Device Server Password Security

January 11, 2006

Rev 0

Technical Editor:
Curtis E. Stevens
Western Digital
Phone: 949-672-7933
E-Mail: Curtis.Stevens@wdc.com

1 Introduction

There are a variety of devices that are being bridge from a bus that uses a SCSI function protocol to a bus that uses an ATA function protocol. The SAT working group is defining methods for translating SCSI functions into ATA function sequences. This does not address the issue of translating ATA capabilities into SCSI. 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 simply because they do not have access to the ATA capability. This purpose of this proposal is to enable password security as it is defined in ATA/ATAPI-7.

2 Operational Model

2.1 *Overview*

The Device Server Security functions provide a password system that restrict access to user data stored on a device. The system has two passwords, User and Master, as well as two security levels: High and Maximum. The security system is enabled by sending a user password to the device with the SET PASSWORD function. When the security system is enabled, the device server shall deny access to all application clients until the User password is sent to the device server using the SECURITY PROTOCOL UNLOCK function. Once the device server grants access to the media (the device is unlocked), the device server shall remain unlocked until a power cycle.

A Master password may be set in addition to the User password. The purpose of the Master password is to allow an administrator to establish a password that is kept secret from the user, and which may be used to unlock the device if the User password is lost. Setting the Master password does not enable the password system (i.e. require a SECURITY PROTOCOL UNLOCK function before access is granted to the media)..

The security level is set to High or Maximum with the SECURITY PROTOCOL SET PASSWORD function. The security level determines device behavior when the Master password is used to unlock the device or disable security. When the security level is set to High the device requires the SECURITY UNLOCK function and the User or Master password to unlock the device. When the security level is set to Maximum, only the User password shall unlock the device. The Master password may be used to disable the security system. In Maximum security mode, the device requires a SECURITY PROTOCOL ERASE PREPARE function and a SECURITY PROTOCOL ERASE UNIT function with the master password to disable password protection. Execution of the SECURITY PROTOCOL ERASE UNIT function erases all user data on the device.

The SECURITY PROTOCOL FREEZE LOCK function prevents changes to passwords until a power cycle in the device is performed. The purpose of the SECURITY FREEZE LOCK function is to prevent password setting attacks on the security system.

A device that implements the Device Server Security Functions shall implement the following minimum function set:

- SET PASSWORD
- UNLOCK
- ERASE PREPARE
- ERASE UNIT
- FREEZE LOCK
- DISABLE PASSWORD

2.2 *Security mode initial setting*

When the device is shipped by the manufacturer, the state of the Security Mode feature shall be disabled. The initial Master password value is not defined by this standard.

If the Master Password Revision Code feature is supported, the Master Password Revision Code shall be set to FFFEh by the manufacturer.

2.3 *User password lost*

If the User password sent to the device server with the SECURITY PROTOCOL UNLOCK function does not match the user password previously set with the SECURITY SET PASSWORD function, the device server shall not allow the user to access data.

If the Security Level was set to High during the last SECURITY PROTOCOL SET PASSWORD function, the device shall unlock if the Master password is received.

If the Security Level was set to Maximum during the last SECURITY PROTOCOL SET PASSWORD function, the device shall not unlock if the Master password is received. The SECURITY PROTOCOL ERASE UNIT function shall erase all user data and unlock the device if the Master password matches the last Master password previously set with the SECURITY PROTOCOL SET PASSWORD function.

2.4 *Attempt limit for SECURITY PROTOCOL UNLOCK function*

The device shall have an attempt limit counter. The purpose of this counter is to defeat repeated trial attacks. After each failed User or Master password SECURITY PROTOCOL UNLOCK function, the counter is decremented. When the counter value reaches zero the EXPIRE bit (bit 4) of IDENTIFY DEVICE data word 128 is set to one, and the SECURITY UNLOCK and SECURITY UNIT ERASE functions are function aborted until the device is powered off or hardware reset. The EXPIRE bit shall be cleared to zero after power-on or hardware reset. The counter shall be set to five after a power-on or hardware reset.

3 Device Server Security Functions

3.1 *Overview*

The d security functions utilize the security protocol in and security protocol out functions to access the security system in the device server. TRUSTED PROTOCOL XXH has been assigned to the device server security functions.

Bit Byte	0	1	2	3	4	5	6	7
0	OPERATION CODE (B5H)							
1	TRUSTED PROTOCOL (XXH)							
2	SECURITY_FUNCTION					RESERVED		
3	RESERVED							
4	512_INC	RESERVED						
5	RESERVED							
6	(MSB)	TRANSFER_LENGTH						
7								

8		
9		(LSB)
10	RESERVED	
11	RESERVED	

SECURITY_FUNCTION	Description
0	Reserved
1	Set Password
2	Unlock
3	Erase Prepare
4	Erase Unit
5	Freeze Lock
6	Disable Password
7-Fh	Reserved

3.2 *Set Password*

Transfers 1 512 byte block of data as defined in table x1

Table x1

Word	Description	
0	Control Word	
	Bit	Description
	0	0 = Set/Compare User password 1 = Set/Compare master Password
	7:1	Reserved
	8	0 = High Security 1 = maximum Security
	15:9	Reserved
1-16	Password (32 bytes)	
17	Master password revision code (valid if word 0 bit 0 = 1)	
18-255	Reserved	

3.3 *Unlock*

Transfers 1 512 byte block of data as defined in table x1. Unlocks the device server for a specific application client.

3.4 *Erase Prepare*

Shall preceed erase unit. Does not transfer data

3.5 *Erase Unit*

Transfers 1 512 byte block of data as defined in table x3

Table x3

Word	Description	
0	Control Word	
	Bit	Description
	0	0 = Compare User password 1 = Compare master Password
	1	0 = Normal Erase 1 = Enhanced Erase
	15:2	Reserved
1-16	Password (32 bytes)	
17-255	Reserved	

3.6 *Freeze Lock*

Prevent changes to the security system. Does not transfer any data.

3.7 *Disable password*

Transfers 1 512 byte block of data, see table x4. Turn the system off.

Table x4

Word	Description	
0	Control Word	
	Bit	Description
	0	0 = Compare User password 1 = Compare master Password
	15:1	Reserved
1-16	Password (32 bytes)	
17-255	Reserved	