2008

Industrial Espionage from Residual Data: Risks and Countermeasures

Iain Sutherland
University of Glamorgan

DOI: 10.4225/75/57b2771540cc2
Originally published in the Proceedings of the 6th Australian Digital Forensics Conference, Edith Cowan University, Perth Western Australia, December 3rd 2008.

Industrial Espionage from Residual Data: Risks and Countermeasures

Iain Sutherland
University of Glamorgan
isutherl@glam.ac.uk

Dr Andy Jones
Centre for Information & Security Systems Research, BT
SECAU – Security Research Centre, Edith Cowan University
andrew.28.jones@bt.com

Abstract
This paper outlines the possible recovery of potentially sensitive corporate information from residual data. It outlines previous work on the recovery of information contained on second hand hard disks and handheld devices and discusses the risk of individuals conducting industrial espionage by targeting specific organizations. It examines the possible avenues for an attacker to obtain a storage device, then discusses the skill level required to extract information from the storage devices and considers the potential risk to an organization from this particular avenue of attack. The paper concludes by proposing a number of possible countermeasures to enable organizations to reduce the risk of this particular form of attack.

Keywords
Industrial Espionage, Residual Data, Hand Held Device, Hard Disk Drive.

INTRODUCTION

In recent years there has been a massive migration of data from the paper based systems where issues of management and security were well understood to digital systems, where the management and control of data storage is less well defined. When the primary storage means for information was paper, the control of access to it, the storage of it and the disposal of it were well practiced processes; but these have not mapped easily into the digital domain. While there was leakage of corporate information through poor processes, accidents and oversights or malicious activity, the volume of information at risk was, in part, controlled by the sheer bulk of the medium.

The advent of the use of digital processing and storage has removed this constraint and it is now possible to store gigabytes of information on a single piece of magnetic or optical media. This coupled with the low cost and difficulty in controlling the storage media, has significantly increased the potential exposure of organisations. In this paper we address the issue of the risk to an organisation as the result of the disposal of obsolete storage and communication devices in the form of computers hard disk drives and handheld devices such as mobile telephones or RIM Blackberry devices.

The secure deletion of data from storage devices has been an issue of discussion for more than ten years (Gutmann 1996) and of some concern for those involved in data security (Garfinkel 2003). There have been a number of studies examining disk disposal practices; assessing the volume and type of residual data remaining on disks available on the second hand market (Garfinkel 2003, Sutherland *et al* 2006, Valli *et al* 2004, 2007). One such annual study currently collecting a fourth year of data has been sponsored by the Centre for Information and Security Systems Research at BT examining disposal practices in the UK, USA, Germany and Australia (Jones *et al*, 2005, 2006, and 2008a). This disk study project has been conducted in order to obtain an understanding of the amounts and types of information that remained on disks offered for sale on the second hand market through various channels including on-line auctions. Most of the studies undertaken to date have indicated that a proportion of these disks contain some residual data that was stored on the drive by the original owners. The study results have highlighted a number of interesting findings. One particular discovery of thestudy worthy of note was that in each of the annual sample sets of disks a significant number of corporate disks were recovered, some containing sensitive corporate data.

A separate, but related study, again sponsored by the Centre for Information and Security Systems Research at BT was focused on examining disposal practices for hand held devices in the UK, USA and Australia (Jones et al, 2008b). This study looked at mobile phones, RIM Blackberry devices and Personal Digital Assistants (PDAs). While the levels of data that were recovered were different, the handheld device study reflected underlying issues exposed during the disk studies.

STUDY METHODOLOGY

The methodology employed for both the disk study and the hand held device studies were very similar. In the case of the disk study, this involved the purchase of a sample set of disks. In the case of the current UK sample set for 2008, this was in the order of more than 140 disks obtained from computer fairs, computer auctions or via on-line auction sites. The disks were purchased discretely by a number of purchasers and were obtained for the most part either singly or in small batches. These disks were obtained by British Telecommunications (BT) Limited and then supplied 'blind' to the researchers responsible for the imaging and analysis with no indication of where they had been sourced and identified only by a unique sequential serial number and in some cases a manufacturer's label.

The disks were forensically analysed with the objective of determining whether data had been securely erased from the disks or whether they still contained information that was either visible or easily recoverable. If information was present on the disks, this was then examined to determine if it was sufficient to identify an organization or individual. The analysis methods and practices used followed forensic good practice procedures as defined in the Association of Chief Police Officers (ACPO) Good Practice Guide for Computer-Based Electronic Evidence1, with each disk being forensically imaged using commercial software and then stored in secure storage areas; the analysis being undertaken on the forensic images of the original disks. The research to date from the 2005, 2006, 2007 and current 2008 studies indicate that a large proportion of the disks examined still contained information pertaining to a previous owner of the disk, much of which could be considered of a sensitive nature to the organization or individual.

	2005	**2006**	**2007**
Total Number of Disks UK and Australia	116	253	300
Commercial Data Present	60 (70%*)	42 (47%*)	51 (40%*)

** Percentage of readable disks that had not been wiped*

Table 1: Commercial data present on disks in the 2005, 2006 and 2007 surveys (based on Jones 2007)

It was expected that a significant number of inexperienced home users, unaware of the process by which information was stored and removed from the drive, might have left data on a drive when disposing of a disk. However, surprisingly each year a number of business organizations also disposed of disks in an insecure manner. This occurs despite the fact that corporate organizations can be expected to have access to better advice (e.g. Price Waterhouse Cooper (2006)) and resources than the average home user, and that data losses have been discussed heavily in the popular media (AFPS 2006, BBC News 2005, Jenkins 2005, Kerber 2006, Leyden 2004, Vance 2006a, 2006b). Table 1 outlines the percentages of disks recovered containing commercial data. Table 2 outlines the breakdown across the various areas of the study comparing the results from the disks obtained in the different regions. In each of the regions, disks containing corporate data were found within the sample sets.

	UK	Australia	Germany	North America
Total No. of Disks Analyzed	133	79	42	46
Commercial data present	19 (41%*)	22 (46%*)	2 (29%*)	8 (35%*)
Individual data present	34 (74%*)	7 (15%*)	5 (71%*)	15 (48%*)

** Percentage of readable disks that had not been wiped*

Table 2: Disks containing corporate data across the different regions (based on Jones 2007)

The results of the hand held devices study (Jones et al, 2008b) summarized in Table 3 indicate that corporate data is being lost via this route, although this is currently limited due to the number of older 1G devices in circulation. The study showed that as 2G and 3G devices have come into common use within business and our personal lives, people have started to store significant volumes of data on these devices. While there are a number of factors that have contributed to this trend that require further study, these devices are now being offered for sale on the second hand market and many of them still contain significant quantities of information.

Category	Percentage
Broken or not accessible due to physical problem (dead battery – no suitable lead	*82 (51 %)*
Blank – all data removed	*37 (23 %)*
Encrypted	*7 (4%)*
SIM Present	*3 (2%)*
Identifiable to user	*14 (9%)*
Identifiable to organization	*19 (12%)*
Personal Data present	*14 (9%)*
Sensitive Corporate data present	*6 (4%)*
Number of Hand Held Devices Analyzed	*161*

Table 3: Breakdown of Results from hand Held Devices (from Jones 2008b)

This paper addresses the possibility that someone with a motive to make a profit from questionable practices, may deliberately target a commercial organization by seeking to obtain second hand media or devices. In order to achieve this goal, the individual intending to conduct the industrial espionage has to first obtain the disk or device and then also be competent to extract the data from it.

INDUSTRIAL ESPIONAGE

Industrial espionage in the high-tech environment may be either focused on gaining information relating to a particular organisation or may be a more general collection of useful corporate information that can be sold to interested groups or individuals. If the target is a specific organisation, then there will be a requirement for planning and reconnaissance to determine the best attack vector to gain the required information for the lowest investment in time and effort. If the industrial espionage is of an information brokering type, where information is collected and then sold on to interested parties, then it will be unfocussed with the primary aim of gathering as much information that may have value. The latter approach will have the greatest chance of success and be the easiest to undertake. During the disk and mobile device studies, there have been a number of noteworthy discoveries of corporate data that would have been of significant value to competitor organisations. These have included business plans that were less than three months old, profit and loss sheets for each of the elements of a large multinational organisation, detailed communications between a company and its customers dealing with product faults and remedial actions and the detailed advertising strategies for a large multinational corporation with proposed expenditures in millions of dollars.

OBTAINING THE DISK OR DEVICE

The disk and hand held device studies were both aimed at providing a generalized picture of the data available on the second hand market. They did not target a specific organization or type of organization. From the experience gained during the studies, obtaining the disk or device from a particular organization is likely to be the most difficult part of the process. If an organization takes steps to effectively remove data prior to the disposal of equipment, then this successfully denies an attack via this route. If the data has not been effectively removed, there are a number of possible avenues that an attacker could explore:

- Purchasing second hand disks or devices from a disposal company or reseller. If the organisation that has disposed of the disks or devices has put in place suitable arrangements with a competent re-seller, the disks or devices should have been wiped and there would be no data available. The 2005 disk study results highlighted one reseller that was merely formatting the disks as a method of removing the data and this has since been found to be relatively common practice. As a result the majority of data waseasily recoverable, leaving any company using its services open to this form of attack.

- Targeting the company directly, buying up second hard drives, complete computer systems or hand held devices under the guise of charity or a reseller. This could be achieved most effectively if acting as a disk disposal service as this would allow direct access to a selection of drives or devices from the organisation potentially containing corporate data.

- The above method could also be applied to target users to obtain old systems by offering users a secure disposal service. The disk study results in recent years have highlighted a blurring of personal and corporate data and it is most common to find elements of both on disks and devices. This could either be as a result of an increase in the use of corporate systems for personal use or the use of home systems to carry out work activities as a result of home-working.

If the industrial espionage was targeted at a specific organisation, the adversary would probably have to carry out a significant level of research to determine the processes and procedures in use by the organisation for the disposal of obsolete equipment. The adversary would also probably need to be well funded as the success rate for obtaining disks or devices from a specific organization is likely to be fairly low. One finding of the current 2008 study is that the imaging and analysis of SCSI drives resulted in data from a number of commercial system being recovered and the selection of this type of drive may be a used as an attack vector by an adversary.

Even if the adversary has obtained a disk or device from the target organization, it may not contain the type of information that they are seeking. It should be noted that the studies indicated that most corporate disks included a wide range of information: this could be in the form of internal contact details or items such as network configuration. Some of this information might be publically available, whereas other elements could be more sensitive and may, in addition to the damage caused by the exposure of the information also even facilitate some form of network attack.

EXTRACTING DATA OF VALUE

Once a disk has been obtained, the adversary will be interested in extracting any useful and useable data. This can require varying degrees of effort depending on whether an attempt has been made to remove data. If an attempt has been made to remove the data, this may not be a significant impediment to the adversary as there is a surprising amount of software available on the internet that has been developed for forensic analysis and data recovery which they can use to assist them in acquiring the data. There are cracked copies of both of the major forensic tools FTK (AccessData 2008) and Encase (Guidance 2008) in circulation. These are both powerful tools with a range of search utilities which enhance an adversary's ability to examine a drive for useful data. There are also a number of open source tools which can be used to 'carve' (recover) deleted files from unallocated space. This can be hampered by some file systems and if encryption has been used to protect the files it can prevent data recovery. The sampled set of disks and devices indicated that the majority of corporations either do not appear to encrypt their data, or use NTFS encryption which is not sufficient to prevent data recovery.

The actual extraction of the data requires some degree of understanding of the working of a computer hard disk or handheld device and the tools required to recover data from this type of device. Although these tools often require some technical knowledge, there is extensive information readily available on the web (Wikipedia 2008), in text books (Carrier 2005, Casey 2004) and in academic papers (Fragkos 2006) to guide a user. There are in the UK around 17 undergraduate degree courses teaching forensics and presumably data recovery techniques (UCAS 2008). There are also a number of shorter, commercial training courses.

COUNTERMEASURES

This form of attack is likely to be ineffective on an organization which disposes of data in a secure manner, although even then they will be exposed to human failures and subverted staff. The risk of this form of attack being successful can be reduced by employing the following countermeasures:

- Ideally data disposal should be retained as an in house function, but where this function is outsourced there should be an audit system in place to allow the disks or devices to be randomly checked to ensure the quality of the data disposal process.

- Disk and device disposal services should be offered to employees for their home systems to ensure the company is protected against inadvertent data loss via an employees system due to an employee working on their home system. The incentive could be the protection offered to the employee's personal data.

- Encryption is an effective measure for preventing this form or recovery, subject to the limitationsrelating to strength of the encryption and the security of the key.

- Software to allow employees to access work systems from home should ensure a secure work space to prevent residual data being left on home systems.

- A company should understand the risk in terms of what may reside on a corporate disk by carrying out some form of internal review on residual data on a sample of corporate disks.

- Corporate systems should be purged of data if they are to be reused within the organization to prevent the build up (aggregation) of sensitive data on a drive or device.

- Technological solutions can be used to tamper-proof disks and devices or ensure data is wiped if theyare used in an unauthorized manner.

SUMMARY

This paper discusses the risks of an attacker successfully obtaining corporate data from an incorrectly disposed computer disk or hand held device. This paper describes some of the types of information which might be found and raises the question as the skill set and requirements that would be required by individuals to obtain useful data.

It is acknowledged that the risk of a successful attack via this method is limited, in that the adversary would have to be relatively well funded if there was a specific organizational target and that the hit rate for a specific organization depends on the type of disk or device obtained from the organization and the disposal practices in place.

ACKNOWLEDGEMENTS

The authors would like to acknowledge the generous sponsorship of British Telecommunications (BT) who support the disk and hand held device studies each year. In addition to the authors of this paper, we would like to acknowledge the other researchers who participated in the 2007 and previous disk studies and our colleagues at Edith Cowen (Australia), Longwood (United States of America) and Glamorgan (United Kingdom) Universities.

REFERENCES

AccessData (last visited September 2008) www.accessdata.com

American Forces Press Service (2006), *Current Service Members Possibly Affected by VA Data Loss*, 6 June 2006.

Association of Chief Police Officers Good Practice Guide for Computer-Based Electronic Evidence. http://www.7safe.com/electronic_evidence/ACPO_guidelines_computer_evidence.pdf

BBC News (2005), *Data dangers dog hard drive sales*, BBC, 12 September 2005.

Carrier B, (2005) *Forensic File System Analysis,* Addison Wesley.

Casey, E., *(*2004) *Digital Evidence and Computer Crime; Forensic Science, Computers and the Internet,* Academic Press, Second Edition.

Guidance Software (last visited September 2008) www.guidance.com

Fragkos G. et al (2006) *An empirical methodology derived from the analysis of information remaining on second hand hard disks* in Blyth A., and Sutherland I., *WFDIA Proceedings of the first Workshop in Digital Forensics and Incident Analysis*

Garfinkel S.L, Shelat A, (2003), *Remembrance of Data Passed: A Study of Disk Sanitization Practices.* IEEE Security & Privacy, Vol. 1, No. 1, 2003.

Gutmann, P. (1996), *Secure Deletion of Data from Magnetic and Solid-State Memory, Sixth USENIX Security Symposium Proceedings*, San Jose, California, July 22-25, 1996.
Jenkins, C. (2005), *Govt data sent to auction*. The Australian, 2nd August 2005.

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., Thomas P. (2006) *An Analysis of Information Remaining on Disks offered for sale on the second hand market.* Journal of Digital Security, Forensics & Law. Volume 1, Issue 3.

Jones A, Dardick G., Sutherland I, Valli C., (2008a) *The 2007 Analysis of Information Remaining on Disks offered for sale on the second hand market*. Journal of Digital Security, Forensics & Law. Volume 3, Issue 1.

Jones A., Valli C., Sutherland I, (2008b) *Analysis of Information remaining on Hand Held Devices offered for sale on the second hand market.* Journal of Digital Security, Forensics & Law. - *In Press*

Kerber R (2006), *Firm will settle with state over data loss: Missing laptop had information on thousands*, Boston Globe, 12 December 2006.

Leyden, J. (2004), *Oops! Firm accidentally eBays customer database*, The Register, 7 June 2004.

Price Waterhouse Cooper (2006), *DTI Information security breaches survey* 2006, http://www.dti.gov.uk/industries/information_security Sept 2006.

Sutherland I, and Mee V. (2006) *Data Disposal: How educated are your Schools?*, 6th European Conference on Information Warfare and Security, June 2006.

UCAS – The Universities Central Administration System (last visited September 2008). www.ucas.com

Valli, C. (2004), Throwing out the Enterprise with the Hard Disk, In 2nd Australian Computer, Information and Network Forensics Conference, We-BCentre.COM, Fremantle Western Australia.

Valli C. & Woodward A., (2007) *Oops they did it again: The 2007 Australian study of remnant data contained on 2nd hand hard disk* Presented at the 5th Australian Digital Forensics Conference, Edith Cowan University Australia.

Vance A (2006a), *Ernst & Young fails to disclose high-profile data loss: Sun CEO's social security number exposed*, The Register, 25 February 2006.

Vance A (2006b), *Wells Fargo fesses up to data loss: Lightning strikes twice for HP man*, The Register, 12 May 2006**.**

Wikipedia - pages on forensics and data recovery (last visited September 2008)
http://en.wikipedia.org/wiki/Computer_forensics, http://en.wikipedia.org/wiki/Data_recovery

COPYRIGHT