1-1-2011

A 2011 investigation into remnant data on second hand memory cards sold in Australia

Patryk Szewczyk
Edith Cowan University

Krishnun Sansurooah
Edith Cowan University

DOI: 10.4225/75/57b3ab8ffb85d
9th Australian Digital Forensics Conference, Edith Cowan University, Perth Western Australia, 5th -7th December 2011

A 2011 INVESTIGATION INTO REMNANT DATA ON SECOND HAND MEMORY CARDS SOLD IN AUSTRALIA

Patryk Szewczyk and Krishnun Sansurooah
secau Security Research Centre, School of Computer and Security Science
Edith Cowan University, Perth, Western Australia
p.szewczyk@ecu.edu.au; k.sansurooah@ecu.edu.au

Abstract

The use of memory cards is widely used in numerous electronic devices including tablet computers, cameras, mobile phones and multimedia devices. Like a USB drive, memory cards are an inexpensive and portable persistent storage solution. Numerous manufactures are incorporating a memory card interface into their product, allowing for a large array of confidential data to be stored. This research aimed to determine the sensitivity, type and amount of data that remained on second hand memory cards post sale. In 2011, over an eight month period, 119 second hand memory cards were randomly purchased from eBay Australia. The findings from the research show that individuals utilise memory cards to store highly sensitive and confidential data, and as per similar previous studies, continually neglect to permanently destroy the data prior to sale.

Keywords

Digital forensics, memory cards, flash memory, remnant data

INTRODUCTION

A memory card regardless of its format (Compact Flash, SD Card etc.) is inexpensive, versatile and used in many modern electronic devices. The data on a single memory card may be shared, accessed and modified on many different devices such as a digital camera, smart phone, tablet computer or portable media player. Sony, SanDisk and Samsung have all recognised the market benefits of incorporating a memory card interfaces in all of their devices and have used this feature in many marketing and promotional material (Liu, Kemerer, Slaughter & Smith, 2012). Some devices may incorporate different sized memory card interfaces such as standard, mini or micro. Manufactures have solved this issue by releasing adapters allowing a microSD to be used as a miniSD card through the appropriate converter.

There is significant speculation that tablet computer sales will outnumber traditional notebook and desktop computer sales by 2015 (Tofel, 2010). Being highly portable, battery efficient, cheap, and capable of undertaking many of the tasks of a low-end computer, there is significant incentive for the average end-user to purchase a tablet computer. Countering the storage limitations of many tablet computers, manufactures have incorporated memory card interfaces allowing the device to have its persistent secondary storage upgraded by simply using a memory card. In a similar manner, smart phone manufactures allow end-users to upgrade the storage capacity through the use of a memory card. This creates an issue in that end-users may begin using memory cards as external storage devices, and store private and confidential data on the memory card. The memory cards being small and easily concealed may be subjected to theft and other malicious activity.

Research into the types of data end-users leave on disposed of storage media has been an ongoing issue. Valli (2004) identified and confirmed that there was an issue with the way in which organisations disposed of hard disks. Medlin and Cazier (2010) further validated that corporations who disposed of workstations neglected to remove confidential data from their computers. Mobile phones continue to be sold as a second hand items with private data intact (Glisson, Storer, Mayall, Moug & Grispos, 2011), and little has improved in the area of secure USB flash drive disposal (Jones, Valli & Dabibi, 2009). Subsequently one could speculate that similar trends would be present with end-users leaving confidential data intact on second hand memory cards sold in Australia. This study investigates if memory cards sold on second hand auction sites would also contain private and sensitive data.

RESEARCH PROCEDURE

Over an eight month period, 119 second hand memory cards were procured and analysed, providing a representative view of remnant data on memory cards in Australia. All of the memory cards were purchased through the second hand auction site eBay – Australia. Memory cards were located and purchased in each of the

eBay categories of mobile phones, cameras and portable devices. For the purpose of this research a second hand memory card constitutes an item in which the seller on eBay claims that it has previously been used, and has subsequently listed the item as 'used'. All memory cards were purchased individually. The final breakdown of the types of memory cards that were procured are presented in Table 1.

Table 15 Quantity of each type of memory card procured

Memory Card Type	Quantity Purchased
microSD Card	64 (55%)
miniSD Card	4 (3%)
SD Card	13 (11%)
Memory Stick Pro Duo	8 (6%)
M2 Card	18 (15%)
Compact Flash Card	12 (10%)

The purchasing of memory cards was undertaken by numerous individuals, thus minimising the possibility of the sellers detecting that any form of research was being undertaken. This was done to ensure that the seller did not take additional precautions to remove data from the card. Surprisingly the number of second hand memory cards on eBay was not as high as had been anticipated. The researchers continually monitored the quantity of second hand memory cards listed on eBay. During the eight month time period approximately ninety-six percent of all memory cards listed by sellers were purchased from eBay. The storage capacity of each of the cards varied and a depiction of sizes is presented in Table 2.

Table 16 Size and quantity of memory cards

Size of Memory Card	Quantity
32 MB	1 (1%)
64 MB	9 (8%)
128 MB	13 (11%)
256 MB	9 (8%)
512 MB	19 (16%)
1 GB	38 (32%)
2 GB	26 (22%)
4 GB	3 (3%)
8 GB	1 (1%)

The research methodology leveraged the tools and techniques used in previous similar studies undertaken on hard disks and USB drives (Jones, Valli & Dabibi, 2009; Valli & Woodward, 2008). As a result, the imaging of each memory card was undertaken by using the freely available software Access Data Forensic Toolkit Imager 3.0.1 (FTK Imager, 2011). Recovery and analysis was subsequently undertaken through the WinHex 15, *File Recovery by Type* function (Reischmann, 2011) and the analysis tool Autopsy 3.0.0b1 (Carrier, 2011). For each case, a note was made as to whether any attempt had been made to delete, format or wipe the memory card. If data was recovered, then each element was investigated to determine its potential level of sensitivity to its owner.

The research aimed to uncover whether sellers would ship a memory card with data intact. Secondly, should data be present the research aimed to evaluate how sensitive the information is. Warnings are provided by eBay (eBay, 2011) regarding the possibility of data remaining on digital media when an item is sold. Various online and print media publicity has been given to individuals and organisations (Lee, 2011; Moscaritolo, 2010) who dispose of storage media in an insecure manner, resulting in leaked private and confidential data. Despite these warnings, it was assumed that sellers would continue to be negligent in wiping the memory cards prior to shipping.

MEMORY CARD ANALYSIS RESULTS

Seventy-five percent (89) of the memory cards had their data deleted and/or formatted, which is significant in that in a previous USB drive study (Jones, Valli & Dabibi, 2009) only forty-six percent (20) had been formatted or deleted. Furthermore, twelve percent (14) of the memory cards were not recoverable and it would seem that the owner took the appropriate precautions to remove any data. Again, this is significant as this is higher when compared to the USB drive study which only had four percent (2) drives permanently wiped. The remaining

thirteen percent (16) of memory cards were purchased with all data intact and no signs of an attempt by the seller to delete or wipe data. This makes it increasingly easy for an individual to view and use private data, had they been the winning bidder for the item.

Table 3 presents the breakdown of the types of information that were recovered from the 119 memory cards. Unsurprisingly, there was an abundance of photos found on the memory cards. The photos were expected as a common use of memory cards is often associated with photographic devices. The second highest information type recovered on the memory cards analysed were resumes. It would appear appropriate to have a resume conveniently stored on a memory card which is carried with mobile phones or tablet computers, as this can always be sent or provided to an individual in a timely manner upon request.

Table 17 Types of information recovered by memory card quantity

Information Types Recovered	Number of Cards
Photographic images	78 (66%)
Resumes	18 (15%)
Sexualised images	11 (9%)
Business cards (e.g. vCard)	11 (9%)
Banking documents	9 (8%)
Social networking credentials	8 (7%)
Government documents	8 (7%)
Legal documents	6 (5%)
Pornography	4 (3%)
Tertiary institution documents	4 (3%)
Hospital/medical documentation	2 (2%)

The notable information types recovered from the memory cards has been shown below. The case numbers reflect the order of analysis and do not in any way reflect the purchasing order or type of data that had been recovered. In total the authors' identified nine highly notable cases, where there was sufficient data to cause significant damage or misuse of data, to the individuals and companies.

- Case 13 contained two separate PDF documents, with each one containing a copy of a driver's license of an individual including their full name, address, and date of birth. In addition photos showing the driver standing next to a clearly identifiable luxury car with the registration plates visible.

- Case 14 encompassed recent real estate settlement documents. Specifically these included the names, addresses and purchasing information of a property in Australia. Copies of bank deposit cheques were scanned and stored as PDF files.

- Case 29 appeared to belong to an individual who worked in a legal firm and included a personal resume. Included were sixty-eight business cards stored as VCF files. Within these business cards were names, addresses, phone numbers and notes regarding lawyers, law enforcement personnel, and other notable individuals in Australia.
- Case 43 contained hundreds of tax receipts dating back to 2008. In addition, there were Australian bank statements (with transactions exceeding $100,000), loans applications, and employee payslips. A spreadsheet was present containing the names, addresses and banking details for employees of a company. The name of the company to which the data belonged was clearly visible and consistent on numerous documents. Numerous documents from banks, financial brokers, legal firms and debt collectors were present on the memory card.
- Case 47 contained PowerPoint presentations, budgets, and proposals for a Government department. Based on the documents present on the memory card it appeared that the department was applying for funding for research projects.

- Case 48 contained hundreds of photographic images of an office party at a large technology firm. As the images numerically progress they clearly showed the name of the company and progressively resulted in exposed photos of employees towards the end of the night.

- Case 82 may have belonged to an electrical engineering firm with schematics and software source code for an upcoming Australian project. Encompassed amongst the files were budgets and schedule charts for the upcoming project. The company could be identified via the letter head documents which appeared to be sent to clients.

- Case 88 contained photos of a family vacation. Whilst not seeming out of the ordinary initially, a number of the photos contained photos taken with a camera of the individual's passports and ticketing information. Whilst this may be a security precaution for the family in case the documents were lost or stolen, it may also harm the family if it were acquired from the memory card and used in an inappropriate manner.
- Case 30 and 104 belonged to tertiary students. The memory cards stored variations of multimedia, assignment files, enrolment forms and photos. In both cases there was sufficient information to accurately identify the students and potentially use the information for malicious purposes.

Surprisingly eleven of the memory cards encompassed at least one suggestive image with the individual's face clearly visible. This is quite concerning given that in each case there was sufficient data on the memory card to identify the individual via name and address. This trend may further continue with a recent studying revealing that two-thirds of adults and teenagers happily engage in sexting and perceived it as a normal part of a relationship (Henderson, 2011). There are social consequences associated with this behaviour, and with a lack of awareness end-users may fall victim to their images being used against them in a harmful manner.

The results presented in this paper strongly align with those presented in similar (Jones, Valli & Dabibi, 2009; Valli & Woodward, 2008) studies whereby end-users continue to dispose of persistent storage media in an insecure manner. In eighteen of the cases there was sufficient information (through the recovered resume) to identify the individual and potentially use this information to commit fraud. The large quantity of acquired bank related information is a worrying factor which coincidently aligns with one of the top reported crimes in 2010 of financial fraud (IC3, 2011).

CONCLUSION

Many of the memory cards had data which was both personal and organisational based. Subsequently, organisations must take a greater effort to take the proper procedures prior to disposing of persistent storage media. The larger issue emerging from this study was the price at which sellers were disposing of the memory cards. The average price per gigabyte was approximately seven dollars, yet the value of the data present was substantially higher.

The second hand auction site eBay introduced warnings to sellers regarding the possible dangers of leaving personal data on electronic media. The results from this study show that these techniques are quite ineffective or are being overlooked by sellers. To further compliment the warnings, second hand auction sites could provide simplistic step-by-step procedures educating end-users as to how properly remove data. Making sellers aware may encourage them to take action, but without proper instructions end-user may continually be under the belief that deleting or formatting a memory card is permanently erasing data.

There is significant avenue to repeat the research in subsequent years and extend the sample size internationally, thus investigating if the trends continue or improve as more publicity is given to the area of remnant data. Further research needs to be undertaken into educating end-users of the dangers of disposing of their storage devices in an insecure manner. This issue appears to be repeating itself regardless of the actual medium used. The warnings and publicity seem to be having little impact on end-users poor habits. Lastly, there is a vast amount of both commercial and freeware tools for removing data from memory cards. End-users may in fact be using tools to remove their data, but the quality of tools may be far from adequate in removing private data.

REFERENCES

Carrier, B. (2011). The Sleuth Kit. Retrieved August 20, 2011, from http://www.sleuthkit.org/autopsy/download.php

eBay. (2011). Advice for selling mobiles phones safely on eBay. Retrieved January 20, 2011, from http://pages.ebay.co.uk/buy/guides/mobile-phone-advice/#1

FTK Imager. (2011). Forensic Toolkit Imager. Retrieved Auguest 11, 2011, from http://accessdata.com/support/adownloads#FTKImager

Glisson, W. B., Storer, T., Mayall, G., Moug, I., & Grispos, G. (2011). Electronic Retention: What does your mobile phone reveal about you? International Journal of Information Security.

Henderson, L. (2011). Sexting and Sexual Relationships Among Teens and Young Adults. McNair Scholars Research Journal, 7(1), 1-9.

IC3. (2011). Internet Crime Complaint Centre - 2010 Internet Crime Report. Retrieved September 4, 2011, from http://www.ic3.gov/media/annualreport/2010_IC3Report.pdf

Jones, A., Valli, C., & Dabibi, G. (2009). The 2009 Analysis of Information Remaining on USB Storage Devices Offered for Sale on the Second Hand Market. Paper presented at the 7th Australian Digital Forensics Conference, Edith Cowan University, Perth, Western Australia.

Lee, K. (2011). The Dangers of Second Hand Hard Drives. Retrieved September 19, 2011, from https://www.infosecisland.com/blogview/16105-The-Dangers-of-Second-Hand-Hard-Drives.html

Liu, C., Kemerer, S., Slaughter, S., & Smith, M. (2012). Standards Competition In the Presence of Conversion Technology: An Empirical Analysis of the Flash Memory Card Market. Working Paper.

Medlin, B. D., & Cazier, J. A. (2010). A Study of Hard Drive Forensics on Consumers' PCs: Data Recovery and Exploitation. Journal of Management Policy and Practice, 12(1), 27-35.

Moscaritolo, M. (2010). Security risk to office equipment disposal. Retrieved April 20, 2011, from http://www.adelaidenow.com.au/business/security-risk-to-office-equipment-disposal/story-e6fredj3-1225877502647

Reischmann, S. (2011). X-Ways Software Technology. Retrieved March 23, 2011, from http://www.winhex.com/winhex/

Tofel, K. C. (2010). 3 Reasons Tablets Will Take 1 in 4 PC Sales By 2015. Retrieved September 18, 2011, from http://gigaom.com/mobile/3-reasons-tablets-will-take-1-in-4-pc-sales-by-2015/

Valli, C. (2004). Throwing Out the Enterprise with the Hard Disk. Paper presented at the 2nd Australian Digital Forensics Conference, Esplanade Hotel in Fremantle, Western Australia.

Valli, C., & Woodward, A. (2008). The 2008 Australian study of remnant data contained on 2nd hand hard disk: the saga continues. Paper presented at the 6th Australian Digital Forensics Conference, Edith Cowan University, Perth, Western Australia.