International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2014): 5.611

Biometrics: Security Issues and Countermeasures

Irfan Iqbal

College of Science and Arts, Oqlat as Saqour, Al-Qassim University, Saudi Arabia

Abstract: ***One of the fundamental aspects for the protection of information systems is authentication. Authentication involves confirming the identity of a person or any entity that could be a hardware or software program. One way of authentication is biometric technology. Biometric recognition offers a reliable solution to the problem of user authentication. Biometric systems are widely deployed in various applications, so there is a lot of concern regarding to their privacy any security technology. Biometric technology will publicly be accepted when these systems have low error rates, temper proof and are robust. In this paper, we have analyzed various possible attacks associated to biometric technology. Later we have specified the details of dealing with these kinds of attacks, e.g. spoofing attacks. Moreover, biometric live-ness approaches are discussed to deal with security threats.***

Keywords: Biometrics security, Biometrics Issues, Biometrics authentication, Biometric systems. Biometric countermeasures

1. Introduction

Before discussing security and biometrics there is a need for the definition of biometric, "any measurable aspect of a human's physiology that can be reliably captured and used as a distinguishing identifier for that person within a defined population" [1]. There are several types of biometrics used in daily life such as retina/iris, fingerprints, facial recognition, hand veins pattern and voice etc. These types are further divided into two categories i.e. Psychological and Behavioral biometrics [2].

Psychological biometrics is based on the physical parts of the human body like fingerprint, iris, face and hand scan, where behavioral biometrics is based on the measurements and data derived from an action performed by a user like gesture, signature, gait and key stroking [2].

Why there is a variety of biometrics? The reason for that is no biometric is best in all environments for all users. For authentication of the users biometrics can be a good choice. The three ways for authenticating a person is: [1]

- Something you know (e.g. password or PIN code)
- Something you have (e.g. smartcard or token)
- Something you are (e.g. biometrics)

Biometrics is the way used to secure one's identity so that it can't be easily spoofed. For the authentication of one's identity; PIN codes or passwords were used previously. By entering your username and password or PIN you provide your identity. There are many problems related to them, one is that they can be shard and easily intercepted. Physical token or memorized information is not required in biometric authentication. The user is typically authenticated by providing identity (normally a username) and a biometric scan. If the provided scan matches to the stored template then user is authenticated.

Biometric scan identification is carried out to the defined population of users which enrolled there biometric sample in the system.

2. Previous Work

Fake fingers or stolen fingerprints report is early published in 1988 by Network Computing [3]. They perform several experiments on devices and come to know that four devices out of six were subject to forged finger attack.

Additional research was done by Tsutomu Matsumoto in there paper "Impact of artificial gummy fingers on fingerprint systems" in 2002. In research they made "finger sleeves" from "Gelatine", designed it in this way that it covers a fingertip with a fingerprint on the surface. When the test is performed, those fingers have high recognition rate when used on capacitive or optical sensors. Further, those fake fingers would be enrolled with (68-100%) acceptable rate in the system [14].

In 2002, C'T magazine published variety of test results of biometric devices. Vast amount of spoofing attacks were performed and being successful. The categories of biometric devices were facial recognition, fingerprint scanner and iris scanner. Biometric devices were spoofed by playing the video of a person's face. A high resolution iris photograph was placed on the person's face to pretend to be the real one [4].

In 2003, two Germans hackers developed technique by using "latent prints on the scanner" and convert them to "latex fingerprint replacement" [5]. Graphite and tape powder was used to pick up latent prints which were photographed digitally; afterwards graphic software was used to improve the fingerprint image as entire fingerprints were not obtained. Afterwards image was "photo-etched" to 3-Dimentional and used as fake fingerprint.

In 2005, it was exposed in laboratory by demonstrating 90% false rate verification of biometrics devices. Testing was done by using "fake plastic fingers, gelatine, cadavers and modeling compounds". When "liveness" was integrated to the devices the false verification rate cut down to 10% of the spoofed samples [6].

3. Biometric Types

For the verification of individual's identity there are number/forms of biometric devices. Each device has its own strength or weakness according to it functionality. Range from commonplace (fingerprint) to esoteric ("gait analysis") [1]. No biometric device can satisfy the multifunctional requirements as some are for the use of office environment and some are for the use of high security premises.

3.1 Fingerprint

It is the most known type of biometric in human body. Fingerprint devices are capable of taking image of full hand, multiple fingers image or only single finger image.

3.2 Iris Scan

Mostly, iris scanning is puzzled with retinal scan. "The iris is the visible colored part of the eye that surrounds the pupil, and is believed to be unique for each human" [1]. Mostly, iris scanners consist of a digital camera that are used to take picture of an eye by using infrared light, this helps the scanner to take the picture of iris even with contact lenses and eye glasses.

3.3 Retina Scan

"The retina is an area at the rear of the eyeball" [1], for the scanning of retina a specialized scanner is used which scan the eye to very close range. Retina scan is accurate but used seldom due to privacy and other usability issues. It also produces anxiety in several users because the person has to place their eye very close to camera lens.

3.4 Vein Pattern

Veins pattern in hand is thought to be unique. Infrared light is used in the scanner to detect the vein pattern.

3.5 Voice Analysis

Analysis of speaker's voice is the main theme of the voice biometric. As voice biometrics is not very much accurate so it is combined with the preregistered information of the speaker in the system. "For example, a user is requested to "Say your favorite food..." and both their voice and the answer given are used to validate their identity" [1].

3.6 Face

A face biometric system analysis the picture of a face. Picture can be taken from a standard digital camera. It can also be used to capture the stream of pictures (video) and identify the face as a single captured image.

4. Weakness in Biometric Recognition Model

A general biometric system is based on pattern recognition system. The steps of the pattern recognition system are shown in figure 1. More detail and introduction to automated biometrics can be found in [8].

Any generic biometric system compromise of four stages, A to D as shown in fig. In this model we describe nine essential threats that pestilence generic biometric authentication systems. Also Schneier in [9] explains many other types of biometric exploitations.

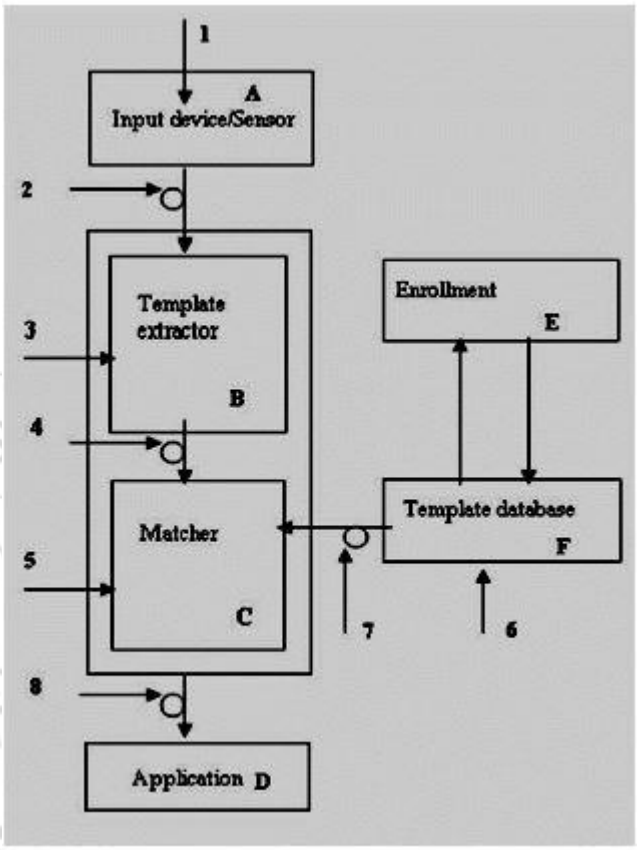

Figure 1: Biometric recognition model

1. In figure 1, a major threat is done by presenting fake biometric to the input sensor. Tempering can be made to the sensor by implementing a replay attack. It can be done by providing a previously submitted biometric data again to the authenticator. The sample of the biometric can be retrieved by a sniffer device or by using sniffer software during process of successful authentication. Sample collection can also be done by collecting a remaining biometric feature left on the sensor after successful authentication. In first situation the sniffed signals are re-provided to the authenticator by circumventing the biometric sensor. In second situation an image is re-submitted to the biometric sensor as previously submitted by a legitimate user.

   For the detection of replay attack, authenticator device makes sure that information is captured from the biometric sensor and not been injected. Due to input deviation and noise in sensor make it difficult for two samples to be hundred percent similar. By using specific products replay attacks can be recognized. Challenge and response mechanism or building timestamp [11] are methods to address replay attacks.

2. By attacking on the channel between the biometric system

and the sensor is a second type of attack. It can also be a type of a replay attack by submitting pre-collected information as mentioned in attack 1 as electronic impression or digital stored biometric signals. When the data is transmitted from one component to another man-in-middle attack can be possible by influencing the input data stream or by injecting an artificial biometric matching pattern.

A number of techniques can be put in practice for the reduction of threats lies in transmission based attacks. Encryption technique can be a vital strategy to send information of captured biometric data through a secure channel. Instead of using a simple authentication process to the security system, provide a complex reply from biometric authenticator. All those biometric components which can actively participate from start to end must be within one device so that no one can tamper or modify.

3. Attack by Trojan horse [11] is categorized to threat 3. "The feature extractor could be attacked so that it will produce a pre-selected feature set at some given time or under some specific condition"[11]. When the expression have been mined from the input signal then after; replaced with different manufacturer expression set.

4. Threat 4 is categorized to the communication channel linking the feature extractor and matcher. When details are sending out to a remote matcher, example is the case of using smart cards as in [10] for storing the template. In this scenario threat is very real.

5. Threat 5 as in figure 1 is again a Trojan horse attack.

6. Enrolled templates are stored in database which is available remotely, locally or been distributed database. Threat is the modification of the templates in the database F and authorization of the attacker becomes possible or due to ruined template denial of service is possible to the person. (Representation is assumed to be known)

7. Threat 7 is categorized to another channel attack. Through a channel, templates are sent from database F to matcher, while in the way attack is possible by changing the templates before they reach to the matcher.

8. Very vital threat (8) is "overriding of the output of the matching module" [11]. The result of the matching unit is either a hard match or no match. Here the probability is that the final decision could be dependent on the application. Threat is same for hard match and no match decision.

9. Finally the security threat mostly neglected is based in enrollment process E as in Fig. 1. By getting unauthorized access to an enrollment device makes that possible for any of the above threats but the most which cause major damage is the unauthorized changing in template database F (Threat 6). E.g. if collusion occurs in between supervisor of the enrollment center and the intruder then a newly formed identity is easy to enroll and consequences could be severe. These types of threats are very real in manual authentication systems. More security is required in enrollment process rather than authentication and should carry out under trusted and competent supervision [11].

5. Biometric and Spoofing

As previously mentioned, if an attacker revealed the template structure he/she can provide fake artifact to the biometric device that can bypass the matching unit or algorithm. It is very common thinking of the general group of the people that stealing and duplication of the biometrics is very difficult as compared with password or pin but certain demonstrations show its is not that difficult[17],[14]. Spoofing consists of two stages: "first, capturing the biometric sample belonging to the enrolled user and second one is creating a copy of the captured sample by means of an artifact" [12].

5.1 Fingerprint Capture

It's difficult to get fingerprints of the enrolled users to spoof a fingerprint system. The attacker needs legitimate user finger print either with there will or lift dormant print without their will. It's quite easy if it is done even without the will of user. Fig 2, demonstrates that how to obtain fingerprints without owner's cooperation and biometrics are not secret.

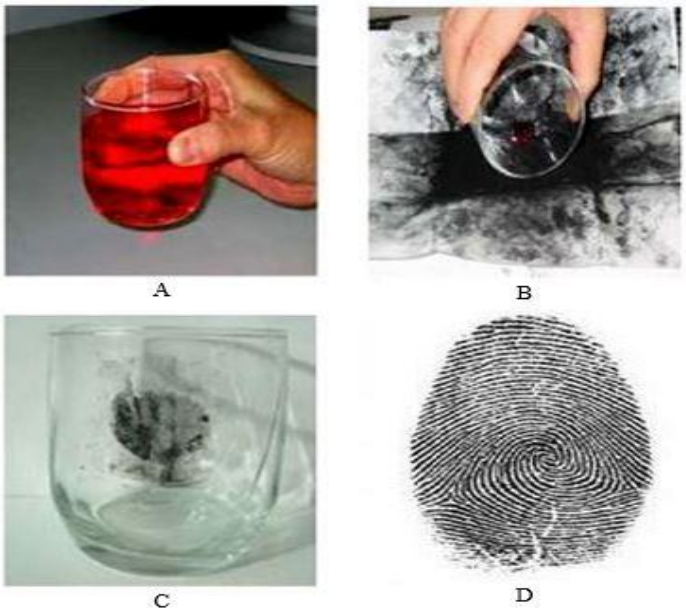

Figure 2: Fingerprint capture

A fingerprint sample which are left on surface, can be picked from hard smooth surface like glass, metal or CD etc. A traditional capture technique is shown in Fig 2, by the use of powder that sticks to the moisture in the fingerprint. A waste toner powder is used to capture the fingerprint as shown in the fig 2, instead of using expensive powders.

When an attacker meets its target in social situation, it's quite easy to steal a glass at that time as shown in Fig. 2(A). After getting glass, gently dust the glass with a paintbrush or by rolling the glass gently on the powder as shown in Fig. 2(B) and by doing this, fingerprint is captured on the glass as in Fig. 2(C). The image is obtained by using a digital camera

and transferred to a computer and edited or enhanced with image software tools as in Fig. 2(D). Normally the fingerprint quality depends on the surface's smoothness e.g. being free from contaminants, nature of object touched, conditions at specific time that the object was touched e.g. dryness [12].

5.2 Spoofing Fingerprints

Tsutomu Matsumoto, a Japanese professor, has successfully fooled several fingerprint sensors using fake fingers [14]. Matsumoto used gelatin and molding plastic to make "gummy fingers" with the collaboration of genuine users as in Fig 3 (a), (b).

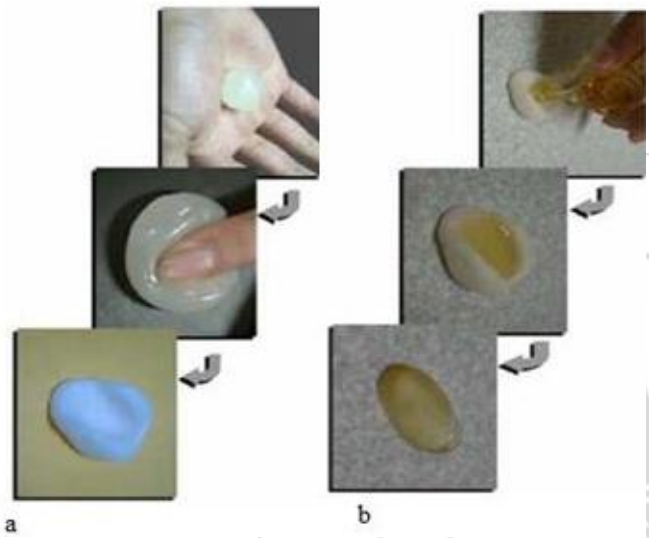

Figure 3: Gummy fingers

By using these fake fingers commercially available fingerprinting readers are fooled with average hit rate of 80%, both for optical and silicon finger readers. This type of attack is successful when cooperated by genuine user, though it's not considered a major security threat to fingerprint sensors. Matsumoto demonstrated another technique which is more hostile as it works on fingerprints which are left by a person on plain surfaces, doors handles or glass. The covert fingerprint is improved by using cyanoacrylate adhesive (super-glue fumes). With the help of digital camera the improved fingerprint image is taken, ridges and valleys are further enhanced in Adobe Photoshop software. The enhanced image of fingerprint is printed onto a transparency. Next step is to transfer the image to the photosensitive printed circuit board from transparency.

A 3-D mould of fingerprint is created by exposing the board to ultraviolet (UV) light. The ratio to fool biometric readers is 80% when using these fake fingers [14].

5.3 Spoofing the Face

As compared with other biometric technologies, facial recognition has significant advantages over them because facial recognition does not require user cooperation. In face recognition, a sample can be taken without the victim's awareness so it's a disadvantage of this technique. Surveillance cameras at shopping centers, banks or in streets usually photograph faces but it's very hard to know that camera is biometrically enabled or not. When the image is taken it is then converted to "2D face photograph or 3D mask" [12], dependent on the authentication algorithm by using certain type of image tools to deceive face recognition systems. Some facial recognition algorithms work by detecting eye blinking to distinguish live or fake face from a picture or painting [18]. But this technique can also be dogged by using a facemask with eyes cutout in that.

5.4 Spoofing the Voice

Voice based authentication can be classified into two groups rather test-dependent or text-independent. "In a text-dependent application, a user needs to speak a fixed phrase, a password, or some words from a vocabulary set. This method is more or less like two-factor authentication, which adds an extra Layer of security to the system. On the contrary, the text-independent method allows the user to choose any phrase or words for authentication, which offers more user convenience at the cost of system security" [12].

An attacker by doing social engineering can easily capture voiceprint of victim. E.g. someone calls you and told that your telephone was experiencing some problems. That person asks you to read some words, numbers or phrases in order to test those problems. You were informed and thanked by that person that testing had been completed. A successful capture of voice print had been completed instead of testing your telephone [12].

6. Anti Spoofing

There are several techniques to overcome spoofing vulnerability which have been recently projected and tested both for software and hardware for biometric systems.

6.1 Liveness Detection

"Liveness Detection" is one method for anti-spoofing. The intention of this technique is to detect a biometric sample whether it is provided by a live human or it's a copy which came from work of art (Fake). This liveness can be attained by detecting physical properties of the live biometric "e.g. electrical measurement, thermal measurement, moisture, reflection or absorbance of light or other radiation" [12]. Some examples are as following [12].

6.2 Temperature

Specifically for fingerprint spoofing, several vendors developed temperature sensing in there biometric devices to anticipate that those devices will be able to distinguish a dummy finger to a real one [13]. Though in room environment epidermis temperature is about 26 to 30C. The temperature reduces a maximum of 2C when a silicone artificial fingerprint is used so this still deceive the biometric sensors [15]. If temperature drops to the lower boundary, by putting warm water bag or blowing warm air on it will increase it temperature to body temperature. Besides, if user is suffering from cold fingers because of reduced blood circulation or user is arriving from out of cold.

6.3 Heartbeat

When user touches the biometric sensor it is recommended that sensor could recognize the live finger by sensing pulse of heart beat. This technique is used by introducing some extra hardware which can compute pulse or blood flow in finger tip [17]. But in this scenario a number of problems are connected. Hear beat cannot be assumed to be a reliable characteristic in biometric because it varies person to person and can be influence by different factors. Another technique to spoof the biometric sensor is by pumping saltwater through the pipe which is put into the fake finger replicating the blood flow.

6.4 Skin Resistance

"Because human skin has a layered structure and the layers have different electrical conductivities, conductivity has been suggested as a feature to recognize fake fingers" [12]. But some tests show that live and gummy fingers resistance is very close [14]. Under unlike temperature and moisture environments skin resistance changes so it's a difficult judgment to distinguish between live and fake fingers based on conductivity.

6.5 Facial Thermograms

Underneath the skin, arteries and veins creates a distinctive pattern in every human being, a "facial thermo gram" image is generated by capturing heat emitted from face by using infrared camera. A 3D latex mask or 2D face photograph can't fool "facial thermo gram" system because right heat emanation can't be produced by fake face. Facial thermo gram is neither exposed to masquerade nor to plastic surgery because alteration to temperature allocation of the face is impractical [16]. Facial thermo-grams are near the beginning of the development. Multi modal biometric systems comprised of thermal and visual face recognition technologies. This technology is quite helpful for face spoofing attacks to be infeasible and accuracy is also improved.

7. Conclusion

Biometric technology is an additional aspect for the enhancement of security but these systems are vulnerable to attacks like replay, spoofing and transmission. In the written paper, numerous attacks are discussed and the ways to overcome them. Spoofing risk and anti-spoofing methods are also discussed in detail because spoofing is a unique type of attack on biometric authenticator. Live-ness detection can be a vital solution to prevent spoofing attacks. Many experiments have been done for discovering and measuring new features so that biometric sensor can differentiate between live and fake users. Finally, the best solution is to manufacture all the working components of a biometric in a temper-proof device. This will decrease the probability of replay attack and also lesser the likelihood of data interception, redirection or analyzing transmission channels. Fully protection of the biometric sensors from users is never being done due to their nature.

References

[1] Crosbie, M. "Biometrics for enterprise security", Network Security Journal, Volume 2005, Issue 11, November 2005, Pages 4-8.
[2] Faundez-Zanuy, M., "Biometric security technology," Aerospace and Electronic Systems Magazine, IEEE , vol.21, no.6, pp.15-26, June 2006
[3] Wills David, Lees Mike. Six biometric devices point the finger at security. Network Computing, http://www.networkcomputing.com/910/910r1 .html 1 June 1998 [accessed 29th April 2009].
[4] Check Body, Thalheim Lisa, Krissler Jan, Ziegler Peter-Michael. Biometrie (Translated from the original German by Robert W. Smith) c't magazine 2002; 114. <http://www.heise.de/ct/ english/02/11/114/> [accessed 21st April 2009].
[5] Harrison Ann. Hackers claim new fingerprint biometric attack. SecurityFocus, http://www.securityfocus.com/print/news/6717,13 August 2003 [accessed 21st,April 2009].
[6] Clarkson University Engineer Outwits High-Tech Fingerprint Fraud, Clarkson University, <www.yubanet. com/artman/publish/printer_28878.shtml >; [accessed 28th April 2009].
[7] Roberts, C. "Biometric attack vectors and defenses", Computer and Security Journal, Volume 2007, Issue 26, Pages 14-25.
[8] Miller, B., 1994. Vital signs of identity.IEEESpectr. 31 (2), 22-30. Ratha, N., Bolle, R., 1999. Smartcard based authentication. In: Jain, A., Bolle, R., Pankanti, S. (Eds.),
[9] Schneier, B., 1999. The uses and abuses of biometrics. Comm. ACM 42 (8), 136.
[10] Ratha, N., Bolle, R., 1999. Smartcard based authentication. In: Jain, A., Bolle, R., Pankanti, S. (Eds.), Biometrics, Personal Identification in Networked Society. Kluwer Academic Publishers, Norwell, MA, pp. 369–384.
[11] Nalini K.Ratha, Jonathan H.Connell and Ruud M. Bolle "Biometrics break-ins and band-aids", Pattern Recognition Letters, Volume 24, Issue 13, September 2003, Pages 2105-2113.
[12] Qinghan Xiao, "Security issues in biometric authentication," Information Assurance Workshop, 2005. IAW '05. Proceedings from the Sixth Annual IEEE SMC , vol., no., pp. 8-13, 15-17 June 2005.
[13] U. Uludag and A.K. Jain, "Attacks on biometric systems: A case study in fingerprints," Proc. SPIE-EI 2004, pp. 622-633, San Jose, CA, January 18-22, 2004.
[14] T. Matsumoto, H. Matsumoto, K. Yamada and S. Hoshino, "Impact of artificial gummy fingers on fingerprint systems", Optical Security and Counterfeit Deterrence Techniques IV, Proc. SPIE, Volume 4677, 2002.
[15] T. Putte and J. Keuning, "Biometrical fingerprint recognition: don't get your fingers burned," In Proc. of IFIP TiWWG8.8 Fourth Working Conference on Smart Card Research and Advanced Applications, pp. 289-303. Kluwer Academic Publishers, 2000.
[16] F. K. Prokoski, "Disguise detection and identification using infrared imagery," Proceedings of SPIE,

Optics.andimages in Law Enforcement IJ. A.S. Hecht, Ed., Arlington, VA, pp. 27-3 I, May 1982.
[17] L. Thalheim, J. Krissler and P. Ziegler, "Body check: Biometric access protection devices and their programs put to the test," (Online) C'TMagarine, 11, 114. URL: http://www.heise.de/ct/englisWO2/11 /I 14/, May 2002.
[18] "How do you know if it's a real finger?" ID Newswire,January 8,2003,(Online)http://www.biometrics.dod.mil/documents /publicaffairs/ I 803-1DNewswire.pdf