Adding Security to Removable Mass Storage

Introduction

As portable media proliferates into more and more consumer products, data security is becoming increasingly important. New products need to be secure in order to protect confidential information from theft.

Biometric security offers an economical solution that doesn't add significant user burdens such as extra passwords or additional log-in steps. Biometric security methods include fingerprint sensing, retina and iris scanning, signature analysis and hand geometry. Consider the case of fingerprint sensing. With a simple swipe of a finger, a user can authenticate himself to gain access to data on a portable storage device.

This article will provide a simple, step by step design sequence to add fingerprint security to a USB mass storage device.

Identification and Security Issues

Identification comes in different forms ranging from passwords to dongles to biometrics. These days, there is a password for everything. Remembering passwords usually involves storing them somewhere, which, in the security sense, is self defeating. Dongles are expensive to manufacture and are prone to being misplaced. Biometric applications need no passwords, require small and relatively inexpensive hardware, and fingerprints are never lost.

There are various methods used to keep data secure from an unauthorized user. These include encryption and drive manipulation, among others. Encryption comes in two forms: software and hardware. Hardware encryption adds cost and size to a design. Software encryption is slow when used on larger drives. Drive manipulation involves hardware locking of the drive to prevent access to unauthorized users. One such locking mechanism is ATA Security, a feature available on all new hard drives. Here, a 32-byte password is sent to the drive electronics to put it into “Secure” mode. After being power cycled, the drive comes up in a locked state until a password is provided. Since only the microcontroller in the enclosure knows the password, moving the drive to an unprotected enclosure won’t make the drive readable.

Sensor Types

Sensor types vary in the way they communicate data as well as in the method of USB communication. Some sensor solutions require image processing on the PC while other solutions use a co-processor to process image data. Different sensors also employ differing USB interfaces for getting data back to the PC. Such interfaces include Printer Class, Storage Class and Human Interface Device (HID) Class. There are pros and cons for all three, but they all share the advantage of using only native Windows drivers, making device installation unnecessary.

On the hardware side, there are various interfaces ranging from SPI to Parallel bus. The type and speed of interface is related to the method of image processing. The sensor with the co-processor requires only a few hundred kilobits per second while the sensor that uses the PC for image processing requires a 6.5-Megabit per second throughput. The sensor used in the implementation described here is available with either an SPI or a Parallel bus interface.

System Requirements

Removable storage is generally made up of a 2.5” or smaller Hard Disk Drive, a drive enclosure, power supply and a USB-to-ATA bridge. This solution allows for a very modular design. Adding a fingerprint sensor, as will be seen, is not that difficult. The USB-to-ATA Bridge for this design will be the Cypress EZ-USB FX2-LP. The following section will detail the addition of the Authentec AES2510, a slide type of fingerprint sensor, to an existing USB Mass Storage device. The AES2510 does not have a coprocessor, so the interface between it and the USB controller

needs to support data burst rates up to 6.5-Mbps to keep up with the data coming from the sensor during a finger swipe. This isn't a problem since the FX2-LP can already keep up with Hard Drives using UDMA-100 transfer rates. Since image processing will be done on the PC, there will be instances where the USB controller will be required to rapidly switch its interface back and forth between an ATA interface and a fingerprint sensor interface. This is easily accomplished by modifying the FX2-LP's interface on the fly. Following is a block diagram of the USB-to-ATA Bridge with the fingerprint sensor added.

Implementation

For this design, the sensor interface will be added to a standard USB-to-ATA Bridge reference design using the Cypress EZ-USB FX2-LP. The FX2-LP contains a USB 2.0 Serial Interface Engine (SIE), an enhanced 8051 microprocessor and a General Purpose Interface (GPIF). The GPIF is a state-machine based interface capable of data transfers of up to 96 Mbps. The GPIF can be configured for various interfaces including ATA, NAND, Utopia, EPP and Compact Flash. Since the GPIF is a RAM based state machine, multiple sets of control waveforms can be copied in and out, making the GPIF a reconfigurable interface under firmware control. Since the GPIF is directly connected to the FX2-LP's USB FIFOs, there is no need for firmware to do any data manipulation on the sensor data stream.

For this design, the GPIF waveforms will include PIO Read and Write as well as UDMA Read and Writes for the ATA interface. Additional waveforms for reading from and writing to the fingerprint sensor will be added to the project. The firmware for the hard drive functionality will be from the CY4611 Mass Storage reference design. Firmware for the fingerprint sensor will be taken from a code library supplied by the sensor manufacturer.

The AES2510 is available with either an SPI or a parallel bus interface. Since our existing hardware already uses a parallel interface, we have chosen the parallel version of the AES2510. I/O requirements include an 8-bit data bus, plus six control bits - RD, WR, CS, A0, INT and PWR_CTRL. We can share the lower byte of the ATA bus for data if we are careful with the chip select inputs to both the sensor and the ATA bus. For the control and status, we can use Port C of the FX2-LP.

Communication between the sensor and the application software is accomplished via the SCSI Pass Thru interface, an extension to the Windows Mass Storage Driver. Use of SCSI Pass Thru enables the sensor to use the same USB interface as the Mass Storage Device, so no additional device drivers are required for this device.

When a Pass Thru command is received, firmware from the sensor library is used to process the command. The very first thing that the firmware does is to overwrite the GPIF waveform memory, replacing the ATA waveforms with sensor waveforms. Then the firmware acts upon the Pass Thru command performing the required reads and writes to the sensor. When the pass thru cycle is complete, the ATA waveforms are copied back into GPIF memory.

User Interface

A typical secure drive will contain 3 partitions. One partition will contain the Biometric Application Software. This partition will usually emulate a CD-ROM for two reasons:

- CD-ROM offers a better AutoRun response than a disk drive in Windows
- CD-ROM is write protected so the Biometric application cannot be accidentally erased

One of the two remaining partitions will be for un-secured storage. The user will be able to access this data at any time. The last partition will contain the protected data area. The user will not be able to access the data in this partition without first verifying ownership via his fingerprint.

A biometric application will Auto-Run from the emulated CD-ROM partition on drive start up. The application will process fingerprint image data sent via the Pass Thru interface for the purposes of both user enrollment and user verification. Verification is based on a comparison of the user's swiped fingerprint to their enrolled fingerprint image. Once the user is verified, the public partition will be "unlocked" and its data will be available to the user. If the drive is disconnected from USB or if power is removed, the protected area will once again become inaccessible to the user.

Summary

This article has described the addition of biometric security to a USB based mass storage design. The Cypress EZ-USB FX2-LP has eased this implementation due to its flexible nature and its configurable interface port. Because of the flexibility of the FX2-LP, adding biometric verification has become an easy task. With some additional proprietary firmware, full drive security can be realized.

Cost of components to add the biometric option is under $7.00. Solutions for other media such as NAND-Flash are currently under development.

For information on the Cypress EZ-USB FX2-LP, please visit www.cypress.com

For information on the AES2510 fingerprint sensor, please visit www.authentec.com