Security Threats of Finger Print Biometric in Network System Environment

Imad F. Alshaikhli, Mohammad A. Ahmad
Computer Science Department, KICT
International Islamic University of Malaysia,
Kuala Lumpur, Malaysia
imadf@iium.edu.my
ma.alahmad@paaet.edu.kw

Article Info

Received: 15 June 2011
Accepted: 04 July 2011
Published online: 01 September 2011

ABSTRACT

Biometrics-based personal authentication systems that use physiological (e.g., fingerprint, face) or behavioral (e.g., speech, handwriting) traits are becoming increasingly popular, compared to traditional systems that are based on tokens (e.g., key) or knowledge (e.g., password). On the other hand, biometric systems are vulnerable to attacks, which can decrease their security. This paper analyzes and surveys the vulnerabilities and security threats of the finger print biometric systems used for access control and the authentication of access to confidential information in network system environment. As analysis tools, two biometric network models are implemented and connected to see some of the arguments of the vulnerabilities and security threats. Based on that, analysis and surveying, experimental solutions and countermeasures are presented.

***Keyword:* Biometric, security threats, telebiometric, finger print.**

1. Introduction

The term biometric is derived from the Greek words bio (life) and metrics (to measure). Biometrics is automated methods of recognizing a person based on a physiological or behavioral characteristic. Among the features measured are faced, fingerprints, hand geometry, handwriting, iris, retinal, vein, and voice. Biometric technologies are becoming the foundation of an extensive array of highly secure identification and personal verification solutions. As the level of security breaches and transaction fraud increases, the need for highly secure identification and personal verification technologies is becoming apparent. This paper addresses and analyzes the security threats of finger print biometrics authentication system in a network system environment. After the introduction given in section 1, section 2, literature view of the nine biometrics network models-based personal authentication technology and their security threats is presented. In section 3, the analysis of the nine biometric network models and their security threats is presented. Based on that, analysis and surveying, surveyed experimental solutions and surveyed countermeasures are presented. But for threat 4, laboratory experiment is accomplished by the authors using packet tracer software called Wire Shark, to capture the data travelled into the network, proving the security vulnerability threat this component. Finally, conclusion will be discussed in section 4.

2. Literature Survey

Based on the ITU RFC, question 8/17 regarding telebiomtric system mechanism study, Yongnyou and Woochang divided biometric models into nine categories (all combinations of the three items in the two table below) (Yongnyou and Woochang, 2009)

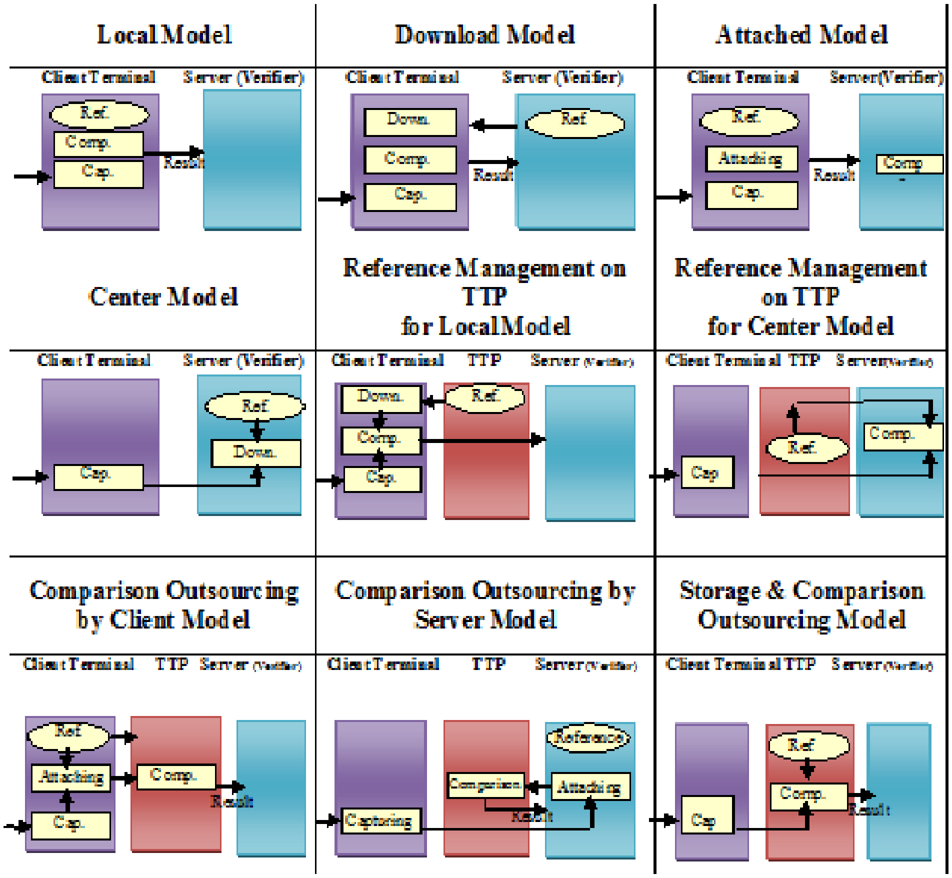


Fig.1. Nine biometric network models

A Telebiometric System Mechanism (TSM) defines the telebiometric authentication models considering the locations in which biometric reference templates are stored and the manner in which they are compared, as shown in Fig.1 (Yongnyou and Woochang, 2009).

Of the nine models, some utilize a Trusted Third Party (TTP) for authenticating a user’s public key, registered biometric reference information, and the security evaluation result based on the common criteria scheme for biometric devices. A TTP can also perform biometric comparison (Yongnyou and Woochang, 2009).

Fig.2 illustrates the biometric component through a network. A component sends biometric data to the component of the next step for processing. The telebiometric functional model refers to the model of the function to be included in transmission in a biometric system. A biometric function obtains the output of the previous stage for input; each function is performed independently. The authentication context for biometrics based on a biometric verification process consists of five sub-processes, which are data capture, signal processing, storage, comparison and decision (Yongnyou and Woochang, 2009).

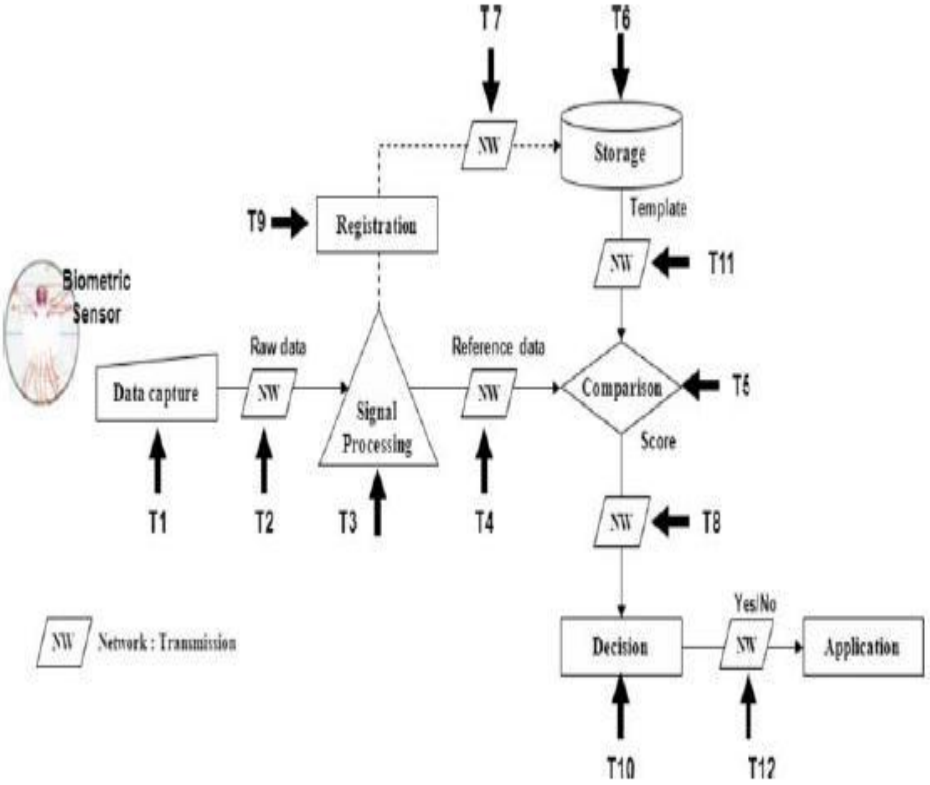


Fig.2. Security threats of biometric network model (Yongnyou and Woochang, 2009)

Fig.2 illustrates the threats associated with the biometric component through a network in the biometric verification process model. In this model, each component sends processed biometric data to the next component. Compared to a general biometric functional model, in a telebiometric functional model, processed biometric data is transmitted between components through telecommunications media, denoted as *NW* in Fig.2 (Yongnyou and Woochang, 2009).

Fig.2 illustrates that not only each component in the model but also the transmissions between components are vulnerable to external attacks. An external attack can be an external invasion when biometric data is delivered to the next step, and may include the modification of processed biometric data. By type, the threats can be defined as follows:

- T1: Threat to biometric input devices

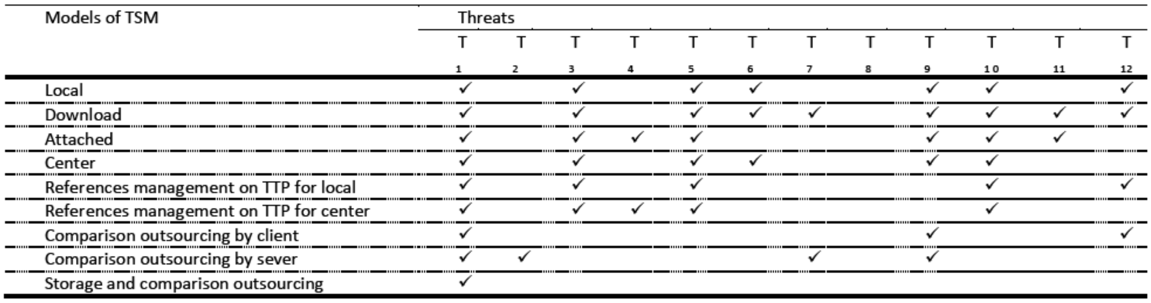
- T2: Threat to the process of transmitting biometric raw data to the signal-processing component
- T3: Threat to the signal-processing component
- T4: Threat to the process of transmitting the extracted biometric templates to the comparison component
- T5: Threat to the comparison component
- T6: Threat to biometric storage component
- T7: Threat to the process of transferring biometric templates from the registration component to the storage component
- T8: Threat to the process of transmitting the matching score from the comparison component
- T9: Threat to the registration component
- T10: Threat to the decision component
- T11: Threat to the process of transmitting the stored biometric template to the comparison component
- T12: Threat to the process of transmitting the decision result to an application system

Biometric raw data can be altered or intercepted by an attacker and used for illegal purposes when being sent to the signal-processing component. The definition of this type of threat was a T2 threat, and provides a guideline for protection (Yongnyou and Woochang, 2009).

Biometric raw data acquired from a capture device can be attacked and disclosed by illegal users before it is safely transmitted to the signal-processing component. The definition for this type of threat was a T7 threat (Yongnyou and Woochang, 2009).

Table 1 expresses the vulnerabilities of the nine models using the threats defined earlier "Threats to telebiometric systems".

Table 1: Vulnerabilities of the nine TSM models (Yongnyou and Woochang, 2009)



Models of TSM	Threats											
	T	T	T	T	T	T	T	T	T	T	T	T
	1	2	3	4	5	6	7	8	9	10	11	12
Local	✓		✓		✓	✓			✓	✓		✓
Download	✓		✓		✓	✓	✓		✓	✓	✓	✓
Attached	✓		✓	✓	✓				✓	✓	✓	
Center	✓		✓		✓	✓			✓	✓		
References management on TTP for local	✓		✓		✓					✓		✓
References management on TTP for center	✓		✓	✓	✓					✓		
Comparison outsourcing by client	✓								✓			✓
Comparison outsourcing by sever	✓	✓					✓		✓			
Storage and comparison outsourcing	✓											

This table assumes that, in general, the models have the data capture component and the signal processing component in the same location. However, for the models that use outsourced comparison, the signal-processing component is located at the same location as the comparison component resides.

It is also assumed that the comparison and the decision components are combined in the same module. Furthermore, TTP guarantees the safety and security of biometric template data that is both stored and transmitted.

When developing a biometrics-based networked manufacturing system, the telebiometric system model of the developed system should be checked, and potential threats should be analyzed according to Table 1, with appropriate security measures taken. (Yongnyou and Woochang, 2009).

3. Security Threats of Finger Print Biometric in Network System Environment

In this section, analysis of the twelve security threats of biometric network models will be discussed in details. Also for each threat, surveyed experimental solutions will be introduced to overcome these security threats. The experimental solutions provided by the authors for threat 4 and threat 6 will be implemented using:

a. Two different commercial finger print biometric devices and HP Pavilion tx2000 laptop to design the biometric network models. The local and download models will be implemented and connected of the nine biometric models due to the fact that is widely used other than the biometric network models.
b. The well known Wire Shark version 1.2.9 sniffer and data capturing to capture the data travelled through the implemented biometric networks.
c. Commercial finger print data base software to show the format of the saved template.

3.1 **Threat 1** (T1): Threat to biometric input devices

According to table 1, this threat is shared by all biometric network models. The analysis and countermeasures of this threat will be discussed below.

3.1.1 Analysis

Threat 1 is the threat to the biometric input device (at the data capturing stage). This means, presenting legitimate users template by an attacker to fool the data capturing component. To analyze this threat, a finger print device will be used as an example of biometric devices.

As an example, lifting a latent fingerprint from finger print device, the attacker must know the legitimate users whereabouts and the surfaces she/he has touched. Next, the attacker must lift a latent fingerprint of good quality.

This is not easy in practice because most latent fingerprints are left are incomplete, wrapped around irregular surfaces, or partially canceled by fingers slipping. Then, the attacker has to make an accurate three-dimensional model of the finger as shown in Fig.3. This requires both expertise and laboratory equipment such as a high-resolution scanner, a three dimensional printing device (such as a stereo-lithography printer), and so on.

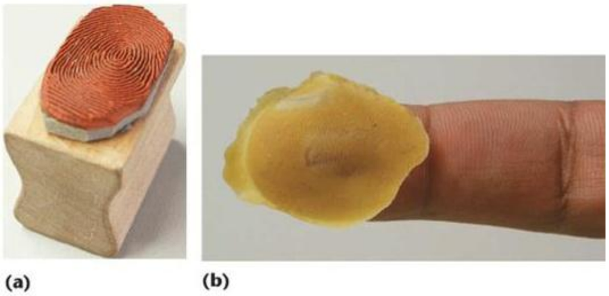


Fig.3. Fake fingers made by: a) Rubber Scan b) Wafer thin plastic (Matsumoto et al., 2002)

Recently, Tsutomu Matsumoto et al. (2002) documented several detailed methods of creating a fake finger from silicone and gelatine to fool many commercially available fingerprint data capturing. Although producing a gummy clone of an available real finger (from a consenting user) is relatively simple, reconstructing a fake finger from a latent fingerprint remains quite complicated. Also, Dead fingers can be counted as fake fingers that can fool the biometric systems.

3.1.2 Countermeasures

The attacker cannot be prevented from collecting biometric data outside the system, but can only do is to detect or deter fake biometric attack. To overcome such threat multiple of surveyed experimental solutions can be considered:

a. Derakhshani et al. (2003) proposed two software-based methods (not based on sensors that measure temperature, conductivity, etc.) for fingerprint liveness detection. They used a commercially available capacitive sensor and the sole input to the liveness detection module is a 5-second video of the fingerprints. In their static method, the periodicity of sweat pores along the ridges is used for liveness detection. In the dynamic method, sweat diffusion pattern over time along the ridges is measured. Live fingers, fingers from cadavers, and dummy fingers made up of play dough are used in the experiments.
b. Heart pulses to be integrated with the input sensor (data capturing) and sensor that measure temperatures.

3.2 **Threat 2** (T2): Threat to the process of transmitting biometric raw data to the signal-processing component

According to table 1, all biometric network models have no such threat except comparison outsourcing by server model. The analysis and countermeasures of this threat will be discussed below.

3.2.1 Analysis

In this mode of attack, a recorded signal is replayed to the system and resubmitting previously stored digitized biometrics signals bypassing it the data capturing. Examples include the presentation of an old copy of a fingerprint image or the presentation of a previously recorded audio signal. Noting that the finger print image presented by the attacker should be a full image before the feature extracted applied.

3.2.2 Countermeasures

To overcome such threat, several countermeasures can be taken:

a. A detection function, such as an encoding technique, can be applied to check the validity of transferred biometric data.
b. Challenge-response protocol shall be established between the capture device and the signal-processing component in order to detect a replay attack. A replay attack in biometrics is the resubmission of illegally intercepted data in order to fool the biometric system. An example of protecting biometric systems from a replay attack is the adoption of a challenge-response protocol in transmission, in which messages hold a freshness property by inserting a nonce, a timestamp or sequential numbers into the messages.

3.3 Threat 3 (T3): Threat to the signal-processing component

According to table 1, this threat is shared only by (local, download, attached, center, references management on TTP for local and references management on TTP for center). The analysis and countermeasures of this threat will be discussed below.

3.3.1 Analysis

It is also called a feature extractor. In this threat, the attacker could override the feature extraction process. The feature extractor is attacked using a Trojan horse, so that it produces feature sets preselected by the attacker.

3.3.2 Countermeasures

To reduce this threat, three facts have to be understood here:

a. If the attacker will change the extracted feature values, she/he should know in advance how vendor algorithm works.
b. Remapping the extracted feature is very complicated in finger print devices due to the fact that the information is not tied to specific geometrical relationships.
c. Algorithm vendors keep their algorithms to be secret code.

Also a practical solution is: the use of the buffer overflow. Any part of a trusted system that takes in information is generally buffering its received data. While the designer makes certain assumptions about the operation of a device, it may be possible to introduce data that would overflow the buffer. When the buffer overflow, the device is compromised and cannot be trusted.

3.4 **Threat 4** (T4): Threat to the process of transmitting the extracted biometric templates to the comparison component

According to table 1, this threat is only exist in the attached and references management on TTP for center models. The analysis and countermeasures of this threat will be discussed below.

3.4.1 Analysis

The features extracted from the input signal or data capturing are replaced with a different, fraudulent feature set (assuming the representation method is known). Often the two stages of feature extraction and comparison component are inseparable and this mode of attack is extremely difficult.

3.4.2 Countermeasures

To overcome this threat, three facts have to be understood here:

a. Biometric vendor algorithms have to be known in advance to apply such attack. Because the discriminating information in fingerprints is not tied to specific geometrical relationships, as it is in face-based systems (e.g., between eyes, nose, mouth, etc.). So, information cannot gather to form the original image.

b. If the attacker injected preselected feature extracted image, encryption mechanism (example watermarking) needed to prevent this attack.

c. Sequencing and timestamp will reduce this kind of attack.

3.5 **Threat 5** (T5): Threat to the comparison component

According to table 1, this threat is shared by all biometric network models (local, download, attached, center, references management on TTP for local and references management on TTP for center). The analysis and countermeasures of this threat will be discussed below.

3.5.1 Analysis

The comparison component also called the matcher. The comparison component is attacked and corrupted so that it produces preselected match scores. When the comparison component compares the templates user retrieved from the storage component and the data captured of the users template retrieved from the data capturing component, the comparison component shows the score result on the device screen. This means, the attacker can attack the biometric device and change the match score to preselected ones.

3.5.2 Countermeasures

The simplest way to stop attacks is to:

a. Have the matcher reside at a secure location (client side).
b. Match score encryption in the compassion component before transmission.
c. Improve the matching accuracy to help decreasing this attack.
d. Limit attempts prevent this attack effectively.
e. Use (Alder, 2003) proposal of an algorithm to immune the template encryption. Any system which allows access to match scores effectively allows sample images to be regenerated in this way. This work implies that biometric templates and biometric match scores be considered identifiable data − they should not be made available to untrusted parties.

Also considering the facts below:

a. If the attacker will change the extracted feature values; she/he should know in advance how vendor algorithm works.
b. Remapping the extracted feature is very complicated in finger print devices due to the fact that the information is not tied to specific geometrical relationships.
c. Algorithm vendors keep their algorithms to be secret code.

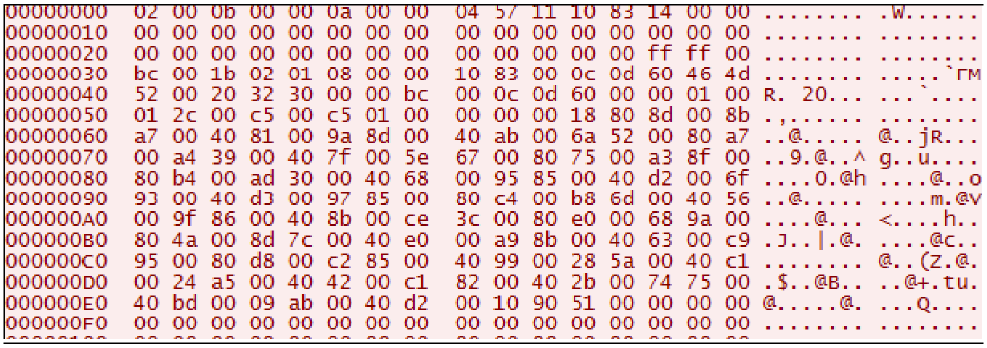
3.6 Threat 6 (T6): Threat to biometric storage component

According to table 1, this threat is shared only by (local, download and center). The analysis and countermeasures of this threat will be discussed below.

3.6.1 Analysis

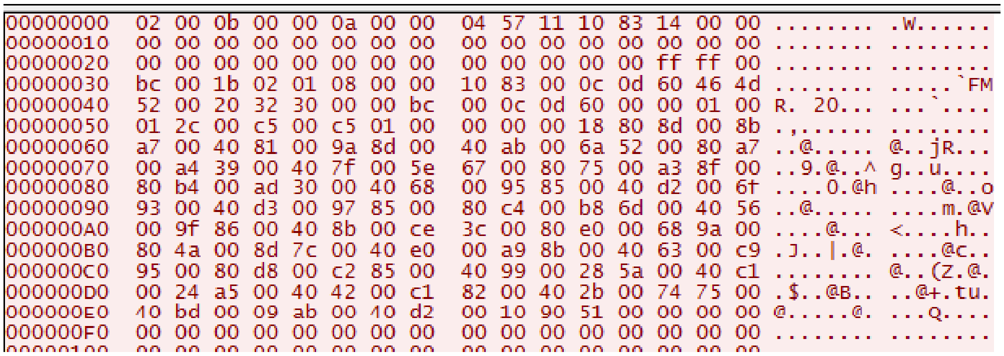
The storage component or the database of stored templates could be either local or remote. The data might be distributed over several servers. Here the attacker could try to modify one or more templates in the database, which could result either in authorizing a fraudulent individual or denying service to the persons associated with the corrupted template. A download model is implemented, the reference template from the server is sent to the client as the model design suggested. The download model uses one to one authentication process. Authentication process means that, the legitimate user enters her/his password into the finger print device, then, the finger print device will import the user's template from the server side "reference" based on the entered password. The Wire shark software is used to capture the data traveling in the UTP cable from the server to the client as Fig.4 shown. The captured data shows the image after the extracted feature applied. It is typically calculated using only a small portion of the original image. So these few hundred bytes in Fig.4 are much smaller than the original image.

In Fig.4, (a) and (b) are the same finger “index finger” where (c) is different finger “middle finger”. Analyzing the data captured, observing that the data are the same in (a) and (b) despite of the time difference captured taken where (c) is different representation other than (a) and (b). This means, the users extracted feature is not time stamped, or the saved templates in the storage component are not encrypted. For example, every time the legitimate user uses the finger print device for the same finger, the extracted feature representation is the same at all time.



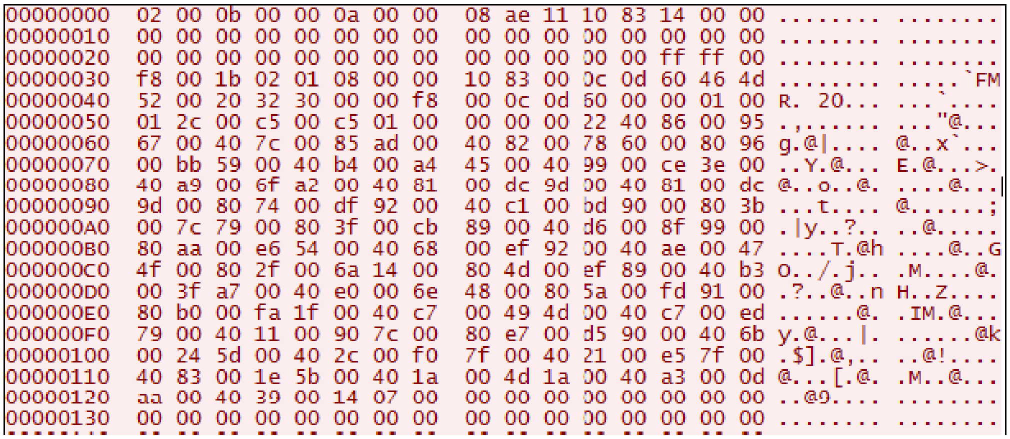
```
00000000  02 00 0b 00 00 0a 00 00  04 57 11 10 83 14 00 00 ........ .W......
00000010  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00 ........ ........
00000020  00 00 00 00 00 00 00 00  00 00 00 00 00 ff ff 00 ........ ........
00000030  bc 00 1b 02 01 08 00 00  10 83 00 0c 0d 60 46 4d ........ .....`FM
00000040  52 00 20 32 30 00 00 bc  00 0c 0d 60 00 00 01 00 R. 20... ...`....
00000050  01 2c 00 c5 00 c5 01 00  00 00 00 18 80 8d 00 8b .,...... ........
00000060  a7 00 40 81 00 9a 8d 00  40 ab 00 6a 52 00 80 a7 ..@..... @..jR...
00000070  00 a4 39 00 40 7f 00 5e  67 00 80 75 00 a3 8f 00 ..9.@..^ g..u....
00000080  80 b4 00 ad 30 00 40 68  00 95 85 00 40 d2 00 6f ....0.@h ....@..o
00000090  93 00 40 d3 00 97 85 00  80 c4 00 b8 6d 00 40 56 ..@..... ....m.@V
000000A0  00 9f 86 00 40 8b 00 ce  3c 00 80 e0 00 68 9a 00 ....@... <....h..
000000B0  80 4a 00 8d 7c 00 40 e0  00 a9 8b 00 40 63 00 c9 .J..|.@. ....@c..
000000C0  95 00 80 d8 00 c2 85 00  40 99 00 28 5a 00 40 c1 ........ @..(Z.@.
000000D0  00 24 a5 00 40 42 00 c1  82 00 40 2b 00 74 75 00 .$..@B.. ..@+.tu.
000000E0  40 bd 00 09 ab 00 40 d2  00 10 90 51 00 00 00 00 @.....@. ...Q....
000000F0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00 ........ ........
```

(a) Hex Representation of the data captured of the index finger (next to the thumb) at time 1



```
00000000  02 00 0b 00 00 0a 00 00  04 57 11 10 83 14 00 00 ........ .W......
00000010  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00 ........ ........
00000020  00 00 00 00 00 00 00 00  00 00 00 00 00 ff ff 00 ........ ........
00000030  bc 00 1b 02 01 08 00 00  10 83 00 0c 0d 60 46 4d ........ .....`FM
00000040  52 00 20 32 30 00 00 bc  00 0c 0d 60 00 00 01 00 R. 20... ...`....
00000050  01 2c 00 c5 00 c5 01 00  00 00 00 18 80 8d 00 8b .,...... ........
00000060  a7 00 40 81 00 9a 8d 00  40 ab 00 6a 52 00 80 a7 ..@..... @..jR...
00000070  00 a4 39 00 40 7f 00 5e  67 00 80 75 00 a3 8f 00 ..9.@..^ g..u....
00000080  80 b4 00 ad 30 00 40 68  00 95 85 00 40 d2 00 6f ....0.@h ....@..o
00000090  93 00 40 d3 00 97 85 00  80 c4 00 b8 6d 00 40 56 ..@..... ....m.@V
000000A0  00 9f 86 00 40 8b 00 ce  3c 00 80 e0 00 68 9a 00 ....@... <....h..
000000B0  80 4a 00 8d 7c 00 40 e0  00 a9 8b 00 40 63 00 c9 .J..|.@. ....@c..
000000C0  95 00 80 d8 00 c2 85 00  40 99 00 28 5a 00 40 c1 ........ @..(Z.@.
000000D0  00 24 a5 00 40 42 00 c1  82 00 40 2b 00 74 75 00 .$..@B.. ..@+.tu.
000000E0  40 bd 00 09 ab 00 40 d2  00 10 90 51 00 00 00 00 @.....@. ...Q....
000000F0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00 ........ ........
```

(b) Hex Representation of the data captured of the index finger (next to the thumb) at time 2



```
00000000  02 00 0b 00 00 0a 00 00  08 ae 11 10 83 14 00 00 ........ ........
00000010  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00 ........ ........
00000020  00 00 00 00 00 00 00 00  00 00 00 00 00 ff ff 00 ........ ........
00000030  f8 00 1b 02 01 08 00 00  10 83 00 0c 0d 60 46 4d ........ .....`FM
00000040  52 00 20 32 30 00 00 f8  00 0c 0d 60 00 00 01 00 R. 20... ...`....
00000050  01 2c 00 c5 00 c5 01 00  00 00 00 22 40 86 00 95 .,...... ..."@...
00000060  67 00 40 7c 00 85 ad 00  40 82 00 78 60 00 80 96 g.@|.... @..x`...
00000070  00 bb 59 00 40 b4 00 a4  45 00 40 99 00 ce 3e 00 ..Y.@... E.@...>.
00000080  40 a9 00 6f a2 00 40 81  00 dc 9d 00 40 81 00 dc @..o..@. ....@...
00000090  9d 00 80 74 00 df 92 00  40 c1 00 bd 90 00 80 3b ...t.... @......;
000000A0  00 7c 79 00 80 3f 00 cb  89 00 40 d6 00 8f 99 00 .|y..?.. ..@.....
000000B0  80 aa 00 e6 54 00 40 68  00 ef 92 00 40 ae 00 47 ....T.@h ....@..G
000000C0  4f 00 80 2f 00 6a 14 00  80 4d 00 ef 89 00 40 b3 O../.j.. .M....@.
000000D0  00 3f a7 00 40 e0 00 6e  48 00 80 5a 00 fd 91 00 .?..@..n H..Z....
000000E0  80 b0 00 fa 1f 00 40 c7  00 49 4d 00 40 c7 00 ed ......@. .IM.@...
000000F0  79 00 40 11 00 90 7c 00  80 e7 00 d5 90 00 40 6b y.@...|. ......@k
00000100  00 24 5d 00 40 2c 00 f0  7f 00 40 21 00 e5 7f 00 .$].@,.. ..@!....
00000110  40 83 00 1e 5b 00 40 1a  00 4d 1a 00 40 a3 00 0d @...[.@. .M..@...
00000120  aa 00 40 39 00 14 07 00  00 00 00 00 00 00 00 00 ..@9.... ........
00000130  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00 ........ ........
```

(c) Hex Representation of the data captured of the middle finger

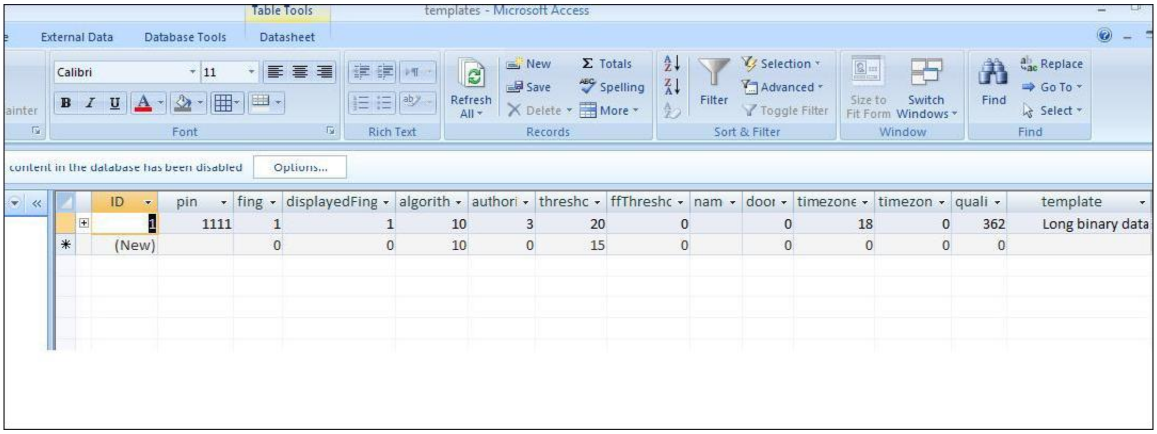
Fig.4. Data captured using Wire Shark

3.6.2 Countermeasures

The simplest way to stop attacks is to: 1-Have the database resides at a secure location (client side). 2-Instead of storing the original biometric signal in the system database during enrollment, the system could store only its noninvertible transformed version.

During recognition, the biometric sensor would transform the signal using the same noninvertible transform and perform matching in the transformed space.

Different applications can use different noninvertible transforms (or different parameters of the same transform), so a template would be usable only by the application that created it. In fact, the user herself/himself could provide the transforms parameters in terms of a password or PIN. If an attacker ever compromises such a biometric template, the system can issue a new one using a different transform or different parameters. 3-A simple and effective method of creating an easily revocable biometric template is to encrypt the biometric template with the users password. 4-An experiment example of finger print device data base is shown in Fig.5. The figure shows the template stored in the user account (in the server side) is non invertible (long binary data format) and template entry is not accessible.



content in the database has been disabled Options...

ID	pin	fing	displayedFing	algorith	authori	threshc	ffThreshc	nam	door	timezone	timezon	quali	template
1	1111	1	1	10	3	20	0		0	18	0	362	Long binary data
(New)		0	0	10	0	15	0		0	0	0	0	

Fig.5. Snap shot of data base showing template of user with ID1

3.7 Threat 7 (T7): Threat to the process of transferring biometric templates from the registration component to the storage component

According to table 1, this threat is only exist in the download and comparison outsourcing by server models. The analysis and countermeasures of this threat will be discussed below. The details of this threat look like T4.

3.7.1 Analysis

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 the comparison component are inseparable and this mode of attack is extremely difficult.

The Wire shark software is used to capture the data traveling in the UTP cable from the client to the server as Fig.4 shown. The captured data shows the image after the extracted feature applied. It is typically calculated using only a small portion of the original image. So these few hundred bytes in Fig.4 are much smaller than the original image.

3.7.2 Countermeasures

To overcome this threat, three facts have to be understood here:

1. Biometric vendor algorithms have to be known in advance to apply such attack. Because the discriminating information in fingerprints is not tied to specific geometrical relationships, as it is in face-based systems (e.g., between eyes, nose, mouth, etc). So, information cannot gather to form the original image.
2. If the attacker injected preselected feature extracted image, encryption mechanism (example watermarking) needed to prevent this attack "As Fig.4 showed that the data captured are not encrypted.
3. Sequencing and timestamp will reduce this kind of attack

3.8 **Threat 8** (T8): Threat to the process of transmitting the matching score from the comparison component

According to table 1, all biometric network models have no such threat. Consequently, no analysis and countermeasures for this threat will be discussed.

3.9 **Threat 9** (T9): Threat to the registration component

According to table 1, this threat is shared by all biometric network models (local, download, attached, center, comparison outsourcing by client and comparison outsourcing by server) except references management on TTP for local, references management on TTP for center and storage and comparison outsourcing models. The analysis and countermeasures of this threat will be discussed below.

3.9.1 Analysis

In recent biometric devices, registration component is the same as the signal processing component. So this threat is look like T3 except that the feature extracted is the first time to be extracted since this is the enrollment stage and to be sending to storage component. So, the registration component could be attacked using a Trojan horse, so that it produces feature sets preselected by the attacker.

3.9.2 Countermeasures

To reduce this threat, three facts have to be understood here:

a. If the attacker will change the extracted feature values, she/he should know in advance how vendor algorithm works.
b. Remapping the extracted feature is very complicated in finger print devices due to the fact that the information is not tied to specific geometrical relationships.
c. Algorithm vendors keep their algorithms to be secret code.

Also practical solution is: the use of the buffer overflow. Any part of a trusted system that takes in information is generally buffering its received data. While the designer makes certain assumptions about the operation of a device, it may be possible to introduce data that would overflow the buffer. When the buffer overflow, the device is compromised and cannot be trusted.

3.10 **Threat 10** (T10): Threat to the decision component

According to table 1, this threat is shared by all biometric network models (local, download, attached and center, references management on TTP for local and references management on TTP for center). The analysis and countermeasures of this threat will be discussed below.

3.10.1 Analysis

If the decision component can be overridden by an attacker, then authentication system has been disabled. Even if the actual pattern recognition framework has excellent performance characteristics, it has been rendered useless by the simple exercise of overriding the match result.

3.10.2 Countermeasures

The decision component needs to: Encrypt the decision before it is transmitted to the application. The biometric templates and biometric match scores are considered identifiable data they should not be made available to untrusted parties.

3.11 **Threat 11** (T11): Threat to the process of transmitting the stored biometric template to the comparison component

According to table 1, this threat is only exist in the download and attached biometric models. The analysis and countermeasures of this threat will be discussed below.

3.11.1 Analysis

An attacker could attack the channel between the stored templates and the comparison. The stored templates are sent to the comparison through a communication channel. The data traveling through this channel could be intercepted and modified

3.11.2 Countermeasures

The simplest way to stop attacks is to:

a. Have the matcher and the database reside at a secure location (client side).
b. Sequencing and timestamp will reduce this kind of attack.

To overcome this threat, two facts have to be understood here:

a. Biometric vendor algorithms have to be known in advance to apply such attack. Because the discriminating information in fingerprints is not tied to specific geometrical relationships, as it is in face-based systems (e.g., between eyes, nose, mouth, etc). So, information cannot gather to form the original image.
b. If the attacker injected preselected feature extracted image, encryption mechanism (example watermarking) needed to prevent this attack "As Fig.4 showed that the data captured are not encrypted.

3.12 **Threat 12** (T12): Threat to the process of transmitting the decision result to an application system

According to table 1, this threat is only exist in the local, download, references management on TTP for center and comparison outsourcing by server biometric models. The analysis and countermeasures of this threat will be discussed below.

3.12.1 Analysis

If the final match decision can be overridden by the attacker, then the authentication system has been disabled.

3.12.2 Countermeasures

The decision component needs to: Encrypt the decision before it is transmitted to the application. So, while the final answer is transmitting to the application it is encrypted and the application can only decrypt the decision and view it.

3.13 Summary of countermeasures

As the discussion and the analysis showed in the previous pages all of the twelve threats presented in the biometric technologies in open system networks and summarizing these solutions to be more effectively used in the future systems.

By type, the solutions can be defined as follows:

- S1: Solutions of mechanisms to be integrated with sensor (data capturing): temperature sensor, heart pulses measurement sensor and the use of challenge-response protocol.
- S2: Solutions of using challenge response protocol, encoding technology.
- S3: Solutions of knowing that remapping extracted feature is very complicated in finger print devices and the use of the buffer overflow.
- S4: Solutions of using encryption mechanism (for ex, watermarking, sequence and timestamp).

- S5: Solutions of residing comparison component in secure location (for ex, client side). Increasing the threshold “matching accuracy” and matching score should be encrypted.
- S6: Solutions of residing comparison component in secure location (for ex client side) and templates stored in data base should be in non-invertible format.
- S7: Solutions of using encryption mechanism (for ex, watermarking, sequence and timestamp).
- S8: No such threat.
- S9: Solutions of knowing that remapping extracted feature is very complicated in finger print devices and the use of the buffer overflow.
- S10: Solutions of encrypting the final decision.
- S11: Solutions of residing comparison component in secure location (for ex, client side) and encryption mechanism (for ex, watermarking, sequence and timestamp needed).
- S12: Solutions of encrypting the final decision in decision component before transmission in open system network.

d. Conclusion and Future work

The researchers’ findings are a compound of two related strategies. The First are a complete survey on eleven threats and their existing corresponding eleven solutions. The second part, which pertains to be threat 6 by proving the data, was not encrypted. The researchers have pointed out a number of specific solutions out of the solutions mentioned (section 3.13) which practically predicted to enrich future work, solutions are as follow:

1. Heart pulses measurement sensor to be integrated with data capturing devices.
2. The use of challenge response protocol to detect replay attack.
3. Encryption technique needed to be implemented in the comparison component “matching score” and the final decision.
4. The use of the hash technique for the templates resides in the database.

Based on the previous study, a proposal of a secure biometric network model will be suggested. The suggested biometric network model will overcome all the vulnerabilities and security threats discussed earlier. Also, at the physical and electronic levels of the device itself, some of countermeasures should be considered to achieve the highest degree of security.

References:

Alder, A. (2003). Sample images can be independently restored from face recognition templates. http://www.site.uottawa.ca/~alder/publications/2003/alder-2003-fr-templates.pdf

Derakhshani, R. Schuckers, S.A.C. Hornak, L.A and Gorman, L.O. (2003). Determination of vitality from a non-invasive biomedical measurement for use in fingerprint scanners. Pattern Recognition, Vol. 36, pp. 383-396.

Matsumoto T., Matsumoto, H., Yamada, K. and Hoshino, S., (2002). Impact of Artificial Gummy Fingers on Fingerprint Systems. Proc. SPIE, Optical Security and Counterfeit Deterrence Techniques IV, vol. 4677, Int'l Soc. for Optical Engineering, 2002, pp. 275–289.

Yongnyou S., Woochang S. (2009). A telebiomtric system mechanism model and biometric network protocol security of networked manufacturing, Seokyeong University, Seolol, Korea.