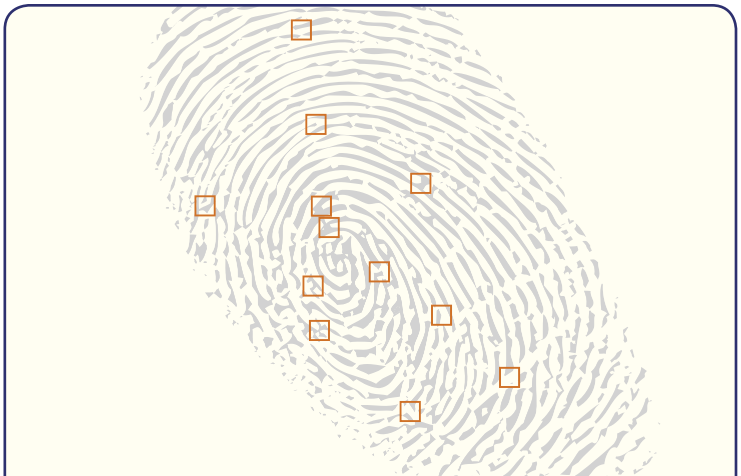
LaCie SAFE Hard Drive

Biometric Access
&
Data Encryption

What is biometrics?

The term refers to the emerging field of technology devoted to the identification of individuals using biological traits. Biometrics 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.



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

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 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 pre-processed 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 well accepted compared to other identification technologies. Fingerprint verification also has a lower error incidence rate in comparison to other biometrics solutions.

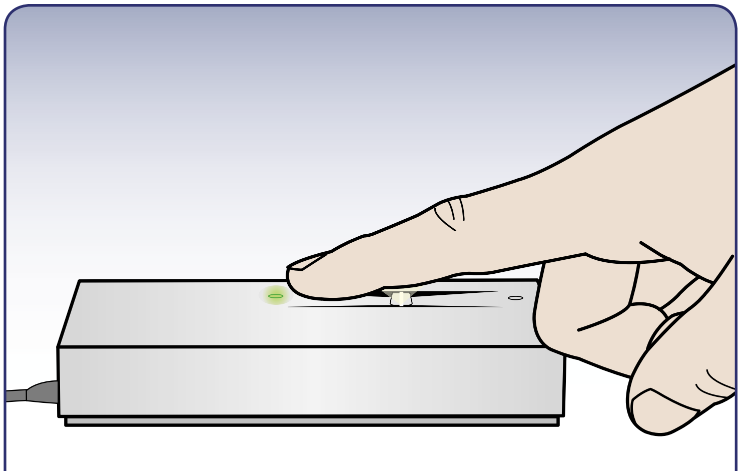
What kind of biometric technology is used in the SAFE drive?

The LaCie SAFE Hard Drive integrates 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. 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 our fingerprint sensor, the risk of non-matching between the fingerprint and the stored biometric data are very low thanks to this 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-cost 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, the LaCie SAFE Hard Drive is a fully self-contained drive that does 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.



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

What are the current applications of biometrics?

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 are already benefiting from this 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.

What is encryption?

Encryption is the most effective way to achieve data security. Encryption is the conversion of data into a kind of understandable text code, which cannot be understood by unauthorized users. Unencrypted data is called plain text. Encrypted data refers to cipher text. Decryption is the process of converting encrypted data back into its original form, so it can be understood.

Data stored on the SAFE Hard Drive with Encryption is automatically hardware encoded, making this storage solution fully secure.

What is the decryption key?

In order to easily recover the contents of encrypted text, a correct decryption key is required. The key is part of the algorithm that "undoes" the work of the encryption algorithm. The more complex the encryption algorithm, the more difficult it becomes to eavesdrop on communication without access to the key. Regarding the SAFE drive, the key is stored in the SDRAM memory. Thus, it is almost impossible to access - except of course for authorized governmental organizations if requested.

Why encrypt data?

Cryptography is used whenever someone wants to send a secret message to someone else, in a situation where anyone might be able to get a hold of the message and read it. The use of encryption/decryption is as old as the art of communication. In wartime, a cipher, often incorrectly called a "code," can be employed to keep the enemy from obtaining the contents of transmissions. Simple ciphers include the substitution of letters for numbers, the rotation of letters in the alphabet, and the "scrambling" of voice signals by inverting the sideband frequencies. More complex ciphers work according to sophisticated computer algorithms that rearrange data bits into digital signals.

Encryption is especially important in wireless communications. This is because wireless circuits are easier to "tap" than their hard-wired counterparts. Nevertheless, encryption is an efficient solution when carrying out any kind of sensitive transaction, such as online credit-card purchases or the discussion of confidential corporate information among various departments in an organization.

How does the SAFE drive encrypt data?

The SAFE drive encrypts data through a hardware, and not a software, solution. Thus, encryption and decryption don't require more manipulation by the user. The drive's use stays the same, as with any other external drive, during file transfers, data saving, etc. The data transfer speed is not altered compared to a typical external USB drive and encryption is optimized. The encryption key depends on a 24-character pass phrase stored on the board and not on the host computer, making each drive unique and impossible to hack. Data stored on the drive can be encoded in either DES (56-bit key) or Triple-DES (128-bit key) mode.

What are the different encryption modes used by the SAFE Drive?

DES: Data Encryption Standard

DES is a symmetric public algorithm that was developed by an IBM team around 1974 and adopted as a national standard in the US in 1977. DES encrypts and decrypts data in 64-bit blocks, using a 64-bit key. DES takes a 64-bit block of plaintext as input and outputs a 64-bit block of ciphertext. Since it always operates on blocks of equal size and it uses both permutations and substitutions in the algorithm, DES is both a block cipher and a product cipher.

Although the input key for DES is 64 bits long, the actual key used by DES is only 56 bits in length. The least significant bit in each byte is a parity bit, and should be set so that there is always an odd number in every byte. These parity bits are ignored, so only the seven most significant bits of each byte are used, resulting in a key length of 56 bits.

Triple DES

Triple DES is simply another mode of DES operation. It takes two 64-bit keys, for an overall key length of 128 bits. The procedure for encryption is exactly the same as regular DES, but it is repeated three times—hence, the name: Triple DES. The data is encrypted with the first key, decrypted with the second key, and finally encrypted again with the same key as the first one. Triple DES is three times slower than regular DES but can be billions of times more secure if used properly. Triple DES was the answer to many of the shortcomings of DES.

How secure are DES and Triple DES encryptions?

The DES algorithm specification was published in January 1977, and with the official backing of the US government, it became a very widely employed algorithm in a short amount of time. Unfortunately, over time various shortcut attacks were found that could significantly reduce the amount of time needed to find a DES key with brute-force.

As computers became progressively faster and more powerful, it was recognized that a 56-bit key was simply not large enough for high-security applications. Despite growing concerns about its vulnerability, DES is still widely used by financial services and other industries worldwide to protect sensitive on-line applications.

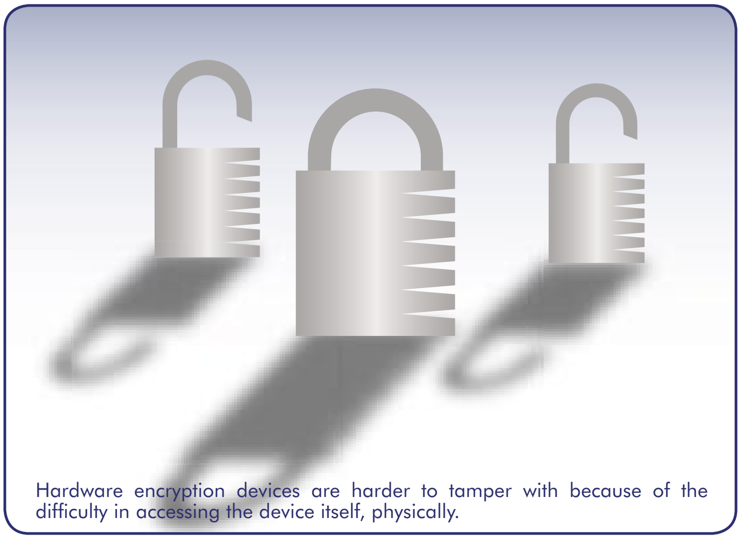
Triple DES has the advantage of proven reliability and a longer key length, which eliminates many of the shortcut attacks that can be used to reduce the amount of time it takes to break DES. DES has 16 rounds, meaning the main algorithm is repeated 16 times to produce the cipher text. It has been found that the number of rounds is exponentially proportional to the amount of time required to find a key using a brute-force attack. So as the number of rounds increases, the security of the algorithm increases exponentially. In general, the stronger the cipher is, the harder it is for unauthorized users to break it.

Are unpublished algorithms safer than those publicly known?

It has happened several times in the past that an encryption algorithm was broken just because of a mistake in its design. In the majority of cases, the principles of new encryption algorithms are publicized. This allows any cryptologist to review and evaluate them, and point out their weak points, if any are found. These algorithms are therefore generally considered to be more secure and trusted than those whose principle is not known. The majority of user applications nowadays implement these generally approved algorithms.

Why prefer hardware encryption compared to software encryption?

There are two major considerations for choosing hardware over software-based encryption: security and performance. The main reason for choosing hardware encryption over software is speed. Cryptographic algorithms require complex manipulation of data at the level of individual bits. General purpose microprocessors such as those found in normal PCs cannot perform these operations efficiently. In addition, encryption is usually a computationally intensive process, handing this off to another processor or to a separate device allows the main processor to concentrate on the primary function of the server. The SAFE hardware board is specially designed to perform cryptographic operations at high speeds. Algorithms such as DES were designed to be fast when implemented in hardware and are much slower in software. Thus, hardware encryption is usually faster than pure software systems but also safer.



Hardware encryption devices are harder to tamper with because of the difficulty in accessing the device itself, physically.

Another reason for choosing hardware encryption is added security. If encryption is performed in software and the encrypting host is compromised, then the attacker could alter the code used to perform the encryption. Moreover, most hackers are specialized in software hacking with brute-force attacks on encryption keys or middleman attacks. The altered algorithm could insert deliberate backdoors in the encryption software, which may be easily detectable by hackers. Hardware encryption devices are harder to tamper with because of the difficulty in accessing the device itself, physically. The second benefit of using an internal microprocessor to encrypt is that it provides a secure location to store the algorithm key. This prevents the key from being stolen and used elsewhere. Private keys in software can easily be copied and attacked off-line. In contrast to software encryption, our hardware encryption solution does not include any backdoors, keeping your data even safer.

How safe is it against hacking?

The technical details of many encryption methods used in public networks today are common knowledge. For these methods the security function is contained in a bit of addition information (the key), which is inserted during encryption. Theoretically, any encryption method can be cracked by trying all the possible keys. In practice, however, when a key of sufficient length is used, security breaches of this type can be prevented. DES is relatively easy to break with today's rapidly advancing technology. In 1998, the Electronic Frontier Foundation, using a specially developed computer called the DES Cracker, managed to break DES in less than 3 days. And this was done for under $250,000. The encryption chip that powered the DES Cracker was capable of processing 88 billion keys per second. In addition, it has been shown that for a cost of one million dollars, a dedicated hardware device can be built that can search all possible DES keys in about 3.5 hours. This just serves to illustrate that any organization with moderate resources can break through DES with very little effort these days.

Regarding the SAFE drive, the secret key is stored in the buffer, which is encrypted itself. Consequently, it is nearly impossible for non-authorized users to obtain the key and access the data. Moreover, there are practical limits to encryption block lengths. At 128 bits, as with Triple DES, decoders run up against physical and practical limitations. A computer that could test all the keys of this length would have to possess unimaginable computing power. Currently, this is only theoretically possible. To avoid brute-force attacks, some IT departments tend to over-encrypt data. People tend to think: "If 128 is good, then 256 is better." That's true to some extent but encrypting data slows performance, even with today's high-powered processors, so security executives should carefully weigh the need for strong encryption versus speed deterioration.

Sources:

http://www.biometrics.org/html/introduction.html
http://csrc.nist.gov/cryptval/des/tripledesval.html
http://www.iusmentis.com/technology/encryption/des/#SecurityofDES

Established in the US, Europe and Asia, LaCie is the world's leading producer of PC and Macintosh compatible storage peripherals. Through a specialized sales dealer network, LaCie offers innovative solutions for professionals in many applications (graphics, audio, video, web design, digital photography, etc.). What differentiates LaCie is the quality and design of its products—original creations by designers such as Philippe Starck, Porsche Design GmbH and Neil Poulton. LaCie is listed on the Paris Nouveau Marché (code 5431).

LACIE