Securing Data With Hard Disk Shredding

*Siti Hajar Nasaruddin, Johana Yusof and Nur Hasni Nasrudin

***Abstract*—** The purpose of this paper is to develop a securing data with hybrid security shredding concept. This paper is based on a study that review the mechanism apply in securing data using hard disk data shredder, erasing data standard methods and data wiping algorithms for real time based software. It was found that there are several shredding methods that can be implemented to ensure high security of data. Nevertheless, this method required long processing time, and not suitable for developing real time based software. Hybrid hard disk shredding can be used to overcome this situation, that include data securely delete and cannot be recovered. This paper is limited to securing the data after shredding concept. Further study may combine other methods and hard disk shredding concept to provide high security of data. Three algorithms of securing data may be used by developing a solution to suit the real time based software. This paper is a new way of securing data with hard disk shredding and introducing new hybrid technique by combining three erasing and data wiping algorithms. (Abstract)

***Keywords*--** Securing data, hard disk shredding, data wiping, data remanance, erasing algorithms, real time software based and notebook/laptop. (Keywords)

I. INTRODUCTION

THE paper is for developing a securing data shredding with combining hybrid mechanism. The research is combining of securing data concepts to ensure high security in order to secure the data inside the laptop. It will determine the replacement to the hard disk made by unauthorized user. This mechanism used will allows the user to securing their laptop and keeps safe all the information. People and organization in Malaysia nowadays realize the important of securing the confidential data by using hard disk shredding concept. Some organizations that might operate the critical operation such as military department, government agencies should consider more on this issue to prevent from data theft. In certain period of time, the agencies might want to donate their machine to society or other parties, so the agency involved need to think about this security issue to avoid from some data or information exposed to public by irresponsible party and preventing from any losses to the organization as well.

The hard disk data shredder helps to reduce the incidences of identity theft, and there is no compromise on confidentiality of keeping the data.

Many companies have adopted the hard disk shredder approach for deleting the data and completely protecting the data. The research covers approach to prevent from data theft by irresponsible party, the software was planned to incorporate with external encryption program, method to blocking the laptop usage from been used by unauthorized party and mechanism used to offer high data security by wiping the hard disk after meets certain criteria. This process made to secure the confidential and private data of an individual and organization as well.

II. RESEARCH SCENARIO

Many parties nowadays realize the importance of securing the confidential data by using hard disk shredding concept. Organizations or individual that involve in operating critical operations such as military department should consider this issue in order to prevent from data theft. Sometimes, computer donors also need to consider the security issue to avoid information from being exposed to public by irresponsible party and to prevent data loss. This research is to produce a securing data algorithm with security shredding concept. This new method is based on a study on the mechanism applied in securing data using hard disk data shredder, erasing data standard methods and data wiping algorithms for real time based software. Based on previous research, it was found that there are several shredding methods that can be implemented to ensure high security of data. This method required long processing time, and is not suitable for developing real time based software. Hard disk shredding can overcome this problem as data is securely deleted and cannot be recovered. Research may combine other methods and hard disk shredding concept to provide high security of data. Three algorithms of securing data will be used to develop a solution to suit the real time based software. The result of this new way of securing data with hard disk shredding and introducing new algorithm by combining three erasing and data wiping algorithms. The mechanism use will allow users to secure their laptops and keep all the information safe. The hard disk data shredder will help to reduce the incidences of identity theft, and there is no compromise on confidentiality of keeping the data. The method used will block the stolen laptop from being used by unauthorized party and the mechanism used will offer a high data security by wiping the hard disk after meeting a certain criteria.

*Lecturer, Universiti Teknologi MARA (Perak), Malaysia

III. Background Study

1. Existing Techniques

Recently, many organizations have really detailed out the security of their information. Some agencies operate and are involved with high level of security operation and they also produce secretive data. Therefore hard disk shredding concept is the best solution for preventing the data theft from hackers or irresponsible person. This study is reflected based on a few scenarios. A scenario is when one of the workers lost a laptop. At the same time, the information that has been stored in the personal computer is highly secured with a high privacy level. Any data leaks will reflect on the organization. Meanwhile, the thief cannot access and perform an action on the files inside the machine because the files encrypted by the encryption program. So, in order to use the machine, the irresponsible person changes the hard disk with a new hard disk. The developed software for this project is useful at this stage because it blocks unauthorized user from using the laptop.

A. NIST

According to NIST [1], shredding is a process of irreversible file destruction, so that its contents could not be recovered. Sometimes the same process is referred as erasing or wiping; we prefer to call it shredding in an analogy with paper shredding machines, which are used for disposing sensitive documents. Data remanence may make an unintentionally disclosure of sensitive information possible in case if the storage media be released into an uncontrolled environment such as thrown in the trash or hands on to third party. Over the time, many techniques have been developed to encounter data remanence. Depending on the effectiveness and inventiveness, this is often classified as either clearing or sanitizing data.

B. Guttman Method

The Gutmann method by Peter Gutmann, [2] is an algorithm purposely develop to determine secure erasing of the content in computer hard disks. Created by Peter Gutmann and Colin Plumb, this approach does so by writing a series of thirty five patterns over the region that has intention to be erased. The selection of patterns by assuming that the user do not know the encoding mechanism used by the hard disk, and it will include patterns designed specifically for three different types of disks [3].

C. DoD 5220.22-M

DoD 5220.22-M [4] is sometimes refered as a standard tool for sanitization to counter data remanence. The DoD 5220.22-M actually covers the scope for entire field of government industrial security process, of which data sanitization is a very small part of it. Furthermore, DoD 5220.22-M does not involve in specifying any particular method. The standards for sanitization data or information are left to the Cognizant Security Authority to figure out. The Defense Security Service provides a Clearing and Sanitization Matrix which already specifies the method used [4].

The most secured method is using Peter Gutmann theory, which the data will be passed in writing series for thirty five times. Nevertheless, this method required long processing time, and is not suitable for developing real time based software. DoD 5220.22-M standard related to the Data Remanence concept which is found can be recovered by forensic software. The new technique that will be produce will fastern the shredding process to less than fifteen seconds and in the same time securing data from being manipulated by irresponsible person .

IV. Problem Statement

Data shredding is a technique that used to wipe and ensure data security. There are various algorithms used to achieve the data shredding. Existing algorithm consume time to shred the hard disk because its depending on the number of passes to the address and bootloader required in order to complete the shred process. We are going to implement a new version of this technique. Shredding can be time consuming, however it will depend on the algorithm and implementation used. Therefore, the intended is to propose algorithm that can speed up hard disk shredding process and no retrieval capability of deleted data. On top of that, the comparison of new algorithm with the existing data shredding algorithm will be produced. Prior to that, a study on the three existing algorithms will be conducted and analysed. It is believed that a significant speed up and secure method will be achieved using the new algorithm. Once proven, this approach will be used in the shredding technique.

V. Solution Proposed

A. Grub Bootloader

GNU GRUB short for GNU GRand Unified Bootloader is a boot loader package from the GNU Project. GRUB is the reference implementation of the Multiboot Specification, which enables a user to have multiple operating systems on their computer, and choose which one to run when the computer starts. GRUB can be used to select from different kernel images available on a particular operating system's partitions, as well as pass boot-time parameters to such kernels [5]. GNU GRUB was developed from a package called the Grand Unified. It is predominantly used on Unix-like systems. The GNU operating system uses GNU GRUB as its boot loader, as do most Linux distributions.

GRUB can download operating system images from a network, and thus can support diskless systems. GRUB supports automatic decompression of OS images prior to booting from them.

GRUB differs from other boot loaders by being able to communicate with a user directly via a GRUB prompt. A GRUB prompt is the stage before GRUB loads an operating system and can be triggered at a text mode GRUB booting screen which is controlled by the configuration file "menu.lst" [7]. A prompt which similar to bash can also be obtained by

booting GRUB without an operating system attached, or in a GRUB installation with an operating system where the file "menu.lst" is absent. From the GRUB prompt a user can manually select and control booting from any installed operating system by using bash-like commands. To boot an operating system automatically, the appropriate commands are placed in a configuration file named "menu.lst" in a designated subdirectory.

GRUB Legacy is used because this version is compliant with the Multiboot Specification, provide basic functions are easy for an end-user to use and in the same time offer rich functionality for OS experts or designers. This version is compatibility for booting FreeBSD, NetBSD, OpenBSD, and GNU or Linux [8]. Proprietary OS's such as Windows 9x/NT/2000/XP, and OS/2 are supported via a chain-loading function. In addition to the requirements above, GNU GRUB Legacy has the following features such support multiple executable formats, support non-Multiboot OS's, load multiple modules, and support a human-readable configuration file. This version of GRUB have menu interface, flexible command-line interface, support multiple filesystem types, support automatic decompression, have capability to access data on any installed device, functionality on supporting diskless systems and remote terminals.

B. Boot Process Module

When a computer is turned on, the computer's BIOS finds the primary bootable device usually the computer's hard disk and loads the initial bootstrap program from the Master Boot Record (MBR), the first 512 bytes of the hard disk, then transfers control to this code.

The MBR contains GRUB “Stage 1”. Given the small size of the MBR, “Stage 1” does little more than load the next stage of GRUB which may reside physically elsewhere on the disk. “Stage 1” can load “Stage 2” directly, or it can load “Stage 1.5”. GRUB “Stage 1.5” is located in the first 30 kilobytes of hard disk immediately following the MBR. “Stage 1.5” loads “Stage 2” [5].

When GRUB “Stage 2” receives control, it presents an interface where the user can select which operating system to boot. This normally takes the form of a graphical menu. If this is not available, or the user wishes direct control, GRUB has its own command prompt. The user can then manually specify the boot parameters. GRUB can be set to automatically load a specified kernel after a user defined timeout.

Once boot options have been selected, GRUB loads the selected kernel into memory and passes control to the kernel. Alternatively, GRUB can pass control of the boot process to another loader, using chain loading. This is the method used to load operating systems such as Windows that do not support the Multiboot standard. In this case, copies of the other system's boot programs have been saved by GRUB. Instead of a kernel, the other system is loaded as though it had been started from the MBR [5], [6].

This could be another boot manager, such as the Microsoft boot menu, allowing further selection of non-Multiboot operating systems. This behavior is often automatic when modern Linux distributions are installed on top of an existing Windows installation. This enables retention of the original operating system without modification, including systems that contain multiple versions of Windows [7].

C. Validity Check

1. Portable Media

A physical USB device may consist of several logical sub devices that are referred to as device functions. Such a device is called a compound device in which each logical device is assigned a distinctive address by the host and all logical devices are connected to a built-in hub to which the physical USB wire is connected. A host assigns one and only one device address to a function. USB endpoints actually reside on the connected device and the channels to the host are referred to as pipes.

The control transfers offer in USB functionality that is typically used for short, simple commands to the device, and a status response, used, for example, by the bus control pipe number makes this device is compliant to the software that need to communicate in shorten time.

2. Hard Disk

The operation of the hard disk is when the file is open program or really anything on personal computer, the hard drive must find it. The CPU will tell the hard drive what file looking for. The hard drive will spin extremely fast and it will find the image in a nano-second. It will then “˜read’ the image and send it to the CPU. The time it takes to do this is called the read time [9].

3. Self Encrypting USB Drives

USB drives that embed encryption algorithms within the hard drive thus eliminate the need to install any encryption software. The limitation of such devices is that the files are only encrypted when residing on the encrypted USB drive, which means files copied from the USB drive to be sent over email or other file sharing options will not protected. These USB drives are also typically more expensive than non encrypting USB drive.

4. Secret Key

The secret key will be stored in Sector 62 for removable media and Sector 2 in hard disk. Currently secret key is stored at starting from byte offset 1. If secret key check failed, time and date during first checking failed will be stored in US sector 62(byte offset 33) [10] for countdown timer reference. Force shutdown method can be used in order to ensure machine automatically reboot if the validation fail.

REFERENCES

[1] NIST Data Remanence ,"Special Publication 800-88: Guidelines for Media Sanitization" (PDF). NIST. September 2006.

[2] Peter Gutmann, Secure Deletion of Data from Magnetic and Solid-State Memory, July 1996

[3] Peter Gutmann, Data Remanence in Semiconductor Devices http://www.cypherpunks.to/~peter/usenix01.pdf
[4] DoD 5220.22-M National Industrial Security Program Operating Manual (NISPOM) January 1995 http://www.usaid.gov/ policy/ads/ 500/d522022m.pdf
[5] Linux MBR Overwritten after Installing Windows http://www. articles base. com/data-recovery-articles/linux-mbr-overwritten-after- installing -windows-1021322.html
[6] "About Ubuntu". Canonical Ltd. http://www.ubuntu.org/about 2006
[7] "5.04 Release Notes". Canonical Ltd. http://www. ubuntu. Org /releas e. 2008
[8] "RootSudo". http://www.ubuntu/command.2008
[9] Wright, Craig; Kleiman, Dave; Sundhar R.S., Shyaam "Overwriting Hard Drive Data: The Great Wiping Controversy". 2008
[10] Gutmann, Peter (2001): Data Renanence in Semiconductor Devices, In SSYM'01: Proceedings of the 10th Conference on USENIX Security Symposium, pages 4-4, Berkeley, CA, USA, USENIX Association.