



WHITE PAPER: BIOMETRICS

Exploiting Biological Traits to Achieve Data Security

This white paper analyzes the potential for biometric technology to safeguard data against the growing threat of unauthorized access in the form of identity theft or software hacking. Additionally, different implementations of biometric technology are discussed, with an emphasis on fingerprint recognition.

This document then presents the LaCie products that take advantage of biometrics technology to safeguard files from unauthorized access.

INTRODUCTION

Identity theft, fraud, hacking, and computer viruses are posing increasingly formidable challenges to individuals, companies, and governments as they seek to protect their data from theft. (For more information, refer to LaCie's *Digital Security White Paper*.) These concerns have given rise to a multi-billion dollar security industry, whose solutions often require significant resources to implement. The most common software-level form of protection, the password, is vulnerable and highly subject to human error. Its widespread use has required individuals to memorize dozens of passwords, and the cost to large organizations for tech support to manage and reset forgotten passwords can be staggering.

In this climate of data security risk and limited resources for information security, the field of fingerprint biometrics has emerged as the most popular and widespread implementation of biometrics technology.

WHAT IS BIOMETRICS?

The term refers to the field of technology devoted to the identification of individuals using biological traits. Automated methods of recognition measure individuals' physical or behavioral characteristics. Common physical biometrics include fingerprints, hand or palm geometry, and retina, iris, or facial characteristics. Behavioral characteristics include signature, voice (which also has a physical component), keystroke pattern, and gait. Of this class of biometrics, technologies for signature and voice are the most developed.

WHAT IS FINGERPRINT RECOGNITION?

Fingerprint matching is by far the most successful biometric technology because of its ease of use, non-intrusiveness and reliability. Fingerprints consist of ridges and valleys formed in complex patterns that are unique for every person and thereby provide an optimal verification method. Rather than scan each



Fingerprint-based biometrics looks for minutia, which are the points on a fingerprint where a ridge ends or splits in two.

ridge, fingerprint-based biometrics looks for minutia, which are the points on a fingerprint where a ridge ends or splits into two. An algorithm extracts the most promising minutia points from an image and then creates a template, usually between 250 to 1,000 bytes in size.

At registration (enrollment) the minutia points are located and the relative positions to each other and their directions are recorded. This data forms the template—the information later used to authenticate a person. At the matching stage, the incoming fingerprint image is preprocessed and the minutia points are extracted. The minutia points are compared with the registered template, trying to locate as many similar points as possible within a certain boundary. The result of the matching is usually the number of matching minutiae. A threshold is then applied, determining how large this number needs to be for the fingerprint and the template to match.

Fingerprint verification is well adapted to access-controlled devices. In fact, this biometric technology is easy-to use and quite well accepted compared to other identification technologies. Fingerprint verification also has a lower error incidence rate in comparison to other biometrics solutions.

WHAT KIND OF BIOMETRIC TECHNOLOGY IS USED IN LACIE SAFE DRIVES?

LaCie Safe drives integrate active fingerprint-sensing technology. Each sensor cell (pixel) contains an active capacitive feedback circuit whose effective feedback capacitance is modulated by the presence of live skin close to the surface of the sensor. For instance, the sensor can't match the fingerprint of a deceased person or of a finger detached from the body. In contrast to optical sensors with panels, capacitive sensors—also called "solid state"—are difficult to imitate. Solid-state technology enables sensing the skin capacity variation of a finger. For example, if you draw a line using ink on your fingertip, the image in solid state won't show the line. Solid-state technology is based on sensing the finger—not looking at it the way optical detection does.

The silicon fingerprint sensor integrated into the LaCie Safe drive produces a full, clean image around all portions of the finger that come in contact with the sensor. Optical solutions can produce edges of the image that are not crisp because sensors only focus on a small area. With the LaCie fingerprint sensor,

the risk of non-matching between the fingerprint and the stored biometric data are very low thanks to superior image quality.

Integrating a swiping fingerprint sensor minimizes corruption risks. It is extremely hard for end users to copy a fingerprint because the finger movement immediately eliminates any possible traces. Many low-quality optical solutions can be compromised by a simple photocopy of a fingerprint. Some low-cost optical solutions also have problems with latent fingerprints being left on the sensor by grimy hands. By integrating all fingerprint-matching technology into the hardware, LaCie Safe hard drives are fully self-contained drives that do not have to rely on the host computer to perform fingerprint matching. This maintains full portability for the user by eliminating the need to install any driver software on the host computer prior to use.

WHAT ARE THE CURRENT APPLICATIONS OF BIOMETRICS?

There are over 24 million biometric laptop computers and peripherals on the market today.



LaCie Rugged Safe Hard Disk, Design by Neil Poulton



LaCie Safe hard drives feature proprietary software for fingerprint registration and access

LaCie Rugged Safe hard drive with biometric access control and AES 128-bit hardware encryption



Biometric technologies are becoming the foundation of an extensive array of highly secure identification and personal verification solutions. Many technological devices and systems are now developed with biometric solutions to control access to rooms, workstations, networks and some software applications. Utilized alone or integrated with other technologies such as smart cards, encryption keys and digital signatures, biometric technology is set to pervade many aspects of the economy and our daily lives. More and more consumer electronics products integrate biometric identification such as in some laptops, PDA, mobile phones, or MP3 players.

Are there real needs for biometric solutions? These days, people are generally not opposed to using their biological traits instead of passwords for identification. In their daily lives, people have so many passwords to remember (credit card, door access, car computer control...) that they find it easier and faster to scan their fingers on a panel than to remember and enter a new password. Utilizing biometrics for personal authentication is becoming more convenient than other current methods (such as passwords or smart cards).

The trend is toward centralizing identity management—employing a combination of both physical and logical access parameters for gaining access to different types of resources. Many companies are now looking for this sort of identity management solution, which requires the use of biometrics.

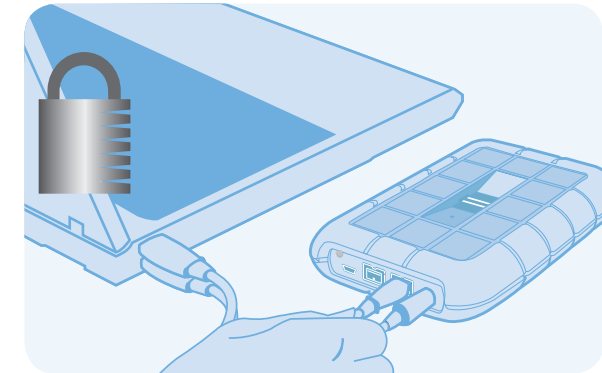
As the level of security breaches and transaction frauds increases, the need for highly secure identification and personal verification technologies is becoming apparent. The need for biometrics can be found in federal, state and local governments, in the military, and in commercial applications. Enterprise-wide network security infrastructures, government IDs, secure electronic banking, investing and other financial transactions, retail sales, law enforcement, health and social services have already begun to implement biometric technology.

IS BIOLOGICAL TRAIT IDENTIFICATION SAFE AND RELIABLE?

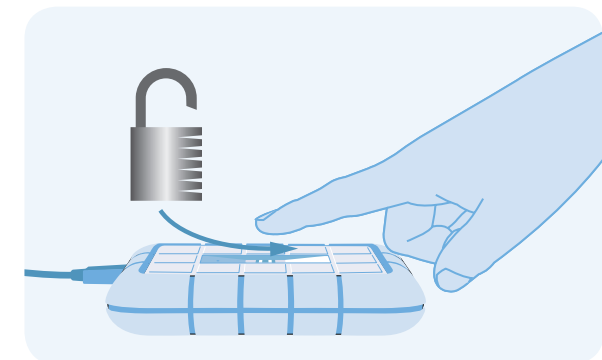
The security field uses three different types of authentication: something you know (a password, PIN), something you have (a card key, smart card) or something you are (a biometric trait). Of these, biometric trait identification is the most secure and convenient authentication tool. It cannot be borrowed, stolen or forgotten, and forging one is practically impossible. Each human has his/her own biological identity that is different from anyone else's, which explains the difficulty in corrupting this kind of data.

To show how reliable biometrics is, many governments are choosing to use fingerprint and face digitalization on identity papers and visas to better identify people. Using biometric identification avoids the risks of forgotten passwords or data access control corruption.

SAFE HARD DRIVE CONNECTION



Connect to the computer



Swipe a finger



Access the drive

SOURCES

1. <http://www.biometrics.org/html/introduction.html>
2. <http://csrc.nist.gov/cryptval/des/tripledesval.html>

MORE INFORMATION

www.lacie.com

ABOUT LACIE

Through a combination of cutting-edge engineering and a rich history of unique design aesthetics, LaCie has earned an excellent reputation for producing products that are the perfect synthesis of form and function. Our hard disks, network and RAID solutions, optical drives, displays, and accessories are created to enhance and expand your computing environment, no matter its platform or configuration.

Featuring the exclusive styles of world-renowned designers such as Neil Poulton, Sam Hecht, and 5.5 Designers, LaCie's award-winning products look stunning and perform with unparalleled reliability and versatility. LaCie is a global leader in manufacturing top-of-the-line tools that are often first-to-market, constantly raising the bar and re-establishing industry standards.

Please visit our website: www.lacie.com, for up-to-date product specifications—available in multiple languages for worldwide accessibility. Use it to purchase items online, contact our excellent technical support or locate the sales office or reseller nearest you.



www.lacie.com

While reasonable efforts have been made in the preparation of this document to assure its accuracy, LaCie assumes no liability resulting from errors or omissions in this document, or from the use of the information contained herein.