



Integrated fingerprint reader

*By Akira Hino
IBM ThinkPad Security Architect*

*Stacy Cannady
IBM Client Security Product Manager*

Table of contents

2 Executive summary
4 Biometric authentication
4 Fingerprint authentication
5 Integrated fingerprint reader
6 Origins
7 Fingerprint matching
8 Uses for the IBM integrated fingerprint reader
9 How it works
9 Tips on use
10 Frequently asked questions

Executive summary

In addition to passwords, biometric technology like fingerprint recognition is one of the latest forms of identification for entry into IT systems. This white paper discusses fingerprint recognition technology – how it works, some of its advantages and disadvantages, and its application in select IBM ThinkPad® notebook computers.

Fingerprint authentication systems consist of three elements: a sensor, a feature extractor, and a matcher. The sensor scans the finger and extracts features from the captured image. The matcher compares the extracted features with a template of stored features.

On select models of IBM ThinkPad notebook computers, an integrated fingerprint reader is conveniently located on the palm rest. The technology employs a *slide sensor* that extracts certain characteristics of the fingerprint as it is swiped over the sensor. *Capacitive sensing* is used to construct a template of the fingerprint based on variations in the electrical properties of the living layer of the skin. Because these properties are different than the properties of the skin's superficial dead layer, they provide some protection against an attack from fingerprints lifted from a surface.

To activate the fingerprint reader, a user must first register his or her fingerprint in association with an ID. This means swiping a finger about three times so that enough information is stored to create a template, which will be used to match the finger in the future. The IBM integrated fingerprint reader uses an algorithm to identify certain patterns in the ridges of a fingerprint. These patterns are identified during registration, and, when a swiped print is compared to a registered print, the matching algorithm looks for the same patterns to give a positive ID. Computationally, this technique is fast, easy to program, and does not require an overly large program.

Once a user has registered his or her fingerprint, the IBM integrated fingerprint reader can serve as an authentication device to replace BIOS and Microsoft® Windows® passwords. It can also be used as an authentication device with the IBM Embedded Security Subsystem, which is now preloaded on select systems.

The strengths of biometric authentication like the IBM integrated fingerprint reader lies in the fact that a fingerprint cannot be forgotten, misplaced or shared. Fingerprint readers can reduce the need for users to remember multiple passwords, and this can lower the number of support calls for forgotten passwords. However, fingerprint recognition is not 100% accurate. Inaccuracies can be due to the condition of the finger (injured, worn, clean/dirty, wet/dry) or its presentation to the sensor (position, orientation, pressure, swiping speed). The matching algorithm also can mistakenly find a match between a swiped fingerprint and a registered fingerprint if patterns in the two prints match closely enough, although the probability of this is very low.

The white paper concludes with answers to specific questions regarding fingerprint recognition technology that might be important to security-conscious corporations and individuals. Answers note how fingerprints can be centrally managed, how many people might access the same computer, how to change passwords, what happens if the reader breaks, and how the fingerprint reader integrates with IBM Client Security Software and the IBM Embedded Security Subsystem,

Reliability issues are also discussed. In this regard, the paper concludes that fingerprint reading technology, although not perfect, has many security features that other technologies do not provide. It is a strong alternative to passwords and, when used with them as is possible, creates the opportunity for an even stronger security choice.

Highlights

Biometric identification such as fingerprint recognition can eliminate problems of forgotten passwords or lost cards and is currently becoming more popular for convenient and secure authentication.

Biometric authentication

Most IT systems require verification or identification of users. Known as “authentication,” this identification is commonly done with passwords (“what you know”) or cards and badges (“what you have”). Biometric authentication – biometrics for short – is a third method based on “who you are.” It has definite advantages. For example, biometrics can eliminate problems of forgotten passwords or lost cards because “who you are” is always with the user. Because of these advantages, biometrics is currently becoming more popular for convenient and secure authentication.

The principles behind biometrics are common and used in everyday life. People recognize family members by their faces, and individuals know friends by their voices and even their smell. Although human beings are excellent at doing this complex job, even they are not perfect – it may be very difficult to distinguish between identical twins, for example. The challenge for biometrics lies in the measurement and decision of what exactly is similar. There’s no arbitrariness in matching a password – it either matches or it doesn’t. And while biometric technology is advancing rapidly, it is not yet 100% accurate in matching a previously enrolled biometric feature to a present feature. For this reason, biometrics is still not quite as natural as human beings recognizing each other.

Every authentication method has both strengths and weaknesses. Although biometric authentication is no exception to this, it does provide another choice. Its strength lies in the fact that it cannot be forgotten, misplaced or shared. Its weakness comes from not being 100% accurate and because some people may be unwilling to use it.

Fingerprint authentication

Although some biometric measurements such as height and weight are not good characteristics for authenticating individuals, fingerprints are both universal to every human being and unique to each person. They are also persistent through time (barring certain types of physical injury) and quantitatively measurable. Fingerprint authentication has a long history of use. In the nineteenth century, Dr. Henry Faulds, a British surgeon superintendent

Highlights

Most fingerprint authentication systems consist of three elements: a sensor, a feature extractor, and a matcher. The sensor scans the finger, extracting features, and the matcher compares the extracted features with the stored template.

Introduced on select models of IBM ThinkPad notebook computers, the IBM integrated fingerprint reader can replace BIOS and Windows passwords.

living in Japan, published a paper about fingerprints in *Nature* magazine. Since then, fingerprint authentication has been widely used and affordable.

Most, if not all, fingerprint authentication systems consist of three elements: a sensor, a feature extractor, and a matcher. The system works in a way similar to the manner human beings recognize each other. The first time you meet a person, you observe that person and remember his or her features, although you cannot remember everything you observe. Later, when you meet that person you observe and then match the person with the features you remember. In a similar fashion, the sensor in a typical fingerprint reader scans a finger and extracts features from the captured image. The matcher compares the extracted features with remembered features. Fingerprint readers typically don't store the image itself. Instead, they typically store only extracted features, called a template. Similar to meeting an individual for the first time, the person using the fingerprint reader needs to register (or enroll) his or her fingerprint so that there are features to remember.

The fact is, though, that fingerprint authentication is not 100% accurate. Inaccuracies can be caused by the condition of the finger (injured, worn, clean/dirty, wet/dry) or its presentation to the sensor (position, orientation, pressure, swiping speed). As will be shown on pages 12-13, the matching algorithm also can mistakenly match a swiped fingerprint and a registered fingerprint if patterns in the two prints match closely enough, though the probability of this is very low.

The IBM integrated fingerprint reader

The IBM integrated fingerprint reader is a new biometric security device that has been introduced on select models of IBM ThinkPad notebook computers. This device allows a user to register his or her fingerprint on the system and then employs the fingerprint reader as an authentication device to replace BIOS and Windows passwords. The integrated fingerprint reader can also be used as an authentication device with the IBM Embedded Security Subsystem, which is now preloaded on select systems.

Highlights

The IBM integrated fingerprint reader is a slide sensor. As a finger swipes over it, the sensor takes sequential “snapshots” of the finger and from them forms a template of the fingerprint.

The IBM integrated fingerprint reader provides a convenient means for authenticating to a Windows system and can eliminate the need for users to remember multiple passwords, thereby reducing the number of support calls for forgotten passwords. In conjunction with IBM Client Security Software with Password Manager, the fingerprint reader can be an additional means for authenticating to secure operations using the IBM Embedded Security Subsystem.

Origins

Software for the IBM integrated fingerprint reader is supplied by UPEK and runs on the Windows 2000 and XP operating systems. This software performs three functions: it serves as the interface to the fingerprint reader for registering and managing fingerprints; it also interfaces with the IBM Client Security Software (CSS) for managing authentication calls; and it is a means to cache/manage fingerprints for use in place of BIOS and Windows log-on passwords.

Form factor and location

The form factor of the IBM integrated fingerprint reader is innovative. Traditional postage stamp-shaped fingerprint sensors are called contact sensors. This means that the finger is pressed down flat and held on the reader while the device takes an impression. The IBM integrated fingerprint reader is a *slide sensor*. To get a reading, the user must slide or swipe a finger across the reader. The slide sensor takes sequential “snapshots” of the finger as it glides over the sensor. It then “stitches” those snapshots together to form a fingerprint image that can be as large as, or even larger than, the image taken by a contact sensor.

A slide sensor has three advantages over a contact sensor. First, the slide sensor can make a larger image of the finger being read. This means the matcher software has more data to analyze and is less likely to make a mistake. Second, the slide sensor does not have “latent” print problem because the finger itself swipes off the latent print every time. Third, a slide sensor is only 20% the size of a typical contact sensor. The smaller footprint is a key feature in terms of ergonomic and engineering considerations for placement of the device.

Highlights

The IBM integrated fingerprint reader uses capacitive sensing, which means that the fingerprint reader constructs an image of the print based on variations in the electrical properties of the living layer of the finger's skin.

The IBM integrated fingerprint reader on select ThinkPad models is located on the notebook in an easily accessible and unobtrusive place.

Technology

There are several ways to produce a fingerprint image – optical (the traditional law enforcement method), infrared, radar, laser and *capacitive sensing*. IBM has selected the last method because it is mature, reliable, and cost-efficient. Capacitive sensing means that the reader constructs an image of the fingerprint based on variations in the electrical properties of the living layer of the skin of the finger. These properties are somewhat different than the properties of the superficial layer of the skin and this provides some protection against an attack based on a fingerprint lifted from a surface. Variations in electrical properties allow the reader to construct a map of the finger showing the differences created by the ridges and valleys as they wind across the finger.

Fingerprint matching

Since the purpose of biometric matching is authentication, the first step in the matching process is registration. That means defining a user ID and then registering fingerprints in association with that ID. To register a fingerprint, the user repeatedly swipes one finger across the sensor until the registration software has captured enough information to recognize the finger if it is presented in the future. Usually three swipes are enough.

With each swipe, the software records certain pattern elements of the fingerprint. The recorded pattern elements from the swipe are translated into a mathematical formula. This formula, called a template, is then encrypted and stored. The process that generates the “statistically” best possible template out of three fingerprint images is called consolidation. In the consolidation process, a good pair of templates (i.e., templates that match with high scores) out of three is used. Statistical research has shown that the consolidation of two templates produces the highest quality enrolled templates. The consolidation of more than two templates results, on average, in a “statistically” worse template. Fingerprint software does not store the actual digital image of the fingerprint. When a finger is subsequently presented for authentication, the fingerprint reader creates a new template

Highlights

The fingerprint reader can be used to authenticate IBM Client Security Software (CSS) applications like Password Manager, Windows password replacement, file and folder encryption (FFE), and certificate protection.

for the finger, and the fingerprint matching program compares that new template to the stored registered template. If it finds a match, access is granted; if it finds no match, access is denied.

Uses for IBM integrated fingerprint reader

The IBM ThinkPad notebook can be configured to request a fingerprint when turned on – provided that the system has been configured with one or more BIOS passwords. The fingerprint reader subsystem has the ability to securely remember these passwords and can provide them to BIOS when a registered fingerprint has been authenticated. The fingerprint reader can store the power-on password (POP) and hard drive passwords for access to hard drives in the PC. It has the capacity to store up to three hard drive passwords and one POP per fingerprint used for pre-boot authentication.

When prompted, if a fingerprint is provided and matched by the software, it releases the previously stored passwords to BIOS. An additional configuration option enables the same fingerprint to be used to log into a Windows account as well. In short, one swipe at power-on and the PC comes up all the way to the desktop.

All models of the ThinkPad series with the integrated fingerprint reader also have the IBM Embedded Security Subsystem (ESS) as a standard feature. This means the fingerprint reader can be used as another means of authentication for existing IBM Client Security Software (CSS) applications like Password Manager, Windows password replacement, file and folder encryption (FFE), and certificate protection.

The fingerprint reader can replace Windows 2000 and Windows XP log-on passwords. It can select your user ID and provide your password based on the fingerprint provided. Entering or selecting a user ID at the login screen is not necessary; it can all be handled by the fingerprint reader software. This feature can operate independently of IBM Client Security Software, but this would leave the computer unprotected by the Trusted Platform Module (TPM), also called the security chip. Thus, for best security results, Windows password replacement should be implemented through CSS and not outside of CSS.

Highlights

Up to 21 registered fingerprints can be designated for BIOS password use.

How it works

The first time a user turns on an IBM notebook computer with the integrated fingerprint reader, he or she is presented with a splash screen and a prompt to begin the fingerprint enrollment process. The user can either agree to enroll or bypass enrollment. Users can also check a box that says “Don’t remind me again.”

The enrollment process consists of storing the user’s Windows password, enrolling one or more fingerprints, and configuring pre-boot support (selecting fingerprints for use in the pre-boot environment). A person begins the enrollment process by swiping fingers to register one or more prints. Fingerprint templates are stored in the system in such a way that they are associated with the same active user ID.

After completing registration, the user is asked whether he or she wants to enable any of these passwords for the pre-boot environment. This relates to power-on password (POP) and the hard-drive (HDD) password. Once set, the power-on password and hard drive passwords should be recorded in a secure, off-line location. If the PC needs service or if no registered user is available, these passwords are needed to boot. Up to 21 registered fingerprints can be designated for BIOS password use.

Tips on use

Because fingerprint recognition technology is not quite as natural as human beings recognizing each other, some people may experience difficulties. Here are some general tips:

- Because it is possible to damage one or all the fingers on one hand, users are encouraged to enroll at least one finger from each hand.
- Careful enrollment is essential. Once a fingerprint is enrolled, its template will be used for future authentication, and careful enrollment helps obtain better (beyond the threshold quality) templates and hence will help to avoid false matches in the future.
- Attention should be paid to the sensor surface as the “eye” of the system. It should not be touched or scratched with dirty fingers or anything hard. If the sensor is dirty, wet, or fails to work, it should be gently cleaned with a dry, soft, lint-free cloth.

Highlights

Two factor authentication – biometric and password – make the IBM ThinkPad notebook the most secure notebook computer available.

- If someone has difficulty enrolling or authenticating, the hands should be cleaned or a different finger used. If the hands are too dry, lotion can be applied, but not too much because that can have the opposite effect. If appropriate, the user might rub the finger to be matched on his or her forehead to moisten it with the skin's natural oil.

Frequently asked questions

1. What makes IBM ThinkPad notebook computers the most secure notebooks available today?

The answer is simple: two-factor authentication. In addition to authentication of a user via the integrated fingerprint reader, password authentication may also be required. These two forms of authentication make ThinkPad notebooks very secure. The IBM Client Security Subsystem (CSS) can be set to request both forms of authentication.

2. I use Windows Domain Services to enable user roaming to any PC in the Windows Domain. Can I use the IBM fingerprint reader and my fingerprint to log on to any PC in my domain that has an IBM fingerprint reader?

IBM will soon be able to refer interested customers to several business partners for biometric servers that will enable fingerprint-based authentication for Windows logon to any PC equipped with an IBM fingerprint reader. Information about biometric servers can be found at <http://www.pc.ibm.com/us/security/index.html>

3. Can I enroll other people to access my computer via the fingerprint reader, and how many can I enroll?

Several people may share the same PC using the integrated fingerprint reader. Each user that has a Windows user ID and password can register up to ten fingerprints, all of which are stored with that person's Windows user ID and password. That means that if Bob and Alice share a PC, when Bob turns it on and slides his finger, he gets Bob's desktop. When Alice turns on the PC and slides her finger, she gets her desktop.

The number of fingerprints that can be stored for pre-boot authentication is 21, so no more than that number of people can share this feature on a PC. There is no practical limit to the number of Windows users that can enroll

Highlights

With the IBM fingerprint software users can configure their system to replace BIOS and Windows passwords. The fingerprint software stores these passwords in a secure cache.

fingerprints to replace their Window's logon password or for use with the IBM Client Security Password Manager. However, for Password Manager operation, each person must be enrolled in CSS so that CSS can keep each person's passwords separate from everyone else's on that PC.

4. What happens when I need to change my BIOS and/or Windows passwords?

Users can change their BIOS passwords using the BIOS utility in the same manner they would in a non-fingerprint model. Likewise, they would change the Windows password through their Windows software as usual. However, the next time they are asked for a fingerprint prompt after making this kind of password change, they are prompted to re-enter the new password. The IBM fingerprint software verifies that the user has keyed in the correct password and now banks this password in the secure, encrypted cache area on the hard drive.

5. What happens if the integrated fingerprint reader breaks? Will I be able to get into my computer?

If the integrated fingerprint reader is not available, it will be necessary to use the CSS administrative tool to change the policy with regard to the fingerprint reader. Once that is done, normal use can proceed without the fingerprint reader.

6. How does the integrated fingerprint reader interoperate with IBM Client Security Software?

From the CSS perspective, the integrated fingerprint reader acts as another authentication device.

7. How does the integrated fingerprint reader work with third party applications that take advantage of the IBM Embedded Security Subsystem (ESS)?

The integrated fingerprint reader operates as another authentication device for ESS. Any CSS application that generates a request to the user to authenticate can take advantage of this reader. For example, it can be used with IBM Client Security Password Manager and file and folder encryption.

Highlights

Third-party applications that require their own authentication, such as Utimaco SafeGuard Easy, still require that authentication even in the presence of the fingerprint reader.

Any third-party applications that require their own authentication will still require that authentication even in the presence of the fingerprint reader. For example, Utimaco SafeGuard Easy (SGE) uses its own pre-boot user ID and password as security elements. There is no current functionality between the IBM fingerprint reader software and Utimaco SGE. So if a user had BIOS Passwords set to be bypassed by fingerprint swipe, the power-up experience would be to swipe finger for BIOS, and then enter Utimaco SGE user ID and password, and then proceed to Windows. Since most customers who are interested in full hard drive encryption are on the top end of security consciousness, this can be presented as a means of two-factor authentication.

8. How reliable are the fingerprint matchers? What is the chance that it won't let me in? What is the chance that someone can "fake it out" and get in even though they are not enrolled?

There are three ratings used to evaluate the reliability of a matcher.

- False Non-Match Rate (or False Reject Rate). The matcher decides there is no match when there is, in fact, a match. When security is less important and it is important to do the best you can with only one measurement, you want a low False Reject Rate.
- False Match Rate (or False Accept Rate). The matcher decides there is a match when there is, in fact, no match. When it is really important to be sure that there is a match, you want to have a very low False Accept Rate.
- Cross-over Error Rate. In general matcher programs can be tuned to improve either False Reject at the expense of False Accept, or the other way around. In order to do both, you either have to improve the matcher program or change to an inherently more accurate matcher program type. (More accurate matcher programs typically are larger and slower). The Cross-over Error Rate is the point at which False Accept Rate is the same as False Reject Rate.

Error rates have been steadily declining as matching and sensor technologies evolve. In general, the fingerprint matching software is designed to reduce the False Accept Rate at the expense of a higher False Reject Rate. The reason is that if you are falsely rejected, you can just swipe your finger

Highlights

Fingerprint reading error rates have been steadily declining as matching and sensor technologies evolve.

again. If you are falsely accepted, you have been allowed access to something you should not have access to.

For the IBM integrated fingerprint reader, the False Reject Rate given three attempts to validate your finger is less than half a percent, and the False Accept Rate is even lower.

There are a number of known attacks against fingerprint readers. Some are rather intricate, such as building a fake finger out of something like ballistic gel or soft plastic and taping a fingerprint taken from a glass to that finger, then using it to touch the sensor. There has been limited success in laboratory settings against some sensor technologies. The sensor manufacturers keep on top of these attacks and continually update their matchers to resist them.

In short, fingerprint reading technology, although not perfect, has many security features that other technologies do not provide. It is a strong alternative to passwords and, as mentioned above, when used with them creates the opportunity for an even stronger security choice.

9. What if I cut my finger, cut my finger off, or otherwise damage the pad of my finger?

It is possible to so damage a finger that the integrated fingerprint reader cannot perform a match. If the damage is permanent, re-register the finger once it has healed. Because it is possible to damage a finger, or all of the fingers on one hand, users are encouraged to enroll at least one finger from each hand. If the integrated fingerprint reader is not available, it is necessary to use the CSS administrative tool to change the policy with regard to the fingerprint reader. Once that is done, normal use can proceed without the fingerprint reader.

10. Can a severed finger be used with the integrated fingerprint reader?

Capacitive sensors like the one used in the integrated fingerprint reader measure the electrical properties of a living finger. The electrical properties of a severed finger are not the same. In fact, they are so different that a capacitive sensor cannot read a severed finger once the electrical properties

Highlights

Existing databases of fingerprints cannot be used with the integrated fingerprint reader.

of the finger have decayed beyond a certain point. The electrical properties of a finger begin to decay as soon as it is separated from the body or the body dies. It takes about 15 minutes for the properties of a severed finger to decay to the point where a capacitive sensor will no longer recognize the finger.

11. Can an existing database of fingerprints be used with the integrated fingerprint reader?

No. Many law enforcement agencies keep digital fingerprints of their own personnel for a variety of reasons, including the need to eliminate them from crime scenes. Fingerprints collected for this purpose are usually digitized images of ink-pad fingers or of fingers taken using some other optical technology. As mentioned above, the integrated fingerprint reader uses a capacitive sensor to capture a particular type of template of a fingerprint, and the fingerprint software matcher is designed to work only with this type of template. The bottom line is that, for optimal performance and security, users need to register their fingerprints using the IBM fingerprint software.

12. Do the templates need to be erased when the system is repaired or scrapped?

No, but you can erase them if you like. Start IBM Fingerprint Software and select "Fingerprints" on the left. You will see "Edit Passport and Fingerprints," "Delete Passport and Fingerprints" and "Power-on Security." From there you can delete selected fingerprint templates or the entire database (called Passport).

Conclusion

In a world that has become extremely security conscious in recent years, IBM believes that its new integrated fingerprint reader, available on select notebook models, is an excellent advance. Many individuals are using their notebooks as their main computers, and these computers are more and more likely to contain sensitive information. In this context, IBM ThinkPad notebooks with integrated fingerprint readers make an excellent choice for those looking to protect the information stored on their computers.



© 2004 IBM Corporation

Produced in the USA

12-04

All Rights Reserved

Availability: All offers subject to availability. IBM reserves the right to alter product offerings and specifications at any time, without notice. IBM is not responsible for photographic or typographic errors.

Warranty: For a copy of applicable product warranties, write to: Warranty Information, P.O. Box 12195, RTP, NC, 27709, Attn: Dept JDJA/B203. IBM makes no representation or warranty regarding third party products or services.

This publication was developed for products and services offered in the United States. IBM may not offer the products, services or features discussed in this document in other countries. Information is subject to change without notice. Consult your local IBM representative for information on offerings available in your area.

Trademarks: The following are trademarks or registered trademarks of IBM Corporation: IBM, the IBM logo and ThinkPad.

Microsoft and Windows are trademarks or registered trademarks of Microsoft Corporation.

Other company, product and service names may be trademarks or service marks of others.

Visit www.ibm.com/pc/safecomputing periodically for the latest information on safe and effective computing.