White Canyon Software

CRYPTO ERASE & DATA ERASURE:
A PATENT FOR THE IT ASSET MANAGEMENT CYCLE
Executive Summary

Disk encryption is a useful way to secure data, but there are problems with relying on encryption alone to protect data after drive disposal. Using drive wiping in conjunction with cryptographic key erasure solves these problems.

Disk Encryption and Cryptographic Key Erasure

Encryption is the process of encoding a message or information in such a way that only authorized parties can access it. Encryption has become a popular way to secure data both when it is being transferred and when it is at rest (stored on disk).

Most modern hard drives and solid state drives offer encryption either natively (as part of the hardware solution) or using disk encryption software.

There are different levels of sophistication in encryption, but all encrypted data can be unlocked with the corresponding key. With current decryption technologies, losing or erasing the key makes the data effectively unrecoverable, and as a result, some organizations’ IT staffs are relying on key erasure (crypto erase) to protect data on drives that are being retired.

While crypto erase is quick and encrypted data may seem inaccessible after a crypto erase is performed, it should never be considered “sanitized.”

Here are some of the weaknesses of crypto erase:

Data Persistence

Cryptographic erase relies on removing the encryption key to protect data on a decommissioned hard drive. However, when the key is removed, the data persists on the storage device and thus exposes organizations to the risk that the data may be compromised in the future. For example, if there are advances in decryption technology, the encrypted data may become accessible. It is difficult to say if or when this could occur, but if the data remains on the drive, it remains a target and liability.
Password Weakness

Some encryption technologies rely on passwords to unlock data. Unfortunately, passwords are a notoriously weak form of security because they are often easily guessed or broken. Tools like multi-factor authentication can make password security more effective, but it is critical to not rely solely on a password to prevent a data breach.

Encryption Algorithm Weakness

The encryption used on drives and with software tools relies on complex algorithms, and these algorithms vary between vendors in both hardware and software tools. Because there are so many different implementations of the algorithms, any that were implemented poorly or with ulterior motives are at risk to be cracked.

For example, the New York Times recently reported that an algorithm for generating random numbers, which was adopted in 2006 by the National Institute of Standards and Technology (NIST), contains a backdoor for the NSA.

This means vulnerabilities in encryption algorithms already exist and some have not yet been discovered.

For an analysis of more encryption system and algorithm weaknesses, read this article by the International Association for Cryptologic Research:


Decryption Technology Progress

The argument for relying on encryption as a sanitization method points to the strength of 128- or 256-bit encryption and that they could take many years to break given today’s computing power. However, these calculations don’t account for the advancement of decryption technologies and techniques. It is possible that some day decryption technologies will advance to the point where they can break these encryption methods. For example, the US federal government currently has a program to decode encrypted messages with an $11 billion yearly budget and 35,000 employees. Some researchers are investigating whether quantum computing could nearly instantaneously break encryption keys.

As the race to decrypt data progresses, organizations face the risk that cryptographic erasure will become obsolete as a way to protect data on retired drives.
Software Error

Encryption systems may state they have removed the current key, but it’s possible the technical process did not complete successfully. This would leave the key on the drive, making the data vulnerable to attack. Furthermore, some encryption schemes don’t verify the key has been replaced, meaning IT asset managers would have no method to ensure the cryptographic erase has completed successfully.

Human Error

In order to perform a crypto erase, a human must properly perform all of the necessary steps to remove and replace the encryption key used on the drive. Each drive’s procedure can be different, and if the steps are not performed properly, the data will still be accessible on the drive.

Procedural Difficulty

Cryptographic erasure is a tedious and time consuming process to set up. It typically requires a technician to individually handle each computer to remove the encryption key. This process typically takes 10-20 minutes and can include multiple reboots of the system to ensure the encryption key was changed.

Reporting

One of the most important aspects of a reliable data-sanitization process is the ability to keep a secure and accurate record of all activities performed. Having proof that data was properly sanitized can provide legal and regulatory protection and makes the sanitization process easier to audit.

Cryptographic erasure is a multi-step process and it’s important to receive a certificate that the process has successfully completed. Logs or reports should be verified and stored in a protected location or database, allowing access to key IT, regulatory, and legal stakeholders, but some encryption schemes don’t produce proof the key has been removed or provide a method to store such proof in a centralized database. Current self-encrypting drive (SED) solutions don’t provide the robust, secure reporting capabilities required for sanitization tracking.

Without reporting, it is impossible to be sure that every drive was handled and verified as being sanitized.
Data Erasure by Drive Wiping

Simply deleting an encryption key on an SED is insufficient to provide complete protection for the data on discarded drives. If the data is still there, even in encrypted form, it remains vulnerable.

A more secure way to protect sensitive data during hardware disposition is to overwrite every sector on the drive. There are various patterns and standards for wiping drives, but they all basically achieve the same thing—storing new, meaningless values in every drive sector removes the old, sensitive data and makes it impossible to read.

Data erasure by hard drive or SSD wiping is the best way to ensure the data has been sanitized without destroying the hard drive.

Combined Crypto Erase and Data Erasure

A key best practice for data sanitization is redundancy at each level, including methods of data erasure or destruction, multiple levels of data security (such as encryption), and multiple reviews of processes to ensure compliance. At WhiteCanyon, we like to say you should wear both your belt and suspenders—even if one fails, you won’t be caught with your pants down!

If a secure data erasure tool worked in tandem with cryptographic erase, it would provide an added layer of protection to the data sanitization process.

WhiteCanyon’s WipeDrive data erasure software employs a patented process to both replace encryption keys and wipe all data on the disk.

Patented Process for Drive Sanitization

There are three main steps in WipeDrive’s process:

1. Reset the encryption key

   By programmatically resetting the encryption key at the beginning of the process, any stored data is instantly rendered unreadable and irretrievable, even to the wiping program.

2. Wipe the hard drive

   The drive is overwritten with the desired pattern, eliminating the old data from the drive.

3. Reset the encryption key a second time
Resetting the key again makes any data left in unreadable sectors and even the wipe data irretrievable and prepares the drive for reuse.

Additional details about how the process works and what systems it relies upon can be found in the patent text located here: https://www.google.com/patents/US9396359

Benefits of WipeDrive’s Patented Process

By resetting the encryption key and then wiping the data, WipeDrive realizes the following benefits:

**Rapid, Redundant Data Protection Process**

Because the encryption key is reset at the beginning of the process, the data on the drive is protected nearly instantly, even before wiping. The data is also protected in the case that some sectors aren’t writeable during the overwrite passes.

**Total Data Removal**

Because the data is overwritten, it is no longer on the drive at all, encrypted or not.

**Security**

Because the drive is wiped, over-reliance on passwords or encryption algorithms is avoided.

**Reduction of Human Error**

The software performs the encryption key reset(s), which avoids human error in this step of the process.

**Ease of Use**

WipeDrive makes resetting the encryption key and wiping the data from a SED drive faster and much easier than performing these tasks manually and with other software.

**Reporting**

WipeDrive includes logging and reporting features that aren’t included in a standard key reset or many other wiping programs and that make reviewing or auditing your drive disposition process accurate and efficient.
Summary

Encryption is extremely useful for keeping data safe while the drive is in your organization’s control, but it has weaknesses after drive disposal. WipeDrive resets the encryption key before and after wiping all of the data on a drive, thus combining a cryptographic erase with data erasure and avoiding the problems of relying on drive encryption alone.