2005

An Investigation into the Efficiency of Forensic Erasure Tools for Hard Disk Mechanisms

Craig Valli
Edith Cowan University

Paul Patak
Edith Cowan University

An investigation into the efficiency of forensic erasure tools for hard disk mechanisms

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

Abstract

One of the common anecdotal complaints used when defending the insecure erasure of hard disks is the length of time taken to affect a secure erasure. This paper discusses results of experiments conducted with Unix/Linux based hard disk wiping software when run on various machines and hard disk mechanisms in terms of size, speed and interface. The initial research has uncovered a range of issues and factors that affect the speed of erasure of hard disk mechanisms. Some of these factors included memory configuration and CPU but not in ways that were expected. This paper includes results from contemporary ATA and the newer SATA IDE hard disk drives in use today.

Keywords
erasure, hard drive, forensics, Knoppix

INTRODUCTION

A large volume of confidential, secret and sensitive information is stored on millions of mass storage devices such as hard drives. All organisations and individuals that use computers will have to dispose of them at some stage due to obsolescence of the equipment. Many organisations or individuals will simply on sell or trade in the computer. The problem is that many of these computers have drives that are in a state where information contained on the drives can be recovered (Duvall 2003; Monroe 2003; de Paula 2004; de Paula 2004). Recent studies by (Garfinkel and Shelat 2003; Jones, et .al 2005; Valli, 2004) have indicated significant problems with the safe and secure disposal of hard disk assets. Over 80% or more of drives examined in these studies indicate they had information that was readily retrievable some simply by powering up the hard disk.

The market for hard disks is not decreasing but expanding. Gartner Dataquest predicts that shipments of desktop-class 3.5-inch hard disks will grow from 190.8 million in 2003 to 298.7 million in 2008. For laptops with 2.5-inch hard disks the growth is expected to go from 3.6 million units in 2003 to almost 20 million units in 2008 (Monroe 2003). This indicates that the problem of disk disposal will continue to increase as these drives become obsolete. One of the remedies for this is the secure erasure of the hard disk device by software that conforms to the US Deparment of Defense (DoD) 5220.22-M or uses other techniques to write psuedo-random strings of data to a hard disk several times over. The US Department of Defense (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, (Department_of_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. One of the paragons of the erasure literature Gutmann(1996) stated that 35 wipes or passes of a drive made it sufficiently expensive to recover data off of hard disks.

One of the common anecdotal complaints used when defending the insecure erasure of hard disks is the length of time taken to affect a secure erasure. This paper discusses results of Linux based hard disk wiping software when run on various machines and hard disk mechanisms in terms of size, speed and interface. The tests yielded some anomalous performance with various software and hardware configurations. This paper only dealt with speed issues; a subsequent paper will be produced that looks at the ability to recover the data from the mechanisms.

EXPERIMENTAL PROCEDURE

A range of hard disks types and Intel based PCs of varying processing power and RAM configurations were utilised to conduct the experiments. The hard disks and supporting technology utilised were a range of IDE drives and computers taken from recently redundant computers from Edith Cowan University. The different configurations are shown in Table 1.

Mainboard/Computer	CPU
ASUS	Pentium 3 - 733 Mhz
ASUS	Pentium 3 - 866 Mhz
	AthlonXP - 1800
IBM NetVista	Pentium 4 - 1.8Ghz
IBM	Pentium 4 - 3.0Ghz

Table 1 - Types of Computer used in Experiments

The software used to perform the wipes was the wipe program from the Auditor CD (Version 1.6). The wipes were performed in quick mode on the wipe utility. The hard disk parameters were extracted using the hdparm utility and the /proc system. No changes to the disk configuration as is possible with the hdparm utility were made this was done so as to reflect normal practice.

For each drive that was utilised there were 3 sets of tests performed these were 1, 3 and 7 wipes/passes of the drive with the software used. Due to time constraints 35 wipe tests were not conducted however, as can be seen later from the results and extrapolation via simple mathematics is possible to ascertain wipe times if such tests were conducted. Each test was conducted 3 times and the resultant time in seconds was averaged from these 3 results for each wipe set. If there were significant variance in the results then the test set was run again until such time as there was minimal variance. A baseline of RAM for each machine was set these were 256MB for the P3s, 512 for the IBM P4s. Then tests were rerun using varying the original baseline RAM to allow comparative analysis on varying RAM configurations. The variety of configurations was limited by the technical resources available and the ability to acquire/use various RAM stick configurations.

The intention of the experiment was to validate a range of KNOPPIX based CDs that are in common use these being Knoppix STD, Autopsy and Helix. However, during the testing procedure the first CD used was the Knoppix STD and it gave exceptional performance for erasure of drives across on all machines tested. The figures when tested in fact were so exceptional that the times were not physically possible. The defect or why this occurred at this stage has not been investigated the experimental conditions will be replicated at a later stage.

EXPERIMENTAL RESULTS AND DISCUSSION

This section of the paper is a summary of the tests conducted so far a full copy of the results from all of testing is available on-line from http://scissec.scis.ecu.edu.au/wipers and will be updated as new testing is conducted and results become available. The current results will be used to infer trends and patterns but should not be relied upon as ultimately conclusive.

As can be seen in Table 2 the time taken to erase hard disk mechanisms to recognised standards such as Department of Defence is significant. If some of the more modern ATA mechanisms e.g. drives above 40 GB in size are correctly wiped with 35 passes the time taken to complete this is not an insignificant hurdle. For example to securely erase a mechanism on a typically redundant SOE computer with a 80GB ATA mechanism taken from Table 2 takes between 28 and 45 minutes per pass with quick settings which means a completion time of approximately 16 to 26 hours. Indications are that Serial ATA (SATA) mechanisms are even more of a problem with the 250GB SATA as tested taking a calculated 61 hours to complete.

SATA drives are replacing conventional ATA mechanisms and most new mainboards now natively support this type of bus. The SATA standards promise higher speed transfer rates than conventional ATA with its maximum speed now at 72 Mbytes, having SATA-I specified as 150Mbytes per second and SATA-II (which is now in limited release) at 300Mbytes per second. The speed advantages from the new mode of operation are now lost against larger capacity drives with the entry level for this class of drive being 80 Gigabytes. The results from the testing conducted are not promising with a 250GB SATA taking 58 - 61 hours to erase to the DoD 35 pass standard. The 80GB SATA mechanism used in this test actually performed worse than the 80GB ATA mechanism by 26% which is somewhat strange give then SATA by default is supposed to be the faster technology. This warrants further investigation as to why this has occurred.

In another scenario a defective PC or laptop that needs to be sent to a repairer for repair would take considerable time before the machine with hard disk erased could be released to the repairer. It would appear from these preliminary results that there may be some credence in the claims that secure erasure takes too long to accomplish given restricted time frames.

Regardless of SATA/ATA misnomer these results indicate that the amounts of time that a PC must be powered on and left running to achieve erasure of the mechanism to the DoD standards is not insignificant. This amount of time to effect erasure if taken in the context of a critical path for a new system rollout that may only be as long as 48 hours is a significant impost or in the case of SATA impossible to achieve.

	Number of Wipes			
Processor, RAM, Drive	**1**	**3**	**7**	**35**
ATH-1.8-S256-IBM-40	0.30	0.89	2.07	10.34
ATH-1.8-S256-QTM-20	0.23	0.68	1.60	7.98
ATH-1.8-S256-WD-80	0.52	1.57	3.66	18.29
P3-733-128-IBM-40	0.45	1.38	3.19	15.99
P3-733-128-QTM-20	0.26	0.77	1.80	9.00
P3-733-256-IBM-20	0.23	0.68	1.59	7.95
P3-733-256-QTM-10	0.24	0.72	1.70	8.47
P3-733-256-QTM-20	0.28	0.81	1.89	9.47
P3-733-256-WD-80	0.76	2.26	5.28	26.38
P3-733-384-IBM-40	0.48	1.43	3.33	16.68
P3-733-S256-IBM-20	0.22	0.70	1.59	8.00
P3-866-256-IBM-40	0.47	1.40	3.25	16.28
P3-866-256-QTM-10	0.23	0.68	1.59	7.95
P3-866-256-WD-80	0.67	2.02	4.71	23.54
P4-1.8-256-WD-80	0.47	1.40	3.25	16.27
P4-1.8-384-IBM-40	0.25	0.76	1.78	8.89
P4-1.8-384-IBM-60	0.25	0.76	1.78	8.89
P4-1.8-384-QTM-10	0.23	0.70	1.63	8.15
P4-1.8-384-QTM-3.2	0.10	0.29	0.67	3.35
P4-1.8-384-WD-80	0.47	1.40	3.25	16.27
P4-1.8-512-WD-80	0.47	1.40	3.25	16.27
P4-3-512-QTM-20	0.22	0.60	1.37	7.76
P4-3.0-1024-IBM-40	0.33	0.98	2.28	11.38
P4-3.0-1024-SATA250	1.66	4.98	11.63	58.12
P4-3.0-1024-SATA80	0.55	1.66	3.87	19.36
P4-3.0-1024-WD-80	0.60	1.81	4.23	21.10
P4-3.0-512-QTM-3.2	0.09	0.28	0.66	3.29
P4-3.0-512-SATA250	1.75	5.24	12.24	61.19
P4-3.0-512-SATA80	0.59	1.75	4.09	20.44
P4-3.0-512-WD-80	0.47	1.40	3.25	16.28
P4-3.0-NOHT-1024-WD-80	0.60	1.81	4.23	21.10
P4-3.0-S512-QTM-20	0.22	0.60	1.37	6.99

Table 2 – Time Taken to Wipe Drive in Hours

More RAM not necessarily faster but CPU does have an impact

RAM configuration for the same machine can have an marked impact on erasure speeds. These preliminary results indicate that single sticks of RAM will out perform 2 sticks for the same RAM configuration. For example from Table 2 P3-733-384-IBM-40 performed 6% slower than P3-733-128-IBM-40 utilising combinations of 128 MB 133 MHz SDRAM sticks from the same manufacturer. Similarly the 3.0 GHz P4 with 512MB (P4-3.0-1024-WD-80) is 29.7% faster than (P4-3.0-1024-WD-80) on the 80GB mechanism. Differences in performance on the P3 were expected due to the use of Synchronous DRAM (SDRAM) chips in the machines used these were 133Mhz modules and as such are rated to transfer at 1.1GB/sec . However, the P4-3.0 has DDR (Double Data Rate) technologies and as such the addition of extra RAM should not present as much of a problem due to the purported increases in transfer rates as the chips were DDR 400. The 29.7% difference in performance on the P4-WD-80 possibly indicates that DDR technologies suffer the same problems as SDRAM. However, in fairness it should be pointed out that this could be a problem with mainboard design and will have to be tested on other mainboards to see if the same results are garnered.

The ability for CPU to affect the erasure of hard disks is not to be discounted either if we isolate the RAM difficulties and examine results from the same hard disk mechanism across the same family of CPU types we notice a plateau in performance.

It is apparent from Figure 1 that the erasure speed of the hard past a given CPU performance barrier does not improve. Both the P4-1.8Ghz and P4-3.0Ghz machines return identical results on the same hard disk. What further points to this being a hard disk performance bottleneck is that the two P4s had different hard disk controller chipsets yet returned near identical wipe times with differences of seconds over 16 hours of operation. Excluding a software fault this would indicate that a hard drive performance affects erasure speed dependent on sufficient CPU to drive them. This theme has since being repeated with drives still under test.

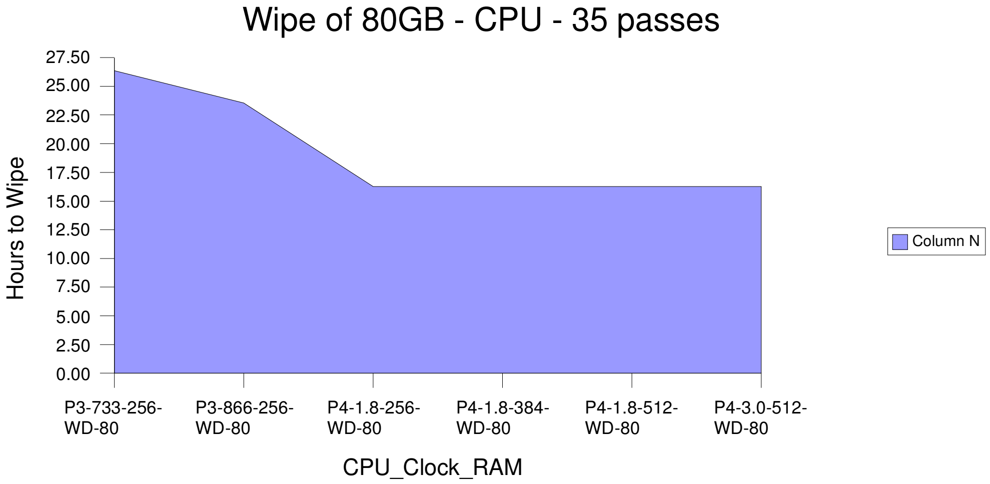

Figure 1 – Graph of CPU Type vs Wipe times for hard drive erasure

CONCLUSION

This research in progress has indicated that there are a range of factors and issues that can affect the ability of hard disks to be erased forensically. Indications from this initial study are that memory configuration can affect wipe times significantly and that single stick configurations out perform dual stick combinations. For older architectures that used SDRAM this was an expected outcome but seeing as the newer DDR based machine suffered from similar problems this will need further examination. The time savings by using a single stick of RAM are significant and these would indicate that should a machine have more than 1 stick of RAM that the extra sticks be removed to increase wipe speeds.

CPU is another factor that has some impact on wiping performance. The ability of the CPU to drive the hard disk controller s to maximum performance levels has been an observed phenomenon in these tests. A sufficiently fast CPU can garner significant speed advantages up to the point of hard drive performance limits.

Some software in particular the KNOPPIX STD wipe program performed wipes erroneously in that the wipe speeds achieved for the ATA drives in our initial tests had wipe rates faster than the technology could provide. The experimental results for the KNOPPIX STD need replication and extensive forensic examination of the hard disks to determine if the hard drive surfaces have been correctly erased. Initial evidence is that the drives wiped by this tool were not properly erased.

The research has accurately measured performance of the drives under forensic erasure procedures and has found that the time to wipe drives sufficiently is not insignificant. If drives need to be wiped to stringent levels such as disks from government departments, financial services sectors or any other entity having sensitive information then time taken is a impediment. In the case of large 80GB plus ATA and SATA drives times are measured in days not hours to achieve the DoD 35 passes standard. Protection of data by physical destruction of the drives in these cases becomes a logical and potentially cheaper alternative. Even for conventional ATA hard drives less 80GB the time taken to affect a high level of erasure is sizable. These findings provide some credence to the argument that forensic erasure of hard drives is a time consuming process.

REFERENCES

CCSE (2000). Clearing and Declassifying Electronic Data Storage Devices, Government of Canada, Communications Security Establishment.

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

de Paula, M. (2004). "Security: Risk Of Improper Disposal Of Computer Trash Grows ; Wamu found out the hard way that special care is necessary when discarding software and hardware." Bank Technology News 17(6): 12.

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

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

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

Gutmann, P. (1996). Secure Deletion of Data from Magnetic and Solid-State Memory. Sixth USENIX Security Symposium, San Jose, CA.

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

Monroe, J. (2003). Forecast: hard disk drives, worldwide, 1999-2008 (executive summary), Gartner.

Valli, C. (2004). “Throwing out the Enterprise with the Hard Disk”, Proceedings of 2nd Australian, Computer, Network and Information Forensics Conference, Fremantle, Western Australia

COPYRIGHT