BIOMETRIC SYSTEMS SECURITY

Eduard Eusebiu EMANDII[1]
Claudiu ARAMĂ[2]
[1] Head Office, Information Technology Center, Naval Academy "Mircea cel Bătrân", Romania, eduard.emandii@anmb.ro
[2] Head Office, Romanian Air Force, Romania

Abstract: *Biometrics will play a major role in different industries, from medicine, science, robotics, defence and many areas of enterprise business. Promoting the use of biometrics for security today is a measure to minimize actions on identity theft. A phone number and address are enough to begin the process of identity theft. It is a predominant concern for many companies and individuals, particularly given the rapid growth in Internet use for business. Implementing a robust security technologies involves advanced authentication, and biometric systems fall into this category. They are used to recognize individuals and regulate access to information, services, physical spaces and many other rights and benefits. Although lately, there is an increase of their use, there are still questions about their usability, effectiveness, social impact and effects on privacy. Like any new technology, even if it offers extra security, it presents some issues by confronting with a series of vulnerabilities which can affect the implementation of an acceptable security level.*
Keywords: *key words: biometric, security, authentication*

General presentation

Biometrics is a continues emerging branch within information technology. Biometric technologies are automatic identification methods based on biological and behavioral characteristics of an individual. Biometric methods has advantages compared with conventional methods of identification. That is way biometric systems are an important element of information security systems.

Biometric features are divided into two main categories:

- Physiological: face, hand, fingerprint, iris, DNA;

- Behavioral: handwriting, signature, voice.

Figure 1: Examples of biometric features

Promoting the use of biometrics for security today is a measure to minimize actions on identity theft. A phone number and address are enough to begin the process of identity theft. It is a predominant concern for many companies and individuals, particularly given the rapid growth in Internet use for business. Victims of identity theft know how hard it is to prove that there are those who committed the crime. Authorities are working continually to this type of crime, and its randomness makes it difficult to prevent. A biometric system enhances the actions of prevention of identity theft because it is based on something that is specific to an individual. It is unique and very difficult to duplicate.

The implementation of a biometric system requires coordination between individual and organization or company to implement the technology. During the registration process, an individual provides a biometric sample: fingerprint, iris scan, voice, and so on. Samples are taken several times for higher accuracy and are stored in a database, token or smartcard as a digital representation, called template.

Vulnerability analysis is a systematic check of systems to determine the adequacy of security measures, to determine security weaknesses and to acquire data for prognosis effectiveness of the security measures proposed. Vulnerability assessment is the sequence of the following steps [1]:

- searching for potential vulnerabilities;
- development of tests of intrusion;
- intrusion tests;
- processing of results and reporting.

Step search of potential vulnerabilities has two phases, one of which is the search for

DOI: 10.21279/1454-864X-17-I1-066

weaknesses and the other is potential attacks assessment. Sources of information about potential vulnerabilities include journals, scientific articles, conference materials and expert opinions.

Vulnerabilities in biometric systems come mainly from the system structure, biometric features (fingerprints, iris, etc.) and management policy. Each of these areas has a set of special vulnerabilities and needs to be reviewed and to take action against them.

A primary source of vulnerabilities is represented by information about attacks against biometric systems. An approach based on logical structures of biometric systems is used to describe attacks. Each biometric system consists of four main modules:

Sensor Module

A sensor perceives an individual's biometric characteristic and make a digital description of it.

Extraction Module

Proof of entry is processed and generates a compressed image called template. The resulting template is stored in a database or smart card.

Comparison Module

This module compares the presented biometric sample template. In check mode, the processed image is compared with more templates and only one result is the final solution.

Decision module

This module accepts or rejects the user by matching score or security threshold.

Figure 2 is a biometric system and possible points of attack [2].

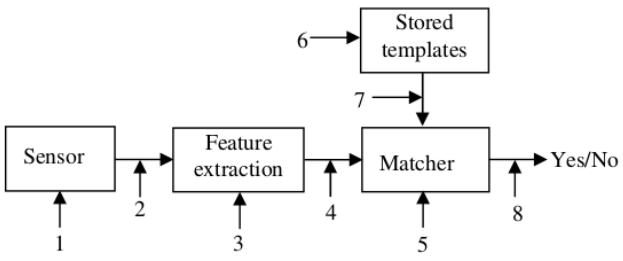

Figure 2: Attack points of a biometric system

According to the above scheme were identified 8 points of attack:

1. Presentation of a fake biometric sample to sensor: A fake biometric sample, such as a fake finger, a signature image, or a face mask is shown to the sensor to enter into the system.

2. Reinterpretation of the stored biometric digital signals: A stored signal is output in the system, ignoring sensor. For example, reversing an old copy of a fingerprint image or audio recorded.

3. Refusal of feature extraction: a set of features is introduced into the system by impostor using an attack of "Trojan horse".

4. Interception of characteristics biometric transmissions: features extracted from the input signal are replaced with a fake set of features.

5. Matching Module attacks: attacks on matching module has as result matching scores with false ones.

6. Patterns of "spoofing" in the database: Database templates can be saved local or remote. The attacker attempts to tamper with one or more biometric templates in the database, resulting in a false identity authorization or an authorized user will face a DoS attack type (Denial of Service).

7. Attacking on the communication channel between the database and template matching module: templates stored are transmitted over a communication channel to the matching module and an attacker can intercept and modify data transmitted.

8. Attacking the final decision process: If the final decision can be made or blocked by hacker then the function authentication system will be replaced.

Structure, architecture, production or implementation of a system can introduce a biometric system vulnerability. In some cases, a secondary system can be integrated into the biometric system, which eventually makes biometric system vulnerable. There are five points of vulnerabilities:

- OS
- management system database
- biometric software
- software for sensor
- hardware and drivers

Other main issues can be categorized as follows:

- operations management
- management parameters

DOI: 10.21279/1454-864X-17-I1-066

- system configuration

There are several classification schemes vulnerability [2], suggesting a generalized list of vulnerabilities of the biometric systems:

- **Administration:** systems management mistakes, intentional or unintentional;
- **User:** an ordinary user wants to obtain administrative privileges for its account;
- **Register:** breaking registration procedures;
- **Spoofing:** using a false biometric template that is used to authenticate legitimate user;
- **Mimica:** attacker mimics a legitimate user biometric characteristics;
- **Undetected:** undetected attacks by system can encourage new attacks;
- **Application security failure:** as a result has a faulty utilisation of biometric system conditions or IT environment;
- **Power supply:** power failures may affect ongoing biometric systems;
- **Bypass system:** bypassing biometric access systems. This can be achieved by overcoming physical barriers, forcing a legitimate user to submit his biometric features for authentication or cooperation with it;
- **Attack by system failure:** weakening the system by making changes in the IT environment or biometric system, for example, modification or replacement of system parameters;
- **Degradation:** certain applications in the IT environment can favor lowering system security;
- **Counterfeiting:** a firmware modification system hardware;
- **Waste:** latent fingerprints can be used to make artificial fingerprints or can be accepted directly by the sensor;
- **Attack Cryptology:** encrypted transmittion can be decrypted and the intercepted biometric data can be used for another type of attack;
- **Attack of "brute force":** the attacker present biometric characteristics repeatedly in order to be authenticated. This type of attack depends on parameter FAR (False Accept Rate);
- **Type attack - "Evil Twin":** false biometric feature is very similar to the legitimate one;
- **False template:** the introduction of a false biometric template into database or smart-cards;
- **Noise:** access to the system can be constructed by the attacker using a "noise" on the biometric system;
- **Poor image quality:** quality supervision can be used. If poor-quality images are accepted for registration, then the attacker may be misleading the system with images with noise;
- **Weak ID:** similar to the previous vulnerability, the attacker tries to trick biometric systems using weak templates;
- **FAR / FRR:** attackers use FAR / FRR values to deceive system;
- **Blocking System (Denial-of-Service):** aims to prevent a user to obtain a legitimate service.

Consequently, there are several points of attack and vulnerabilities in biometric systems. A biometric system may not have all vulnerabilities or attack points. The list presented is quite general and can be easily applied to any system. For a specific system, it is essential to consider the properties of the system in order to identify vulnerabilities.

The aim of the vulnerability analysis is to determine the possibility of using weaknesses of biometric systems in an application environment. Tests penetration are conducted to determine vulnerability in the application of an imposter with some potential attack. The level of potential attack can be low, medium or high.

There are three categories of threat for biometric systems [3]:

The impostor: A person claiming to be authorized, intentionally or unintentionally

Attacker: Any individual or any system that attempts to compromise the functioning of the biometric system. The reason could be unauthorized access or denial of service.

Authorized users: authorized users of the system biometric unintentionally compromising the biometric device or system. This category corresponds to unintentional human error, eg system configuration management mistakes.

It is important to develop and perform penetration tests for each attack using specific vulnerabilities. There is therefore a matter of the appropriate test methodology for determining the resistance of biometric systems by considering measures against certain attacks.

Direct attacks on systems based on fingerprint recognition

Fingerprints verification systems are currently the most widespread biometric products on the market [4] due to their high acceptability among users and the easily use in forensic environments but also because it can be easily incorporated into many devices electronics such as PDAs, mobile phones, keyboards, etc. This rise a great interest in the scientific community to study the robustness of such systems to direct attacks.

DOI: 10.21279/1454-864X-17-I1-066

There have been various studies reported in the literature on vulnerability analysis of fingerprint biometric systems to direct attacks. In the book "Biometrical Fingerprint Recognition Don't Get Your Fingers Burned " by Van der Putte and T. Keuning, J. authors classified the different ways to create gummy fingers in two main ways: with and without the cooperation of the legitimate user. In the same book he describes two methods (one from each class) and results are reported on six sensors trading. Of the six sensors tested five of them accepted as genuine imitation on the first attempt while the remaining sensor permitted to access the system on his second attempt.

Matsumoto and colleagues [6] conducted experiments similar to those reported by the authors listed in the previous paragraph, but this time with fake fingerprints made of gelatin. Again, they made a distinction between where the owner had cooperation fingerprint and the situation when they had to be lifted from a surface. In the case when the user has cooperated to make false fingerprints, recognition rates reported for all 11 systems tested were between 68 and 100%. In the case when the user did not cooperated, the generated imitations acceptance rate was always above 60%.

More recently, in [7], the authors tested two systems check fingerprints, one based on minutiae and the other based on the pattern of crest on a database of over 500 real samples and as many false images captured two different optical sensors (optical and thermal). False fingers were made from silicone and were considered three scenarios, namely:

i) enrollment and test with real fingerprints;

ii) enrollment and test with fake fingerprints;

iii) enrollment with real fingerprints and test with the fake ones.

Both systems showed a considerable decrease in their level of performance when they were attacked (third scenario considered).

Indirect attacks on systems based on fingerprint recognition

Although Hill [8] reported an attack on a database of a biometric system (vulnerabilities no. 6 of Fig. 1), most of the works on indirect attacks use some type called the technique "hill climbing "[9]. The technique is tested in a simple image recognition system, based on the correlation. This attack uses Matcher score given by iterative change to a synthetic template created until the score exceeds a fixed threshold decision and grants access to the system. Thus, even if we create an image file summary or we directly generate vector synthesis, these attacks can be categorized into type 2 or 4.

When the technique "hill climbing" is directed to the entrance of the feature extractor attack (type 2) is not necessary any information about the storage format template. Only required size and file format introduced the feature extractor. Adler proposed in [13], an attack type 2, a face recognition system. The input image is conveniently modified by a score of match you want to achieve. Adler reports the results on three commercial recognition systems and show that after 4000 iterations is attained a score that corresponds to a very high confidence (99.9%) of matching scores for all systems tested.

In [10] Uludag and Jain have introduced the art such as "hill climbing" to attack a fingerprint verification system that was studied further in [11]. In these attacks a randomly synthetic template is presented at the entry of "matcher" module (attack type 4) of the biometric system and, depending on the overall score, it is changed iteratively until the system returns a positive verification. Minutiae template are changed one by one, and the change is stored only if the score returned by the module "matcher" is better than the previous one, otherwise it is ignored. Thus, to perform this type of attack we need:

i) resolution and size of images captured by the sensor (which is usually a parameter specified by the seller);

ii) the format template;

iii) access to input matcher (to present synthetic templates) and output (to get the necessary feedback from scores).

In this case, we know how information is stored, but we do not know the information.

In [12] Cappelli and his collaborators describe a fast and reliable method to generate realistic images with synthetic fingerprints, that are implemented in software Sfinge (Fingerprint Generator synthesis). With this application, an attack type 4 (entry in "matcher") using generated synthetic templates could be easily converted to an attack type 2 (entry into module "feature extraction") using corresponding synthetic fingerprint images. Thus, the attack would be simplified and the intruder would not need to know the storage format used in the system. Also, an algorithm to reconstruct the fingerprint image of the real minutiae template based on ISO has recently been proposed in [13]. In this case, if the template of a legitimate user is compromised, it could be used to perform an attack type 2 against the system (rebuilding the image of the real fingerprint), or even a direct attack (building a fingerprint 3D-based image).

Direct attacks on systems based on iris recognition

While scanning the iris leaves room for improvement (iris scan at medium distances is still a problem), iris is one of the strongest emerging market biometric traits due to high precision algorithms used in its recognition. Verification

DOI: 10.21279/1454-864X-17-I1-066

systems based on iris showed outstanding performance in normal operating conditions, however, several studies have pointed to their vulnerabilities at very simple direct attacks carried with photos of the user's iris.

One of the first efforts in the study of the iris verification systems vulnerabilities was conducted and presented by Thalheim and Krissler [14]. In this paper an iris image of a legitimate user was printed with an inkjet printer with high resolution to fraudulently access the system. The experiment was successful only if the eye was cut from the image and faced on the impostor face to give the impression of a real eye. Only one commercial system (Panasonic BM-ET100's authenticator) has been tested in the experiment showing high vulnerability of this type of attack. Not only allowed with fake iris, but also allowed the attacker to connect to the system using iris image.

In [6] Matsumoto conducted the first experiment systematic falsification of the iris. They tested three different verification iris, two portable: IrisPass-h conducted by Oki, and Authenticator BM-ET100US made by Panasonic, and the third was a system for monitoring a gate (IrisPass-WG conducted by OKI). Two different devices were used in experiments to obtain fake iris images, the built-in IrisPass-h system and a digital microscope with infrared illumination. The images were printed using an inkjet printers, the high resolution eye has been removed from the image in order to place the eye behind the false iris of the impostor. When using images taken with the camera IrisPass, all three fake iris systems accepted as real, with a probability of 50%. In case of digital microscope image obtained with the success rate of attacks was over 15% for portable systems, and around 5% for application control gate.

Biometric systems based on facial recognition

A facial recognition system is built using high-end hardware and software able to verify or identify a person from a digital image automatically. The process of identification is done by comparing facial features. It can be used as a security measure for ATMs. Facial recognition system may be compromised by intercepting communication and change the template used for comparison with the inserted image.

This attack can be prevented by limiting the number of attempts and configuration of this result with only yes / no options.

Biometric recognition systems based on hand

Hand vein image is captured by a special type of sensor. Palm scanning process involves using its infrared illumination. Hemoglobin in the blood absorbs infrared rays which results in the generation of a model with veins subject. Possible issues related to this type of authentication is to ineffective communication between the subject and the biometric system, thus compromising system template and can be attacked.

Possible attacks are eavesdropping, replay and transmission. These attacks can be prevented by using a multimodal biometric system or by combining a biometric password system and watermarking. Cryptography is one of the best feasible solution, we would ensure better protection against replay type attacks and attacks on the database.

Biometric systems based on voice recognition

Voice recognition is the process whereby words, sounds or phrases spoken by humans are converted into electrical signals and these signals are then exchanged into coded templates that are assigned a specific meaning and the person is authenticated. A person's voice can be easily recorded and used on a PC. Biometric systems based on voice recognition has low accuracy, if we take into account a disease such as a cold voice that can change an individual voice, making identification absolutely difficult. Although this method has some advantages for different areas have been identified security threats associated with it. The threat type "hill climbing" is a threat that is played back repeatedly and biometrics with small differences that result in obtaining an improved score helped them to obtain system access. This attack can be prevented by limiting the number of tests and checks using yes / no. Victrio is one of the most popular technologies used in voice detection and correction.

Biometric systems based on signature recognition

The signature verification biometrics and behavioral attribute is used to authenticate a person. A signature verification system generally consists of different parts, such as data acquisition, pre-processing, feature extraction and verification. The issue of security is recognizing the signature attack of "hill climbing" in the submission repeatedly of biometric data with small differences and that affords an improved score and thus ensuring system security can be compromised. This attack can be prevented by limiting the number of attempts and encryption templates.

Methods to improve detection

Implementation of interactive detection (liveness detection) in biometric systems is a preventive measure against attacks of "spoofing". Methods such as "liveness detection" were designed and implemented in some biometric systems, these being represented by hardware devices that have the ability to scan across the surface of the skin and can make the difference between living tissue and a 3D model in a second.

DOI: 10.21279/1454-864X-17-I1-066

The table below contains the interactive detection techniques which may be used as a countermeasure to the detection of various attacks [15]:

Biometric sensor	Presenting attack	Interactive detection technique (liveness detection)	Remarks
Scanning fingerprints	2D images, the finger of a dead person, artificial finger	Passive: -Measuring pulse; -Temperature measurement; -Detection of perspiration; -Detection of skin resistance *. Active: - Demand scanning multiple fingers in random order.	* Depends on the consistency of artificial finger
Scanning veins	2D images, the finger of a dead person, artificial finger	Passive: -Measuring pulse; -Temperature measurement; -Detection of perspiration; -Detection of skin resistance *.	
		Active: - Demand scanning multiple fingers in random order.	
Facial scan	2D, 3D masks, video attack	Passive: - Natural blinking eye *; -Natural movement of muscles during speech; Active: - Requests for closure of the eyes, use voice applications or requests for the return of the head **;	* It does not have a very high accuracy for 3D masks ** Has no effect on video attack
Scanning fingerprints, veins and facial scan	2D, 3D masks, body parts, artificial fingers and hands or digital fate	Passive: - Infrared and ultraviolet light, thermal scanning, medical equipment, ex. EKG, heart rate reading apparatus or the blood pressure	

Conclusion

Since the use of biometric authentication has increased in recent years, the number and complexity of attacks has increased dramatically. This includes in particular attacks presentation. However, threats from these attacks can be reduced by using interactive detection techniques (liveness detection).

As shown in this paper, there are many different methods and techniques of working against current attack scenarios which have effectiveness. Here it should be noted that none of these techniques do not provide full protection of the biometric systems. Among the most effective attacks are the video type. As a consequence, it is recommended a combination of different techniques of attack detection and protection against manipulation of biometric systems to increase overall security.

DOI: 10.21279/1454-864X-17-I1-066

Bibliography

[1] https://danishbiometrics.files.wordpress.com/2009/08/1-13.pdf
[2] Dimitriadis C., Polemi D., Application of multi-criteria analysis for the creation of a risk
[3] Roberts C., Biometric attack vectors and defenses, Computers and Security, vol. 26, no. 1, pp. 14–25, 2007.
[4] IBG: Biometrics market and industry report 2007-2012. Technical report, IBG (2006)
[5] Van der Putte, T., Keuning, J.: Biometrical Fingerprint recognition don't get your fingers burned. In: IFIP. (2000) 289-303
[6] Matsumoto, T., Matsumoto, H., Yamada, K., Hoshino, S.: Impact of artificial gummy fingers on fingerprint systems. In: Proc. SPIE, Optical Security and Coun-terfeit Deterrence Techniques IV. Volume 4677. (2002) 275-289
[7] Galbally, J., Fierrez, J., Rodriguez-Gonzalez, J.D., Alonso-Fernandez, F., Ortega- Garcia, J., Tapiador, M.: On the vulnerability of fingerprint verification systems to fake fingerprint attacks. In: Proc. of IEEE International Carnahan Conference on Security Technology. Volume 1. (2006) 130-136
[8] Hill, C.J.: Risk of masquerade arising from the storage of Biometrics, B.S. Thesis. Department of Computer Science, Autralian National University (2001)
[9] Soutar, C.: http://www.bioscrypt.com/assets/security soutar.pdf. biometric system security. (2002)
[10] Uludag, U., Jain, A.K.: Attacks on biometric systems: a case study in fingerprints. In: Proc. SPIE. Volume 5306. (2004) 622-633
[11] Martinez-Diaz, M., Fierrez, J., Alonso-Fernandez, F., Ortega-Garcia, J., Siguenza, J.A.: Hill-climbing and brute force attacks on biometric systems: a case study in match-on-card fingerprint verification. In: Proc. IEEE of International Carnahan Conference on Security Technology. (2006) 151-159
[12] Maltoni, D., Maio, D., Jain, A.K., Prabhakar, S.: Handbook of Fingerprint Recognition. Springer (2003)
[13] Cappelli, R., Lumini, A., Maio, D., Maltoni, D.: Can fingerprints be reconstructed from ISO templates? In: Proc. International Conference on Control, Automation, Robotics and Vision. (2006) 191–196
[14] Thalheim, L., Krissler, J.: Body check: biometric access protection devices and their programs put to the test. c´t magazine (2002)
[15] http://subs.emis.de/LNI/Proceedings/Proceedings245/311.pdf

DOI: 10.21279/1454-864X-17-I1-066