Mass Storage Media Locking

By

Curtis E. Stevens

WD
Agenda

• The Problem
• ATA Security
• OS Detection
• Possible Approaches
The Problem

• Small or externally attached devices can be lost or stolen
  – USB
  – 1394
  – SATA
  – PATA
  – CFA

• Many of these devices accept SCSI CDB’s as their primary commands
ATA Security

- ATA Security was introduced in ATA/ATAPI-4 in 1997 and has been developed over a period of 7 years.
- Provides the ability to password lock a device.
- Provides a mechanism to erase the media and the passwords in the normal security mode.
- Can turn the drive into a brick if passwords are lost in the high security mode.
Commands

• Security Disable Password
  – Turns off the password subsystem

• Security Erase Prepare
  – Security Erase is a 2 step process

• Security Erase Unit
  – Erase the media and as a last dying act, erase the passwords

• Security Freeze Lock
  – Prevent changes until the next power cycle

• Security Set Password
  – Enable the password subsystem

• Security Unlock
  – Open a password protected drive.
ATA Security

- Prevents the average user from gaining access to the data
- Protects the device, not the data
- Has been in use and tested for several years
- Implementation is light and well understood
- Other more complex methods are still being developed, but ATA style security can be implemented now.
OS Detection

- Some existing operating system standard drivers do not assign a drive letter if they are unable to read the media
- A locked device needs to be understood as locked
  - If the operating system does not have the capability to unlock the device it should prompt the user for a driver
- Detection is probably going to be bus specific
Proposal #1

- Use the SAT ATA pass through mechanism or create a new SCSI CDB that enables the 6 ATA security commands
- Use Inquiry byte 1 bit 0 to indicate that a device is locked
- Define a security mode page to indicate that security is implemented and the current status of the drive
Proposal #2

• Define a mode page for locking and unlocking

• Change write same to clear password where appropriate
  – Require Mode Select prior to write same
  – Use byte 1/10 bits 3 or 4 to indicate security erase.