SecuGen

Contents

1. Biometrics Defined

What qualities distinguish one person from his neighbor? Of course our personalities differ to some extent, but there is a physical uniqueness as well. Once identified, these physical characteristics can be exactly measured, numbered, counted – the statistical use of the variations in these unique elements of living organisms is known as biometrics. Biometrics data in human beings can be collected and analyzed in a number of ways, and are currently being used as a method of personal identification in which people are recognized by their own unique corporal or behavioral characteristics. Human traits and behaviors that can be used in biometrics include fingerprints, voice, face, retina, iris, handwriting, and hand geometry. Essentially, it is the same system the human brain uses to recognize and distinguish the man in the mirror from the man across the street.

Using biometrics for identifying and authenticating human beings offers some unique advantages over more traditional methods. Only biometrics authentication is based on the identification of an intrinsic part of a human being. Tokens, such as smart cards, magnetic stripe cards, and physical keys can be lost, stolen, or duplicated. Passwords can be forgotten, shared, or unintentionally observed by a third party. Forgotten passwords and lost "smart cards" are a nuisance for users and an expensive time-waster for system administrators.

Biometrics can be integrated into any application that requires security, access control, and identification or verification of users. With biometric security, we can dispense with the key, the password, the PIN code; the access-enabler is *you* – not something you know, or something you have. Remember, biometrically secured resources are based on *who a person is,* effectively eliminating all of the risks associated with less advanced technologies, while at the same time offering a higher level of security and convenience to users and administrators alike.

With our increasing reliance on online technology and other shared resources, the information age is quickly revolutionizing the way transactions are initiated and completed. Everyday actions are increasingly being handled electronically, and this growth in electronic transactions has resulted in greater demands for fast and accurate user identification and authentication methods. Advances in technology occur at a lightning pace, changing the way we do things at home and at work. Increasingly we find ourselves struggling to retain mastery of a host of constantly evolving technologies and services. Biometrics may soon be the rudder we need to guide us through these rapidly shifting and interconnected seas. It not only offers a solution for well-known and established security issues, but in all likelihood, biometrics may help to prevent future issues from surfacing. Perhaps the best way to fully comprehend the potential market for biometrics devices is to answer a simple question: what thief would steal something that

only operates in the hands of its rightful owner? You don't have to think about it very long. The biometrics age may soon be upon us.

Types of Biometrics Systems Currently in Use:

- Fingerprint Recognition
- Face Recognition
- Iris Recognition
- Retina Recognition
- Hand Geometry
- Finger Geometry
- Palm Recognition
- Voice Recognition
- Signature Recognition

2. Biometrics Applied

Essentially, there are two key functions offered by a biometric system. One is identification, a one-to-many matching process, in which a biometric sample is compared against a database of stored users. The other is verification, a one-to-one matching process, in which the biometric system will verify whether or not an individual's biometric sample matches previously enrolled data.

In computer security, the term biometrics refers to authentication techniques that rely on measurable biological characteristics that can be automatically checked. Examples include computer analysis of fingerprints or speech. Biometrics security technology basically acts as a front end to a system that requires precise identification before it can be accessed or used. That system could be a sliding door with electronic locking mechanisms, an operating system, or an application where individual users have their own rights and permissions. Of course, this is partly what passwords have done all along. Again, the problem is that a password has nothing to do with your actual identity. There is simply no foolproof way to make password-protected systems completely safe from unauthorized intrusion. Nor is there any way for password-based systems to determine user identity beyond doubt.

Biometrics have been around for decades in the public sector, adopted by the military and law enforcement agencies almost from the outset. Today, public agencies are using biometrics to prevent welfare fraud and to determine eligibility for health care benefits. A wide range of pilot projects involving biometrics are taking place around the world. Homes in Japan are already being secured by fingerprint recognition devices. Facial recognition is being incorporated into an ATM (Automated Teller Machine) system by Siemans Nixdorf in Germany. Iris recognition is being incorporated into ATMs in Japan, produced by its leading supplier, Oki Electronic. MasterCard and Visa are exploring the use of biometrics to increase the security of their credit cards (annual losses attributed to credit

card fraud are estimated at $2 billion, much of which is believed would be eliminated through the use of biometrics). Customers of the Standard Bank of South Africa are having their fingerprints scanned at ATM machines instead of using a PIN (Personal Identification Number) when they wish to withdraw cash, make deposits or inquire into their balance. Chemical Bank announced that it had selected a voice verification system for customer identification in banking transactions. Charles Schwab and Co. are using a finger scanning system with employees at its head office to conform to the requirements of the Securities and Exchange Commission. Other businesses (Coca-Cola and Woolworth, Australia) use biometrics for their time and attendance systems. Visitors purchasing an annual pass to Walt Disney World in Florida are being enrolled in a finger geometry system -- finger geometry readers are being installed at all turnstiles. This is intended to replace the photo identification that used to be issued in the past to ticket purchasers. None of the above examples include any of the government applications of biometrics increasingly beginning to be used in the administration of entitlement programs such as welfare benefits, health care, or pension benefits. The potential applications for this technology are endless.

It is not only the large corporations and individual users that are looking into what the future will hold for use of biometric encryption in society. The U.S. government has felt that the technology is important enough to form a panel of experts to study the latest developments in the industry and their potential government applications. The Biometric Consortium was chartered by the National Security Policy Board through the Facilities Protection Committee to help develop, test and evaluate biometric devices on behalf of the Department of Defense. The government utilizes biometric verification for access to computer networks as well as physical access to facilities, and uses biometric controls for monitoring entitlement benefits to reduce fraud in these programs. Some other government programs that make use of biometrics are the Immigration and Naturalization Services (INS) and Passenger Accelerated Service System (INPASS) which allows frequent visitors to the United States to quickly pass through inspection points utilizing hand geometry as the biometric. Along the Canadian border the government uses a system called CANPASS that is similar to the INPASS system but uses fingerprint biometrics instead. Government will continue to be a hot market for biometric security, but experts see huge potential in the financial community and the medical industry. The security issues that haunt corporate IT and e-commerce make them obvious markets for biometrics too.

The Gartner Group has predicted that by the year 2001 iris recognition and fingerprint recognition systems will become the tools of choice for corporations that adopt biometrics. Of the several available types of biometric systems currently in use, fingerprint recognition is the most popular for a number of reasons. Fingerprints have been used to identify people since the dawn of civilization. It is the oldest and most commonly accepted form of biometrics technology. Ancient kings and queens sealed letters and authenticated them

with their fingerprints on hot wax thousands of years ago. Over a hundred years ago, both the United States and Europe began documenting the use of fingerprints for identification and verification purposes. Amazingly, after all this time, and millions of fingerprints later, no two identical fingerprints have ever been found. Based on this kind of hard physical evidence, it is safe to say that fingerprints are truly a unique human characteristic. No other biometrics technology can boast this level of scientific history and documented support. Accordingly, its advantage over other biometric solutions lies in its historically and scientifically proven accuracy, reliability, convenience, user acceptance and familiarity.

3. The Controversy Over Privacy

It is worth noting that biometrics has met some resistance from privacy advocates, for a number of reasons. One of the primary reasons for this may stem from the association of biometrics (primarily fingerprints) with police activity. Fingerprints have historically been used by law enforcement agencies to track down those suspected of committing criminal acts, and for maintaining the ability to track their whereabouts. For this reason, fingerprints have raised concerns over loss of dignity and privacy. Furthermore, the central retention of fingerprints and multiple access by different arms of government evokes images of "Big Brother" surveillance.

These fears are justified in the context of identifiable fingerprints of the kind commonly used by the police. A fingerprint, and the broader family of biometrics including body parts such as the retina, iris, hand, and voice prints, offer irrefutable evidence of one's identity since they are unique biological characteristics which distinguish one person from another, and which can only be linked to one individual. A fingerprint in this context can act as a powerful unique identifier that can serve to associate disparate pieces of personal information about an individual, creating the potential for personal information from different sources to be linked together to form a detailed personal profile. If used as a unique identifier, a fingerprint enables individuals to be pinpointed and tracked. It also represents a clear invasion of privacy, one that most people would object to.

The threat to privacy arises not from the positive identification that biometrics provide, but the ability of third parties to access this in identifiable form and link it to other information, resulting in secondary uses of that information without the consent of the data subject. This erodes the personal control of an individual over the uses of his or her information. And informational privacy is defined as the ability to maintain control over the uses and dissemination of one's personal information. Privacy revolves around freedom of choice; without the ability to exercise some reasonable sense of control over the uses of one's information, privacy will become but a quaint notion. But can the biometric become a *protector* of privacy?

The above threat arises from the use of *identifiable* (raw image) biometrics, which can function as a unique identifier (such as the SSN, a driver's license, etc). As with all unique identifiers, it is the secondary uses of personal information that cause the greatest concern, and the subsequent linkages that may be achieved through the use of the unique identifier. With the application of encryption to biometrics, however, biometric technology will evolve to the point where systems can be configured to put the power of the biometric into the hands of the individual, as opposed to the government or the police.

4. Biometrics Today and Tomorrow

The acceptance of biometrics for a variety of purposes unrelated to law enforcement is growing. In “The Body as Password,” an article appearing in the July, 1997 issue of Wired, Ann Davis observes: “Doubters call the digital age dehumanizing, but the joke is on them: the human body lies at the heart of plans to wire banks, streamline government handouts, secure the workplace, even protect your PC. Driver's licenses, credit cards, and office keys as we know them are dinosaurs; the age of the body-part password, or biometric, is upon us.” In another article appearing in the December, 1997 issue of COMPUTERWORLD, Deanne Gage notes: "the best security measures may lie in our own anatomy. While identification cards and PINs can be lost, shared and forgotten, corporations are looking at alternative ways of distinguishing Mary from Jane and John from Joe. Welcome to the world of biometrics, where our body parts like fingerprints, eyes, faces, and even voices, can confirm who we say we are." A comprehensive article on biometrics also appeared in the Communications of the IEEE. In his article entitled, "Biometrics, Privacy's Foe or Privacy's Friend?" John Woodward concluded the latter was the case because biometrics safeguarded identity and data integrity: "While critics of biometrics contend that this new technology is privacy's foe, the opposite, in fact, is true. Biometrics is a friend of privacy whether used in the private or public sectors."

There also appears to be a corresponding shifting in views among the public with respect to acceptance of biometrics, specifically, finger imaging technology based on the use of fingerprints. A 1996 ORC (Opinion Research Corporation) survey on finger imaging technology found that 75% of the respondents said they would be comfortable taking part in a finger scanning exercise: "When the new process of finger imaging was described to respondents, three out of four (75%) said they would be 'comfortable' in having such a process administered to them to identify themselves and prevent someone else from assuming their identity." When four identity verification situations were presented to survey respondents, 76% to 91% indicated a high level of support for finger imaging. Further, 83% of those surveyed rejected the view that using finger imaging to verify someone's identity was tantamount to treating them like a criminal. Instead, a different view emerged – surprisingly, one that saw finger imaging as a convenient, easy-to-use process that helped protect individuals against identity fraud. Consistent with

these American findings was a Canadian survey where over 80% of the respondents supported the use of a biometric to control welfare fraud in Toronto.

It seems certain that the use of biometrics for security and other purposes unrelated to law enforcement will grow dramatically in the next decade. The prices of biometric devices continue to drop, and their sophistication and level of integration continue to increase. Device manufacturers understand your need for privacy and do not record actual images of fingerprints, faces, or signatures. Instead, they use mathematical models representing those attributes and store only those models. But it's possible that these "representations" might be able to be used to identify you in any case. And corporations are usually cooperative when authorities ask for an employee photo or work record; who's to say they will be less forthcoming with biometric data? All we can say definitively is that this is a new technology area largely untested by civil law, law enforcement, and criminals alike. Corporations should treat this highly personal and sensitive data as such.

5. Biometrics and the World Wide Web

Most of the firms who manufacture biometric encryption devices see the Internet as the "Holy Grail" for widespread acceptance of their devices. Two-way public systems are the safest for use over public networks. Therefore, individuals would need to be able to combine their biometric identifiers to code a common encryption key to perform electronic commerce over the Internet domain. A firm would be able to code information that would only allow its intended recipient(s) to receive the information. Organizations would be able to perform paper intensive transactions such as billing and payments over an open network without the concern of easy access to sensitive banking information afforded by account numbers or access numbers. Companies would benefit from these types of secure transactions because it would speed up the amount of time required to obtain payments from their customers while at the same time avoiding bank charges for processing of paper transactions such as checks.

Companies could manage their entire supply chain in a secure environment using biometric encryption technology. Electronic Data Interchange (EDI) would be easier to facilitate without the need for dedicated networks to deter outside agents from obtaining a company's sensitive information. Orders could be placed with vendors without allowing outside parties to know quantities and prices, and corporate officers could communicate with one another about sensitive company policies using email on open networks. It is not a matter of "if" biometric technology will come into play in electronic commerce in the future, but *when* it will come into play. As technology continues to grow, the need for this particular technology will grow at an equal pace. Corporations, governments, and individuals all see the potential of biometric encryption to further electronic commerce in the future.

6. SecuGen Corporation

SecuGen is a Silicon Valley company incorporated in San Jose, California, U.S.A. The name of the company is derived from “Secure Generation” and, as the name implies, SecuGen is dedicated to developing the next generation of security technology – biometrics. SecuGen is involved with global marketing, sales, and R & D of biometric applications, focusing primarily on fingerprint technology. SecuGen is a world leader in the production and distribution of fingerprint recognition devices due in large measure to an advanced optical scanning method and a very compact, durable product design that is much easier to integrate than the larger, more cumbersome products available elsewhere in the marketplace. Extremely accurate and innately less complex than face or eye recognition systems, fingerprint recognition devices are also less expensive to implement. SecuGen’s fingerprint recognition devices (or FRD in the parlance of the industry) make use of embedded scanners to capture fingerprint images rather than full-motion video, and do not incur any significant drains on computer resources. Another reason for the widespread acceptance of fingerprint recognition devices is that the general public is unfamiliar with the methods used in iris and retina scanning. We flinch from the idea of exposing our eyes to anything potentially intrusive; this reaction may occur regardless of whether or not a hazard is actually present. For instance, one popular misconception is that eye scans are performed with lasers; however unfounded, the idea evokes instinctive distrust in users who would not think twice about looking into a video camera or an electric light bulb. It will take a little more time and education on the part of the public before these technologies develop the level of trust already associated with fingerprint scanning, although this, in its turn, will happen.

Like other biometrics systems, SecuGen’s consists of both hardware and software; the hardware captures the salient human characteristic, and the software interprets the resulting data and determines acceptability. The crucial step in building an effective biometric system is enrollment, which can also be described as the registration process. During enrollment, each user, beginning with the administrator who controls the system, provides samples of that system’s specific biometric characteristic by interacting with the scanning hardware. You then interact with the biometric device again, and the system verifies that the data corresponds to the template. If the software fails to get a match, more tries may be needed, just as dictation software learns to recognize the user’s speech patterns over time. Once this procedure is complete, the system is operational. The next time you try to access the system, you are scanned by whatever device is being used (you might be asked to supply a user name as well) and the hardware passes the data to the software, which checks the user’s templates. If there is a match, you are granted access; otherwise, a message reports that the system can’t identify the user. If access is granted, it is

based on your profile. If you are trying to log on to a Windows 98 or NT machine, for example, the system will unlock just as if you had typed your user name and password at the log-in prompt.

Using SecuGen's system to illustrate these concepts, you would first touch a finger or thumb to a fingerprint reader. When a user places their finger on SecuGen's Fingerprint Recognition Device (FRD) for the first time, the fingerprint is scanned and a 3-D fingerprint image is captured using SecuGen's Surface Enhanced Irregular Reflection (SEIR) optical technology. Used in combination with SecuGen's proprietary fingerprint reading algorithm, an extremely high quality, accurate, and distortion-free image is captured which is virtually fool-proof since it only accepts three-dimensional fingerprints for use as input.

7. Fingerprint Matching

All fingerprints contain a number of unique physical characteristics called minutiae, which includes certain visible aspects of fingerprints such as ridges, ridge endings, and bifurcation (forking) of ridges. Most of these minutiae (between 70 and 200 of them) are found in the core points of fingerprints, and the core points themselves are found near the center of the fingerprint on the fleshy pad. Figure 7-1 shows the positions of core points within fingerprints. It is this minutiae data that is used by fingerprint recognition devices. Studies have shown that a person can be correctly identified by as little as a 12% match of minutiae.

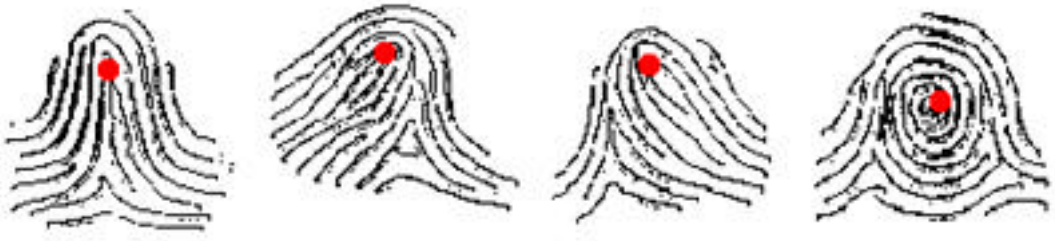

Fig. 7-1 Core points on different fingerprint patterns. A core point is defined as the topmost point on the innermost recurving ridge line.

The quality of a fingerprint image is relative to the number of minutiae points captured. If the number and locations of the minutiae remain consistent whenever an individual's fingerprint image is scanned and captured, the fingerprint image is successfully matched to a template. Fingerprint images that do not possess an adequate number of minutiae points may be unusable. Figure 7-2 shows poor-quality fingerprints, characterized by smudged, faded, or otherwise distorted areas on the fingerprint. These conditions can be caused by excessive dryness or wetness, or scarring of the skin at the fingertip.

Dry Wet Scarred

Fig. 7-2. Poor-quality fingerprints

SecuGen's advanced fingerprint matching algorithm is capable of extracting the correct minutiae even without benefit of a perfect print. However, the positioning of the finger and the relative wetness or dryness of the fingerprint when it is placed on the optic window for scanning are both important factors in getting a match. The user enrolls by placing their finger or thumb on SecuGen's Fingerprint Recognition Device. The FRD scans the individual's finger and captures the live 3-D fingerprint image. SecuGen's minutiae-based algorithm then extracts minutiae points from the image and convert's the data into a unique mathematical template, comparable to a 60 digit password – a password that a supercomputer running at full power for a year could not break. This unique template is then encrypted and stored to represent the user. Again, no actual image of the fingerprint is stored.

Performance of the algorithm is measured by two things, the False Rejection Rate (FRR) and the False Acceptance Rate (FAR). The False Rejection Rate states the percentage of instances an authorized individual is falsely rejected by the system. Generally speaking, SecuGen's False Rejection Rate is 0.1%. The False Acceptance Rate states the percentage of instances an unauthorized individual is falsely accepted by the system. Generally speaking, SecuGen's False Acceptance Rate is 0.001%. FRR and FAR are diametrically opposed, therefore, raising the FAR will lower the FRR and vice-versa. FRRs and FARs can be adjusted according to the needs of a given security system.

Fingerprint recognition methodology is divided into two distinct processes: Verification and Identification. The verification process is a one-to-one matching process (1:1) in which the user must first tell the system who they are by logging on and entering their name and other pertinent information about themselves for storage in the system database. This information need only be entered once in order to associate personal information with their first registered fingerprint. They can then scan in another fingerprint sample which is compared to their previously enrolled fingerprint. If the fingerprints match, the user is "verified" as who they say they are, and granted all the privileges and access of the stated user – in other words, the system *verifies* who the user says they are. The Identification

process differs in that it is a one-to-many matching process (1:N) in which users need not enter any information about themselves prior to the fingerprint scan. A new fingerprint sample is simply taken from the user and compared to a database of existing fingerprints known to the system. When a match is found, the user is "identified" as the pre-existing user – the system *finds* who the user is. This one-to-many matching process is how the Automated Fingerprint Identification System (AFIS) works. SecuGen offers both verification and identification technology.

8. Superior By Design

Traditional fingerprint devices require fine hand-calibration of the optical components. These types of devices can cause image quality to vary significantly from one unit to another, and mass production of such units is costly or nearly impossible. Furthermore, systems with strict calibration requirements lack durability, limiting their potential uses. Additionally, conventional optical fingerprint recognition systems use the FTIR (Frustrated Total Internal Reflection) image processing methodology. For purposes of image quality, these types of systems require longer focal lengths and therefore longer and larger modules. To make these types of optical systems smaller, image quality must be compromised and the system is left to work with inherently distorted images. Image distortion effectively lowers accuracy and reliability.

By contrast, SecuGen's fingerprint recognition system utilizes the unique SEIR (Surface Enhanced Irregular Reflection) image processing methodology. Using this breakthrough technology, SecuGen's fingerprint modules are able to achieve distortion-free image capturing while drastically reducing its physical size. The actual dimensions of the optic sensor module are (mm) 21(W) X 31(L) X 59(H), and provides a 450 dpi resolution (Fig. 8-1).

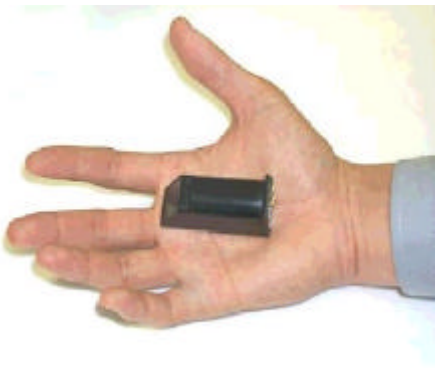

Fig. 8-1 The small size of the FDx01 optic sensor allows it to fit into all kinds of hand-held devices, including computer mouse and keyboard.

The innovative SEIR optical design adopted by SecuGen enables the fingerprint reader to capture high contrast images from fingerprints even when the fingerprints themselves are imperfect, and vastly contributes to the speed and accuracy of fingerprint enrollment (the actual registration of users into the system). In addition, the compact design makes it possible to embed this cutting-edge technology into a normal-sized, ergonomically designed computer mouse. In fact, SecuGen's fingerprint reader is one-third to one-fifth the size of other optical systems on the market today. Both the fingerprint reader and the minutiae-based fingerprint reading algorithm are designed to receive only 3-dimensional fingerprints, and will not allow 2 dimensional fingerprint images (e.g. "faked" fingerprints on a film or paper) to be input.

9. Product Overview

The SecuGen FDP01 (Fig. 8-1) is a fingerprint recognition device designed for use with a PC parallel port, and can easily be embedded in peripheral devices such as computer mice and keyboards. FDP01 captures fingerprint images and digitizes them to an 8-bit gray-scale image at 450 dpi resolution, and the host system then retrieves the image through its parallel port. SecuGen's EyeD Mouse and EyeD Keyboard are examples of FDP01 implementations. The small size of the SEIR optic module makes it easy for application developers and system integrators to assimilate into their own products, especially hand-held devices. SecuGen offers software evaluation and development kits expressly for this purpose. Accurate fingerprint verification and superior image quality are hallmarks of the FDP01, offering maximum reliability for security-based applications.

Key Features

- Small size – 21mm(W) X 31mm(L) X 59mm(H)
- Integration-readiness
- Durability, both impact- and scratch-resistant
- Fine image quality (extremely low distortion, superior performance)
- Competitively low price
- Pass-through connectivity
- Compatibility (works with any Windows system that supports EPP or ECP)

FDP01 System Requirements

- IBM-compatible PC 486 or later
- 1.44MB FDD
- 1 Parallel Port
- 1 PS/2 Port
- 16MB RAM
- 20MB available hard disk space
- Microsoft Windows 95/98 or Windows NT 4.0

SecuGen's FDP01 Developer's Kit includes the following:

- EyeD Mouse
- Evaluation Manual
- Dynamic Link Library (DLL) files
    - Image capture driver for Windows 95/98
    - Image capture driver for Windows NT 4.0
    - Fingerprint minutiae extraction module
    - Fingerprint verification module

The FDP01 software developer's kit allows programmers to build applications quickly and easily. Based on SecuGen's unique technologies, the optical module captures high contrast images with extremely low distortion, and its uncommon ability to accurately capture dry fingerprints (a known challenge for optical fingerprint reading systems) puts the FDP01 in the top of its class worldwide.

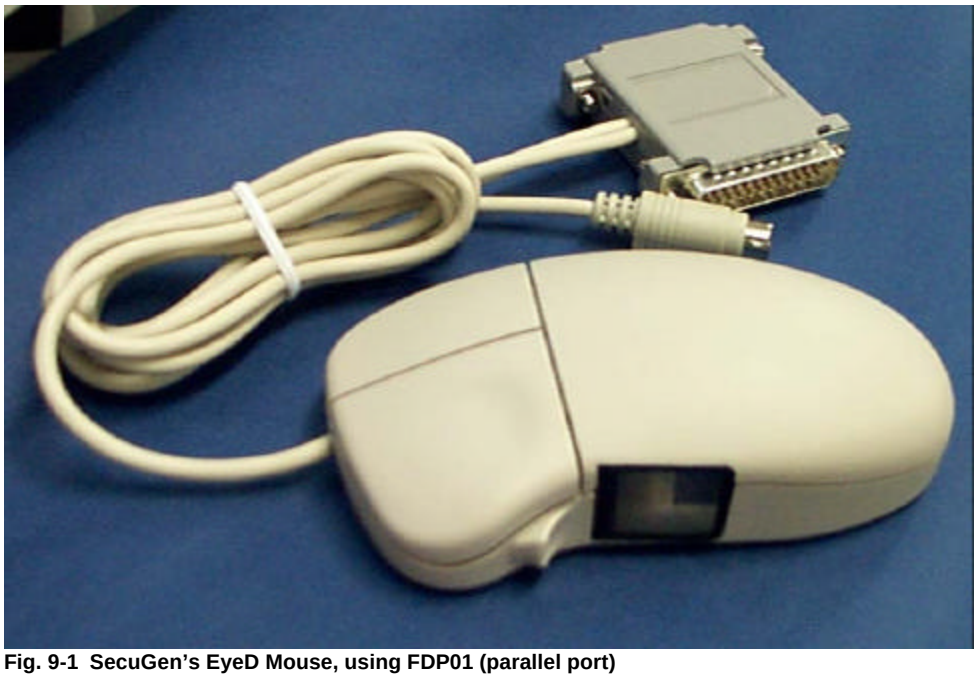

Fig. 9-1 SecuGen's EyeD Mouse, using FDP01 (parallel port)

Fig. 9-2 SecuGen's EyeD Keyboard, using FDP01 (parallel port)

Similar to the technology that powers the EyeD Mouse and EyeD Keyboard (Figures 9-1, 9-2) the FDU01 (Figure 9-3) is a fingerprint recognition module designed for USB connections. Like the FDP01, the FDU01 is easily integrated into a variety of peripheral devices by application developers and system integrators. SecuGen's EyeD Hamster is an FDU01 fingerprint recognition device designed to secure computer resources without replacing the existing mouse or keyboard.

Fig. 9.3 EyeD Hamster

Like the parallel port version, the FDU01 (USB port) captures a fingerprint image and digitizes it to an 8-bit gray-scale image at 450 dpi resolution. SecuGen is currently developing USB versions of the EyeD Mouse and EyeD Keyboard, available in the Spring of 2000.

FDU01 System Requirements

- IBM-compatible PC 486 or later
- 1.44MB FDD
- 1 USB Port
- 16MB RAM
- 20MB available hard disk space

- Microsoft Windows 98 (OSR 2.1) or Windows NT 5.0

10. SecuGen's Stand-Alone FDA01

SecuGen's stand-alone fingerprint recognition device with built-in CPU is called FDA01. Like all SecuGen products, it boasts high levels of performance coupled with durability and weather-resistance; this product is the perfect choice for outdoor applications. The optic module is connected to the FDA01 processing board, so it is slightly larger than the FDP01 or FDU01, but it's still substantially smaller than comparable optics-based fingerprint recognition devices available today. The FDA01 unit is being integrated into an ever-increasing number of applications – this is the "engine" behind BOGO door-locks, biometrically secured time/attendance systems, and Automated Teller Machines (ATM).

The FDA01 communicates with the main controller through a serial port connection. The main controller can be a normal micro controller with a serial port (Z80, 8051 or PC). Predefined protocols are used for communication between the FDA01 and the main controller; these are provided in the FDA01 Developer's Kit. Contents of the FDA01 Developer's Kit include sample source code (8051 source codes) and sample applications.

Functions of FDA01

- Master Registration
- User Registration & Deletion
- Upload and Download User's Fingerprints
- Centralized Fingerprint Matching at the Host Computer
- Diversified Fingerprint Matching at the FDA01 Processing Unit
- Data Log (up to 8,000 records)
- System configuration setup (brightness, security level, communication speed, auto tuning
- FDA01 Update Program

FDA01 Applications

- Building Access Control
- Time & Attendance Management
- Vehicle Control
- Door-Lock System
- ATM
- POS
- Individual Verification of credit cards/smart cards
- Secure Network System

The FDA01 Developer's Kit contains all the hardware and the software needed by system integrators. All programs in the Developer's Kit run on Microsoft Windows 95/98 or Windows NT 4.0 platforms.

Contents of FDA01 Developer's Kit

- Fingerprint Reader interfaced to CPU board, 1 each
- Main Controller with keypad and LCD unit
- AC-DC 5V Adapter
- Developer's Manual
- Programs (Windows based)
  - Main controller emulator demo
  - Flash-memory download & update utility program
  - Database editor & log-file viewer
- Protocol info & header files
- Main controller source code
- Full project completion technical support

The Developer's Kit works with Windows 95/98 and NT 4.0 platforms. It helps programmers build applications quickly and easily. It is provided with the fingerprint recognition module FDA01, and like all of SecuGen's patent-pending technologies, the optic module (FDP01) captures high-contrast, low-distortion fingerprint images, then extracts and compares the feature points (minutiae) with an existing template to decide whether it matches or not. The minutiae data is then encrypted, stored and transmitted by the FDA01.

The high-tech explosion sparked by the introduction of desktop computers in the late 1970's continues to expand at a furious pace. As an industry leader, SecuGen's biometrics security technology offers a solution for today's worldwide security needs in the increasingly unified landscape of modern communications.

For more information, visit the SecuGen website at http://www.secugen.com.

11. Appendix_A

SecuGen PC Peripheral Products

Device	Type	Name	Contents
EyeD Mouse	Parallel interface	MFDP01-001	Mouse, adapters, SecuDesktop software
	USB interface	MFDU01-001	Mouse, adapters, SecuDesktop software
EyeD Keyboard	Parallel interface	KBFDP01-001	Keyboard, adapters, SecuDesktop software
	USB interface	KBFDU01-001	Keyboard, adapters, SecuDesktop software
EyeD Hamster	Parallel interface	HFDP01-001	Hamster, adapters, SecuDesktop software
	USB interface	HFDU01-001	Hamster, adapters, SecuDesktop software

SecuGen Stand-Alone Products (Built-in CPU)

Device	Type	Name	Features
Stand-Alone FRD	Adapter	FDA01	1 MB memory (720 users)
	Battery	FDA01B	1 MB memory (720 users)
Stand-Alone FRD	Extended Memory	FDA01E2	2 MB memory (2000 users)
	Extended Memory	FDA01E4	4 MB memory (4560 users)

12. Appendix B

SecuGen Software Summary (for system integrators and developers)

Category	Type		Name	Contents
Basic Device Driver	**Parallel interface**		SBP01	Basic device driver for parallel interface
	USB interface		SBU01	Basic device driver for USB interface
Evaluation Kit	Parallel interface		SEP01	Evaluation kit for parallel interface
	USB interface		SEU01	Evaluation kit for USB interface
	Standalone type		SEA01	Evaluation kit for standalone type
Developer's Kit	Parallel interface		SDP01	Developer's kit for parallel interface
	USB interface		SDU01	Developer's kit for USB interface
	Standalone type		SDA01	Developer's kit for standalone type
SecuDesktop	Parallel interface		SAP01	SecuDesktop for parallel interface
	USB interface		SAU01	SecuDesktop for USB interface
Utility	HAAPI BSP Module	Parallel interface	SHP01	HAAPI BSP module for parallel interface
		USB interface	SHU01	HAAPI BSP module for USB interface
	META Frame Module		SMF01	Server based module for META-Frame
	Identification Module		SIM01	Identification module