Using the ATA Security Feature on Mac OS X with the Cypress MSC Driver

Cypress Semiconductor Corporation • 3901 North First Street • San Jose • CA 95134 • 408-943-2600
February 28, 2002

Overview

This document discusses the implementation of the ATA Security Feature in the Cypress MSC Driver on Mac OS X. The ATA Security Feature is a way to password protect the data on hard drives as documented in section 6.13 and 8.36 through 8.41 of the *Information Technology AT Attachment with Packet Interface (ATA/ATAPI-6)* specification from the T13 working group http://www.t13.org.

The Cypress MSC driver for Mac OS X provides password compatibility with the Cypress MSC driver for Mac OS 9 and the Cypress MSC driver for Windows. The first section of this document describes the Mac OS X solution from a user perspective. The second part of this document describes the implementation.

Cypress MSC Driver – User Interface

Assuming the Cypress MSC driver has been installed and supports the USB hard drive, when the user attaches a password protected USB hard drive, the driver will launch the ATASecurityHelper application. The ATASecurityHelper application provides the user interface for this feature. The ATASecurityHelper.app is localized into English and Japanese.

The main dialog is the Password Protected dialog, shown in Figure 1. This dialog provides a text entry field where the user enters the password. The text field is a standard password entry field so bullet "•" characters will be displayed instead of the actual password. This provides extra password security.

Typing the correct password and clicking the OK button will dismiss the dialog and the USB hard drive will be mounted on the desktop. The driver sends the `SECURITY UNLOCK (F2h)` command to the drive. This allows read/write access to the drive until the hard drive is removed from the USB. The next time the hard drive is attached to the USB the user will have to enter the password again.

Figure 1. The Password Protected dialog.

Checking the Disable Password Protection checkbox when sending down the correct password will permanently unlock the drive in addition to mounting the hard drive. The driver sends the `SECURITY DISABLE PASSWORD (F6h)` command to the drive. So from this point forward, whenever the hard drive is attached to a computer it will mount normally. Until which time as password protection is turned back on, of course.

Typing the incorrect password and clicking the OK button will cause an error dialog to be presented. Acknowledging the error by clicking the OK button and dismissing the error dialog, will bring you back, once again, to the Password Protected dialog.

Clicking the Cancel button will dismiss the dialog and the drive will remain on the USB locked and un-mounted.

The Secure Erase dialog, shown in Figure 2, is displayed when the user selects the I Forgot… button from the Password Protected dialog.

Figure 2. The Secure Erase dialog.

Clicking the Erase button will cause the driver to send the `SECURITY ERASE PREPARE (F3h)` send the `SECURITY ERASE UNIT (F4h)` commands to the drive. Both the Secure Erase dialog and the Password Protected dialogs will be dismissed and to provide feedback to the user a that the secure erase is in progress the Secure Erase in Progress dialog is displayed, shown in Figure 3. Once the command has been sent to the hard drive it cannot be cancelled. Actually, the command sent never completes, at least not until the secure erase process on the drive completes. And this can take on average a minute and a half per gigabyte of disk size. This requires the ATASecurityHelper.app to send the secure erase command on a seperate thread.

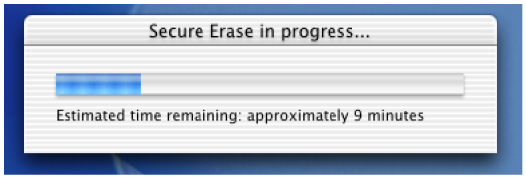

Figure 3. The Secure Erase in Progress dialog.

The Secure Erase in Progress dialog shows the estimated time remaining by way of a progress bar as well as a text description. It's the drive that reports the estimated amount of time that the secure erase process will take. The Secure Erase in Progress dialog continues to count down from the time reported until the time expires or the secure erase command completes.

Once the secure erase completes the user must format the drive in order to use the drive again. The Mac filesystem will display an Initialize Disk alert, shown in figure 7, when trying to mount the drive. If the user does not respond to the Initialize Disk alert within one minute, the dialog goes away and leaves the drive unmounted. During development and testing, it was common for the user to walk away while the secure erase was in progress. If the user misses the Initialize Disk dialog, the user has no feedback that the secure erase completed correctly, or not. So, when the secure erase command completes one more dialog is displayed – the Secure Erase Completed dialog.

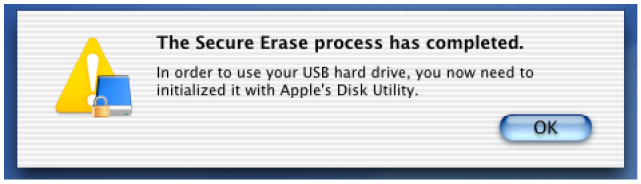

Figure 4. The Secure Erase Completed dialog.

In the event that the secure erase command completes and the ATASecurityHelper application has been moved to the background, we use the Notification Manager to tell the user to bring the ATASecurityHelper application back to the front. This is done in two ways. First, the alert in Figure 5 is displayed, which appears in front of all open windows. And second, the ATASecurityHelper application icon will repeatedly spring up from the Dock enticing the user to click it's icon and thus bring the application to the front.

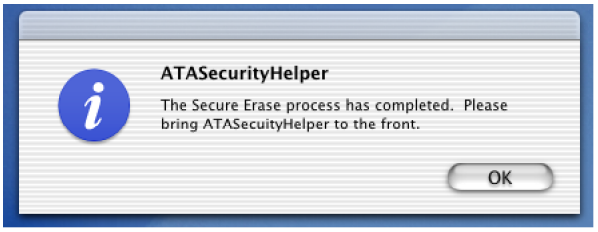

Figure 5. The Notification of Secure Erase Complete dialog.

Figure 6. The ATASecurityHelper icon in the Dock.

Once the application has been brought to the front, the Secure Erase Completed dialog will be display. When the Secure Erase Completed dialog is dismissed the driver will attempt to mount the drive. The filesystem will fail to read any partition information on the drive and display the Initialize Disk alert, see figure 7, which was discussed earlier. Clicking the Initialize…buttion in the Initialize Disk alert will launch Apple's Disk Utility. Then the user can reformat or repartition the drive.

Figure 7. The Initialize Disk Alert.

Cypress MSC Driver – Implementation Information

There are two passwords defined in the ATA Security Feature – a user password and a master password. The Cypress MSC Driver for Mac OS X provides password compatibility with the Cypress MSC Driver for Mac OS 9 and Windows by using the same master password. This allows users to set the user password and lock and unlock the drive, but if the user forgets the user password, the master password is needed to perform a secure erase of the drive and thus disable password protection of the drive.

Support for the Security Mode feature set is detected by the driver in the Security status field (Word 128) of the IDENTIFY DEVICE (ECh) command. The IDENTIFY DEVICE command is sent during initialization of the driver. If the Security locked bit of the Security Status field is set, the Cypress driver will build up the USB and ISDBlockServices layers in the driver stack but report to the OS that no media is present. This will prevent the upper layers of the driver stack from building up. The driver will then attempt to get help supporting the locked device (as will be discussed next) and then go idle. The driver will stay in this state until either the drive is removed from the

USB or a user space application communicates with the driver via the ATASecurity User Client interface. Once the drive has been unlocked, the driver sends a message that media is now present. This causes the upper layers of the driver stack to continue building up and the driver being mounted on the desktop.

The Cypress driver attempts to handle the Security Locked in two methods. First, the driver will attempt to launch a known helper application packaged with the driver called ATASecurityHelper.app. If that fails, the driver will then broadcast a General Interest Notification message that help is needed to mount this disk. This General Interest Notification could be handled by any vender provided user space application.

The application ATASecurityHelper.app was developed to provide a user interface for the ATASecurity Feature. This ATASecurityHelper application provides the user interface for entering the password, disabling the password lock, and if the user has forgotten the password the user can perform a secure erase. The ATASecurityHelper.app is bundled with the driver - literally. The ATASecurityHelper is shipped inside of the com_cy_driver_USB_Device.kext Bundle, in the Resources directory.

The anatomy of the Cypress MSC driver for Mac OS X is as follows:

```
com_cy_driver_USB_Device.kext
  |--- Contents
       |----     Info.plist
       |----     PkgInfo
       |----     MacOS
                 |---- com_cy_driver_USB_Device
       |----     Resources
                 |---- Enlish.lproj
                          |----InfoPlist.strings
                 |---- ATASecurityHelper.app
```

The ATASecurityHelper.app can be deleted from the kext to reduce the size of the kext bundle without issue. The ATASecurityHelper.app could also be completely replaced by an OEM customer. As long as the customer gives the custom application the name "ATASecurityHelper.app" and put it into the Resources directory of the kext bundle, the driver will launch it.