2005

A UK and Australian Study of Hard Disk Disposal

Craig Valli
Edith Cowan University

Andrew Jones
Edith Cowan University

This is an Author's Accepted Manuscript of: Valli, C., & Jones, A. (2005). A UK and Australian Study of Hard Disk Disposal. Proceedings of 3rd Australian Computer, Network and Information Forensics Conference. (pp. 74-78). Perth, Western Australia. School of Computer and Information Science, ECU.
This Conference Proceeding is posted at Research Online.
https://ro.ecu.edu.au/ecuworks/2763

A UK and Australian Study of Hard Disk Disposal

Craig Valli
Edith Cowan University
School of Computer and Information Science
c.valli@ecu.edu.au

Andy Jones
British Telecom Labs
Edith Cowan University Adjunct
School of Computer and Information Science

Abstract

Recent studies in Australia and the United Kingdom indicate that a broad cross-section of organisations are failing to adequately protect or erase confidential data stored on hard disk drives before subsequent disposal. Over 90% of hard disks that were examined as a result of the two Independent studies were in an easily recoverable state with some drives simply requiring a boot. This paper will give an overview and comparison of the two studies conducted. Then an examination of possible factors responsible for the inadequate erasure of hard disk devices will be undertaken. Furthermore, possible future research directions will also be explored

Keywords

hard disk, erasure, forensic recovery

INTRODUCTION

Hard drives are the primary storage devices for most modern Internet enabled organisations. Whether these drives are in large server based Raid arrays, a desktop PC or a laptop they all, potentially, contain information which, if it is discovered or disclosed, could have catastrophic consequences for the organisation or an individual. Recent studies in Australia (Valli, 2004) and the United Kingdom (Jones et.al, 2005) indicate that a broad cross-section of organisations are failing to adequately protect or erase confidential data stored on hard disk drives before subsequent disposal. Over 90% of hard disks that were examined as a result of the two Independent studies contained data that was in an easily recoverable state with some drives simply requiring a boot. Earlier studies conducted by (Garfinkel & Shelat, 2003) in the US found similar issue with erasure of hard disks.

The US Department of Defense (USDoD) erasure standards (Defense, 1997) have become a de-facto standard and supporting commercial and freeware software exists for the secure erasure of such devices based upon these. The USDoD standard *DoD 5220.22-M* is stated as **"**Overwrite all addressable locations with a character, its complement, then a random character and verify**"** p58, (Defense, 1997). It should be noted that this level of erasure is recommended for all devices except those containing Top Secret classification materials, which must be disposed of by disintegration into particles. The use of USDoD standards and other similar stringent erasure techniques are designed to make it sufficiently expensive or highly improbable that recovery can be achieved by using standard forensic recovery techniques. Furthermore, the use of high number of forensic rewrites (normally 35 as per the USDOD standard) is meant to provide protection against recovery of data via magnetic remanence techniques using electron microscopes to scan the disk surface.

There are some perceived technical constraints for the timely secure erasure of software and data contained on these hard drives when systems have to be rapidly replaced as is common practice during system rollovers. This paper will give an overview and comparison of the two studies conducted. Then an examination of possible factors responsible for the inadequate erasure of hard disk devices will be undertaken. Furthermore, possible future research directions will also be explored.

OVERVIEW OF THE STUDIES

Two studies were conducted into the ability to forensically recover data contained on disposed or second-hand hard disk mechanisms available for sale to the public. The Australian study experimented on 23 independent cases that were acquired through public computer auctions. The UK case study experimented on 105 independent hard disks that were acquired from computer auctions, computer fairs and the on-line auction at e-Bay. In the UK the disks were blind sourced to the University by a computer recycling company. In each study a battery of forensic techniques were applied to the hard disks to affect recovery. In the Australian study 21 of the hard disks were easily recoverable, one hard disk was erased and one hard disk had mechanical failure. In the UK study 105 disks were examined. Of these 13 were unreadable due to mechanical failure, with 10 of these having been physically tampered, 16 had been erased and 76 were easily readable.

The level of forensic expertise needed to recover the data contained on the disposed hard drives was very low. In several cases simply powering on the hard drive revealed its contents *virgo intactica* from point of disposal to the examiners. In both the Australian and the UK studies, simple use of the unformat command or the use of a hexadecimal editor allowed recovery of nearly all data.

The profile of organisational types uncovered in both studies was broad from small home owned computer systems to government critical infrastructure provider server hard drives. In Australia the only hard drive that was properly erased was a large telecommunications infrastructure provider hard disk from a desktop PC. In the UK, of the 16 hard disks that had been properly erased, it was subsequently revealed that 12 had come from a computer recycling company that undertakes government contracts. The origin of the remaining four erased disks could not be determined. All of the hard drives that were recoverable contained information that was confidential or commercial in nature whose disclosure could have had catastrophic consequences for the individual or the organisation concerned. None of the drives examined were using cryptography to protect the sensitive confidential or commercial data contained on the disks.

In some of the cases the hard disk drives had files that carried date stamps that were less than two weeks old at the time that they were acquired, implying that the information contained on the hard disks was current. It should be noted that this two-week turnaround is often well within organisational security policy constraints relating to password changing on systems for instance. This narrow window of time from disposal to resale makes the data highly contextual and relevant to intelligence gathering for attack or other malicious intentions.

While it might be expected that the disks that had come from home use computers and from small companies would be more likely to contain information that should have been erased, the reality was that there was no significant difference between these and the larger enterprises discovered in the studies.

The level of organizational information that was recovered from the disks included a wide range of information that would be of value and interest to a number of groups, including;

The disks (16) from one major leisure service organisation, had originally been used by the finance department, including those used by the finance manager and their assistant (the root directories of the disks were named FMANAGER/STOCK and FASSISTANT/FMANAGER) that contained detailed documents on their property holdings, names, addresses and telephone numbers of members of staff, wage information, balance sheets, incident reports, profit and loss balance sheets, expenses details for members of staff – all of which was less than three months old. Another example from a large financial institution gave details of confidential memos marked ‘for internal use only’, staff directories and staff profiles. Disks from a third organisation (a food biotechnology company) gave details of crop trials in the UK, including locations dates of the trials.

The disks that were recovered from academic institutes, which were found to contain a large amount of information, including course work and exam results – actual and predicted, letters of reference, together with template letters and logos.

The information on one disk that was recovered that was found to have been used by a primary (elementary) school was particularly disturbing in that it contained a significant level of information relating to children that could be identified, including reports on student progress throughout the year, a report that related to a bullying incident and another that related to medical treatment for another child.

Examples of disks recovered from private systems included a database of passwords from the system of one (identifiable) user and emails relating to an extra-marital affair, where the participants could be identified.

IMPLICATIONS FOR PRACTICE

The implications of information being available to people who have no right to access it are wide ranging. From the point of view of the corporation, there is the potential exposure for industrial espionage, non-compliance with statutory or industry sector requirements and potential litigation. In the case of the disks that could be attributed to the commercial sector, the potential cost to the organisation of a leakage of information is high. For the leisure service industry organisation (a household name in the UK), the information could be attributed to its finance department and the loss of it could be considered to be nothing short of negligent. To any competitor or a potential supplier, the level and detail that was available would allow for a very accurate analysis of the financial viability of a number of the operations being run by the organisation. It provided details of turnover, stock levels and the names and contact details for staff.

The disks that had previously belonged to a financial institution gave information including directories of staff and business plans, all of which would be of high potential value to anyone outside the organisation and of great potential embarrassment to the organisation. Some of the issues that failure to dispose of the data effectively exposed the organisations to include: breach of statutory or industry sector regulations, fraud, industrial espionage and potential network intrusion or hacking. Where credit card or at other account details have been left on the devices simple and significant theft can occur. Furthering this premise, what would occur if a high-value, high transaction customers' details were compromised? The potential for financial malfeasance is large, immediate and potentially catastrophic.

The discovery of information in the studies from major information and critical infrastructure providers has significant implications for national security. Since the initial research over a year ago and more recently again in Australia (Jenkins, 2005) government servers acquired at an auction were found to contain sensitive information. This risk is further substantiated in research by (Valli, 2004) where computers acquired at auction had information from state owned infrastructure utilities present. The potential for misuse of this information by people wishing to impact on the nation state such as other governments, activist and terrorist groups is something that cannot be discounted as an unrealisable threat. If we run a scenario where servers came out of a major infrastructure provider and these servers contained SCADA control software and codes, the potential impact of this could be catastrophic.

For an individual or small business, some of the issues that the failure to erase the information can cause are identity theft, blackmail and fraud. Identity theft is one of the fastest growing new trends in criminal activity and much of the activity is now focused on the Internet with the growth of spyware. One has to ask the question: why should thieves spend time developing spyware programs when much of the information they require is readily available at auction or computer recyclers?

Furthermore, the high level of discovery that was encountered in both of these studies demonstrates that many organisational security initiatives have been negated because of the poor asset disposal procedures. It is almost incongruous that large organisations could spend millions if not tens of millions in currency per year defending the corporate edifices from external and internal compromise and leave the very data that people are trying to acquire on disposed hard drives or equipment. This approach by organisations to erasure negates the money spent on deploying and maintaining countermeasures such as firewalls, virus scanners, spyware removers and content filters which are used to reduce the risk of systems penetration or compromise.

WHY NOT ERASED?

The length of time it takes to erase a hard disk is an issue, particularly if the hard disk is in a machine that is to be rolled out over a weekend period for a large organisation. The redundant computer is often live until the close of business at weeks end, leaving little time for the secure erasure let alone removal and de-registration of the equipment. It would be impractical in terms of time and human resource to remove each drive and erase it. This problem will only increase as hard disk capacities continue to climb and secure erasure which involves the need multiple overwrites is needed to ensure confidentiality. In the case of the large organisations that were identified in the UK study, it was subsequently discovered that in all cases, the organisations had agreements with third party organisations to securely dispose of the material. It is clear that these arrangements had failed to achieve the objective and the organisations must be considered to remain responsible, as they had not tested that the arrangement worked.

Recovery from drives that may actually still be functional on a computer that has failed is a possibility. This is could be categorised as a loss of data by misassumption i.e. the specialist has assumed that the hard disk is the cause of the failure. Or in the case of the Australian study the hard drives were recovered from laptops that were sent in for repair and then having been taken off of organisational asset registers were disposed of by third parties.

A lack of legislative requirement could be a contributing factor in the lack of proper erasure of digital media. Many Australian State and Federal Acts cover the use, storage and transmission of information. One such act is the Privacy Act, 1988 which provides legislated requirement to protect information collected on individuals. It covers the transmission and transferral of data and private information but does not cover the destruction or disposal of this data particularly in digital form. This is an area that could be considered for incorporation into legislature to ensure the correct erasure of data from drives. The efficacy of this approach is also questionable as the UK study found hard disks that under the Data Protection Act should have been erased.

Hardware vendors are realizing the need for protecting data on hard disk drives and Seagate have released a hard disk in 2.5" form factor that has onboard hardware based encryption of data (Seagate, 2005). Other vendors such as (Systems, 2002) have had third party hardware encryption for hard disks for some time. These types of hardware based solutions provide the only real protection from compromise of sensitive data. They provide protection by encryption of the hard disk drive in hardware

CONCLUSION

Further studies need to be conducted into the reasons why organizations do not adequately ensure that their hard drives are erased properly. Freeware utilities exist that will adequately perform erasure of hard disk drives so cost of software acquisition is a relatively minor issue.

Research should focus on the human and organisational impediments to the secure erasure of data devices. The inability to erase drives from a technology perspective, as a defence for non-erasure does not hold the drives can be erased. However, as entry level hard disks are now approaching 80 Gigabytes in size the issue of time is a significant factor and warrants investigation as this will only continue to grow as the use of larger digital storage technology expands.

Sales of other storage technology such as USB flash memory sticks, Compact Flash, Secure Digital Card Memory are also rapidly increasing, as is their usage. These other alternate channel repositories of corporate memory will also require investigation. In particular flash memory may be recoverable particularly Flash Translation Layer (FTL) types of memory. As erasers may only erase the FTL leaving the data intact in the memory space on the device.

Research into effective strategies to educate end users is urgently needed to combat the extreme risk of data recovery from incorrectly cleansed data storage devices that for the best part individuals and organisations appear to be either ignorant of or simply unwilling to address adequately. This will then provide mechanisms for the proper and correct protection of corporate data.

REFERENCES

Defense (1997). DoD 5220.22-M: National Industrial Security Program Operating Manual, Department of Defense.

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

Jenkins, C. (2005, August 2nd). Govt data sent to auction. The Australian.

Jones, A. et.al (2005) *Analysis of Data Recovered from Computer Disks released for Resale by Organisations*, Journal of Information Warfare, 4, (2)

Seagate (2005) *Seagate Introduces World's First 2.5-Inch Perpendicular Recording Hard Drive; First Major Hdd Maker To Deliver Notebook Pc Drive With Hardware-Based Full Disc Encryption Security*, http://www.seagate.com/cda/newsinfo/newsroom/releases/article/0,,2732,00.html

Systems, (2002) *Secure Data Vault,* Secure Systems, Perth. http://www.securesystems.com.au

Valli, C. (2004) *Throwing out the Enterprise with Hard Disk,* In *2nd Australian Computer, Networks & Information Forensics Conference,* School of Computer and Information Science, Edith Cowan University, Perth, Western Australia, pp. 124-129.

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

COPYRIGHT