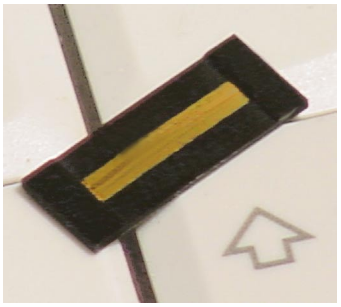
THE POSSIBILITIES ARE INFINITE FUJITSU

Simple Fingerprint-Based Security Protects Notebook PCs



TECHNOLOGY BACKGROUNDER

Introduction

Lost or stolen notebook computers make headlines when they contain personal information on millions of people or data from nuclear weapons research. More quietly, corporations are becoming increasingly alarmed by the loss of notebooks that contain company-confidential information and enable access to corporate networks. Given that many thousands of notebooks go missing every year, increasing numbers of companies and government agencies are looking for security solutions.

These solutions typically begin with tightened policies on the use of employee notebooks and—as these measures inevitably fail to prevent security breaches—expand toward technological solutions. Data encryption is a good step, but when users' passwords are compromised along with their notebooks, thieves instantly gain access to the data. Even if password protection is unbroken on encrypted files, the temporary files stored by widely used Windows applications leave un-encrypted data on a disk for access by thieves.

The key to locking up notebook data successfully is to prevent thieves from gaining any access to notebook functions that enable data retrieval—in other words, keep unauthorized users from even booting the operating system. This lock-up requires two pieces of technology that are readily available today: an authentication step built into the machine's BIOS and an authentication method that is extremely difficult to compromise. Fingerprint matching is such a method. It relies on compact, low-power hardware and pre-integrated software that is highly accurate and easy to use. Unlike plug-in tokens, fingerprints cannot be lost or stolen.

This technology backgrounder describes a complete pre-boot authentication (PBA) system for x86-based PCs that includes the following low-cost hardware and software/firmware:

- The Fujitsu Microelectronics MBF320 fingerprint Sweep Sensor™ IC
- Pre-boot user authentication powered by TrustedCore PBA from Phoenix Technologies
- Cogent Systems' fingerprint-matching algorithms

Phoenix Technologies also offers additional security options, including the ability to password-protect ATA-5 (or later) hard drives. Even if a secured drive is physically removed from one system and put into another, the disk data cannot be accessed until the drive receives the password. Though managed by the Phoenix TrustedCore firmware, this password protection is part of the ATA-5 specification.

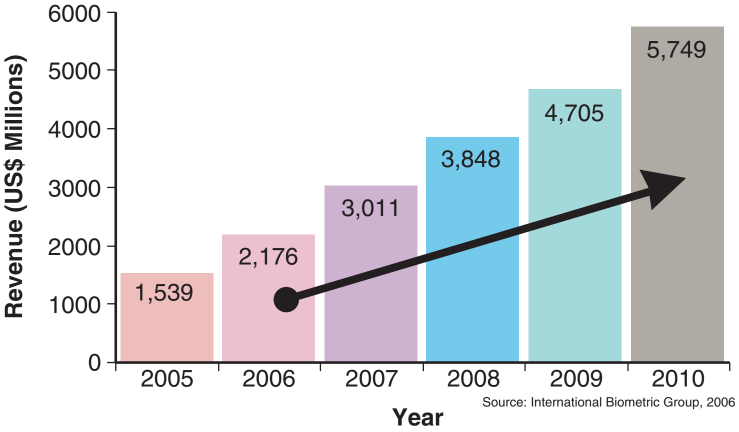
Growing Demand for Notebook Security

Significant drivers for the adoption of fingerprint authentication include the individual's desire to avoid identity theft and the need to prevent the compromise of corporate information. Much more important, however, is the role of government. In the US, federal, state and local governments are tightening their data security. The White House Office of Management and Budget (OMB) has introduced new guidelines for federal employees that include encrypting sensitive data on notebooks and authenticating users with both passwords and some other physical method. These new guidelines came out after a single month in which five different agencies of the US federal government admitted that data thefts or disclosures had compromised Social Security numbers and other private data on millions of people.

Numerous government programs are pushing the use of biometric authentication worldwide. For example, one of the United States Department of Homeland Security's top-priority programs, the United States Visitor and Immigrant Status Indicator Technology (US-VISIT), includes fingerprint authentication. The European Union's Visa Information System (EU-VIS) is currently entering its second phase, which will include the addition of fingerprints to the Schengen Information System.

Moreover, government legislatures are mandating that enterprises use multi-factor authentication to access critical data. A biometric credential in the form of a fingerprint helps enterprises meet such mandates cost-effectively. The increasing familiarity with the use of fingerprints for government-mandated security will help drive the acceptance of this method into many applications—including notebook security.

As a result of the new security requirements in and out of government, the overall biometric authentication market is expected to continue its rapid growth rate (Figure 1), with fingerprint authentication accounting for 44 percent ($957M) of the total biometric market in 2006, according to the market projection of International Biometric Group.

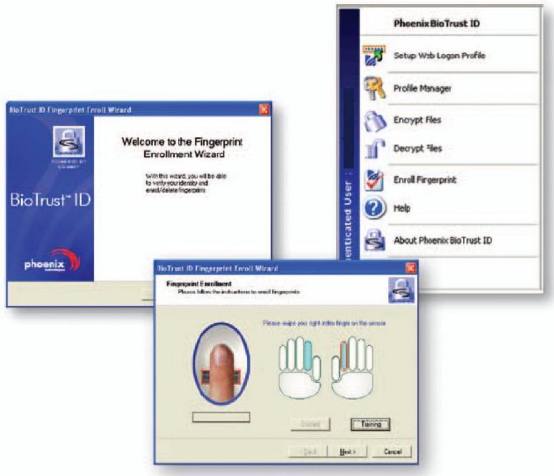


Source: International Biometric Group, 2006

Figure 1 - Annual Biometric Industry Revenue

The User's View of Fingerprint Authentication

Before looking at the operation of each element in the authentication system, consider how the system works from the user's point of view. When setting up a new notebook, the user enters his or her fingerprint to be used for authentication. This enrollment step is done via a Windows wizard (Figure 2). Physically, the user swipes a finger across a tiny sensor built into the notebook. When the wizard has confirmed that the authentication engine recognizes the user's fingerprint over multiple swipes, the enrollment process is complete.


BioTrust ID Fingerprint Enroll Wizard

Welcome to the Fingerprint Enrollment Wizard

With this wizard, you will be able to verify your identity and enroll/delete fingerprints

BioTrust ID Fingerprint Enroll Wizard

Fingerprint Enrollment

Please follow the indications to enroll fingerprints

Please swipe your right index finger on the sensor

Figure 2 - BioTrust ID Enrollment Wizard by Phoenix

As part of the enrollment process, the user can set up several authentication options. For example, the system can give access to all functions after one fingerprint authentication. Alternatively, separate fingerprint authentications and/or password entries can be required for each type of privileged access, such as network logon or file decryption.

The next time the user turns on the notebook, an authentication message requests that the user enter a fingerprint. After the user swipes a finger across the sensor, the authentication firmware confirms the user's identity and allows the system to boot normally.

If the fingerprint does not match that of the enrolled user(s), the notebook will not boot the operating system. The unauthorized user cannot use Windows or DOS commands to access the notebook's hard drive, logon to a network or use any other system function.

MBF320 Fingerprint Sweep Sensor IC

The only new hardware needed to enable the fingerprint authentication system is the Fujitsu Microelectronics MBF320 fingerprint Sweep Sensor IC (Figure 3) with a few passive components. Packaged in a 43-pin plastic fine-pitch ball grid array (FBGA), this IC provides a single-chip solution, in contrast to the multiple-device products offered by most competitors. Measuring just 16 x 6.5 x 0.9 mm, the Fujitsu chip

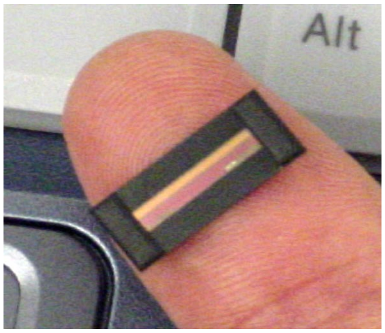


Figure 3 - Fujitsu Microelectronics MBF320 Fingerprint Sweep Sensor IC

integrates the sensor array, associated data-collection circuitry, and a USB 2.0 full-speed interface as shown in Figure 4. The device is designed for fully automated, high-volume assembly.

Because the sensor stays in low-power mode except when needed for a fingerprint scan, low standby current is crucial. At 12 microamperes typical (3.0V to 3.6V), the MBF320 causes negligible battery drain. Even when the device's auto-finger-detection circuit is enabled, current increases to only 150 microamperes. Typical operating power consumption is 55 milliwatts.

A 256 x 8 array of metal electrodes on the chip's surface captures the image of a fingerprint using capacitance detection. The surface of the finger acts as one plate of the capacitor, and each electrode in the array acts as the other plate. The detector surface is protected by a patented, ultra-hard abrasion- and chemical-resistant coating, which also acts as the capacitor dielectric. A patented finger-guide feature helps center the finger over the sensor array.

When a user swipes a finger across the sensor surface, the finger's ridges and valleys cause minute capacitance variations. The sensor reads the related voltage changes via an 8-bit A/D converter, automatically adjusting the circuit to ensure full-scale readings. The result is a high-resolution image of the fingerprint—500-dpi resolution with 8-bit grayscale. Software provided by Fujitsu captures the multiple 256 x 8-dot fingerprint image frames from a scan and constructs the complete fingerprint image.

The MBF320 is the latest device in a family of fingerprint sensors introduced by Fujitsu Microelectronics in 2001. This family includes both scan devices, such as the MBF310, and the full-array area sensor MBF320. In addition to the PC pre-boot authentication described in this paper, the sensors suit a wide range of applications, including USB flash drives and ID tokens, systems that authenticate citizens at border crossings, point-of-sale systems, and stand-alone fingerprint-matching devices. The latter can be used in door lock applications, time and attendance terminals, handheld devices, safes, lockers and many other devices that do not include a PC.

PC Software/Firmware

For PC applications, the Fujitsu MBF320 sensor has been pre-integrated with fingerprint recognition algorithms from Cogent Systems and three software products from Phoenix Technologies. Figure 5 shows the hardware, software and firmware involved.

The fingerprint recognition algorithms are implemented in a matching engine that plugs into the Phoenix software framework. The algorithms use an approach first developed by Cogent Systems in 1990 and refined through several product generations. This area-based modeling recognition approach performs pattern recognition by evaluating small regions of a fingerprint (Figure 6) rather than individual points or curves.

Making more than two million comparisons per second, this method provides quick, highly accurate results and is used in access control solutions by governments, law enforcement agencies and commercial customers. Most recently, Cogent's technology was selected to support the US-VISIT program. Cogent has also provided the core matching platform for EURODAC, a European Union system used by 26 nations to verify political asylum applications.

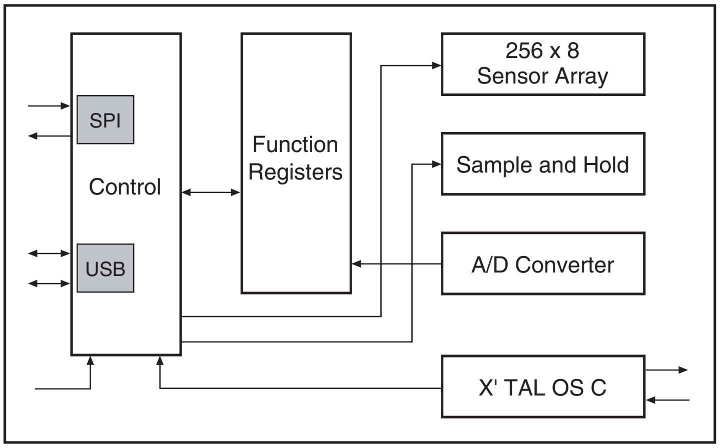
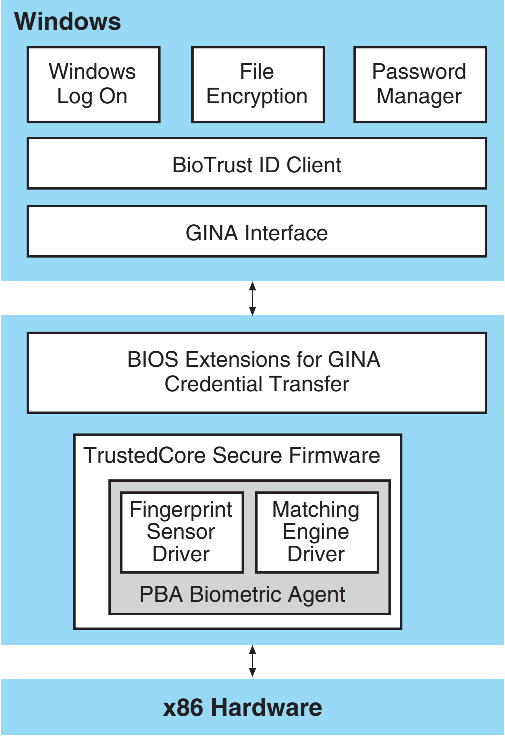


Figure 4 - MBF320 Fingerprint Sweep Sensor IC Block Diagram



Source: Phoenix

OS Level
- Industry leading matching algorithm
- End-to-End Solution

PBA Biometric Agent
- Matching engine and biometric sensor driver
- No development time (turn-key)
- Standardized pre-boot solution, not vendor specific boot
- End-to-End Solution

No Companion Chip
- USB integrated controller
- Cost saving ($3 to $5)
- Power saving

Figure 5 - Fingerprint Authentication System

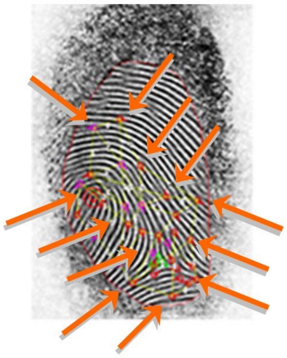


Figure 6 - Cogent Area-Based Recognition Approach

Working with the matching engine in the PC application are the three Phoenix software products:

- TrustedCore SP2+
- PBA Biometric Agent
- BioTrust ID

TrustedCore is Phoenix Technologies' widely used BIOS firmware—the BIOS product used in approximately 50 percent of the world's notebook PCs. For pre-boot authentication, the BIOS works with the PBA Biometric Agent, which is also implemented in firmware. The Agent runs at system start-up without use of the operating system or hard drive. Because this authentication functionality is always present in the firmware, it cannot be avoided or circumvented.

The third Phoenix product, BioTrust ID for Windows, enrolls new users and uses the TrustedCore PBA services to validate existing users after Windows has booted. All data is synchronized with the PBA Biometric Agent, and all changes to fingerprints and new enrollments are sent to the PBA for secure storage in firmware. Note that the Windows client is not involved in booting the PC, but this client provides a fully integrated turnkey solution for enrolling new fingerprints, including a friendly user interface with wizards.

Additionally, BioTrust ID integrates easily with existing enterprise infrastructure such as Active Directory, Lightweight Directory Access Protocol (LDAP) directory servers. Such solutions enable enterprises to manage user access from a central location.

Integrated Authentication System

Because the hardware, software and firmware for fingerprint authentication have been pre-integrated, installing them in a target platform requires few adaptations. PC OEMs develop the BIOS as usual and fill in the code that communicates with the target hardware. This hardware-specific code includes a sensor driver and matching engine driver, both available from Fujitsu Microelectronics.

In fact, the only hardware-specific code is in these drivers, so only the drivers need to be changed for integration. Typically, OEMs need to modify about six lines of this code for the target platform. The code is then compiled and put into the BIOS firmware. The only other integration requirement is that the platform include enough NVRAM to store the fingerprint templates. For customers who want to integrate PBA with their Windows client logon software, Phoenix provides a security software developer's kit that includes full biometric authentication API support into Trusted Core and the PBA biometric stack.

With this authentication system in place, users have a simple way to secure notebook PCs without worrying about forgotten passwords, misplaced tokens and other inconveniences. As the demand for data security grows, this type of simple fingerprint authentication promises to offer strong product differentiation.

For More Information

For more information about the Fujitsu biometric sensors, please visit the company's website at http://us.fujitsu.com/micro/biometricsensors or send e-mail to inquiry@fma.fujitsu.com

FUJITSU MICROELECTRONICS AMERICA, INC.
Corporate Headquarters
1250 East Arques Avenue, M/S 333, Sunnyvale, California 94085-5401
Tel: (800) 866-8608   Fax: (408) 737-5999
E-mail: inquiry@fma.fujitsu.com   Web Site: http://us.fujitsu.com/micro

Printed in U.S.A.
BMS-TB-21211-8/2006