

RoHS Compliant

Quick Flash Erase Application Note

February 20, 2009



Apacer Technology Inc.

9/F, No. 100, Hsin Tai Wu Rd., Hsichih, Taipei Hsien 221, Taiwan

Tel: +886-2-2696-1666 Fax: +886-2-2696-1668

www.apacer.com

Revision History

Revision	Date	Description	Remark
0.1	05/20/2008	Preliminary	
1.0	09/30/2008	Initial Release	
1.1	01/20/2009	Updated commands	
1.2	02/20/2009	Updated commands and diagram	

Quick Flash Erase

Overview

Erasure of data on a disk drive is not a simple task. Deleting a file merely removes its name from the directory structure's special disk sectors. The user data remains in the drive data storage sectors where it can be retrieved until the sectors are overwritten by new data. Reformatting a disk drive clears the file directory and severs the links between storage sectors, but the user data remains and can be recovered until the sectors are overwritten.

The cardinal rule of computer storage design has been to protect user data at all costs. Disk drives supply primary mass storage for computer systems, designed to prevent accidental erasure of data. Techniques such as "recycle" folder and "Unerase" commands are common ways that operating systems try to prevent accidental sanitization of user data. Deletion of file pointers is standard to speeds data writing, because actual overwriting of file data is far slower. Drives use elaborate error detection and correction techniques to make sure that they don't return incorrect user data. All this means that true computer data erasure is an abnormal event. These measures taken to protect and speed access to user data can make that data vulnerable to recovery by unauthorized persons. If data is not erased beyond recovery, data on disk drives that leave the physical control of owners can and often does fall into hands of others. Data can be recovered with little effort, from discarded, warranty repaired, or resold disk drives. Therefore, there is an urgent need for a capability to reliability erase data and prevent access to data from retired computer disk drives for security and privacy reasons.

Secure Erase command

The Secure Erase (SE) command, which added to the open ANSI standards that control disk drives, is built into the disk drive itself and thus far less susceptible to malicious software attacks than external software utilities. It is a positive easy-to-use data destroy command, amounting to electronic data shredding. Executing the command causes a drive to internally completely erase all possible user data. This command is carried out within disk drives, so no additional software is required. When power failure encountered, this command will be resumed once power is back on. The process of secure can be referred as a diagram in figure 1.

Security-Set-Password – F1H

Bit ->	7	6	5	4	3	2	1	0
Command (7)	F1H							
C/D/H (6)	X			Drive	X			
Cyl High (5)					X			
Cyl Low (4)					X			
Sec Num (3)					X			
Sec Cnt (2)					X			
Feature (1)					X			

This command requests a transfer of a single sector of data from the host. Table 1 defines the content of the sector of information. The data transferred controls the function of this command.

Table 1: Security password data content

Word	Content
0	Control word: Bit 0: Identifier 0: Compare user password 1: Compare master password Bit 1-15: Reserved
1-16	Password (32 bytes)
17-256	Reserved

Security-Disable-Password – F6H

Bit ->	7	6	5	4	3	2	1	0
Command (7)	F6H							
C/D/H (6)	X			Drive	X			
Cyl High (5)					X			
Cyl Low (4)					X			
Sec Num (3)					X			
Sec Cnt (2)					X			
Feature (1)					X			

This command requests a transfer of a single sector of data from the host. Table 1 defines the content of this sector of information. If the password selected by Word 0 matches the password previously saved by the device, the device disables the lock mode. This command does not change the Master password that may be reactivated later by setting a User password.

Security-Erase-Prepare – F3H

Bit ->	7	6	5	4	3	2	1	0
Command (7)	F3H							
C/D/H (6)	X			Drive	X			
Cyl High (5)					X			
Cyl Low (4)					X			
Sec Num (3)					X			
Sec Cnt (2)					X			
Feature (1)					X			

This command is issued immediately before the Security-Erase-Unit command to enable device erasing and unlocking. This command prevents accidental erasure of the data in the flash media.

Security-Erase-Unit – F4H

Bit ->	7	6	5	4	3	2	1	0
Command (7)	F4H							
C/D/H (6)	X			Drive	X			
Cyl High (5)					X			
Cyl Low (4)					X			
Sec Num (3)					X			
Sec Cnt (2)					X			
Feature (1)					X			

This command requests transfer of a single sector of data from the host. Table 1 defines the content of this sector of information. If the password does not match the password previously saved by the ATA-Disk Module, the ATA-Disk Module rejects the command with command aborted. The Security-Erase-Prepare command should be completed immediately prior to the Security-Erase-Unit command. If the ATA-Disk Module receives a Security-Erase-Unit command without an immediately prior Security-Erase-Prepare command, the ATA-Disk Module aborts the Security- Erase-Unit command.

Security-Freeze-Lock – F5H

Bit ->	7	6	5	4	3	2	1	0
Command (7)	F5H							
C/D/H (6)	X			Drive	X			
Cyl High (5)					X			
Cyl Low (4)					X			
Sec Num (3)					X			
Sec Cnt (2)					X			
Feature (1)					X			

The Security-Freeze-Lock command sets the ATA-Disk Module to Frozen mode. After command completion, any other commands that update the ATA-Disk Module Lock mode are rejected. Frozen mode is disabled by power off or hardware reset. If Security-Freeze-Lock is issued when the ATA-Disk Module is in Frozen mode, the command executes and the ATA-Disk Module remains in Frozen mode. After command completion, the Sector Count Register shall be set to 0. Commands disabled by Security-Freeze-Lock are:

- Security-Set-Password
- Security-Unlock
- Security-Disable-Password
- Security-Erase-Unit

If security mode feature set is not supported, this command shall be handled as Wear- Level command.

Security-Unlock – F2H

Bit ->	7	6	5	4	3	2	1	0
Command (7)	F2H							
C/D/H (6)	X			Drive	X			
Cyl High (5)					X			
Cyl Low (4)					X			
Sec Num (3)					X			
Sec Cnt (2)					X			
Feature (1)					X			

This command requests transfer of a single sector of data from the host. Table 2 defines the content of this sector of information. If the identifier bit is set to Master and the device is in high security level, then the password supplied shall be compared with the stored Master password. If the device is in the maximum security level, then the unlock command shall be rejected. If the identifier bit is set to user, then the device compares the supplied password with the stored User password. If the password compare fails then the device returns command aborted to the host and decrements the unlock counter. This counter is initially set to five and is decremented for each password mismatch when Security-Unlock is issued and the device is locked. Once this counter reaches zero, the Security-Unlock and Security-Erase-Unit commands are command aborted until after a power-on reset or a hardware reset is received. Security-Unlock commands issued when the device is unlocked have no effect on the unlock counter.

Table 2: Identifier and security level bit interaction

Identifier	Level	Command Result
User	High	The password supplied with the command shall be saved as the new User password. The lock mode shall be enabled from the next power-on or hardware reset. The ATA-Disk Module shall then be unlocked by either the User password or the previously set Master password.
User	Maximum	The password supplied with the command shall be saved as the new user password. The lock mode shall be enabled from the next power-on reset or hardware reset. The ATA-Disk Module shall then be unlocked by only the User password. The Master password previously set is still stored in the ATA-Disk Module shall not be used to unlock the ATA-Disk Module.
Master	High or Maximum	This combination shall set a Master password but shall not enable or disable the Lock mode. The security level is not changed.

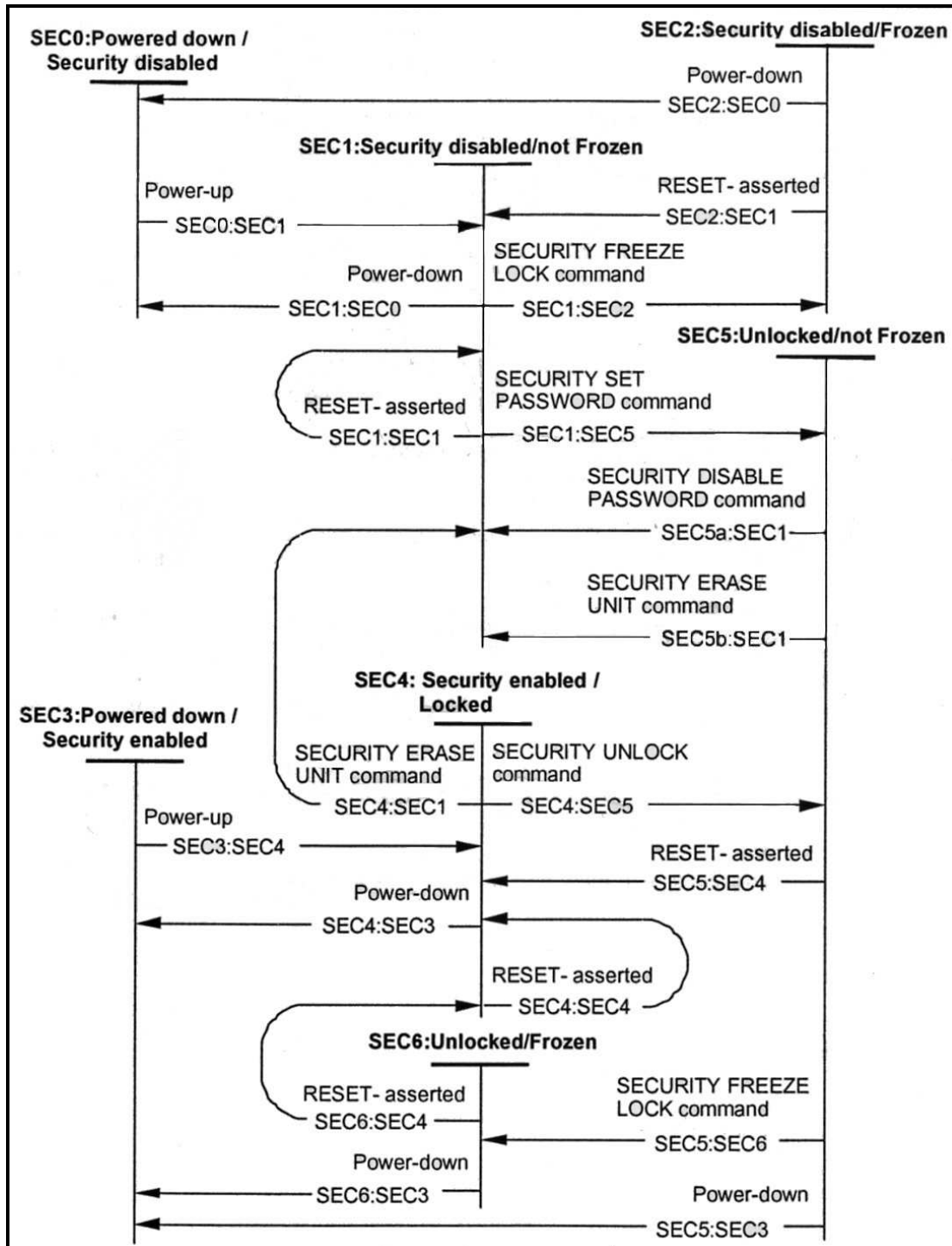


Figure 1 Diagram of Secure Erase Process

Conclusion

Data security has risen to be one of the highest concerns of computer professionals, and a high security protocol that requires special software and days to accomplish will be avoided by most users, making it little used and of limited practical value. For all but top-secret information, users will usually turn to erasure methods that take minutes rather than hours or days. They will select a method that gives them an acceptable level of security in a reasonable time window, which makes Secure Erase a good call for the need.

Apacer Technology Inc.

9/F, No. 100, Hsin Tai Wu Rd.
Hsichih, Taipei County 221, Taiwan
Tel: +886-2-2696-1666 Fax: +886-2-2696-1668
www.apacer.com

Copyright © 2009 Apacer Technology Inc. All Rights Reserved.

Information in this document is subject to change without prior notice.

Apacer and the Apacer logo are trademarks or registered trademarks of Apacer Technology Inc. Other brands, names, trademarks or registered trademarks may be claimed as the property of their respective owners.