Western Digital Corporation
20511 Lake Forest Drive
Lake Forest, CA 92630

To: T10 CAP Working Group
Contact: Curtis E. Stevens
Phone: 949-672-7933
Email: Curtis.Stevens@wdc.com
Date: 10 July 2007

Subject: SPC-4, SAT-2, Proposal to add the ATA device password security feature

1 Related documents

ATA8-ACSr4b, AT Attachment 8 - ATA/ATAPI Command Set (ATA8-ACS) revision 4b
SPC-4r11, SCSI Primary Command Set – 4 (SPC-4) revision 11
SAT-r09, SCSI / ATA Translation (SAT) revision 09

2 Introduction

There are a variety of devices that are being bridged from a bus that uses a SCSI functional protocol to a bus that uses an ATA functional protocol. The SAT working group is defining methods for translating SCSI functions into ATA function sequences. One ATA capability with no translation is the Security Feature Set. Many ATA devices have this capability, but systems are unable to take advantage of this level of security because they do not have access to the ATA capability via a bridging device. This purpose of this proposal is to enable password security in ATA devices as it is defined in ATA8-ACS via the SECURITY PROTOCOL OUT command defined in SPC-4.

3 Proposed addition to SPC-4

A new additional sense code is proposed for SPC-4: ATA SECURITY CONFLICT.

4 Proposed additions to SAT-2

The following are the proposed additions to SAT-2.

8.a SECURITY PROTOCOL IN command

8.a.1 SECURITY PROTOCOL IN command overview

The SECURITY PROTOCOL IN command is used by the application client to cause the SATL to return Security feature set data extracted from the IDENTIFY DEVICE data from the ATA device. See ATA8-ACS for a description of the Security feature set and all of the functions defined therein. Table 6 shows the translation for fields specified in the SECURITY PROTOCOL OUT CDB.

Table 1 — SECURITY PROTOCOL OUT CDB field translations

Field	Description
OPERATION CODE	Set to A2h
SECURITY PROTOCOL	Set to EFh
SECURITY PROTOCOL SPECIFIC	Set to 0000h
INC_512	Set to zero
ALLOCATION LENGTH	Set to 0000_0010h
CONTROL	See 6.4

8.a.2 SECURITY PROTOCOL IN parameter data

Table 8 defines the parameter data sent in response to for the set password function.

Table 2 — SECURITY PROTOCOL IN parameter data

Bit Byte	7	6	5	4	3	2	1	0
0	Reserved							S_SUPRT
1	Reserved							S_ENABLD
2	(MSB)	SECURITY ERASE TIME						
3								(LSB)
4	(MSB)	ENHANCED SECURITY ERASE TIME						
5								(LSB)
6	(MSB)	MASTER PASSWORD IDENTIFIER						
7								(LSB)
8	Reserved							MAXSET
9	Reserved		EN_ER_SUP	PWCNTEX	FROZEN	LOCKED	S_ENABLD2	S_SUPRT2
10	Reserved							
15	Reserved							

If the security feature set supported (S_SUPRT) bit is set to zero, then the ATA device does not support the Security feature set. If the S_SUPRT bit is set to one, then the ATA device supports the Security feature set.

If the security feature set enabled (S_ENABLD) bit is set to zero, then the Security feature set is not enabled in the ATA device. If the S_ENABLD bit is set to one, then the Security feature set is enabled in the ATA device based on the setting of the user password via a set password function (see 8.b.1).

The value in the SECURITY ERASE TIME field indicates the time required by the ATA device to complete its security erase procedure in normal mode. Table 3 defines the values in the SECURITY ERASE TIME field.

The value in the ENHANCED SECURITY ERASE TIME field indicates the time required by the ATA device to complete its security erase procedure in enhanced mode. Table 3 defines the values in the ENHANCED SECURITY ERASE TIME field.

Table 3 — SECURITY ERASE TIME and ENHANCED SECURITY ERASE TIME field definition

Value	Time required for erase process
0000h	The time is not specified or the Security feature set is not supported
0001h - 00FEh	(Value in the field) x 2 minutes
00FFh	Greater than 508 minutes
0100h - FFFFh	Reserved

If the ATA device does not support the Security feature set (i.e., the S_SUPRT bit is set to zero) or the master password identifier, then the MASTER PASSWORD IDENTIFIER field shall be set to 0000h or FFFFh. If the ATA device supports the Security feature set and the master password identifier, then the MASTER PASSWORD IDENTIFIER field shall be set to the master password identifier set when the master password was last changed.

If the master password capability setting (MAXSET) bit is set to zero, and the Security feature set is enabled (i.e., the S_ENABLD bit is set to one), then the security level is set to high. If the MAXSET bit is set to one, then the security level is set to maximum.

If the enhanced erase mode supported (EN_ER_SUP) bit is set to zero, then the ATA device does not support the enhanced erase mode. If the EN_ER_SUP bit is set to one, then the ATA device supports the enhanced erase mode.

If the password attempt counter exceeded (PWCNTEX) bit is set to zero, then the password attempt counter has not decremented to zero. If the PWCNTEX bit is set to one, then the password attempt counter has decremented to zero.

If the frozen state (FROZEN) bit is set to zero, then the ATA device is not in the security frozen state. If the FROZEN bit is set to one, then the ATA device is in the security frozen state.

If the locked state (LOCKED) bit is set to zero, then the ATA device is not in the security locked state. If the LOCKED bit is set to one, then the ATA device is in the security locked state.

If the security feature set enabled 2 (S_ENABLD2) bit is set to zero, then the Security feature set is not enabled in the ATA device. If the S_ENABLD2 bit is set to one, then the Security feature set is enabled in the ATA device based on the setting of the user password via a set password function (see 8.b.1).The S_ENABLD2 bit shall be set the same as the S_ENABLD bit.

If the security feature set supported 2 (S_SUPRT2) bit is set to zero, then the ATA device does not support the Security feature set. If the S_SUPRT2 bit is set to one, then the ATA device supports the Security feature set. The S_SUPRT2 bit shall be set the same as the S_SUPRT bit.

8.a.3 SCSI commands allowed in the presence of various security modes

Certain commands may be allowed or conflict depending on the security mode setting that is in effect for an ATA device.

There are three possible modes:

a) security locked;
b) security unlocked or security disabled; and
c) security frozen.

If a SATL receives a command that is allowed for the current security mode setting of the ATA device, then the SATL translates the command and sends it to the ATA device. If a SATL receives a command that conflicts with the current security mode setting of the , then the SATL shall terminate the command with CHECK CONDITION status with the sense key set to ILLEGAL REQUEST and the additional sense code set to ATA SECURITY CONFLICT.

Table 4 shows the commands defined in SPC-4 and whether each command is allowed or conflicts depending on the security setting that is in effect for an ATA device. If a command in table 4 is not implemented by the SATL, then processing of the command is vendor specific.

Table 4 — SPC commands allowed in the presence of various security modes (page 1 of 2)

Command	Locked	Unlocked or Disabled	Frozen
ACCESS CONTROL IN	Allowed	Allowed	Allowed
ACCESS CONTROL OUT	Allowed	Allowed	Allowed
CHANGE ALIASES	Allowed	Allowed	Allowed
EXTENDED COPY	Conflict	Allowed	Allowed
INQUIRY	Allowed	Allowed	Allowed
LOG SELECT	??	Allowed	Allowed
LOG SENSE	Allowed	Allowed	Allowed
MANAGEMENT PROTOCOL IN	Allowed	Allowed	Allowed
MANAGEMENT PROTOCOL OUT	Allowed	Allowed	Allowed
MODE SELECT(6) / MODE SELECT(10)	??	Allowed	Allowed
MODE SENSE(6) / MODE SENSE(10)	Allowed	Allowed	Allowed
PERSISTENT RESERVE IN	Allowed	Allowed	Allowed
PERSISTENT RESERVE OUT	Allowed	Allowed	Allowed
READ ATTRIBUTE	Allowed	Allowed	Allowed
READ BUFFER	Allowed	Allowed	Allowed
READ MEDIA SERIAL NUMBER	Allowed	Allowed	Allowed
RECEIVE COPY RESULTS	Allowed	Allowed	Allowed
RECEIVE DIAGNOSTIC RESULTS	Allowed	Allowed	Allowed
RELEASE(6) / RELEASE(10)	Allowed	Allowed	Allowed
REPORT ALIASES	Allowed	Allowed	Allowed
REPORT IDENTIFYING INFORMATION	Allowed	Allowed	Allowed
REPORT LUNS	Allowed	Allowed	Allowed
REPORT PRIORITY	Allowed	Allowed	Allowed
REPORT SUPPORTED OPERATION CODES	Allowed	Allowed	Allowed
REPORT SUPPORTED TASK MANAGEMENT FUNCTIONS	Allowed	Allowed	Allowed
REPORT TARGET PORT GROUPS	Allowed	Allowed	Allowed
REPORT TIMESTAMP	Allowed	Allowed	Allowed
REQUEST SENSE	Allowed	Allowed	Allowed
RESERVE(6) / RESERVE(10)	Allowed	Allowed	Allowed

Table 4 — SPC commands allowed in the presence of various security modes (page 2 of 2)

Command	Locked	Unlocked or Disabled	Frozen
SECURITY PROTOCOL IN	Allowed	Allowed	Allowed
SECURITY PROTOCOL OUT	Allowed	Allowed	Allowed
SEND DIAGNOSTIC	Allowed	Allowed	Allowed
SET IDENTIFYING INFORMATION	Allowed	Allowed	Allowed
SET PRIORITY	Allowed	Allowed	Allowed
SET TARGET PORT GROUPS	Allowed	Allowed	Allowed
SET TIMESTAMP	Allowed	Allowed	Allowed
TEST UNIT READY	Allowed	Allowed	Allowed
WRITE ATTRIBUTE	Allowed	Allowed	Allowed
WRITE BUFFER	Allowed	Allowed	Allowed

Table 5 shows the commands defined in SBC-3 and whether each command is allowed or conflicts depending on the security setting that is in effect for an ATA device. If a command in table 5 is not implemented by the SATL, then processing of the command is vendor specific.

Table 5 — SBC commands allowed in the presence of various security modes (page 1 of 2)

Command	Locked	Unlocked or Disabled	Frozen
FORMAT UNIT	Conflict	Allowed	Allowed
ORWRITE	Conflict	Allowed	Allowed
PRE-FETCH (10) / (16)	Conflict	Allowed	Allowed
PREVENT ALLOW MEDIUM REMOVAL (Prevent=0)	Conflict	Allowed	Allowed
PREVENT ALLOW MEDIUM REMOVAL (Prevent<>0)	Conflict	Allowed	Allowed
READ (6) / (10) / (12) / (16) / (32)	Conflict	Allowed	Allowed
READ CAPACITY (10) / (16)	Allowed	Allowed	Allowed
READ DEFECT DATA (10) / (12)	Conflict	Allowed	Allowed
READ LONG (10) / (16)	Conflict	Allowed	Allowed
REASSIGN BLOCKS	Conflict	Allowed	Allowed
START STOP UNIT with START bit set to one and POWER CONDITION field set to 0h	Allowed	Allowed	Allowed
START STOP UNIT with START bit set to zero or POWER CONDITION field set to a value other than 0h	Allowed	Allowed	Allowed
SYNCHRONIZE CACHE (10) / (16)	Conflict	Allowed	Allowed

Table 5 — SBC commands allowed in the presence of various security modes (page 2 of 2)

Command	Locked	Unlocked or Disabled	Frozen
VERIFY (10) / (12) / (16) / (32)	Conflict	Allowed	Allowed
WRITE (6) / (10) / (12) / (16) / (32)	Conflict	Allowed	Allowed
WRITE AND VERIFY (10) / (12) / (16) / (32)	Conflict	Allowed	Allowed
WRITE LONG (10) / (16)	Conflict	Allowed	Allowed
WRITE SAME (10) / (16) / (32)	Conflict	Allowed	Allowed
XDREAD (10) / (32)	Conflict	Allowed	Allowed
XDWRITE (10) / (32)	Conflict	Allowed	Allowed
XDWRITEREAD (10) / (32)	Conflict	Allowed	Allowed
XPWRITE (10) / (32)	Conflict	Allowed	Allowed

8.b SECURITY PROTOCOL OUT command

8.b.1 SECURITY PROTOCOL OUT command overview

The SECURITY PROTOCOL OUT command is used by an application client to send Security feature set commands and data to the ATA device. See ATA8-ACS for a description of the Security feature set and all of the functions defined therein. Table 6 shows the translation for fields specified in the SECURITY PROTOCOL OUT CDB.

Table 6 — SECURITY PROTOCOL OUT CDB field translations

Field	Description
OPERATION CODE	Set to B5h
SECURITY PROTOCOL	Set to EFh
SECURITY PROTOCOL SPECIFIC	See table 7
INC_512	Set to zero
TRANSFER LENGTH	Based on the value in the SECURITY PROTOCOL SPECIFIC field
CONTROL	See 6.4

Table 7 defines the SECURITY PROTOCOL SPECIFIC field.

Table 7 — SECURITY PROTOCOL SPECIFIC field

SECURITY PROTOCOL SPECIFIC field	Description	ATA command (see ATA8-ACS for the specific actions)	Parameter data reference
0000h	Reserved		
0001h	Set password	SECURITY SET PASSWORD	8.b.2
0002h	Unlock	SECURITY UNLOCK	8.b.3
0003h	Erase prepare	SECURITY ERASE PREPARE	No data is transferred
0004h	Erase unit	SECURITY ERASE UNIT	8.b.4
0005h	Freeze lock	SECURITY FREEZE LOCK	No data is transferred
0006h	Disable password	SECURITY DISABLE PASSWORD	8.b.5
0007h - FFFFh	Reserved		

8.b.2 Set password parameter data

If the SECURITY PROTOCOL SPECIFIC field is set to 0001h in the SECURITY PROTOCOL OUT CDB, then the TRANSFER LENGTH field in the CDB shall be set to 24h. Table 8 defines the parameter data for the set password function.

Table 8 — Set password parameter data

Bit Byte	7	6	5	4	3	2	1	0
0	Reserved							MAXLVL
1	Reserved							MSTRPW
2	(MSB)	PASSWORD						
33								(LSB)
34	Reserved							
35								

If the maximum security level bit (MAXLVL) is set to zero, then the ATA device shall set the security level to high. If the MAXLVL bit is set to one, then the ATA device shall set the security level to maximum.

If the master password bit (MSTRPW) is set to zero, then the ATA device shall set the user password to the value in the PASSWORD field. If the MSTRPW bit is set to one, then the ATA device shall set the master password to the value in the PASSWORD field.

The PASSWORD field contains a 32-byte binary value.

8.b.3 Unlock parameter data

If the SECURITY PROTOCOL SPECIFIC field is set to 0002h in the SECURITY PROTOCOL OUT CDB, then the TRANSFER LENGTH field in the CDB shall be set to 24h. Table 9 defines the parameter data for the unlock function.

Table 9 — Unlock parameter data

Byte \ Bit	7	6	5	4	3	2	1	0
0	Reserved							
1	Reserved							MSTRPW
2	(MSB)	PASSWORD						
33								(LSB)
34	Reserved							
35								

If the master password bit (MSTRPW) is set to zero, then the ATA device shall compare the value in the PASSWORD field to the user password. If the MSTRPW bit is set to one, then the ATA device shall compare the value in the PASSWORD field to the master password.

The PASSWORD field contains a 32-byte binary value.

8.b.4 Erase unit data

If the SECURITY PROTOCOL SPECIFIC field is set to 0004h in the SECURITY PROTOCOL OUT CDB, then the TRANSFER LENGTH field in the CDB shall be set to 24h. Table 10 defines the parameter data for the erase unit function.

Table 10 — Erase unit parameter data

Byte \ Bit	7	6	5	4	3	2	1	0
0	Reserved							EN_ER
1	Reserved							MSTRPW
2	(MSB)	PASSWORD						
33								(LSB)
34	Reserved							
35								

If the enhanced erase mode bit (EN_ER) is set to zero, then the ATA device shall be set to use the normal erase mode. If the EN_ER bit is set to one, then the ATA device shall be set to enhanced erase mode.

If the master password bit (MSTRPW) is set to zero, then the ATA device shall compare the value in the PASSWORD field to the user password. If the MSTRPW bit is set to one, then the ATA device shall compare the value in the PASSWORD field to the master password.

The PASSWORD field contains a 32-byte binary value.

8.b.5 Disable password parameter data

If the SECURITY PROTOCOL SPECIFIC field is set to 0006h in the SECURITY PROTOCOL OUT CDB, then the TRANSFER LENGTH field in the CDB shall be set to 24h. Table 11 defines the parameter data for the disable password function.

Table 11 — Disable password parameter data

Byte \ Bit	7	6	5	4	3	2	1	0
0	Reserved							
1	Reserved							MSTRPW
2	(MSB)	PASSWORD						
33								(LSB)
34	Reserved							
35								

If the master password bit (MSTRPW) is set to zero, then, if the value in the PASSWORD field matches the user password, the ATA device shall disable the user password. If the MSTRPW bit is set to one, then, if the value in the PASSWORD field matches the master password, the ATA device shall disable the master password.

The PASSWORD field contains a 32-byte binary value.