GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

User authentication by integrated fingerprint solution on Laptop computers and possible attack points

GIAC Security Essentials
Certification (GSEC)
Practical Assignment
Version 1.4b

Option 1 - Research on Topics
in Information Security

Submitted by: Tamas KOROMPAY, January 22, 2005
Location: SANS Conference - London - June 2004

Paper Abstract:

This paper will examine the user authentication process through the integrated fingerprint solution of IBM's latest T series laptop computer. The paper is based on the key factors of biometrics mechanisms: *technology, reliability, user acceptance and cost.* Finally it will investigate possible attack points to a generic biometric system and give answer to the most frequently asked user questions.

© SANS Institute 2005, Author retains full rights.

Table of Contents

1. INTRODUCTION 1

2. TECHNOLOGY AND RELIABILITY 1

2.1. FINGERPRINT REPRESENTATION 1
2.2. FORM FACTOR AND LOCATION 2
2.3. THE TOUCHSTRIP SWIPE-SCANNER 3
2.4. THE TWO PROCESSES OF A TYPICAL BIOMETRIC APPLICATION 3
2.4.1. Enrolment Process 4
2.4.2. Verification Process 6
2.5. ERROR RATES 6

3. USER ACCEPTANCE AND COST 8

3.1. IT ADMINISTRATOR 8
3.2. THE PUBLIC 8

4. VULNERABLE POINTS OF A BIOMETRIC SYSTEM 9

5. FREQUENTLY ASKED QUESTIONS [] 11

6. CONCLUSION 12

7. REFERENCES 13

List of Figures

FIGURE 1: ENROLMENT AND VERIFICATION 3
FIGURE 2: ENROLMENT PROCESS – FINGER SELECTION 4
FIGURE 3: ENROLMENT PROCESS - FINGER SWIPE 5
FIGURE 4: BIOMETRIC SYSTEM ERROR RATES 7
FIGURE 5: POSSIBLE ATTACK POINTS IN A GENERIC BIOMETRICS-BASED SYSTEM [] 9

© SANS Institute 2005, Author retains full rights.

1. Introduction

More than one century has passed since Alphonse Bertillon discovered the uniqueness of the human fingerprint. Since then many law enforcement departments use to book the fingerprint of criminals for identify determination. As the demand on manual fingerprint identification became higher and higher research has been initiated to acquire fingerprints through electronic medium based on their digital representation. These first efforts led to development of automatic/semi-automatic fingerprint detection systems over the last few decades.

"What was once considered science fiction technology is now available to all enterprises in the everyday business" announced IBM on 4th October 2004 for its latest T series Think Pads [1]. The laptop has a built in fingerprint reader which eliminates the need for users to remember multiple passwords.

In a world that has become extremely security conscious in recent years, IBM's new Integrated Fingerprint Reader on some laptop models is an excellent offer of biometric technology for person identification for non-forensic applications. Who is authorized to access confidential or privileged information on a system? The answer to this question is really valuable to all business organizations [2] as many individuals are using their laptops as their main computers containing sensitive information.

The benefit to the user is increased security through the ability to implement additional authentication elements - in this case the fingerprint - for system logon, as well as the capability to defend against password hammering techniques [3].

2. Technology and reliability

IT systems require authentication of users. This identification is commonly done with passwords ("what you know") or cards and badges ("what you have"). Biometric authentication is a third method based on "who you are." It has definite advantages: biometrics can eliminate problems of forgotten passwords or lost cards because "who you are" is always with the user. Biometrics is currently becoming more popular for convenient and secure authentication.

2.1. Fingerprint representation

Fingerprints are usually split into two types: global and local. The global representation is an overall characteristic of the finger and a single representation is valid for the entire fingerprint. Generally used for fingerprint indexing and can be categorized into classes e.g.: whorl, right loop, left loop, arch, twin loop and tented arch. The local representation consists of several

[1] http:/www.technewsworld.com/story/37017.html
[2] www.research.ibm.com/ecvg/pubs/sharat-forensic.pdf
[3] http://www.pc.ibm.com/us/security/userauth.html

© SANS Institute 2005 Author retains full rights.

components derived from a restricted region of the fingerprint and used for fingerprint matching [4].

The most typical representations of the local information are based on finger ridges, pored on the ridges or salient features derived from the ridges. The most frequently used local feature is based on minute details (minutiae) of the ridges.

In automatic fingerprint matching only the two most important types of minutiae details are used: ridge ending and ridge bifurcation. The reason is their stability and robustness. The simplest minutiae based representations constitute a list of points defined by their spatial coordinates with respect to a fixed image-centric coordinate system. The ANSI-NIST standard representation of a fingerprint is mainly based on minutiae and includes its location and orientation [5].

2.2. Form factor and location

IBM has chosen the swipe-scanner rather than a touch-scanner, for a number of reasons [6].

Firstly the swipe-scanner has better security. The fingertip has to be dragged across the scanner and it is not possible to "lift" it from the surface. With the swipe-scanner it is not possible to leave a thin oil print of the fingerprint on the surface of the scanner which could be a real problem with the touch-scanner: if someone else has physical access to it and has the required "fingerprint removal tools" could get that print and try to authenticate themselves misusing it.

The second advantage of the swipe-scanner is its size which can be five times smaller than the touch-scanner since it doesn't have to accommodate the whole fingertip. This is particularly important for laptop models with limited free space for additional built-in devices.

The third reason is that the slide sensor can make a larger and more accurate image of the fingerprint being read. This helps a lot for the matcher software which has more data to analyze and is less likely to make a mistake.

The fourth and final reason is that touch scanners need more care as they can easily become dirty. They need to be cleaned often to maintain an accurate read of the fingertip. With the swipe-scanners it takes a bit longer to become familiar but once the user gets the hang of drawing his finger across the surface smoothly, there won't be any problem.

The IBM Integrated Fingerprint Reader on latest T series Think Pads models is located at the right side of the palm rest under the directional arrows. This position eliminates the need for attached external devices that get in the way and can be lost.

[4] www.research.ibm.com/ecvg/pubs/sharat-forensic.pdf
[5] American National Standard for Information Systems
[6] http:/www.trustedreviews.com/article.aspx?art=749

© SANS Institute 2005 Author retains full rights.

2.3. The TouchStrip swipe-scanner

The TouchStrip swipe-scanner of UPEK [7] is using a capacitive sensor technology. It means that the reader constructs an image of the fingerprint based on variations in the electrical resistance over the surface of a living finger.

Because the skin cells on the exterior surface of the human skin are dead however under a few layers of these cells is the first layer of living skin cells. These cells have specific qualities of electrical resistance, and they fall into specific shapes over the surface of the skin to form the familiar ridges and valleys of a fingerprint. From security point of view “living” is very important as it makes authentication impossible with “cut off” fingers. In fact a capacitive sensor cannot read a severed finger once the electrical properties 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, and it takes about 15 minutes for the properties of a severed finger to decay so much that a capacitive sensor will no longer recognize that finger.

The combination of specific electrical qualities of the living cells and specifically how the cells are arranged results in measurable and unique variations of electrical resistance over the surface of the finger. These allow a capacitive reader to record variations in the electrical resistance of the living surface of the finger and construct a map of the finger showing those variations. That map looks like a standard police image of a fingerprint.

2.4. The two processes of a typical biometric application

The figure below shows the processes involved in a typical biometric system: Enrolment and Verification (see Figure 1) [8]:

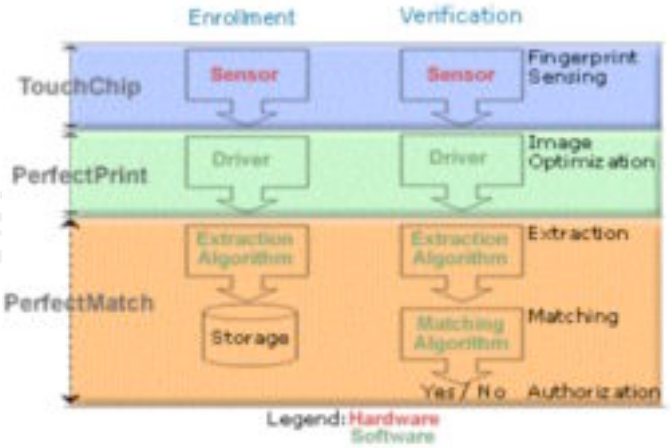


Figure 1: Enrolment and Verification

[7] http://www.upek.com/promlit/pdf/fltcs3a-0903.pdf
[8] http://www.upek.com/techno/biom.htm

© SANS Institute 2005 Author retains full rights.

Extraction takes place during the enrolment and verification processes. The PerfectMatch algorithm extracts the fingerprint's minutia - the set of unique characteristics of a given fingerprint - and creates a fingerprint template. This template is a mathematical representation of the original fingerprint based on the analysis of the ridge patterns. It takes up far less space (520 bytes) than the original fingerprint image [9].

2.4.1. Enrolment Process

Before the identity of an individual can be verified via his/her fingerprints, it is essential that the user repeatedly presents one of his finger to the sensor until the registration software has captured enough information to recognize the finger if it is presented in the future. This process is called enrolment. The samples are referred to fingerprint templates and can be stored on a broad range of media such as PCs, servers (for a central repository database), smartcards and in the memory of an embedded application. During the first boot up of the ThinkPad the user is welcomed by the "IBM Fingerprint Software" window. This is where he can configure the fingerprint scanner and enroll the fingers that he wishes to use. He has two options: 1) agrees and starts the enrolment or 2) bypasses it even saying “Don’t remind me again.” [10]

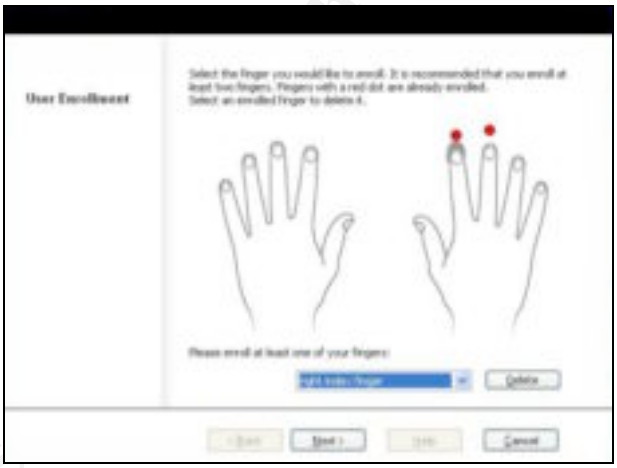


Figure 2: Enrolment process – finger selection

If he agrees he can enroll one of his fingers in the Power On security section (see Figure 2). This would allow him to boot the laptop with a fingerprint instead of a password. The Power On password has to be obviously enabled in the BIOS for the Power On fingerprint security to work. After he scanned his finger three times successfully (see Figure 3) the software amalgamates all three images into a single image (minutiae template), to which it will compare any scans that it receives in the future [10].

[9] http://www.upek.com/techno/techpm.htm
[10] http://www.trustedreviews.com/article.aspx?art=749

© SANS Institute 2005 Author retains full rights.

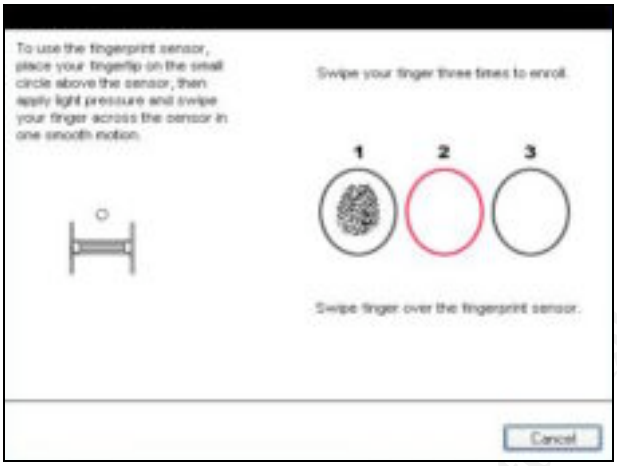


Figure 3: Enrolment process - finger swipe

The user can store maximum a total of 21 profiles. This should be enough if the laptop is not shared between a high numbers of users. There is no need to be worried about someone extracting the fingerprint data from the scanner and breaking the security: with each swipe, the software records only certain pattern elements of the fingerprint. These elements are averaged over the three swipes and a mathematical formula is generated that is statistically unique to that finger. This formula, called a template, is then encrypted and stored on the hard drive. Fingerprint software does not store the actual digital image of the fingerprint.

The fingerprint authentication can be used for Windows login as well. It can be configured in the fingerprint software for the users to login automatically to Windows after successful PowerOn authentication. This can be a big advantage if more than one person uses the laptop as users can quickly and easily switch using the fingerprint scanner instead of passwords. Some recommended tips to the enrolment process [11]:

- Because it is possible to damage one or all of the fingers on one hand, users are encouraged to enroll at least one finger from each hand
- Once a fingerprint is enrolled, its template will be used for authentication every time. Therefore, careful enrolment is a good practice. Although the system is designed to accept only fingerprints that have certain level of quality, careful enrolment helps obtain better (beyond the threshold quality) templates and hence helps a user to authenticate him or herself comfortably to avoid false matches
- 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 cleaned gently with a dry, soft, lint-free cloth

[11] IBM internal information source

© SANS Institute 2005 Author retains full rights.

- 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 forehand to moisten it with the skin's natural oil.

2.4.2. Verification Process

The verification process requires users to verify their identity by placing their finger on the fingerprint reader. The live fingerprint is compared with the stored template using a matching algorithm. The output is a matching score (s) which is compared with a modifiable security threshold (t). The user is only granted access if the matching score is higher than the threshold [12].

2.5. Error rates

The challenge for biometrics lies in the measurement and decision of what exactly is similar. Although biometric technology is advancing rapidly it is not yet 100% accurate in matching a previously enrolled biometric feature to a present feature.

The fact is 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). In some cases, even the user's own finger (two matching fingers) looks different to the sensor. Therefore, a biometric matching system's response is typically a matching score *s* (usually a single number) that quantifies the similarity between the input and the database template representations. The higher the score the more certain the system is that the two biometric measurements come from the same person [13].

A threshold (*t)* regulates the system decision:

- pairs of biometric samples generating scores higher than or equal to (*t)* are *mate pairs*, they belong to the same person. The distribution of scores generated from pairs of samples from the same person is called a *genuine distribution* (see Figure 4) [14]
- pairs of biometric samples generating scores lower than (*t)* are *non-mate pairs*, they belong to different persons. The distribution of scores generated from pairs of samples from different persons is called an *impostor distribution* (see Figure 4) [14]

The curves show false match rate (FMR) and false non-match rate (FNMR) for a given threshold *t* over the genuine and impostor score distributions. FMR is the percentage of non-mate pairs whose matching scores are greater than or equal

[12] http://www.upek.com/techno/techpm.htm
[13] http://biometrics.cse.msu.edu/j2033.pdf
[14] http://www.upek.com/promlit/pdf/fltcs3a-0903.pdf

© SANS Institute 2005 Author retains full rights.

to *t*, and FNMR is the percentage of mate pairs whose matching scores are less than *t* [13].

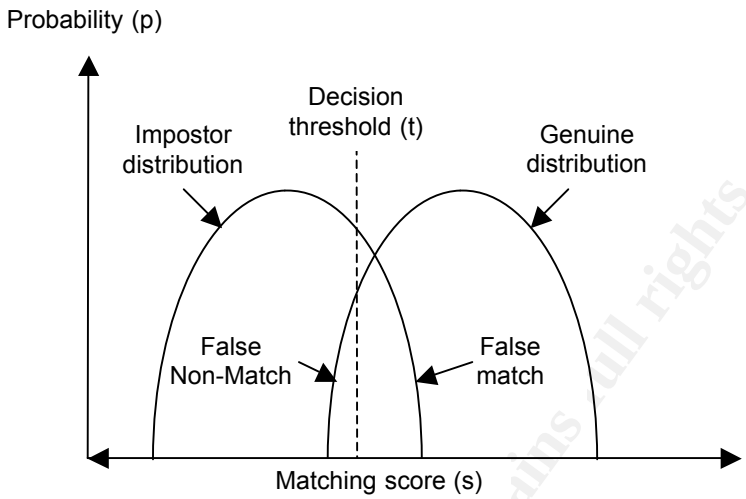


Figure 4: Biometric system error rates

A biometric verification system can make two types of errors [15]:

- *False Match Rate (FMR) or False Acceptance Rate (FAR)*
  – the percentage of impostors the biometrics mechanism falsely authorizes. In this case two non-matching fingerprint images look similar to the authentication system
- *False Non-Match Rate (FNMR) or False Reject Rate (FRR)*
  – the percentage of legitimate users falsely rejected. In this case two matching fingerprint images look dissimilar to the authentication system.

An operational biometric system makes a trade-off between false match rate (FMR) and false non-match rate (FNMR). In fact, both FMR and FNMR are functions of the system threshold: if the system's designers reduce it to make the system more tolerant to input variations and noise, FMR increases. On the other hand, if they raise it to make the system more secure, then FNMR increases accordingly [16].

Most current sensors have error rates on single measurements 1% or less FMR and around 3% FNMR. That means there is less than a 1% chance that a random person can slide his finger on the sensor and be accepted. For the IBM Integrated Fingerprint Reader, the False Reject Rate given three attempts to validate the finger is less than half a percent.

[15] SANS Security Essentials Version 2.2. Defense-In-Depth. Page 160.
[16] http://www.biometrics.org/html/bc2002_sept_program/Grother_9_02.pdf

© SANS Institute 2005 Author retains full rights.

3. User acceptance and cost

3.1. IT administrator

IT administrators are being required to secure their systems, as viruses, hackers, and other malicious attacks continue to increase. At the same time, policies and security solutions to help secure systems often have been problematic or difficult for individual users to implement. USB and smart card solutions can be lost or compromised. This has meant that systems often were left unsecured, jeopardizing key corporate data and systems. The TouchStrip solution [17] provides security with convenience – users merely have to touch their finger to the sensor, which is highly accurate [18]. A typical TouchStrip solution provided by UPEK adds less than $50 to the overall cost of the PC. This cost is a very small part of the overall system cost after the amortization over the life of the system and when considered important to reduce today's security problems. Analysts have suggested that the annual cost per user for password-related problems can range from $50-$350. According to a study done by IDC last year, the average yearly cost to IT departments to assist with and fix password-related problems is $48! Analyst Roger Kay states that "This last figure would seem to justify a means that would avoid these costs if it cost on the order of $50 per user per year or less, well within the range of a biometric-based sign-on schema" [18].

3.2. The Public

Biometrics-based authentication has lots of usability advantages comparing to traditional password authentication systems. Users can never lose their biometrics, and the biometric signal is relatively difficult to steal or forge. Next to the easy usage of biometrics for user authentication for Laptop computers the public is going to be worried about the information that is being collected about individuals. The possible wide usage of biometrics in a mass market, like bank ATM access or credit card authorization also can raise additional concerns next to the security of the transactions. One of these worries is the public's sensitivity of a possible offensive of privacy. Next to personal information such as name and date of birth, more and more biometric data contained information is being stored about individuals like body parts and fingers. These images, or other biometric signals, usually stored in digital form in different databases raises the concern of data management and date sharing. UPEK also offers a fingerprint template management tool which gives the possibility to store fingerprint templates of employees in a centralized database. All above the most important fact is that a person's biometric data are given and cannot be changed. The big advantage that makes biometrics so attractive for authentication purposes - their invariance over time - is also its drawback if biometric data is stolen. When the biometric data are compromised, replacement is not possible [19].

[17] http://www.upek.com/promlit/pdf/fltcs3a-0903.pdf
[18] http://www.upek.com/company/UPEK_IBM_QA.pdf
[19] www.research.ibm.com/journal/sj/403/ratha.pdf

© SANS Institute 2005 Author retains full rights.

4. Vulnerable points of a biometric system

A generic biometric system can play the framework role of a pattern recognition system. The stages of such a generic system are shown in Figure 5.

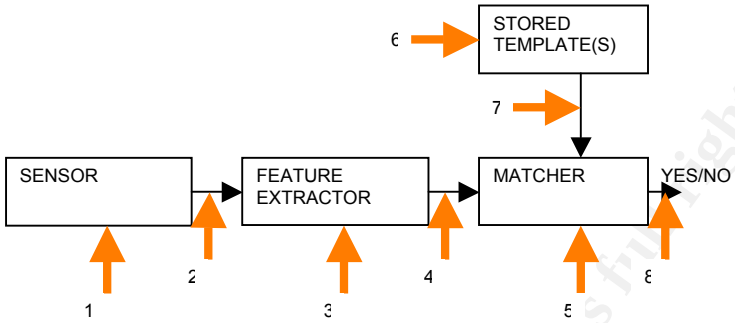


Figure 5: Possible attack points in a generic biometrics-based system [20]

After a biometric signal is received from the user (e.g.: the fingerprint scan) a unique template is saved in a database that represents the particular individual. During the authentication process the corresponding template is retrieved from the database and matched against the template based on the newly received input signal. The matcher must make a decision based on the closeness of these two templates.

Password-based authentication systems can also described using this framework: the keyboard is the input device, the password encryptor is the feature extractor and the comparator is the matcher. The template database is equivalent to the encrypted password database.

There are eight possible attack points identified in the generic biometric system of Figure 5. The items in the following list correspond to the numbers in the figure [20]:

1. Fake biometrics is presented at the sensor: In this mode of attack, a possible reproduction of the biometric feature is presented as input to the system. Examples include the presentation of an old copy of a fingerprint image.

   Possible defense: Firstly finger conductivity or fingerprint pulse at the sensor can stop simple attacks. A capacitive fingerprint sensor cannot read a severed finger once the electrical properties of the finger have decayed beyond a certain point. Secondly with the swipe-scanner it is not possible to leave a thin oil print of the fingerprint on the surface of the scanner so get an older copy of a fingerprint image is not possible.

[20] www.research.ibm.com/journal/sj/403/ratha.pdf

© SANS Institute 2005 Author retains full rights.

2. Previously stored digitized biometrics signals are resubmitted: in this mode of attack, a recorded signal is replayed to the system, bypassing the sensor.

   Possible defense: this attack involves generating all possible fingerprint images in order to match a valid fingerprint image, would have an even larger search space and consequently would be much more difficult.

3. The feature extraction process is override: The feature extractor is attacked using a Trojan horse, so that it produces feature sets pre-selected by the intruder.

   Possible defense: protection against Trojan horses.

4. The biometric feature representation is tampered: The features extracted from the input signal are replaced with a different, fraudulent feature set (assuming the representation method is known). Often the two stages of feature extraction and matcher are inseparable and this mode of attack is extremely difficult. However, if minutiae are transmitted to a remote matcher (say, over the Internet) this threat is very real.

   Possible defense: Encrypted communication channels can eliminate at least remote attacks. If the minutia is stored locally the risk of tampering is much lower.

5. The matcher corrupted: The matcher is attacked and corrupted so that it produces pre-selected match scores.

   Possible defense: have the matcher and the database reside at a secure location. Of course, even this cannot prevent attacks in which there is collusion.

6. Templates tampered: The database of stored templates could be either local or remote. The data might be dispersed over several servers. Here the attacker could try to modify one or more templates in the database, which could result either in authorizing a fraudulent individual or denying service to the persons associated with the corrupted template.

   Possible defense: have the matcher and the database reside at a secure location. If the minutia is stored locally the risk of tampering is much lower.

7. The channel attacked between the stored templates and the matcher: The stored templates are sent to the matcher through a communication channel. The data traveling through this channel could be intercepted and modified.

   Possible defense: have the matcher and the database reside at a secure location. Of course, even this cannot prevent attacks in which there is collusion.

8. Final decision override: If the final match decision can be overridden by the hacker, then the authentication system has been disabled. Even if the actual pattern recognition framework has excellent performance

© SANS Institute 2005 Author retains full rights.

characteristics, it has been rendered useless by the simple exercise of overriding the match result.

It can be remarked that the threats presented in Figure 5 are very similar to the threats to password-based authentication systems. One difference is that there is no "fake password" equivalent to the fake biometric attack at point 1. Furthermore, in a password- or token-based authentication system, no attempt is made to thwart replay attacks (since there is no expected variation of the "signal" from one presentation to another). [20].

5. Frequently asked questions [21]

- ***Is there any way to centrally manage fingerprints across the company?***

Since the fingerprint templates are stored in a folder, they can be managed by standard Windows management software through the Windows Active Directory. In addition, there's a fingerprint template management tool available from UPEK; however, this server application is not offered by IBM or supported by IBM.

- ***What happens if the Integrated Fingerprint Reader breaks? Will the user be able to get into its computer?***

If the Integrated Fingerprint Reader breaks, the system will revert to the use of passwords. At system power-up the user will be required to enter his Power-On Password and/or his Hard Drive Password, if they are being used. At Windows sign-on, he will be prompted for his Windows password. During use of Client Security Software applications such as Password Manager he will be required to enter his CSS pass phrase.

- ***What to do if the user cuts his finger?***

It is possible to so damage a finger that the Integrated Fingerprint Reader cannot perform a match. If the damage is permanent the user should re-register the finger once it has healed. Because it is possible to damage a finger, or all of the fingers on one hand, all users are encouraged to enroll at least one finger from each hand. However, if a user is unable to get a fingerprint match, it is possible to bypass the Integrated Fingerprint Reader and return to BIOS, Windows, and/or CSS passwords, depending on which are set.

- ***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

[21] IBM internal information source

© SANS Institute 2005 Author retains full rights.

technology. As mentioned above, the Integrated Fingerprint Reader uses a capacitive sensor. Digitized fingerprints cannot be used in place of the normal registration process. A capacitive sensor does not read the dead surface skin, but the live subsurface skin. There are enough subtle differences that an optical fingerprint merely looks like the capacitive fingerprint of the same finger. If the matching software is run against the two looking for a match, unacceptably poor results will occur – a very high rate of false rejection (deciding that the images are not of the same finger when in fact they are).

6. Conclusion

Biometrics-based authentication has lots advantages comparing to traditional password authentication systems. Low fingerprint sensor prices, easy availability of cheap computing power and relatively good understanding of individuality information in fingerprints (compared to other biometrics) raised lot of commercial interest in fingerprint-based personal identification. As a result, many fingerprint identification vendors appeared in the last few years. Embedded applications of fingerprint-based identification (e.g., in Laptops and in cell phones) are on the market already [22].

From IT manager's point of view biometric security based on fingerprint solutions makes life much easier. Firstly there will be fewer phone calls from users who have forgotten their passwords. Secondly he won't need to be worried any more about insecure log-on passwords and keystroke loggers which could pass them onto hackers.

Problems of privacy of biometrics are also mentioned. Next to the easy usability the public is going to be worried about the information that is being collected by biometric authentication systems. It is ironic that the big advantage that makes biometrics so attractive for authentication purposes - their invariance over time - is also its drawback if biometric data is stolen. Once a set of biometric data has been compromised, it is compromised forever.

Unfortunately biometric systems are also vulnerable when attacked by determined hackers. In this paper eight possible vulnerability points of a generic biometric system are discussed and propositions are suggested to lighten some of these security threats.

In a world that has become extremely security conscious in recent years, IBM believes that its new Integrated Fingerprint Reader on some laptop models makes an excellent choice on the side of greater security.

[22] www.research.ibm.com/ecvg/pubs/sharat-forensic.pdf

© SANS Institute 2005 Author retains full rights.

7. References

1. A. K. Jain and S. Pankanti: "Automated Fingerprint Identification and Imaging Systems" Advances in Fingerprint Technology, 2nd Edition, H. C. Lee and R. E. Gaensslen (eds.), Elsevier Science, 2001.Elsevier Science, 2001.
URL: www.research.ibm.com/ecvg/pubs/sharat-forensic.pdf

2. Jack M. Germain “IBM Introducing Fingerprint Reader into Laptop”
URL: http://www.technewsworld.com/story/37017.html (4th October 2004)

3. Riyad Emeran “Biometric IBM ThinkPad T42 – Exclusive Preview”
URL: http://www.trustedreviews.com/article.aspx?art=749 (4th October 2004)

4. Salil Prabhakar, Sharath Pankanti and Anil K. Jain: "Biometric Recognition: Security and Privacy Concerns"
URL: http://biometrics.cse.msu.edu/j2033.pdf (March 2003)

5. Patrick Grother,P. Jonathon Phillips, Ross Michaels: "New Evaluation Statistics for Measuring the Performance of Biometric Technologies"
URL: http://www.biometrics.org/html/bc2002_sept_program/Grother_9_02.pdf (2002)

6. RATHA, CONNELL: "Enhancing security and privacy in biometrics-based authentication systems"
IBM SYSTEMS JOURNAL, VOL 40, NO 3, 2001
URL: www.research.ibm.com/journal/sj/403/ratha.pdf

7. American National Standard for Information Systems. Data format for the interchange of fingerprint information
URL: http://www.itl.nist.gov/iad/894.03/fing/slides/IAFIS_Overview/

8. SANS Security Essentials Version 2.2. Defense-In-Depth. Pages 160-161.

9. IBM “Embedded Security System”
URL: http://www.pc.ibm.com/us/security/userauth.html

10. UPEK: “PerfectMatch -- Fingerprint template extraction and matching”
URL: http://www.upek.com/techno/techpm.htm

11. UPEK: “The two processes of a typical biometric application”
URL: http://www.upek.com/techno/biom.htm

12. UPEK: “IBM Selects UPEK as the Sole Fingerprint Authentication Solution for the New Thinkpad® Notebook; Questions and answers”
URL: http://www.upek.com/company/UPEK_IBM_QA.pdf

13. UPEK: “TCS3B-TCD41B TouchStripTM chipset”
URL: http://www.upek.com/promlit/pdf/fltcs3a-0903.pdf

© SANS Institute 2005, Author retains full rights.

© SANS Institute 2005 Author retains full rights.