X3T13/D96156R1

Enhanced Security
Erase Unit Proposal

To: X3T13 Technical committee
From: Dan Colegrove
IBM Corporation
5600 Cottle Rd.
San Jose, CA USA 95193
Phone: 408-256-1978
Fax: 408-256-1044
Email: colegrove@vnet.IBM.com
Date: 15 January 1997
Subj: Proposal to enhance the Security Erase Unit command

Introduction:
Erasing data on devices to a degree which makes recovery of previously written data impossible may require multiple write passes over the media with differing data patterns. User data may remain in sectors which have been relocated. The proposed enhanced erase feature of Security Erase Unit overwrites the data entire device, including
sectors that have been reallocated, with pre-selected patterns.

In high security applications it is necessary to insure that all data on a non-removable drive is erased when the drive is moved from one user or application to another. Currently there is no way to insure that all user data areas on a drive can be erased. Many ATA drives reallocate user data area when a sector on the media appears to be failing. Rewriting drives with a write command can not rewrite the area on the media in use before the reallocation.

To support applications where maximum security is required during a unit erase operation this proposal adds a new mode to the Security Erase Unit command. The Enhanced Erasure Mode allows a device manufacturer to store the data pattern used when overwriting the unit when the device is manufactured. All user data areas, including reallocated sectors, are to be overwritten with the stored pattern. If all user data can not be overwritten the device returns an Abort status.

The Enhanced Erasure Mode requires a new bit in Identify word.

Edits to 1153D:

Identify Device

Table 8: Add word 128 bit 5 1=Enhanced Security Erase Unit feature supported

7.8.47 Bit 5 of Word 128 indicates the Enhanced Security Erase Unit feature is supported

Identify Packet Device

Table 8: Add word 128 bit 5 1=Enhanced Security Erase Unit feature supported

7.8.47 Bit 5 of Word 128 indicates the Enhanced Security Erase Unit feature is supported

Security Erase Unit

7.25.6 Error Outputs

ABRT if this command not supported, device is in Frozen mode, not preceded by a SECURITY ERASE PREPARE command, or if the data area is not successfully overwritten.

7.25.8 Description

This command requests transfer of one sector of data from the host Table XX defines the content of this information. If the password does not match then the device rejects the command with an Aborted error.

The SECURITY ERASE PREPARE command shall be completed immediately prior to the SECURITY ERASE UNIT command. If the device receives a SECURITY ERASE UNIT command without an immediately prior SECURITY ERASE PREPARE command, the device aborts the SECURITY ERASE UNIT command.

When normal erasure mode is selected SECURITY ERASE UNIT command writes binary zeros to all user data areas. When enhanced erasure mode is selected SECURITY ERASE UNIT command writes data patterns stored at manufacturing to all user data areas. In enhanced erasure mode all previously written user data is overwritten, including sectors that are no longer in use due to re-allocation.

The unit erase command normal erase mode may require up to 30 minutes to complete. The unit erase command enhanced erase mode may require up to 8 hours to complete.

This command disables the device lock function, however, the master password is still stored internally within the device and may be reactivated later when a new user password is set.

Table XX– Security password content

Word	Content
0	Control word Bit 0 Identifier 0=compare user password 1=compare master password Bit 1 Erase Mode 0=Normal Erase 1=Enhanced Erase Bit 2-15 Reserved
1-16	Password (32 bytes)
17-255	Reserved

I.