Edith Cowan University
Research Online

Australian Digital Forensics Conference | Security Research Institute Conferences

2007

Oops they did it again: The 2007 Australian study of remnant data contained on 2nd hand hard disks

Craig Valli
Edith Cowan University

Andrew Woodward
Edith Cowan University

Originally published in the Proceedings of the 5th Australian Digital Forensics Conference, Edith Cowan University, Perth Western Australia, December 3rd 2007.
This Conference Proceeding is posted at Research Online.
http://ro.ecu.edu.au/adf/12

Oops they did it again: The 2007 Australian study of remnant data contained on 2nd hand hard disks

Dr. Craig Valli[1]
Dr. Andrew Woodward[2]
School of Computer and Information Science
Edith Cowan University, Perth, Western Australia
c.valli@ecu.edu.au[1]
a.woodward@ecu.edu.au[2]

ABSTRACT

The 2007 study used a biased selection process where the primary focus was the purchase of high-speed SCSI drives and drive packs, in addition 2.5 inch laptop drives were targeted. Conventional IDE based hard drives were also examined in the study. A total of 84 drives were examined this year, 23 yielded data that represented significant and in some cases profound exposure if data. Encouragingly more hard disks were erased in this study than in previous studies. However, there is still a significant gap in erasure procedures in organisations, which is particularly concerning given that the drives were from large corporations.

Keywords

Hard disks, forensics, erasure, enterprise drives

INTRODUCTION

The Australian study this year used a biased selection process where the primary focus was the purchase of high-speed SCSI drives and drive packs, with 2.5 inch laptop drives also targeted. This was done with the intent of building a profile of large corporate and government sources and essentially this was achieved as an outcome. In addition, USB memory sticks were also targeted this year although there were only three able to be purchased and analysed in the study. The sources for the hard disk drives were a mixture of national on-line auctions and also traditional face to face auctions in the metropolitan area of Perth, Western Australia.

The research of the disks was again undertaken using only tools that achieved the same effect that it was considered would be available to anyone who had obtained such disks. Should the hard disk not boot in suitable hardware, tools were used which carried out the same functions as the Windows Unformat and Undelete commands. In these cases a hex editor was also used to view any information that existed in the unallocated portion of the disk. The Helix CD was utilised in the analysis, and in particular the Foremost file carver (Foremost 2007) and Autopsy the forensic browser (Sleuthkit 2006) were used in the analysis phase of disks that had been formatted.

As with previous years (Valli, 2004; Valli & Jones, 2005; Jones 2006), the first objective of the research was to determine whether there was any information on the disk that was readily recoverable with the tools identified above. The second stage of the research was to look for specific elements of information that would allow for the identification of the organisation or individual that had used the disk. Further, and, if possible, information such as the usernames, email addresses or documents, spreadsheets and data types of interest were examined. The purpose of this phase of the research was to determine the proportion of the disks that could be traced to an organisation or an individual and the level of exposure that data recovered would represent.

OVERALL TRENDS UNCOVERED IN THE RESEARCH

Overall in the study once again a lack of pornographic material was uncovered given the hyperbole and claims made by some parties with respect to the use of the Internet to access this material. There was one standout case of a 40GB drive that contained over 8000 images of hardcore pornography. It had no other material on the drive at all, and would appear to have been used as a slave drive for storage of such material. Unlike the 2006 study, there were no detected cases of child pornography in any of the analysed hard disks from Australia.

A high percentage of the examined hard disks that yielded data contained significant personal and corporate exposure of confidential and commercial information. This year, however, did see an increase in the amount of competently erased hard disks. This could be a reflection of the fact that many of the hard disks were from

organisations with the ability and resources to erase the hard disks. Potentially also with many of the disks coming from servers, there may be a recognised need to erase these before disposal.

SIGNIFICANT CASES OF INTEREST

Case15-16AU these were unformatted 9 GB Sun SCSI hard disks that contained information from a major international merchant bank and stockbroking firm. The disk of Case16 had a last access date on the hard disk of July of 2006. The hard disk contained computer account details, VPN connection details and other password files. In the hard disks also contained sensitive network information that could be used to perform reconnaissance or attack these networks. One of the hard disks also contained information that indicated it mounted large disk arrays. What was of even greater alarm was the fact that these hard disks readily booted when installed in appropriate Sun server hardware. The partitioning configurations of the hard disks concerned indicated that they were primary operating system drives in servers from which they were extracted.

Case17-AU This was a 1 GB USB storage stick this was found to contain digital family photos, as well as tourist pictures of Sydney Harbour. In addition to these amateur shots were high-quality stock photos of a range of commercial cleaning products. The high-quality stock photos were small in file size and overall size it could be reasonably deduced they were most probably produced by a web designer.

Case18-AU was a 256 MB USB storage stick that contained only a collection of children's stories and obvious class assignments.

Case23-AU A formatted laptop hard drive from a senior academic in Information Systems school within an Eastern States based Australian university. The hard drive itself not only had the expected student results and communications but also as a result of the academic's position in the school contained confidential minutes of departmental meetings, strategic planning and course development initiatives being undertaken. In addition, the material included confidential information on staff and covered for example a sensitive ongoing industrial relations issue with one of the staff members.

Case24-AU Another 20 GB laptop hard drive appeared initially to be blank because the first areas of the drive appeared erased and in fact it was out to the 8 GB limit, the remainder of the hard drive was not. It would be reasonable to assume that the utility being used to erase the hard disk did not go beyond 8 GB limit either because it was a trial version of software or was faulty with respect to the 8 Gbyte limit on hard drive size. The hard drive still yielded confidential documents and personal information from the remainder of the hard drive.

Case25-AU This case was a unformatted 36GB SCSI hard drive from a Queensland Real Estate agent. The hard disk contained a wide range of confidential documents that would relate to real estate based transactions these included the were not limited to bank account details, credit card details, eviction notices, rent arrears notices, property sale and transfer details with the appropriate signatories to effect same. There was also a limited amount of hardcore pornographic pictures contained on the hard disk. The index.dat file upon review indicated frequent surfing of hardcore pornographic sites in addition to standard business-related activity.

Case28-AU This was a formatted hard drive from a medical provider. It contained personal medical records, including addresses, next of kin, phone numbers and other data that would be contained in a medical record. In addition, there were letters to patients, credit card and banking details of the patients as well contained on the hard disk drive. This case represented significant exposure of patients personal and financial details.

Case29-AU This was unformatted hard disk containing a 60GB NTFS partition from a religiously devout household due to the profile of web sites visited by various members of the family. There was no data of commercial nature found on the hard disk. However it, would appear that a young adult male in the house shaves their pubic regions and takes digital pictures of their erect penis for distribution via the Internet. This was substantiated by family photos found on the hard disk where the young adult male was featured clothed.

Case34-AU this was a 18 GB hard drive recovered from an accounting firm. In addition to a large number of accounting files, there were only thumbnails of pornography and other non-business related browsing present. There were personal digital photographs (wedding), some personal documents and business based form letters were also recovered. There was a large number of password protected PDF files on the hard drive no attempt was made to break the cryptography on these files due to time constraints. However, there are tools that can be used to readily extract these PDF files (REF)

Case54-AU This hard drive was a 18GB SCSI mechanism that contained Adobe Acrobat PDF files with names and addresses, vehicle types, registrations, vehicle identification numbers and policy expiry dates for a motor vehicle insurance company. There were also large ZIP archive files with large amounts of information on many policy holders, and these also contained customer invoices as well expired policy notices. This is a significant exposure on several levels not only could these details be used to commit fraud but also allow a car thief to readily target selected high value cars for theft. The vehicle identification numbers and other details could also

be useful for individuals who steal and re-birth high value or high performance cars which is an increasing trend of criminality.

Case 64 -AU This was a RAID SCSI hard disk pack, the devices were clearly marked as coming from a government based superannuation provider. This had significant exposure of confidential and sensitive information members details and statements in addition to letters of correspondence about members details. This case combined with the previous case has been the worst and most significant exposure of confidential data uncovered by the authors in 3 years of research.

Case70 This case was a pack of unformatted U160 73G SCSI drives purchased on eBay. The drives were less than 1 month old and contained data indicating that they were from a large multi-national mining company. The disks contained a large amount of corporate documents and would be problematic should they have fallen into the wrong hands for either profit through advantage or by fraudulent means. They disclosed operational procedures, purchasing details and other commercially sensitive information. It should be noted that these drives were advertised as coming from a large corporate customer in the sales promotion on eBay.

DISCUSSION OF RESULTS

Once again this study has uncovered significant and alarming levels of exposure from the incorrect and dilettante disregard for defunct data. This year the hard disks were targeted in such a way that it would be highly probable that they were from a corporate entity or significant business. By profile compared to previous studies (Valli, 2004; Valli & Jones, 2005; Jones 2006) conducted in Australia the extent and level of exposure this year has been the highest. A significant number of hard drives contained large volumes of sensitive data that could be used for any number of illegal activities including identity theft, fraud and theft. As an exemplar, the case of the insurance company policies that were recovered the details contained in these would allow for targeted direct theft of high value cars and re-birthing of same. Re-birthing involves the use of substitute Vehicle Identification Numbers to hide the identity of stolen cars and these details were in the policies uncovered. What is of alarm here is that reconnaissance etc that conventional criminals would have to undertake is no longer needed they simply had to extract the records and search for the required car and then drive to the registered address.

It is of considerable concern that so many enterprise level hard disks still contained recoverable data. Of greater concern is that some of this data was essential to the companies operations, and if made public could lead to significant civil and even criminal ramifications for the company. It seems unlikely that the organisations concerned would allow the disposal of such drives without adequate erasure having first been performed. This does beg the question of how is this occurring. The most likely explanation is that individuals within these organisations are using spare or decommissioned server drives as an alternate revenue stream for themselves. A number of the descriptions accompanying these drives on auction sites referred to the items as being surplus or never used and now unwanted. It could be speculated that the surplus or unused spare description is being used to allay any fears of buyers that the drives have been unlawfully obtained. It could also be safely deduced that organisations are failing to conduct adequate risk analysis of the issue of remnant data on secondary memory devices. If not, why are these drives appearing in auctions?

It is clear that public and private organisations across a range of industry sectors are failing to discharge their responsibility to protect customer's details and sensitive data adequately. There is no official mandated law or statute that requires organisations in Australia to erase secondary memory devices such as hard disk drives. Evidence such as that uncovered in this and previous studies surely should now see this being considered by governments. Failing a legislated approach to the problem the creation for government based organisations of a centralised clearance service for the destruction/safe erasure of secondary storage media.

It could also be safely deduced that organisations are failing to conduct adequate risk analysis of the issue of remnant data on secondary memory devices. It could not be similarly reasonably argued that the problem of remnant data is not a new or unknown phenomenon (Anonymous, 2003; de Paula, 2004; Duvall, 2003; Garfinkel & Shelat, 2003; Jones, 2006; Rohan, 2002; Spring, 2003; Valli, 2004; Valli & Jones, 2005; Valli & Patak, 2005).

The risk versus return equation is simply not making sense for any modern organisation or individual. Auctioneers and sellers of these hard disks are also unwittingly providing potential criminals with targeted options for purchase with advertising that clearly indicates that the devices are from financial institutions, superannuation boards, insurance companies to name a few. One has to ask what the provenance of these devices has to do with their suitability or value for use as storage mechanisms.

CONCLUSION

This year has again uncovered significant exposure of private, sensitive or fungible data on inadequately erased secondary memory devices. Organisations spend millions on protecting IT assets annually with firewalls, virus

protection, intrusion prevention systems and other security silver bullets. We argue that these expenditures are largely symbolic and almost supercilious when hard disks are disposed of without adequate protections.

This study and others have found equally as serious exposures of data by the Small Office Home Office (SOHO) user. Likewise the SOHO user will typically purchase a virus package, use a firewall and have maybe a spyware detector but rarely is any mention ever made about safe disposal of secondary storage. The SOHO user is somewhat at the mercy of manufacturers of operating systems and hardware to enable secure erasure but one has to ask how hard is to have a "decommission" process or button that securely erases all secondary media on a computer that is about to be disposed of?

Education is one alternative but again government and policy makers have to be brought to task here. In Australia there have been massive media campaigns on the evils of drugs, or the perils of sharing unclean needles but no argument about for the need for this type of education. One has to ask where are the advertisements for reducing your risks about sharing unclean hard drives when in 2007 the world trade in cybercrime now exceeds US$ 105 billon (www.itnews.com.au, 2007)?

Finally, the most expensive hard disk purchased in this study was a 2.5" 40 GB laptop disk that cost $60. To juxtapose the commercial proposition, do government organisations and company boards see it a legitimate business practise to sell all corporate secrets, customer personal details or commercial sensitive information for $1.50 per gigabyte or less from their stop front? Yet this is exactly what is occurring today somewhere at an IT disposal sale or online auction in Australia.

REFERENCES

Anonymous. (2003). Computer castoffs. *American Bankers Association. ABA Banking Journal, 95*(4), 22.

de Paula, M. (2004). One Man's Trash Is... Dumpster-diving for disk drives raises eyebrows. *USBanker, 114*(6), 12.

Duvall, M. (2003). Memory Loss ; How a missing $100 pocket-sized drive spooked 825,000 customers of canadian companies. *Baseline, 1*(16), 65.

Foremost (2007) Foremost, retrieved 19th October 2007 from http://foremost.sourceforge.net/

Garfinkel, S. L., & Shelat, A. (2003). Remembrance of Data Passed: A Study of Disk Sanitization Practise. *IEEE Security and Privacy, 1*(1).

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, 1*(3), 23-36.

Rohan, R. (2002). The ghost of information past. *Black Enterprise, 33*(1), 47.

Sleuthkit (2006). Autopsy overview, retrieved 19th October 2007 from http://www.sleuthkit.org/autopsy/

Spring, T. (2003, May 2003). Hard drives exposed. *PC World, 21,* 22.

Valli, C. (2004). *Throwing the Enterprise out with the Hard Disk.* Paper presented at the 2nd Australian Computer, Information and Network Forensics Conference, Fremantle, Western Australia.

Valli, C., & Jones, A. (2005). *A UK and Australian Study of Hard Disk Disposal.* Paper presented at the 3rd Australian Computer, Information and Network Forensics Conference, Edith Cowan University, Perth, Western Australia.

Valli, C., & Patak, P. (2005). *An investigation into the efficiency of forensic erasure tools for hard disk mechanisms.* Paper presented at the 3rd Australian Computer, Information and Network Forensics Conference, Edith Cowan University, Perth, Western Australia.

www.itnews.com.au. (2007). Cyber-threats outpace security measures, says McAfee CEO - Security - www.itnews.com.au. Retrieved 12 November 2007, from http://www.itnews.com.au/News/61497,cyberthreats-outpace-security-measures-says-mcafee-ceo.aspx

COPYRIGHT

Craig Valli & Andrew Woodward ©2007. The author/s assign SCISSEC & Edith Cowan University a non-exclusive license to use this document for personal use provided that the article is used in full and this copyright statement is reproduced. The authors also grant a non-exclusive license to SCISSEC & ECU to publish this document in full in the Conference Proceedings. Such documents may be published on the World Wide Web,

CD-ROM, in printed form, and on mirror sites on the World Wide Web. Any other usage is prohibited without the express permission of the authors