Chapter XVI
A “One-Pass” Methodology for Sensitive Data Disk Wipes

Doug White
Roger Williams University, USA
Alan Rea
Western Michigan University, USA

ABSTRACT

Hard disk wipes are a crucial component of computing security. However, more often than not, hard drives are not adequately processed before either disposing or reusing them within an environment. When an organization does not follow a standard disk wipe procedure, the opportunity to expose sensitive data occurs. More often than not, most organizations do not wipe drives because of the intense time and resource commitment of a highly-secure seven-pass DOD wipe. However, we posit that our one-pass methodology, verified with a zero checksum, is more than adequate for organizations wishing to protect against the loss of sensitive hard drive data.

INTRODUCTION

With the advent of legislation such as the Sarbanes-Oxley Act of 2002 (SOX) (Sarbanes & Oxley, 2002) and the Health Insurance Portability and Accountability Act of 1996 (HIPAA, 1996), there are requirements that commercial organizations take action to ensure that the privacy of both employee and customer data is protected from unplanned disclosure to third parties. Increasing pressure from auditors to adhere to strict principles for sanitization of magnetic media may lead to the expensive and time consuming process for disposal and/or redistribution of hard disk media, unless a more efficient and cost effective approach is implemented.

This research focuses on issues surrounding the practice of sanitizing hard drive diskettes for reuse or disposal with a focus on efficiency in terms of reduction of time and effort devoted to sanitization practices. The primary approach focuses not on information of national security or business critical data, but rather on disks retrieved from end user workstations and laptops containing routine or potentially sensitive (but not classified as sensitive) data. The assumption of this research is that while this information should be considered sensitive (per SOX and HIPAA), it would not be considered “secret” or critical to the business.

However, our assumption does not imply that we do not advocate due care and due diligence in the disposal of media, but rather that in the most common cases, it may be sufficient to perform single wipes rather than the repetitive wipes advocated for critical and secret material. The easier it is to sufficiently wipe disks containing routine data, the more often this process will be implemented in a business environment.
Our research tests a “one-pass” methodology and makes a recommendation for business practitioners to sanitize media. Our findings provide a reference study for the use of one-pass wipes—coupled with chksum as a validation method—for the basic, yet effective, sanitization of magnetic media in a business environment.

OVERVIEW

There have always been concerns that data existent on magnetic media could interfere with new data or create problems. Early ANS standards advocate wiping the entire width of the tape to ensure no residual data remained (Kerpelman, 1970). Moreover, there is a long-standing myth that in order to protect sensitive data from recovery, it is necessary to overwrite the data many times (Joukov, Papaxenopoulos, & Zadok, 2006). A common hacker term is the “DOD 99 wipe” that advocates up to 99 overwrites for media to ensure it is unrecoverable.

Many other papers have been written examining this type of practice for effectiveness (Garfinkel & Shelat, 2003; Joukov et al., 2006). In particular, Gutmann (1996) demonstrated that the use of special equipment, such as Magnetic Force Microscopy (Rugar, Mamin, Guenther, Lambert, Stern, McFadyen, & Yogi, 1990) and other Microscopic techniques (Gomez, Adly, Mayergoyz, Burke, 1992; Gomez, Burke, Adly, Mayergoyz, Gorczyca, 1993; Rice & Moreland, 1991), enabled the recovery from wiped media (wiped in the traditional sense), even with multiple passes.

Gutmann (1996) went on to demonstrate techniques to fully ensure the destruction of data using repeated writing along the lines of the DOD 99 wipe. Related works advocate physical techniques such as degaussing (NSA, 1985) or even physical destruction of the media. The seminal work for this type of approach is the NIST Special publication 800-88 which provides guidelines for media sanitization. This work advocates multiple passes—the DOD seven-pass wipe—only for the most critical data (Kissel, Scholl, Skolochenko, & Li, 2006).

Gutmann (1996) went on to demonstrate techniques to fully ensure the destruction of data using repeated writing along the lines of the DOD 99 wipe. Related works advocate physical techniques such as degaussing (NSA, 1985) or even physical destruction of the media. The seminal work for this type of approach is the NIST Special publication 800-88 which provides guidelines for media sanitization. This work advocates multiple passes—the DOD seven-pass wipe—only for the most critical data (Kissel, Scholl, Skolochenko, & Li, 2006).

Gutmann (1996) went on to demonstrate techniques to fully ensure the destruction of data using repeated writing along the lines of the DOD 99 wipe. Related works advocate physical techniques such as degaussing (NSA, 1985) or even physical destruction of the media. The seminal work for this type of approach is the NIST Special publication 800-88 which provides guidelines for media sanitization. This work advocates multiple passes—the DOD seven-pass wipe—only for the most critical data (Kissel, Scholl, Skolochenko, & Li, 2006).

Our research does not criticize these advanced techniques, as they are long established as effective and necessary, but rather we offer proof that in low security situations—such as with a general purpose desktop or laptop—they may not be necessary. Our study describes the need for data to be purged, but it is not expected that complex techniques—which would involve removal of the platters and subsequent microscopic examination as Gutmann and others—would need to be used.

It is common for organizations that dispose or reissue large numbers of general use machines to completely neglect the wiping of drives simply due to time constraints imposed by more complex wiping techniques. DOD 99 wipes that require 99 passes of 0s, 1s, and random 0s and 1s, can take days to perform even on a small drive. Gutmann’s improved approach, which is very effective for sensitive material, requires 35 passes of specialized patterns to complete. In fact, some techniques require special equipment and may not prove economically feasible even for more sensitive equipment. Degaussing may require special housings and facilities and may still prove uneconomical (Preston, 1995).

In our research, we propose a control mechanism for practice which advocates that rather than testing overwrites of the data as the criteria, the remaining content of the drive be used as a mechanism to test for content and recoverability. This is accomplished by using the chksum approach to ensure that all bits have a value of zero prior to release of the drive for reuse or disposal. In this manner, organizations can quickly employ and safely reuse disks that have been cleared of potentially sensitive data without expensive equipment and a large time commitment.

Objective

It is commonly the case that business practitioners are faced with external audit review that advocates media be sanitized (e.g., SOX). Our research will demonstrate that while full seven-pass DOD wipes of drives are sometimes mandated, it may be sufficient for organizations to use a “one-pass” wipe coupled with a chksum validation to establish due care and due diligence in regards to meeting sanitized media criteria. It is again worth noting that we are not advocating this technique be used on any equipment which has been classified as sensitive or greater.

Methodology

In order to test the “one-pass” method of disk wipes, we implemented a software tool called “Wiper” (Riggs, 2008). Wiper allows us to write a single pass of all zeros to eliminate the data on a hard drive. The “one-pass” method is compared to the more time-intensive DOD seven-pass wipe. By comparing the before and after images of each disk drive, we were able to determine how effective our “one-pass” method was