy.

INTRODUCTION

This research was undertaken to gain an understanding of the level and types of information that remained on USB storage devices that had been offered for sale on the second had market. As with the studies into second hand disks and hand held mobile devices, the research revealed that a significant proportion of the USB storage devices that were

examined still contained significant volumes of information, some of which would have been of some sensitivity for the organisations or individuals that had previously owned them. Prior to this study, there have been a small number of commercial and journalistic studies and a number of press reports relating to lost USB storage devices, including a report in the Daily Telegraph (Winnett, 2008) on the loss of data relating to 40,000 criminals, or the incident reported in IPPro (Green, 2008) regarding the loss of information on 250 children. There has been little academic or commercial study into the data remaining on USB storage devices but the most significant report (Kehrer, 2007) highlights the high levels of data remaining on USB devices at the time.

The research undertaken was sponsored by British Telecommunications (BT) which funded the purchase of the USB Storage devices and carried out some of the processing and analysis of the data. The aim of the research was to determine whether any data remained on second hand USB Storage devices and if so, the potential sensitivity of the information that remained on the USB Storage devices. The research was conducted under the same conditions that had been used during the second hand disk and hand held mobile devices studies, using commonly and easily available tools that had similar capabilities. The results of the research are that a number of observations have been made with regard to the level and type of information remaining on second hand USB Storage devices and a number of conclusions and recommendations have been made on ways to improve the situation with regard to data remaining on second hand USB Storage devices.

This paper, the report on the first of what is intended to be a series of surveys, contains the results of the 2009 research that was carried out by the Security Futures Centre of BT, Khalifa University in Sharjah in the UAE and Edith Cowan University in Australia.

THE RESEARCH

To ensure that the results of the research provide a realistic and scientifically sound view of the situation, 43 USB Storage devices were obtained. All of the USB Storage devices used in the research were purchased at computer auctions, computer fairs or through eBay. The USB Storage devices were purchased discretely either singly or in small lots by a number of purchasers. This procedure was adopted in order to minimise the possibility of the sellers becoming aware of the purpose for which the USB Storage devices were being obtained and also to ensure that the actions of one seller did not have a disproportionate effect on the results of the study.

The USB Storage devices were supplied 'blind' to the researchers. The only identifier on the USB Storage devices that were provided to the researchers was a unique sequential serial number so that there was no indication of where or how they had been obtained. Where the USB devices were marked with advertising logos, these were not obscured or hidden as it was not considered to be a significant source of information (many organisations hand out USB Storage devices as a form of advertising and it is more common that they will not be given to staff working for the organisation who's logo appears on the USB Storage device).

The research methodology used was the same as that used in the second hand disk study research (Jones et al. 2005, 2006. 2009, 2009a), with each USB Storage devices being forensically imaged using commercially available software (Guidance Encase or Access data Forensic Tool Kit (FTK)) and then stored in secure storage areas. The analysis was then undertaken on the images of the original USB Storage devices that had been created. There were two main reasons for the adoption of this time consuming step. The first was to preserve the original media in its original state and store it in a secure area in case there was a requirement to pass it on to law enforcement if notifiable criminal activity was discovered. By adopting this procedure, the chain of custody was preserved for any investigation by law enforcement. This allowed the research to be carried out in a non-intrusive manner that did not affect or change the original data. Also, if any anomalies were detected with the image, it would be possible to validate the data against a second image created from the original.

The tools used in this study to analyse the USB Storage devices were fundamentally the same as those used in previous disk and mobile hand held device studies (although the versions of the tools may have changed). The tools performed similar functions to the Windows Unformat and Undelete commands and a hexadecimal editor (which can be used to view any information that exists in the unallocated portion of the USB Storage devices). Tools that perform this type of functionality are readily available and free: examples include forensic analysis tools such as Autopsy (Version 2.08) and the Linux based Helix software. Freeware Hexadecimal editors include `XVI32 and ftweak-hex.` These tools can be used effectively without significant levels of skill or knowledge.

The objectives of the research were the same as those defined for the disk and hand held mobile device studies: firstly to determine whether the USB Storage devices had been effectively cleansed of data or whether they still contained

information that was either visible or easily recoverable with the tools identified above. The second objective of the research was to identify whether there was information that could be used to identify the organisation or individual(s) that had used the USB Storage device.

The initial results indicate that the level and type of information found on the USB Storage devices is in the same range as that found during the disk studies. While the storage capacity of the USB storage devices is, in most cases still smaller than the average computer hard disk, the proportion that still contained data was much higher.

THE RESEARCH RESULTS

This section details the results for the study for the 43 USB Storage devices obtained:

For the 43 USB Storage devices:

- 2 (4%) were damaged and as a result, unreadable. Note: These devices were disassembled by Edith Cowan University and the results of this research will be reported separately.

- 2 (4%) had been effectively cleaned and contained no recoverable data

- 20 (46% of the readable USB Storage devices) had been deleted or formatted, but still contained recoverable data.

- 41 (95% of the readable USB Storage devices) contained data that could be easily recovered,

    – 8 (40%) contained sufficient information for the organisation that they had come from to be identified.

    – 14 (70%) contained sufficient information for individuals to be identified.

Total Number of USB Storage Devices Analysed	43
Data Wiped	2 (4%)
Faulty/Unreadable	2 (4%)
Data removal attempt -data deleted or device formatted	20 (49%^{1})
Commercial data present	19 (46%^{2})
Individual data present	23 (56%^{2})

^{1} *Percentages are of the readable disks*
^{2} *Percentage of readable disks that had not been wiped*

Table 1: A comparison of the results from the USB storage devices.

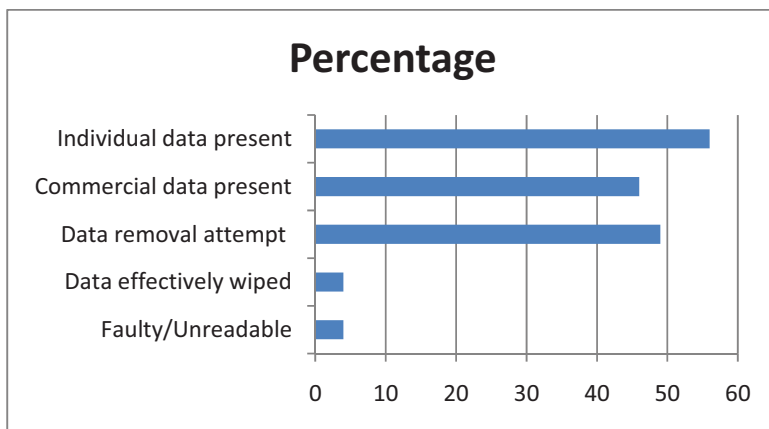Figure 1 below shows these results in a graphical format.

Figure 1: Graphical representation of the analysis results

This analysis showed that while it is still too early to draw any conclusions on possible trends, there are a number of indications that are of significance. Once again, as with the second hand disk and hand held mobile device studies, a surprisingly large volume and range of information that could have a potentially commercially damaging impact or pose a threat to the identity and privacy of the individuals involved was recovered as a result of the analysis. An indication of the quantity and type of material that was recovered, originating from commercial and academic establishments and private individuals is detailed below:

- Two of USB Storage devices from the 43 samples used for this research were from a known university in Manchester with identifiable names of students, their addresses and student registration number. These USB Storage Devices contained group coursework and personal information such as student budget and expenditures. One of them even contained the birth certificate of the student.

- One USB Storage device was from a school teacher from a high school in the UK. The dongle had a scanned copy of the teacher's university certificate, teachers training certificates, videos of kids from the school, teaching resources, and numerous personal materials that the teacher would not want to get to the public.

- Another two of the USB Storage devices belonged to staff of a well known global jewellery and fashion industry organisation. These USB sticks contained the company budget for 2009, sponsorship details, corporate business unit architecture, unit sales presentations and sales result for 2008-2009, details of high profile fashion events etc.

- A number of the USB Storage devices just had pictures of families on holiday trips. One also contained details of the family's ticket confirmation and travel insurance details with identifiable names and details of where they were taking off from, their destination, time of travel and the airline used from what airport in UK.

- Another of the USB Storage devices was from a student studying BTEC in National Business from a college in Blackburn. The storage devices contained the name of the student and address, names of other identifiable persons, personal statements, student CV which details address, date of birth, telephone numbers, assignments, and contract agreements from a law firm, letter of invitation to a speech and business reports from identifiable retail businesses in the UK.

- One USB Storage device contained a detailed house plan from an architectural company to their client, the address of the company, the address of the building site, the clients name and address and date of sale.

- Another USB Storage device had a named organisation located in Birmingham, with an annual turn-over of 687,649 GBP, the date of incorporation as 1994, address and phone number to contact, company status as 'Live', board of directors with their names and addresses, their date of births and positions.

- Two of the USB Storage devices were from private individuals trying to start up a new small scale business: one from Newbury with a plan of recycling operations, and the other storage device had documents related to the set up a beauty salon in Lancashire as well as other documentation about sources of new small scale business support for young people such as the princess trust, etc.

- One USB Storage device contained Church rosters with names and dates for events at a church in Essex. Ages, addresses and phone numbers of parishioners and volunteers are fully disclosed. The device also contained quotations for installation of a loft in a private residence and numerous photos of lofts and renovations and official drawings of same.

- One USB Storage device contained various images of Ministry of Defence Police (UK) officers in action or one case posing as a group in front of the police station with the name of the station on display. The device also contained assignments from a college that undertakes training for police personnel.

- One USB Storage device contained various personal pictures of family, family holidays and friends. Again, this device was from a college that undertakes training for police personnel. It also contained an extensive range of assignments, notes and details from the course of study undertaken by the individual. The individual's name, date of birth and other details of identity were disclosed.

With the increase in the availability and storage capacity and the reduction in the relative cost of USB storage devices, coupled with their relative robustness and easy transportability, they have essentially become the replacement for the 3.5 inch floppy disk and the CD/DVD or external hard disk for the transfer and movement of data. At the same time we have also seen a huge increase in the number of personal digital devices such as cameras, MP3 players and 3G communications devices that contain Secure Digital (SD) storage media that are also connect via the USB port to the computer.

Whilst technology has kept pace with the need to protect this information to an appropriate level and to destroy it effectively, the failures that have been observed seem to be attributable to a lack of corporate policies and procedures for the protection and subsequent disposal of obsolete USB storage devices and to individual awareness of the impact of storing such information and the measures that need to be taken to ensure that data is destroyed when it is no longer required.

The problems that result from the loss of USB storage devices has been extensively reported in the press with cases such as the discovery of stolen U.S. military computer drives and USB thumb drives showing up for sale at local bazaars outside the base in Afghanistan (Myers, 2006). One of the flash drives was reported to have held the names, photos and phone numbers of people described as Afghan spies working for the military and another drive, which was sold for US$40 held a number of military documents, marked "secret", which described intelligence-gathering methods and information. Another example is the report[i] of the loss of a USB stick by the Lothian Scottish NHS trust that contained letters with personal information relating to 137 patients that occurred in July 2008.

The subject of the secure removal of data was first addressed in a paper presented at a 1996 conference (Gutmann 1996) that discussed the subject of the secure deletion of data and a second paper by (Gutmann 2001) examined 'Data Remanence in Semiconductor Devices'. Another paper (Garfinkel and Shelat 2003) examined ways in which disks could be 'sanitized'. A paper by Olzak (Olzak 2006) examined the 'Fundamentals of Storage Media Sanitation' and highlighted some of problems associated with the removal of data from USB storage devices.

There has been significant publicity in recent years on the problem of identity theft and the topic of the protection of personal information. For the effective removal of data from computer hard disks, there have been an increasing number of suitable tools[1] available on the market, however little attention appears to have been paid to the problem of the USB Storage device. Given the concerns regarding personal information, together with the level of press coverage that the subject continues to receive and the capability to address the issue it is strange that the apparent level of awareness of the potential problems related to the disposal of computer media remains poor.

For those USB Storage devices that have originally been for personal use, the survey results are perhaps not surprising. The devices are used for the storage of music, photographs and other, often small items of information that the user will not necessarily consider to be significant. It is only when the individual items of information are combined that they gain additional value and sensitivity. This results in the user not being aware of the overall value of the information that may be stored on their USB Storage devices. When the same type of USB Storage device and indeed in many cases the same actual device is used to transfer and store data from the corporate network it can result in data being stored on devices over which the corporate organisation has no control. It was noticeable on a number of the USB Storage device that there was a combination of corporate and personal data.

CONCLUSION

The issue of the use and subsequent disposal of USB Storage Devices will continue to be a security problem. The results of the survey demonstrate that the problem is widespread and that, for the samples that were tested, there was an almost total failure to effectively dispose of the information that was contained on the USB Storage Devices. A number of the USB Storage Devices were found to contain sensitive corporate or personal information. The potential effect of the failures to remove sensitive data is that this type of information continues to be available to anyone that might seek to exploit it. There is an ongoing requirement for organisational awareness, education and training programmes for appropriate staff to ensure that the use of USB Storage Devices is properly managed and that the data that they contain is effectively protected and then removed before their disposal. For the home user there is a requirement for education and awareness of the potential dangers that may occur when they dispose of USB Storage Devices and the measures that can be taken to effectively remove the data and avoid potential damage.

---

[1] Such as the Blancco tool which is approved for use by the UK Government.

RECOMMENDATIONS

There are a number of measures that organisations and individuals can take to reduce the volume of sensitive information that is inadvertently given away when USB Storage Devices are disposed of. These, in brief, are:

1. **Education -** A public awareness campaign by Government, the media, commerce and/or academia.

2. **Risk Assessment -** Organisational risk assessments to determine sensitivity of the information that may be stored on USB Storage Devices.

3. **Best Practices -** The introduction within organisations of procedures to ensure that USB Storage Devices are disposed of in an appropriate manner.

4. **Roles and Responsibilities** – assign the roles and responsibilities to those charged with issuing, managing and and recovering USB Storage devices.

5. **Physical Destruction -** Where appropriate, the physical destruction of the USB Storage Devices.

6. **Data Erasure** – Provide access to the tools and facilities to enable individuals to effectively remove the information from their USB Storage Devices.

7. **Encryption -** The encryption of USB Storage Devices to ensure that information can not be easily recovered in the event of their loss, theft or disposal.

REFERENCES

Condon, R., (2008), Scottish NHS trust ensures no repeat of USB data loss, *http://searchsecurity.techtarget.co.uk/news/article/0,289142,sid180_gci1337955,00.html* (accessed 10 Oct 2009)

Garfinkel, S., and Shelat, A., (2003), "Remembrance of Data Passed: A Study of Disk Sanitization Practices," *IEEE Security and Privacy*, January/February 2003

Green, C., (2008), BBC dragged into child data loss incident, *ITPro*, 08 August 2008, *http://www.itpro.co.uk/605319/bbc-dragged-into-child-data-loss-incident* (accessed 10 Oct 2009)

Guttman, P., (1996), Secure Deletion of Data from Magnetic and Solid-State Memory, *Sixth USENIX Security Symposium Proceedings, San Jose,* California, 1996

Guttman, P., (2001), Data Remanence in Semiconductor Devices, *Usenix Security 2001 paper,* http://www.usenix.org/events/sec01/full_papers/gutmann/gutmann_html, (accessed 10 Oct 2009)

Jones, A., Mee, V., Meyler, C., and Gooch, J,(2005), Analysis of Data Recovered From Computer Disks released for sale by organisations, *Journal of Information Warfare*, (2005) 4 (2), 45-53.

Jones, A., Valli, C., Sutherland, I., and Thomas, P,(2006), The 2006 Analysis of Information Remaining on Disks Offered for Sale on the Second Hand Market, *Journal of Digital Forensics, Security and Law*, (2006) 1 (3), 23-36.

Jones, A., Valli, C., Sutherland, I., and Dardick, G., (2008), The 2007 Analysis of Information Remaining on Disks Offered for Sale on the Second Hand Market, *International Journal of Liability and Scientific Enquiry 2009 - Vol. 2, No.1 pp. 53 – 68.*

Jones, A., Valli, C., Sutherland, I., Dardick, G. Davies G., (2009), The 2008 Analysis of Information Remaining on Disks Offered for Sale on the Second Hand Market, *Journal of International Commercial Law and Technology*, Vol. 4, No 3 (2009a)

Kehrer, O., (2007), Data Data Everywhere, *O and O Software*, September 2007

Myers, L., (2006), Stolen military data for sale in Afghanistan, *NBC News Investigative Unit*, 13 April, 2006

Olzak, T., (2006), Fundamentals of Storage Media Sanitation, *http://www.usenix.org/events/sec01/full_papers/gutmann/gutmann_html* (accessed 10 Oct 2009)

Winnett, R., (2008), Home Office loses confidential data on all UK prisoners, *Daily Telegraph*, 21 August 2008

COPYRIGHT