Journal of Information Assurance and Security.
ISSN 1554-1010 Volume 8 (2013) pp. 137-146
© MIR Labs, www.mirlabs.net/jias/index.html

Threats Models On Biometric Systems

a comparative study

Dellys Hachemi Nabil[1], Benatchba Karima[1], Koudil Mouloud[1], Bouridane Ahmed[2]

[1] Laboratoire de Méthodes de Conception de Systèmes
(LMCS)
Ecole nationale Supérieure en Informatique (ESI)
Algiers, Algeria
{h_dellys, k_benatchba, m_koudil}@esi.dz

[2] School of Computing, Engineering &
Information Sciences
Northumbria University
Newcastle, UK
ahmed.bouridane@northumbria.ac.uk

*Abstract***— Several threat models on biometric systems have been proposed to facilitate the design, implementation and validation of techniques to secure these systems. Some models classify threats by type of attacks, others by specific attacks and others by using vulnerabilities and threat agent. Each model proposes a vision and a different approach to identify these threats. For example, to design security techniques for wireless biometric card, one should identify all threats facing this kind of device; an adequate model identifying these threats would be very useful for designers. In this paper, a comparative study and synthesis is given.**

Keywords: Biometric; model; threat; attack; vulnerabilities.

I. INTRODUCTION

Biometrics use physiological and behavioral characteristics to identify an individual. It has the advantage of being unique for each person. It cannot be forgotten, stolen, or shared with another person. .

Biometric systems which manages one or more biometric modalities are vulnerable. Usually, these systems manage unique biometric information for each person; therefore, if the information is compromised, it cannot be replaced. Moreover, this type of system is targeted by several attacks. For these reasons, several techniques for securing biometric information have been implemented. These techniques are designed to ensure confidentiality, integrity and availability of biometric system [1,7,10,13,15]. But before designing a security technique, the problem of security should first be clearly defined and identify the threats that system target. For this reason, several threat models on biometric systems have been proposed (Section III).

In this paper, we present these models, highlight their strengths and weaknesses, and make a comparative synthesis.

This paper is organized as follows: in section 2, the main attacks targeting biometric systems are introduced. In section 3, we present the different biometric system threat models that have been proposed in the literature. We conclude, in section 4, by a comparative synthesis on the studied models.

II. MAJOR ATTACKS ON BIOMETRIC SYSTEMS

Most biometric systems threat models identify only attacks on such systems. This is due to the fact that these attacks are the type of threats most used to compromise the biometric systems. Several attack types target biometric systems. To avoid presenting attacks for each model, we present in Table II the most common ones with a brief description.

However, threats on biometric systems do not consist only on attacks; they can be vulnerabilities due to many causes like a bad programming, a non-secure channel communication, a bad system administration ... etc.

Other threats can come from dishonest persons: A person, authorized to manage a biometric system, can abuse the confidence placed in him to spoof biometrics information of users.

The most cited attacks on biometric systems are presented in the following:

- **Brute-force attack**: This attack generates a random template that is gradually modified, pixel by pixel, considering all possible cases of image thumbs until the system is accessed. It is simple to perform this attack, but it is easily detectable due to the large number of attempts it makes. In addition, changing the image pixel per pixel can take considerable time to generate all possible cases, hundreds to hundreds of billions of iterations (depending on the initial template) can be performed before reaching the goal. This may take a few seconds in the best case but few years in the worst case. *Choi* et al use this attack against fuzzy fingerprint vault. Another description of brute-force attack can be found in [25]

- **Invasion attack**: A biometric system usually uses specific characteristics for individuals recognition of, such as minutiae, ridges or texture ... This attack injects a template with maximum number of features that the system uses to recognize one person. As a result, some characteristics will correspond to the legitimate user. For example, if one can generate a random fingerprint with a lot of minutiae; , there will be a strong chance that a few of them correspond to an authorized person. Several iterations are needed for this attack to succeed as it must change the position of minutiae several times before having some of them correspond to those of an authorized person, more details on this invasion attack can be found in [5].

- **Hill-Climbing attack**: This attack injects a random modality, preferably close to the one of an authorized person. Then, it changes the modality, gradually, according to the degree of similarity until it is accepted by the system. This attack needs to access threshhold of similarity in matching subsystem. *Gomez-Barrero et al.* use this attack to test the uphill-simplex algorithm for face biometric [24], more details of this attack can also be found in [17].

- **Spoofing attack**: This attack introduces a false modality resembling the original one in the system, pretending that it is a legitimate user to have access on the system. Several strategies are used in this attack like introducing a rubber finger in sensor (Figure 1), a picture of an authorized person ....ect. This attack is the most used against biometric systems. Venugopalan et al. show how to Generate Spoofed Irises From an Iris Code Template in [30], more description of spoofing attack can be found in [9] [19][31][32][33].

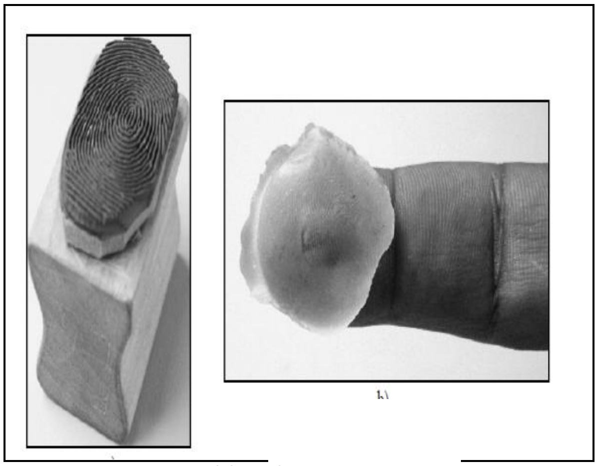

Figure 1. Example of fake fingerprint made with gelatin [12].

- **Attack by Injection or substitution of template**: This attack injects or modifies a biometric template in the database, replacing the original one. Another strategy consists of replacing an original template just before the comparison during the matching process in RAM (Random Access Memory). In [25] *Lafkih et al*. test this attack against their fuzzy vault system. More description of this attack can be found in [19], [6], [29].

- **Attack by manipulating the errors thresholds**: Two different pictures of the same biometric modality, captured by the same sensor, rarely give the same information with accuracy when generating the biometric template within any biometric system. This is why a threshold error is tolerated under which the comparison is successful. This attack consists in increasing this threshold to bypass access control. An error threshold of 100% allows any person to access the system. More information on this attack can be found in [16] [4]

- **Residual attacks**: If the biometric application does not delete temporary data in RAM after a biometric recognition, an attacker can retrieve the biometric template and reuse it later on. It is an attack linked to negligence in programming that can be very dangerous because it is hard to detect. more description of residual attack can be found in [16]

- **Masquerade attack**: This attack presents a fake modality or a template closely resembling the original one to have an access to the system [17]. An example of this attack consist on retrieving a biometric template with residual attack, and introducing this template in a transmission channel between sensor and a biometric application to have access to the system (Figure 2);

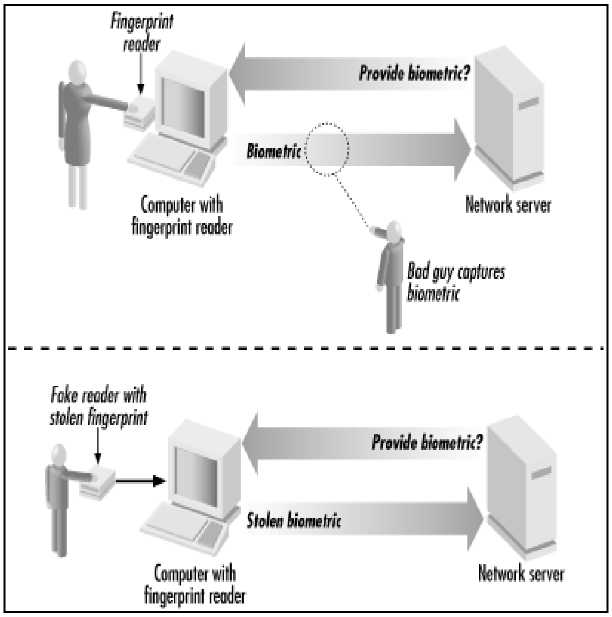
Fingerprint reader
Provide biometric?
Biometric
Computer with fingerprint reader
Network server
Bad guy captures biometric
Fake reader with stolen fingerprint
Provide biometric?
Stolen biometric
Computer with fingerprint reader
Network server

Figure 2. Example of masquerade attack [12].

- **Parallel sessions attack**: It is also called dual messages attack or piggyback attack. An attacker logs at the same time as an authorized user with his parameters, to pretend that there is only one open session. Then the attacker listens to the transactions and uses the time between two messages of the authorized user, to send malicious messages with similar parameters of legal messages. The biometric system will have the impression that the authorized person has sent a message. [17], [20] [13].

- **Replay attack**: This attack consists in capturing data in a legal authentication transaction. Then, later on, recognition with the same information is initiated to have access to the device. In [26] Hirano et al. proposed an authentication schemes based on cancelable biometric secured against replay attack and its related attack, more description of replay attack can be found in [19][27][28].

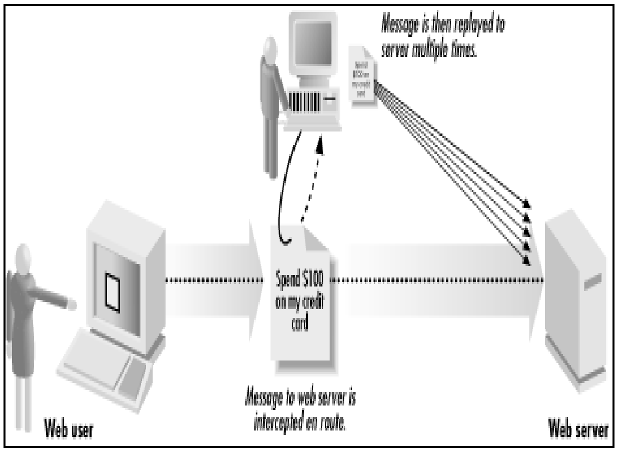
Message is then replayed to server multiple times.
Spend $100 on my credit card
Message to web server is intercepted en route.
Web user
Web server

Figure 3. Example of replay attack [22].

III. THREATS MODELS ON BIOMETRIC SYSTEMS

To identify attacks on biometric systems and facilitate the development of security techniques, taxonomic models of attacks on biometric systems have been proposed. Among the most well-known, those of Ratha, Connel and Boll [16], Bartlow and Cukic [2], Jain, Ross and Pankanti [6] and Cris Robert [17].We present in the following, , their strengths and weaknesses:

A. *Models of Ratha, Connel and Boll*

Ratha, Connel and Boll were the first to suggest a model for classifying biometric attacks in 2001(Figure 4). *Ratha et al* based their classification on the location of the biometric information. Eight vulnerable points where biometric information transits are identified. Each point can be targeted by one or more types of attacks:

1- *The sensor :* It includes all capture devices and softwares that manage them. It includes attacks such as spoofing, when attacker introduces a fake modality in the reader. Masquerade can be used by introducing a false template in sensor software. One can crash the sensor software by denial of service attacks. A bad programming opens a gap to residual attacks...ect;

2- *Communication between sensor and signal processing subsystem :* The transmission channel is ideal for attacks such as replay attack, injection or parallel sessions;

3- *Signal processing subsystem :* Hill-Climbing or invasion can be easily used to attack this subsystem is ideal for attacks such as;

4- *Communication between Signal processing subsystem and correlation subsystem:* the same type of attacks as for point 2 can occurs (replay, injection, parallel sessions, etc.);

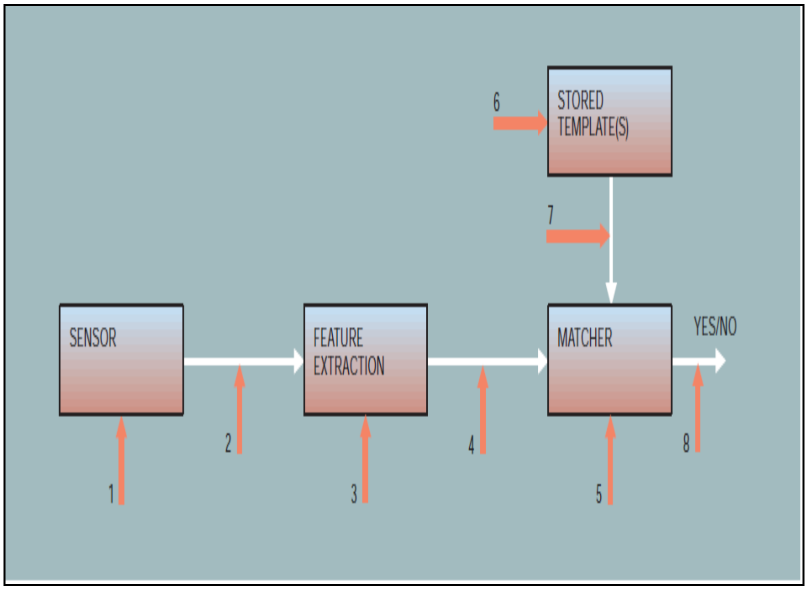

Figure 4. Model proposed by Ratha et al [16].

5- *Correlation subsystem :* attacks based on correlations can occur ;

6- *Storage subsystem :* attacks on Template can be performed such as injection, modification or outright suppression of Template;

7- *Communication between Storage subsystem and Correlation subsystem:* the same types of attacks than those in points 2 and 4 can occur (replay, injection, parallel sessions, etc.);

8- *The decision subsystem :* The decision to accept or reject a biometric recognition is make in this subsystem. Attack by manipulation of decision can take place in this subsystem;

We note that the same types of attacks appear on several points (2, 4 and 7). These points can be modeled as a single subsystem, that we can name the transmission subsystem. Moreover, this model is general and does not give details on the specific attacks. The authors merely represent attacks targeting specific parts of a system as black boxes. (Dahiya et al. cite examples of attacks on the points of this model [34]).

We can say that the model of *Ratha et al* is very general. Moreover, we note that each specific point of a biometric system can potentially be attacked.

The Strengths of the model are summarized in what follows:

- It decomposes the system into separate vulnerable parts;
- It specifies for each vulnerable point, the types of attacks that can occur ;
- It allows to validate parts of the system separately in the step of implementation.

Weaknesses of the model are summarized in what follows**:**

- Several parts are characterized by the same types of attacks;
- Does not give details on how the attack operate on each part, Knowing that each attack differ from one point to another;
- It is a very general model with a high level of abstraction of the architecture of a biometric system on one side, and attacks other side.

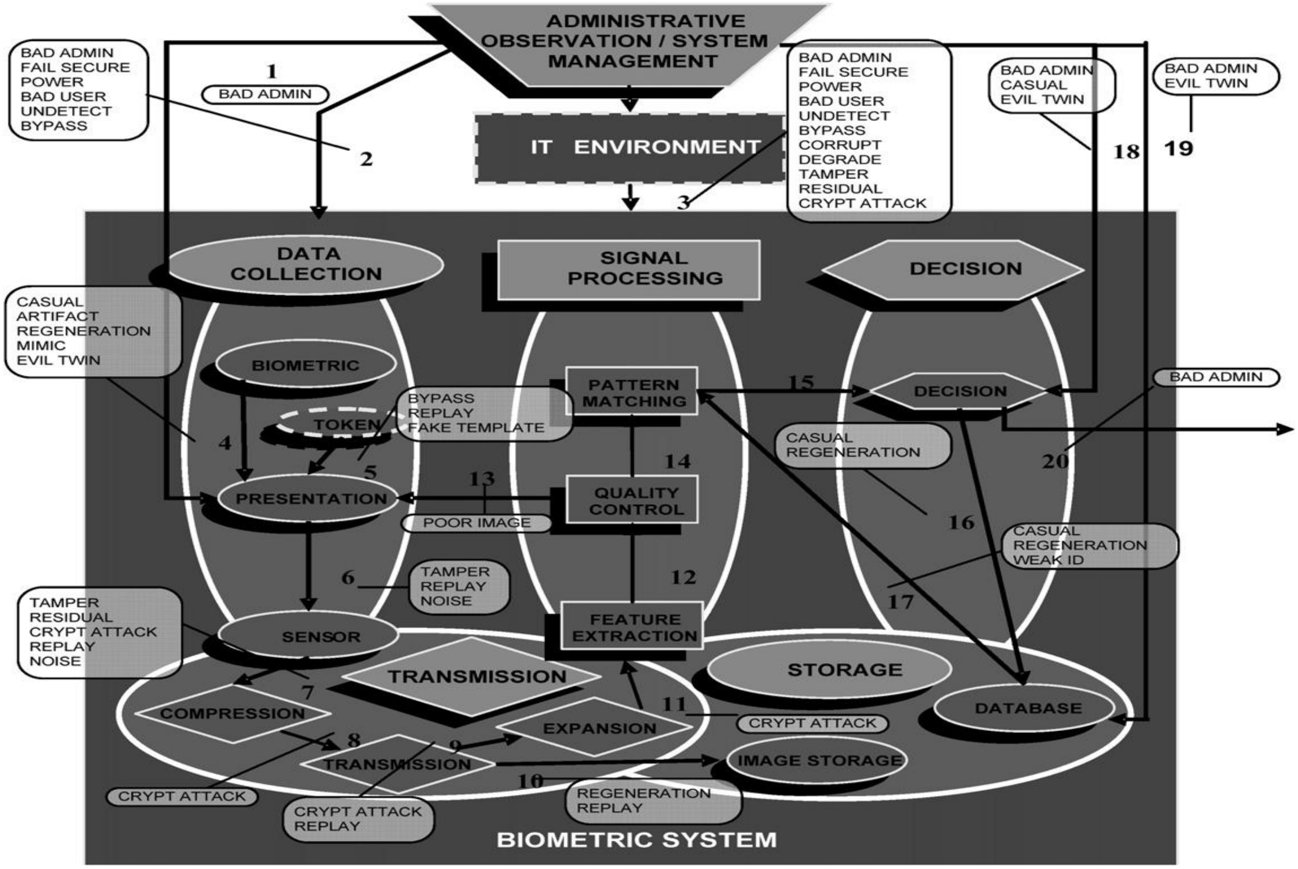

Figure 5. Model proposed by Bartlow et al [2].

B. *Model of Bartlow and Cukic*

Bartlow and Cukic [2] have proposed a model inspired from Wayman's subsystems architecture [20]. This model uses the same logic as *Ratha's* vulnerable points, with a more important level of details. It highlights the vulnerabilities of the five subsystems of a biometric system and the main modules that compose it. *Bartlow and Cukic* modeled the administrative and environmental features as subsystems to stay on *Wayman's* architecture logic while detailing each part (Figure 5). They enriched their model with several attacks and vulnerabilities in the subsystems and the main modules. Moreover, they identified twenty two vulnerabilities, where twenty potential attacks can occur.

Bartlow and Cukic decomposed their model as follows:

1. *Administrative observation/system management module:* these are all the administrative procedures and biometric system management where one can find the administrative attacks carried out by internal staff ;
2. *IT environment module:* these are all applications that interact directly or indirectly with the biometric system. The most important ones are the operating system and management system database. This module is targeted by environmental attacks, targeting vulnerabilities of these technologies to access the biometric system;
3. *The biometrics subsystems:* each subsystem consists of modules that perform specific functionalities, and each can be targeted by some types of attacks. A brief description of each subsystem is presented in the following:

a. *Data collection subsystem:* where the acquisition and presentation of data are carried out. Attacks such as masquerade, replay, or spoofing can be performed on this subsystem ;

b. *Data transmission subsystem:* where the compression and transmission of biometric data can occur. This subsystem is targeted by attacks like replay, parallel sessions or masquerade ;

c. *Signal processing subsystem:* where functions such as quality control, robust feature extraction and template matching can be performed. These are very important features for recognition; therefore, several attacks target this subsystem such as masquerade, Hill-Climbing, brute force attacks, invasion, etc. The insertion of Trojans in this subsystem is very common as well;

d. *Data storage subsystem:* it is the subsystem that manages the biometrics backup. Attacks such as injection or substitution of data or residual attack can be performed;

e. *Decision subsystem:* Where the decision to validate or not recognition is applied. This subsystem is affected by attacks such as manipulation of errors thresholds, manipulation of decision, substitution attacks, etc.

We note that these models classify attacks by types without any details on the specific attacks on each subsystem. For example, the replay attack, mentioned in points 5, 6, 7, 9 and 10 in the model (Figure 2), targets points whose processing logic is different. This model does not give a clear idea for designing and implementing secure techniques taking into account these attacks.

This model provides details on potential points where attacks can be performed. However, it does not simplify the task of designing security techniques, because one has to take into account the specificities of each vulnerability and those of each attack on a given point. Thus, this model is well suited for testing and validating secure techniques.

Strengths of the model are summarized in what follows**:**

- The Model is based on Wayman's architecture subsystem, with a high level of details on components and modules of biometrics systems;
- Significant number of vulnerabilities are identified;
- Identification of several attacks on each subsystem or modules that compose it;
- Identifies environmental and administrative attacks ;
- Very useful for the validation of a system or subsystem biometric.

Weaknesses of the model are summarized in what follows:

- Does not detail the specificities of each attack on subsystems or modules. In this model each of them have a different operating logic, but are affected by the attacks of same type;
- It may be difficult to design an effective securing method a the model may guided towards to a solution as a new attacks may not be detected.

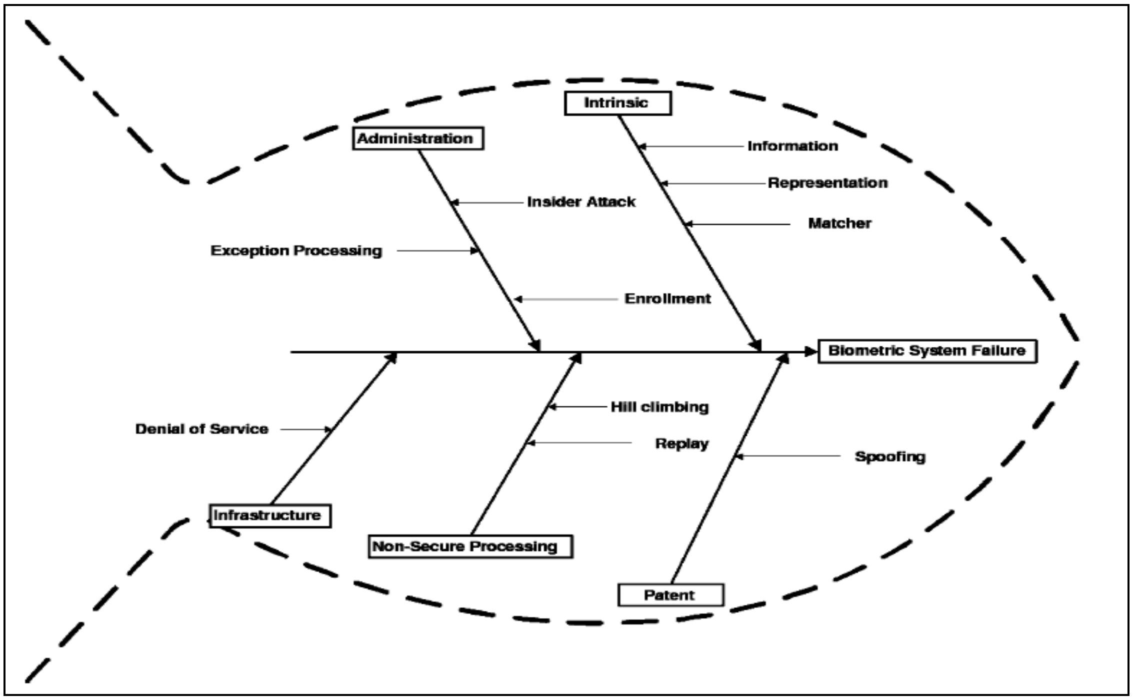

Figure 6. Fishbone Model proposed by Jain et al [6].

C. *Model of Jain, Ross and Pankanti «Fishbone »*

Jain, Ross and Pankanti [6] have proposed a model, called «Fishbone » (Figure 6). It is based on the causes that create the vulnerabilities of a biometric system, and effects that may result (attacks on each one).

Jain et al distinguish five causes that generate vulnerabilities in biometric systems:

1- *Administration causes* : a bad administrative process, or a non-strict control may open the way for attacks by rogue employees ;

2- *Intrinsic causes*: design errors or limited equipment can generate false acceptance and open several loopholes in the system;

3- *Infrastructure causes :* design errors or bad equipments generate vulnerabilities susceptible to provoke denial of service, which can compromise the normal functioning of the system;

4- *non-secure process causes :* vulnerabilities related to an unsecured process(enrolment/identification) open gaps for possible attacks ;

5- *Patent causes:* an unsecured template can be exposed to various attacks.

According to Jain et al, these causes generate two effects: denial of service on infrastructure, and various vector attacks on other causes (Administration, Intrinsic, Process Unsecured, and Patent).

This model does not really show the types of attacks (except for some examples) to which a biometric system is exposed. But it shows that system or hardware poorly designed, malicious managers or non secure backup system can be sources of problems .

This model focuses on errors that has to be avoided when designing a biometric system in general and biometric security techniques in particular. It may be useful for a global view when designing and validating the security techniques.

Nevertheless, it remains very general and does not tell enough about the threats, for which one has to find a security technique. A well designed system (security included) avoiding these causes should theoretically be free of vulnerabilities. This is not the case now; hence there is still a need to design security techniques.

Strengths of the model are summarized in what follows**:**

- Identifies causes that generates vulnerabilities in biometrics systems;
- Warns against adverse attack that may arise from these causes;
- Allows avoiding the mistakes that may open loopholes on biometrics systems;
- Useful for the validation of a biometric system by checking whether any cause of vulnerabilities exists.

Weaknesses of the model are summarized in what follows**:**

- Does not specify, in detail, the threats engendered by each cites causes;
- cannot be used to design security methods because it does not give details about attacks;
- Avoiding the causes cited does not mean that the system will become a 100% safe against different types of attacks.

D. *Model of Nagar, Nandakumar and Jain*

Nagar, Nandakumar and Jain [14] have proposed another scheme (Figure 7). It is based on the same principle of cause and effect as the Fishbone model (Figure 3). However only four causes are identified. One can still find the the administrative and intrinsic causes; however non-secure processes and infrastructure causes, found in the previous model, are combined into a single cause named non-secure infrastructure. There is a fourth cause which includes vulnerabilities and weaknesses of biometrics (not secret, possibility of creation of fake, failure detection vivacity in the sensors ...).
Nagar et al have used the idea of cause and effect as Jain & al. Therefore, the same remarks apply to their model. We can say that this model is useful to get an overall idea when securing and validating a biometric system . But it gives few details for designing a good securing of the system.

E. *Model of Cris Robert*

Cris Robert [17] proposed a model based on the origin of the risks caused by threats aiming biometric systems:

1- *Threat agent :* which are threats from persons

a. *An impostor:* pretending to be an authorized person. The impostor launches attacks such as spoofing, masquerade, injection, etc. to achieve his goals;

b. *An attacker :* it is a person who throws adversary attacks to have access to the system. These attacks can be replay attack, Hill-Climbing attack, invasion attack, etc.;

c. *An authorized person:* that- intentionally or not, commits fraud, opens breaches or compromises the biometric system. Administrative attacks, forcing a person to cooperate [3,17], or configuration errors are examples of this type of threat.

2- *Threat vectors :* these are all attacks conducted on specific points of a biometric system(section 2) ;

3- *System vulnerabilities:* which include all the vulnerabilities of a biometric system (design, implementation, integration, etc.) and those related to its environment (OS, hardware, DBMS, etc.).

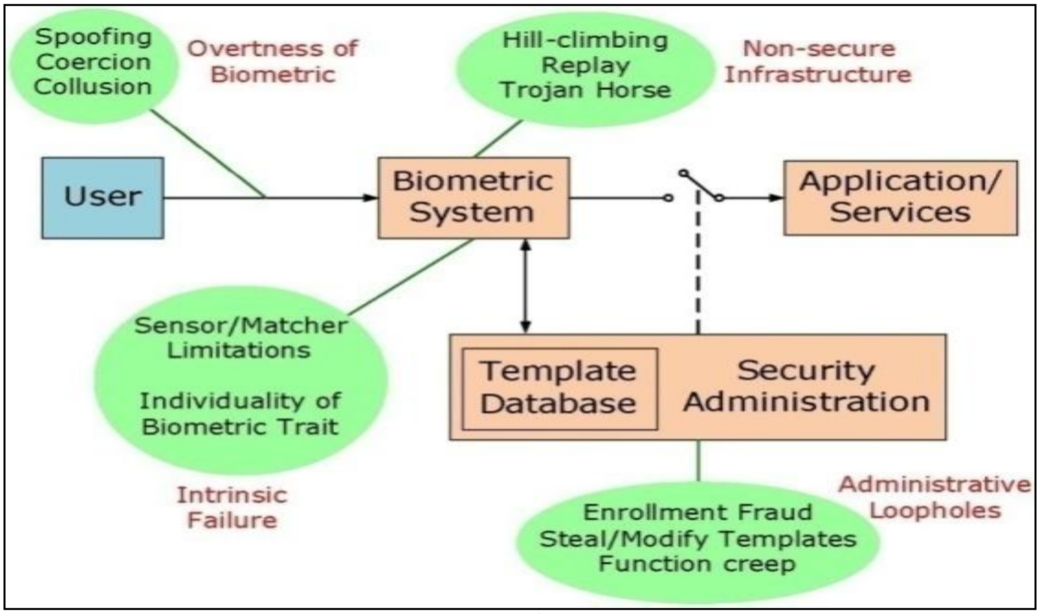

Figure 7. Model of Nagar et al [14].

Strengths and weaknesses of the model of Nagar et al follows the same logic as that of Jain et al; therefore, both models have same strengths and weaknesses

Cris Robert based his model on three dimension: the risk generated by persons who make threats, the attacks that these persons use, and vulnerabilities that allow such attacks to be performed.

Cris Robert divides threats into three different dimensions. Each one requires a different security approach. Security techniques are valid only on adversary attacks. Threat agents and vulnerabilities require other approaches for protection, e.g.: good design, high performance equipment, use policy… are many parameters that one should not overlook.

This model describes all the threats to which a biometric system is exposed. From a global point of view, it is more complete than the model of Jain's and Nagar's. It may be useful for the validation of security techniques of biometric systems. However, it is not exploitable for the design of security methods except for validation against various attacks.

Strengths of the model are summarized in what follows**:**

- Proposes another type of threat compared to other models, that is the threat agent;

- Describes the complete scenario of threats on biometrics systems, which are attacks that compromise the system, agent that runs attacks, and vulnerabilities that benefit to these attacks.

Weaknesses of the model are summarized in what follows**:**

- Defines types of attacks without specifying their scope and how they process;

- Does not allow designing effective security methods, because it gives a classification of types of threats.

IV. Summary of different models

As we have seen, in the previous section, several models have been proposed on threats against biometric systems. These models are intended to draw attention to these threats in order to avoid themes, facilitate the design and implementation of security techniques, or help to validate these techniques.

The models have been proposed with more or less different visions, but none has provided a comprehensive and fully satisfactory answer to the problems of design, implementation and validation of security techniques of biometrics.

We present in Table I a comparative overview of the different models previously presented.

Each model is useful for the design and validation of security techniques for biometric. Models of *Jain et al* and *Nagar et al* define the causes that generate vulnerabilities of biometric systems. Models of *Ratha et al* and that of Bartlow & Cukic classify attacks according to the vulnerability points.

Table 1. SUMMARY OF DIFFERENT MODELS OF THREATS ON BIOMETRIC SYSTEMS.

Model name and authors	**Classification criterion**	**Diagram of the model**	**Properties of attacks**
Model of Ratha, connel and Boll [16]	Vulnerable parts	System components	Specific attacks
Model of Bartlow and Cukic [2]	Vulnerable points	Subsystem	Type of attack
Model FishBone of Jain, Ross and Pankanti [6]	Causes and effects	Structure and procedure	Vulnerabilities
Model of Nagar, Nandakumar and Jain [14]	Causes and effects	Structure and procedure	Vulnerabilities
Model of Cris Robert [17]	Type of threat	Actors	Specific attacks Vulnerabilities Threat agent

Cris Robert's model, on the other hand, focuses on different types of threats components, subsystems, structures and procedures, and the actors (who perform the attacks) of a biometric system are all present - if one takes into account all models. It is the same for the attacks (by type or specific attacks), vulnerabilities and threats agent. Thus, it appears that these models are complementary; each offers a different vision, though incomplete, of biometric systems security problems. However, if one considers all models, we get a much more complete and detailed vision of threats against biometric systems.

V. Conclusion

Biometric systems are subject to many threats, hence the use of security techniques to ensure confidentiality, integrity and system availability. However, the design and validation of security techniques requires threats identification. As a result, several threat models of biometric systems have been proposed. Each offers a different view, based for example on where the attacks are carried out, their types or causes of these attacks.

No model has proposed a comprehensive view of threats on biometric systems. But we noticed that these models complete each other, and if one takes into account all models, he gets a fairly comprehensive idea of these threats, to help for the design, implementation and validation of security techniques.

References

[1] Agrawal N., Savvides M., “Biometric Data Hiding: A 3 Factor Authentication Approach to Verify Identity with a Single Image Using Steganography, Encryption and Matching”, IEEE, 978-1-4244-3993-5/09, 2009.

[2] Bartlow N., Cukic B., “The vulnerabilities of biometric systems – an integrated look and old and new ideas”, Technical report, West Virginia University, 2005.

[3] Breebaart J., Yang B., Buhan-Dulman I., Busch C., “Biometric Template Protection”, DuD • Datenschutz und Datensicherheit, vol.5, 2009.

[4] Buhan I., Hartel P., “The State of the Art in Abuse of Biometrics”.

[5] Cavoukian A., Stoianov A., “Biometric Encryption: A Positive-Sum Technology that Achieves Strong Authentication, Security and Privacy”, March 2007.

[6] Jain A.K., Ross A., Pankanti S., “Biometrics: A Tool for Information Security”, IEEE, Transactions on information forensics and security, vol.1, no.2, June 2006.

[7] Khan M.K., Zhang J., “Improving the security of ‘a flexible biometrics remote user authentication scheme’”, Science Direct, Computer Standards & Interface, vol.29 pp82-85, Elsevier, 2006.

[8] Kholmatov A., Yanikoglu B., “Realization of Correlation Attack Against the Fuzzy Vault Scheme”.

[9] Li C.T., Hwang M., “An efficient biometrics-based remote user authentication scheme using smart cards”, Science Direct, Journal of Network and Computer Applications, vol.33 pp1-5, Elsevier, 2009.

[10] Li C.L., Wang Y.H., Liu L.N. “A Biometric Templates Secure Transmission Method Based on Bi-layer Watermarking and PKI”, International Conference on Multimedia Information Ntworking and Security, 2009.

[11] Lumini A., Nanni L., “An improved BioHashing for human authentication”, Science Direct, Pattern Recognition, vol.40 pp1057–1065, Elsevier, 2007.

[12] Maltoni D., Maio D., Jain A.K., Prabhakar S., “Handbook of Fingerprint Recognition” 2nd edition, Springer, 2009.

[13] Mazhelis O., Puuronen S., “A framework for behavior-based detection of user substitution in a mobile context”, Science Direct, computers & security, vol.26 pp154–176, Elsevier, 2006.

[14] Nagar A., Nandakumar K., Jain A. K., “Biometric template security”, SPIE, Newsroom, 2009.

[15] Nagar A., Nandakumar K., Jain A. K., “Biometric Template Transformation: A Security Analysis”.

[16] Ratha N. K., Connell J. H., Bolle R. M., “Enhancing security and privacy in biometrics-based authentication systems”, IBM Systems Journal, vol.40 no.3, 2001.

[17] Roberts C., “Biometric attack vectors and defences”, Science Direct, computers & security, vol.26 pp4–25, Elsevier, 2007.

[18] Ross A., Shah J., Jain A.K., “From Template to Image: Reconstructing Fingerprints from Minutiae Points”, IEEE, Transactions on pattern analysis and machine intelligence, vol.29 no.4, April 2007.

[19] Sutcu Y., Sencar H.T., Memon N., “A Secure Biometric Authentication Scheme Based on Robust Hashing”, ACM, MM-SEC’05, 2005.

[20] Wayman J.L., “Technical testing and evaluation of biometric devices”, 1999.

[21] Xu J., Zhu W.T., Feng D.G., “Improvement of a Fingerprint-Based Remote User Authentication Scheme”, International Journal of Security and its Applications, Vol.2 No. 3, July 2008.

[22] Garfinkel S., Spafford G., “Web Security, Privacy & Commerce”, 2nd edition, O’Reilly, 2000.

[23] Choi.W.Y., Pan.S.B., Kim.J.M., Chung Y., Hong D., “Fast Polynomial Reconstruction Attack against Fuzzy Fingerprint Vault”, Information Science and Service Science (NISS), 2011 5th International Conference on New Trends, Vol.2, pp.299-302, Oct 2011.

[24] Gomez-Barrero M., Galbally J., Fierrez J., Ortega-Garcia J., “Face Verification Put to Test: A Hill-Climbing Attack Based on the Uphill-Simplex Algorithm”, Biometrics (ICB), 2012 5th IAPR International Conference, pp.40-45, April 2012.

[25] Lafkih M., Mikram M., Ghouzali S., EL Haziti M., Aboutajdine D., “Biometric Cryptosystems based Fuzzy Vault Approach:Security Analysis”, Innovative Computing Technology (INTECH), 2012 Second International Conference, pp.27-32, Sep 2012.

[26] Hirano T., Hattori M., Ito T., Matsuda N., Mori T., “Homomorphic Encryption Based Cancelable Biometrics Secure against Replay and Its Related Attack”, Information Theory and its Applications (ISITA), 2012 International Symposium, pp.421-425, Oct 2012.

[27] Shelton J., Dozier G., Adams J., Alford A., “Permutation-Based Biometric Authentication Protocols for Mitigating Replay Attacks”, Evolutionary Computation (CEC), 2012 IEEE Congress, pp.1-5, june 2012.

[28] Shelton J., Adams J., Alford A., Venable M., Neal S., Dozier G., Bryant K., “Mitigating Replay Attacks Using Darwinian- Based Feature Extraction”, Computational Intelligence for Security and Defence Applications (CISDA), 2012 IEEE Symposium, pp.1-7, July 2012.

[29] Nagar A., Nandakumar K., Jain A.,K., “Multibiometric Cryptosystems Based on Feature-Level Fusion”, Information Forensics and Security, IEEE Transactions, Vol.7, pp.255-268, Feb 2012.

[30] Venugopalan S., Savvides M., “How to Generate Spoofed Irises From an Iris Code Template”, Information Forensics and Security, IEEE Transactions, Vol.6, pp.385-395, June 2011.

[31] Zhang Z., Yan J., Liu S., Lei Z., Yi D., Li S.Z., “A Face Antispoofing Database with Diverse Attacks”, Biometrics (ICB), 2012 5th IAPR International Conference, pp.26-31, April 2012.

[32] Biggio B., Akhtar Z., Fumera G., Marcialis G.L., Roli F., “Security evaluation of biometric authentication systems under real spoofing attacks”, Biometrics IET, Vol.1, pp.11-24, March 2012.

[33] Espinoza M., Champod C., “Using the Number of Pores on Fingerprint Images to Detect Spoofing Attacks” , Hand-Based Biometrics (ICHB), 2011 International Conference, pp.1-5, Nov 2011.

[34] Dahiya N., Kant C., “Biometrics Security Concerns”, Advanced Computing & Communication Technologies (ACCT), 2012 Second International Conference, pp.297-302, Jan.2012.

Hachemi-Nabil Dellys received the ingineer degree in computer science from l’Ecole nationale Supérieure d’Informatique, Algiers, Algeria, in 2009. He is currently pursuing the Ph.D. degree in securing of biometrics devices in the same school, where he is an assistant teacher. His research interest is on Fingerprint,Iris and face biometrics, biometric mobile devices, and securing of biometric template.

Karima Benatchba received her Ph.D. degree in computer science from l’Ecole nationale Supérieure d’Informatique, Algiers, Algeria, in 2005. She is currently professor in the same school. Her research interest is on combinatorial optimization, metaheuristics, biomimetic methods, and biometric.

Mouloud Koudil received the Ph.D. degree in computer science from l’Ecole nationale Supérieure d’Informatique, Algiers, Algeria,in 2002. He is currently professor in the same school. His research interest focus on hardware/software codesign, networks on chips, wireless sensor networks, and biometric.

Ahmed Bouridane received the Ph.D degree in electrical engineering (computer vision) from the University of Nottingham, U.K., in 1992. He is now a full Professor in Image Engineering and Security at Northumbria University at Newcastle (UK), and his research interests are in imaging for forensics and security, biometrics, homeland security, image/video watermarking and cryptography. He has authored and co-authored more than 200 publications and one research book. Prof. Bouridane is a Senior Member of IEEE.