Apacer

Comparative Approaches To Drive Erasure

White Paper

March 29, 2019

Version 1.0

Apacer Technology Inc.
1F, No.32, Zhongcheng Rd., Tucheng Dist., New Taipei City, Taiwan, R.O.C
Tel: +886-2-2267-8000 Fax: +886-2-2267-2261
www.apacer.com

Table of Contents

1. Introduction

A few decades ago, the only people who worried about data security were governments or military contractors. But as computers and smartphones have become ubiquitous in daily life, everyone needs to take data security more seriously, from technology consumers to data administrators in businesses. Hackers and other malicious actors are continuously coming up with new ways to leverage lost or stolen personal data. With those threats in mind, Apacer has developed a wide array of strategies for erasing data. Different problems require different solutions, but Apacer offers an erase technology for every application. This white paper will describe how those erase technologies work.

2. Erase Technologies

The following is a list of erase technologies supported by Apacer devices. Note that not all devices support all erase technologies.

2.1 ATA Secure Command (Erase Function)

One common way to erase a NAND Flash drive is by using the ATA Secure Command erase function. If this function is executed, then all user data and the management table will be destroyed and cannot be permanently retrieved. The amount of time that it takes to carry out this function is dependent on the size of the drive. For example, to carry out this function on a 512GB drive will take approximately 20 seconds.

The ATA Security feature set has implemented commands as follows:

a) SECURITY SET PASSWORD – F1h

b) SECURITY UNLOCK – F2h

c) SECURITY ERASE PREPARE – F3h

d) SECURITY ERASE UNIT – F4h

e) SECURITY FREEZE LOCK – F5h

f) SECURITY DISABLE PASSWORD – F6h

Note:

For more detailed information, please refer to **ATA/ATAPI Command Set - 3 (ACS-3), Security feature set**.

2.2 Military Erase

The Military Erase standards were originally created by different branches of the US armed forces. These include the US Army, US Navy, US Air Force and US Coast Guard. Each branch has its own specification for what constitutes an erased device. Generally speaking, the military erase standards involve erasing the device in question and then performing multiple overwrites using garbage data. The precise number of overwrites and the content of the garbage data varies between the different branches. Although the overwriting process can be time-consuming, especially for larger drives, this process goes a long way to ensuring that the original data cannot be recovered from the device.

The following table lists purge procedure details and respective proposed standards.

Organization	Function description
DoD 5220.22-M	● Erase the blocks + overwrite with single character ● Erase the blocks
NSA Manual 130-2	● Erase the blocks + overwrite with random data (1st) ● Erase the blocks + overwrite with random data (2nd) ● Erase the blocks + overwrite with single character
USA-AF AFSSI 5020	● Erase the blocks + overwrite with random data
USA-Army 380-19	● Erase the blocks + overwrite with random data ● Erase the blocks + overwrite with single character ● Erase the blocks + overwrite with complement of the character
USA Navy NAVSO P-5239-26	● Erase the blocks + overwrite with random data ● Erase the blocks
NISPOMSUP Chap 8, Sect. 8-501	● Overwrite with single character ● Overwrite with complement of the character ● Overwrite with random data
IREC (IRIG) 106	● Erase the blocks + overwrite with 0x55 ● Erase the blocks + overwrite with 0xAA ● Erase the blocks
NSA 9-12 (Gen2)	● Erase the blocks + overwrite with 0x21

2.3 Instant Keychange

AES 256-bit encryption is a popular way of securing drives, since it's extremely resilient to brute-force attacks. All the data stored on a drive protected by AES encryption needs to be decrypted by a matching AES key before it can be read. The real advantage of AES encryption is that the key is automatically generated during production and provides an instant protection mechanism.

This is the Instant Keychange function. When an Instant Keychange command is issued, a new key will be generated to replace the original key stored in the flash memory less than a second. Since the new key does not match the old one, when the host is attempting to access the data present in the flash memory, the data will be irretrievable due to AES key authentication failure. The data has not been erased in the conventional sense of all the bits being rewritten as ones or zeros, but it is functionally unreadable and therefore completely protected.

Another important feature of the Instant Keychange function is that it can be activated in two ways. Either a software command can be sent, or a hardware trigger can be activated.

Command	Time to Execute
Instant Keychange	<1 Second*
ATA Secure Erase	>4 Seconds

**This time is based on current controllers used by Apacer. Products still in development may use alternative controllers that have different times to execute.*

In some publications, "Crypto Scramble EXT" is referred to instead of Instant Keychange. Crypto Scramble EXT can be accessed with the command B4h/0011h (non-data). This 48-bit command is for devices that support the Sanitize Device feature set. It starts a crypto scramble sanitize operation that changes the internal encryption keys that are used for user data. This causes the user data to become irretrievable.

Note:

For more detailed information, please refer to **ATA/ATAPI Command Set - 3 (ACS-3), Sanitize Device feature set, CRYPTO SCRAMBLE EXT**.

2.4 TCG Opal

The Trusted Computing Group (TCG) developed the Opal Storage Specification, more commonly known as Opal. It is a set of specifications which drives can implement to strengthen their security, turning them into self-encrypting drives (SEDs). In Opal drives, the erase functions are located within the commands known as “revert,” since they allow the user to revert the drive to a state before any data was written, essentially erasing the drive.

More specifically, the revert function allows users to remove TCG Opal settings from storage devices, restore factory defaults and erase user data, depending on the revert mode chosen. Users can select from three revert modes as follows by clicking **Enable** and entering the password required to apply the settings.

- **PSID Revert**: Users must enter an up to 32-digit PSID (Physical Secure ID) to activate this function. Once this function is enabled, all data and settings will be erased and the TCG Opal function will be disabled. The PSID can be found on the label on the SSD.
- **Revert Tper**: Users must enter the SID password to revert the Tper (Trusted Peripheral) function. This action will erase all data and disable the TCG Opal function.
- **Revert No Erase**: Users must enter the Admin password to activate this function. This action will only disable the TCG Opal function without erasing data stored on the device. However, to enable TCG Opal again, users must to execute the function of **Revert Tper** first before enabling.

Note:

For more detailed information, please refer to **TCG Storage Application Note: Encrypting Drives Compliant with Opal SSC**

3. Conclusion

Apacer offers a variety of different erase technologies to suit the needs and circumstances of our widely varied customer base. Different erase technologies have different advantages and disadvantages. Some are very fast, while others may take longer but are more thorough. When choosing a suitable SSD for an industrial product, customers should consider which erase technology is most appropriate for the application, and Apacer will be happy to provide that technology.

Revision History

Revision	Description	Date
1.0	Official release	3/29/2019

Global Presence

Taiwan (Headquarters)
Apacer Technology Inc.
1F., No.32, Zhongcheng Rd., Tucheng Dist.,
New Taipei City 236, Taiwan R.O.C.
Tel: 886-2-2267-8000
Fax: 886-2-2267-2261
amtsales@apacer.com

U.S.A.
Apacer Memory America, Inc.
46732 Lakeview Blvd., Fremont, CA 94538
Tel: 1-408-518-8699
Fax: 1-510-249-9551
sa@apacerus.com

Japan
Apacer Technology Corp.
6F, Daiyontamachi Bldg., 2-17-12, Shibaura, Minato-Ku,
Tokyo, 108-0023, Japan
Tel: 81-3-5419-2668
Fax: 81-3-5419-0018
jpservices@apacer.com

Europe
Apacer Technology B.V.
Science Park Eindhoven 5051 5692 EB Son,
The Netherlands
Tel: 31-40-267-0000
Fax: 31-40-290-0686
sales@apacer.nl

China
Apacer Electronic (Shanghai) Co., Ltd
Room D, 22/FL, No.2, Lane 600, JieyunPlaza,
Tianshan RD, Shanghai, 200051, China
Tel: 86-21-6228-9939
Fax: 86-21-6228-9936
sales@apacer.com.cn

India
Apacer Technologies Pvt Ltd,
1874, South End C Cross, 9th Block Jayanagar,
Bangalore-560069, India
Tel: 91-80-4152-9061/62
Fax: 91-80-4170-0215
sales_india@apacer.com