Proposal to modify ATA-3

Secure mode feature set.

Toshiba Ome Works Proposal

v1.1

April 18, 1998

Technical Editor(s):

Tokuyuki Totani 81(428) 33-1292 totani@mdde.ome.toshiba.co.jp

Revisions

Revision 1.0 95/08/10 Initial issue.

Revision 1.1 95/08/11 Modify Secure Set Master Password command

To eliminate erroneous master password deletion, Master password reset requires password matching to the device holding master password.

Contents

BACKGROUND OF THE PROPOSAL.

Implementing Security mode feature set, we encountered a problem about user forgetting password. X3T10/94-087R1 writes about emergency user password feature. I understand that the Compaq Patent “Wipe Data” is a head ache for this feature. The problem about having master password with no wipe feature will allow OEM to have access to the user data. I assume X3T10/94-087R1 SECURE MODE FEATURE didn’t want this to happen and limited the password only to the user. The 360 bytes user emergency password was the answer for this problem.

Thinking about non-English, especially non-alphabetic country, this emergency feature is very difficult to implement. Talking about Japanese as a example, we need a so called front-end-processor to translate key inputs to Japanese characters. This front-end-software is a big program, which can not be implemented as a BIOS function. If we try to input the words in so called “Roma-ji” which is a direct conversion of Japanese language to English characters on how it sounds. This “Roma-ji” has some difficulty about sole translation. For sound like “CHI” in chicken, the “Roma-ji” allows “TI” and “CHI”. Same things with “JI” “ZI”, “SI” “SHI” and so on. So same user may write his home address in many ways.

Still OEM user (PC manufacture) requires access to the incoming drives for evaluation of the problem and etc.

We know that the protection level of the user data will decrease, but we want to propose master password implementation which cannot be accessed and modified by user.

Also thinking about user changing his normal password, which will be normally less than 16 bytes, the system has to set the emergency password again. This is because the “Secure Enable xx” command does not allow single password modification by the system. The system has to send all the passwords again. The BIOS engineer will not want to force user to retype all the emergency password again for changing his short password. Only way for the BIOS programmer is to remember the emergency password by non-volatile memory in the system. This is a big effort for the system to save 512 bytes of data. So we want to allow the device to limit the effective password length to the number less than 512 bytes.

Using secure mode feature set has possibility of user to lock the device by miss operation or some kind of virus to set a new password and lock the device. To protect the device from this kind of operation, we want to add a command to inhibit execution of secure mode feature set command until next power cycle or hard reset. The BIOS engineer should issue this command before the DOS operation begins.

If possible we also want to delete the Secure Unlock option with FT=87h. This option is a security hole for this specification. As the device will not lock itself on power cycle when the device is in this mode, user can easily remove the device and R/W from the device using another PC. When we remove this option, the Secure Lock command is also deleted, as this command will have no meaning. Also Lock Flag in Secure State will be removed. As this is a big change, we want the committee to discuss about this. Current proposal does not involve this change.

OUR PROPOSAL.

- Add a new command to set master password.
- Allow the device to limit the effective password length.
- Modify “SECURE UNLOCK” command
  - Add a counter to count unlock failure operation. If the failure exceeded 5 times during power on state, Lock all the secure command sets.
    The Lock state will break with power cycle or hard reset.
    This will protect the drive form password breaking software.
  - Include Master password for “SECURE UNLOCK” command password comparison.
- Modify “SECURE STATE” command
  - Reflect Master Password setting state.
  - Reflect the unlock failure state.
  - Reflect the Secure command inhibit state.
  - Delete Media Not Present bit, as this status can be detected by Not Ready error code.
- Add a new command to inhibit Secure Commands except Secure State command execution.

Following under lined paragraphs reflects the modification.

SECURE DISABLE

OPCODE - EAh

TYPE - Optional - Security Mode Feature Set.

PROTOCOL - Non-data command.

INPUTS - The Feature register shall be set to 80h.

NORMAL OUTPUTS - none.

ERROR OUTPUTS - Aborted Command error if:

- the device does not support the Secure Mode Feature Set.
- the device supports the Secure Mode Feature Set and the device is not already in Secure Mode.
- the device supports the Secure Mode Feature Set, is in Secure Mode and Locked.

PREREQUISITES - The device must be in Secure Mode and Unlocked.

DESCRIPTION - When the device is in Secure Mode Read Only or Read/Write, unlocked, with an existing set of valid passwords, this command shall remove the device from Secure Mode. When the device is in Secure Mode Write Protect, this command shall remove the device from Secure Mode.

Upon successful completion of this command, the device shall not be in Secure Mode. All passwords ***except Master password*** shall be deleted.

If this command is received when not in Secure Mode Read Only or Read/Write and unlocked state, or Secure Mode Write Protect, the command shall be rejected and an Abort error returned.

SECURE ENABLE READ ONLY

OPCODE - EBh

TYPE - Optional - Security Mode Feature Set.

PROTOCOL - PIO data out.

INPUTS - The Features register shall be set to 81h. The Sector Count register specifies the number of passwords to be set.

NORMAL OUTPUTS - none.

ERROR OUTPUTS - Aborted Command error if:

- the device does not support the Secure Mode Feature Set.
- the device is already in Secure Mode.
- the device supports the Secure Mode Feature Set and the number of passwords indicated in the Sector Count register is less than one or greater than that supported by the device.
- ***the device is in Inhibit mode.***

PREREQUISITES - The device must not be in Secure Mode.

DESCRIPTION - This command shall set the device into Secure Mode Read Only and define the valid set of passwords.

If the device is not in Secure Mode when the command is received, the value set in the Sector Count register indicates the number of 512 byte passwords that will be passed with this command. ***Number of bytes utilized by the device for the password is shown in Identify command word 50.*** If the Sector Count register contains a value less than 1 or greater than the maximum number of passwords supported by the device, the command shall not be executed and Abort error shall be returned.

If the device is in Secure Mode when this command is received, the command shall not be executed and an Abort error shall be returned.

SECURE ENABLE READ/WRITE

OPCODE - EBh

TYPE - Optional - Security Mode Feature Set.

PROTOCOL - PIO data out.

INPUTS - The Features register shall be set to 82h. The Sector Count register specifies the number of passwords to be set.

NORMAL OUTPUTS - none.

ERROR OUTPUTS - Aborted Command error if:

- the device does not support the Secure Mode Feature Set.
- the device is already in Secure Mode.
- the device supports the Secure Mode Feature Set and the number of passwords indicated in the Sector Count register is less than one or greater than that supported by the device.
- ***the device is in Inhibit mode.***

PREREQUISITES - The device must not be in Secure Mode.

DESCRIPTION - This command shall set the device into Secure Mode Read/Write and define the valid set of passwords.

If the device is not in Secure Mode when the command is received, the value set in the Sector Count register indicates the number of 512 byte passwords that will be passed with this command. ***Number of bytes utilized by the device for the password is shown in Identify command word 50.*** If the Sector Count register contains a value less than 1 or greater than the maximum number of passwords supported by the device, the command shall not be executed and Abort error shall be returned.

If the device is in Secure Mode when this command is received, the command shall not be executed and an Abort error shall be returned.

SECURE ENABLE WRITE PROTECT

OPCODE - EAh

TYPE - Optional - Security Mode Feature Set.

PROTOCOL - Non-data command.

INPUTS - The Feature register shall be set to 83h.

NORMAL OUTPUTS - none.

ERROR OUTPUTS - Aborted Command error if:

- the device does not support the Secure Mode Feature Set.
- the device supports the Secure Mode Feature Set and is already in secure mode.
- ***the device is in Inhibit mode.***

PREREQUISITES - The device must not be in Secure Mode.

DESCRIPTION - This command shall set the device into Secure Mode Write Protect. In this mode, the entire device can be read but all write commands shall be rejected.

Once placed in Secure Mode Write Protect state, the device data cannot be written to the device until it is removed from Secure Mode Write Protect by a Disable Secure command.

If the device is in Secure Mode Read Only, Read/Write or Write Protect state when this command is received, it shall be rejected and an Abort error returned.

SECURE LOCK

OPCODE - EAh

TYPE - Optional - Security Mode Feature Set.

PROTOCOL - Non-data command.

INPUTS - The Features register shall be set to 84h.

NORMAL OUTPUTS - none.

ERROR OUTPUTS - Aborted Command error if:

- the device does not support the Secure Mode Feature Set.
- the device supports the Secure Mode Feature Set and the device is not already in Secure Mode.
- the device supports the Secure Mode Feature Set, is in Secure Mode and Locked.
- ***the device is in Inhibit mode.***

PREREQUISITES - The device must be in Secure Mode and Unlocked.

DESCRIPTION - This command shall lock the device any time the device is in Secure Mode Read Only or Read/Write, unlocked. If the device was unlocked with the Features register value 87h, this is the only means of locking the device. If the device was unlocked with the Features register value 86h, either this command or powering-down the device shall cause the device to assume the locked state.

Upon successful completion of this command the device shall be in Secure Mode Read Only or Read/Write, locked, state.

If this command is received when the device is not in Secure Mode, or in Secure Mode Read Only or Read/Write, locked, state, the command shall be rejected and an Abort error returned.

SECURE STATE

OPCODE - EAh

TYPE - Optional - Security Mode Feature Set.

PROTOCOL - Non-data command.

INPUTS - The Features register shall be set to 85h.

NORMAL OUTPUTS - The Sector Count register specifies the Security Mode state as shown in Table 1.

Table 1 - Security Mode State

7	6	5	4	3	2	1	0
Secure Enable RW	Secure Enabled RO	Secure Enabled WP	Unlocked	Lock Flag	***Inhibit***	***Master Password***	***Unlock Failure***

Bit 7 - Secure Enabled RW - If set, indicates that the device has been set in Secure Mode Read/Write.
Bit 6 - Secure Enabled RO - If set, indicates that the device has been set in Secure Mode Read Only.
Bit 5 - Secure Enabled WP - If set, indicates that the device has been set in Secure Mode Write Protect
Bit 4 - Unlocked - If set, indicates that the device has been unlocked.
Bit 3 - Lock Flag - If the device is in Secure Mode and this bit is cleared, the device will assume the locked state when powered down. If the device is in Secure Mode and this bit is set, the device can only be locked by issuing a Lock command.
~~Bit 2 - Media Not Present - Set if the device is a removable media device and no media is present.~~
Bit 2 - Inhibit - Set if the device is in Inhibit mode. Inhibit mode is set by Secure Inhibit command.
~~Bit 1 - reserved.~~
Bit 1 - Master Password - Set if Master Password is set.
~~Bit 0 - reserved.~~
Bit 0 - Unlock Failure - Set if unlock failure exceeded 5 times.

ERROR OUTPUTS - Aborted Command error if the device does not support the Secure Mode Feature Set.

PREREQUISITES - None.

DESCRIPTION - This command shall return the Secure Mode state of a device that implements the Secure Mode Function Set. Upon completion of the command, the Sector Count register shall contain the Secure Mode state as shown in Table 1.

SECURE UNLOCK

OPCODE - EBh

TYPE - Optional - Security Mode Feature Set.

PROTOCOL - PIO data out.

INPUTS - The Features register shall be set to 86h or 87h. The Sector Count register shall be set to 01h. ***The Sector Number register shall be set FFh to unlock the device with master password. Other value for Sector Number register will unlock the device with existing set of valid passwords except the master password.***

NORMAL OUTPUTS - none.

ERROR OUTPUTS - Aborted Command error if:

- the device does not support the Secure Mode Feature Set.
- the device supports the Secure Mode Feature Set and the device is not already in Secure Mode.
- the device supports the Secure Mode Feature Set and the value set in the Sector Count register is not equal to 01h.
- ***the Sector Number register is set to FFh but the master password is not set.***
- ***the device is in Inhibit mode.***

PREREQUISITES - The device must be in Secure Mode.

DESCRIPTION - This command unlocks a device in the Secure Mode to allow data transfers.

When Sector Number register is set to the value other than FFh ,the device shall match the password received with this command with the existing set of valid passwords ***except the master password***. If the unlock password matches a password in the established set of passwords, the device shall unlock.

When Sector Number register is set to FFh ,the device shall match the password received with this command with the master password. If the unlock password matches the master password, the device shall unlock.

The Features register indicates the required action to relock the extent. If the Features register contains the value 86h, the device shall assume the lock state when powered-down. If the Features register contains the value 87h, the device shall only assume the locked state when the LOCK command is received, that is, the device may be powered-down and back up without assuming the locked state.

If this command is received when the device is in Secure Mode Read Only or Read/Write, unlocked state, the command shall be executed and if password does not match, an Abort error shall be returned but the device shall remain unlocked.

Thus when in the unlocked state, this command can be used to verify passwords. The Features register is used as described above to set or clear the Lock Flag.

If the password does not match 5 times, the device will disable all Secure Mode Feature Set commands except Secure State command execution. In this case Hard reset or power cycle is required to enable Secure Mode Feature Set commands.

Upon successful completion, the secure state shall reflect Secure Mode Read Only or Read/Write set and unlocked. Having been unlocked, the device shall now accept and execute all data transfer commands.

If this command is received when not in Secure Mode, the command shall be rejected and an Abort error returned.

SECURE SET MASTER PASSWORD

OPCODE - EBh

TYPE - Optional - Security Mode Feature Set.

PROTOCOL - PIO data out.

INPUTS - The Features register shall be set to 88h. The Sector Count register shall be set to 01h. The Sector Number register shall be set to 00h or FFh.

NORMAL OUTPUTS - none.

ERROR OUTPUTS - Aborted Command error if:

- ***the device does not support the Secure Mode Feature Set.***
- ***the device is already in Secure Mode.***
- ***the device is in Inhibit mode.***
- ***the Sector Number register is set to FFh and the password does not match the device master password.***

PREREQUISITES - The device must not be in Secure Mode.

DESCRIPTION - This command will not change the drive secure mode. This command only sets or resets the master password which is stored in the device.

When the Sector Number register is set to 00h, this command will set the master password. Upon successful completion of this command, the secure state shall reflect Master password set (bit 1 of the Secure Mode State set to 1), unlocked.

When the Sector Number register is set to FFh, this command will reset the master password. Upon successful completion of this command, the secure state shall reflect Master password not set (bit 1 of the Secure Mode State set to 0), unlocked. The received password data shall match the master password in the device.

In case of master password reset operation (Sector Number register = FFh), *if the password does not match 5 times, the device will disable all Secure Mode Feature Set commands except Secure State command execution. In this case Hard reset or power cycle is required to enable Secure Mode Feature Set commands.*

If the device is in Secure Mode when this command is received, the command shall not be executed and an Abort error shall be returned.

SECURE INHIBIT

OPCODE - EAh

TYPE - Optional - Security Mode Feature Set.

PROTOCOL - None-data command.

INPUTS - The Features register shall be set to 89h.

NORMAL OUTPUTS - none.

ERROR OUTPUTS - Aborted Command error if:

- ***the device does not support the Secure Mode Feature Set.***

PREREQUISITES - None.

DESCRIPTION - This command shall Inhibit the Secure Mode Feature Set command execution except Secure State and this command itself. The Inhibit mode will continue until next power cycle or hard reset.

Upon successful completion of this command, the secure state shall reflect Inhibit bit set (bit 2 of the Secure Mode State set to 1).

IDENTIFY command modification.

Word 50: Security mode

Bit 15 of word 50 is used to indicate the device supports the Security Mode Feature Set. The field, bits 14-8, indicate the maximum number of passwords the device can support ***excluding master password. The field, bits 3-0, indicate the number of byte by power of 2 the device supports for each password. The exceeding part of the password will not be used by the device for password comparison.***

Value in bits 3-0	effective bytes
0	**1**
1	**2**
2	**4**
3	**8**
4	**16**
5	**32**
6	**64**
7	**128**
8	**256**
9	**512**
other values	**512**