Security EvaBio: An Analysis Tool for the Security Evaluation of Biometric Authentication Systems

Mohamad El-Abed, Patrick Lacharme, Christophe Rosenberger

Security EvaBio: An Analysis Tool for the Security Evaluation of Biometric Authentication Systems

Mohamad El-Abed and Patrick Lacharme and Christophe Rosenberger
Université de Caen Basse-Normandie, UMR 6072 GREYC, F-14032 Caen, France
ENSICAEN, UMR 6072 GREYC, F-14050 Caen, France
CNRS, UMR 6072 GREYC, F-14032 Caen, France
{mohamad.elabed, patrick.lacharme, christophe.rosenberger}@ensicaen.fr

Abstract

Biometric systems present several drawbacks that may significantly decrease their utility. Nowadays, several platforms (such as the FVC-onGoing) exist to assess the performance of such systems. Despite this, none platform exists for the security evaluation of biometric systems. Hence, the aim of this paper is to present an on-line platform for the security evaluation of biometric systems. The key benefits of the presented platform are twofold. First, it provides biometrics community an evaluation tool to assess biometric systems in term of security. Second, the platform provides a database of common threats and vulnerabilities of biometric systems that can be updated by researchers feedbacks. The presented tool is modality-independent. A keystroke dynamics system is used to illustrate the benefits of the presented platform.

1. Introduction

Biometrics is a promising candidate to either enhance or replace traditional authentication systems based on "what we own" (such as a key) or "what we know" (such as a password). Many biometric authentication systems have been proposed in the last decade going from morphological (such as fingerprint), behavioral (such as keystroke dynamics) and even biological (such as DNA) modalities. They are mainly used to manage the physical (such as border control) and logical (such as e-commerce) access to resources. Despite the obvious advantages of biometric authentication systems in comparison to traditional ones, they are still vulnerable to several kinds of attacks which may deeply affect their utility and functionality. Ratha *et al.* [1] have identified eight locations of possible attacks in a generic biometric system as illustrated in Figure 1. Maltoni *et al.* [2] present several drawbacks of biometric systems related to circumvention, repudiation, contamination, collusion and coercion threats.

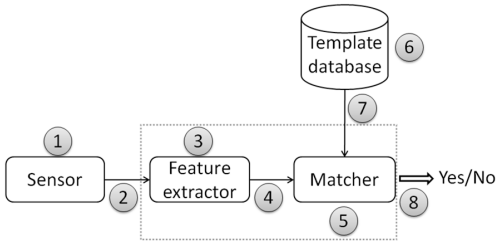

Figure 1. Possible attack points in a generic biometric system: Ratha *et al.* model [1]

The works presented by Ratha *et al.*, Maltoni *et al.* clearly show the weakness of biometric systems which may decrease their utility. Therefore, it is important that biometric systems be designed to withstand the presented threats when employed in security-critical applications and to achieve an end to end security. Towards this goal, the aim of this work is to present a web-based automated evaluation platform towards the security evaluation of biometric authentication systems. The goal of this platform is to let researchers to easily evaluate their systems in a quantitative manner, and to enhance the presented database of common threats and vulnerabilities based on their feedbacks and publications. Since researchers may overestimate the efficiency of their developed systems, the platform should be then used by an independent party (as the case of competitions) in order to produce accurate assessment results.

The outline of the paper is as follows. We present in Section 2 related previous research works focusing on the security evaluation of biometric systems. Section 3 presents the security assessment method implemented within the proposed platform. A synopsis of the database of common threats and vulnerabilities of biometric systems is given in Section 4. The security analysis tool is then presented in Section 5. Section 6 gives a conclusion and some perspectives of this work.

2. Previous works

The International Organization for Standardization ISO/IEC FCD 19792 [3] presents a list of several threats and vulnerabilities of biometric systems. In addition to the threats addressed by Maltoni *et al.*, the standard addresses other typical threats related to system performance and the quality of the acquired biometric raw data. The standard also addresses privacy concerns when dealing with biometric systems. The standard does not present a security evaluation of biometric systems. It aims to guide the evaluators by giving suggestions and recommendations that should be taken into account during the evaluation process. Dimitriadis *et al.* [4] present a security comparison study of several biometric technologies in order to be used as an access control system for stadiums. The presented method can be used easily in comparing biometric systems since it is a quantitative-based method. However, an extended research work should be done in order to take into account the recent threats vulnerabilities of biometric systems (especially those presented by the ISO/IEC FCD 19792 standard). Attack tree technique introduced by Schneier [5], provides a structure tree to conduct security analysis of protocols, applications and networks. However, attack trees are dependent from the intended system and its context of use. Therefore, it is infeasible to be used for a generic evaluation purpose. Matyás *et al.* [6] propose a security classification of biometric systems. Their proposal classifies biometric systems into four categories according to their security level. However, their model could not be considered as discriminative to compare the security level of biometric systems.

Discussion

The evaluation of biometric systems is now carefully considered. Many platforms have been proposed (such as FVC-onGoing) whose objective is mainly to compare biometric systems. Nevertheless, these platforms are dedicated to quantify the performance technology (algorithms, processing time, memory required, *etc.*) without testing the robustness of the target system against fraud. The previous section showed the vulnerabilities of biometric systems which may deeply affect its functionality. Therefore, a dedicated platform towards the security evaluation of biometric systems is a promising solution for two main reasons: first, we need a reliable evaluation methodology to quantify the benefits of new systems. Second, such kind of platforms will not only allow researchers to easily test their new systems, it will also enhance this research topic based on the biometric community feedbacks. We present in the next section the quantitative-based security assessment method implemented within the on-line platform. It is a modality-independent method based on the database of common threats and vulnerabilities of biometric systems (see Section 4) and the notion of risk factors.

3. Risk assessment method

According to ISO/IEC FCD 19792, the security evaluation of biometric systems is generally divided into two complementary assessments: **type-1** assessment of the biometric system (devices and algorithms), and **type-2** assessment of the environmental (*e.g.*, is the system is used indoor or outdoor?) and operational conditions (*e.g.*, tasks done by system administrators to ensure that the claimed identities during enrollment of the users are valid). We present in this paper a **type-1** assessment method for the security evaluation of biometric systems. The presented method is inspired from the security audit methodology EBIOS (Expression of Needs and Identification of Security Objectives) [7]. The principle of the proposed approach contains four steps: study of the context, expression of security needs, risk analysis and security index.

3.1. Study of the context

The first step consists of identifying the utility and the characteristics of the target system. This step consists also of detailing its different components and essential elements (known by assets). Using the generic architecture of biometric systems as illustrated in Figure 1 by Ratha *et al.*, the identified assets to be protected are divided into three types as presented in Table 1: an information (I_), a function (F_) and a material (M_).

Reference	Description
I_DATA_BIO	Acquired biometric raw data
I_TEMPLATE	User template
I_DECISION	System decision (yes or no)
F_EXTRACTION	Processing data function implemented on the feature extractor component
F_MATCHER	Matcher function between the acquired biometric data and its corresponding template
M_SENSOR	Biometric sensor
M_COMPONENT	Materials in which the F_EXTRACTION and F_MATCHER are implemented
M_BD	Storage medium of the biometric templates
M_CHANNELS	Transmission channels connecting the different components of the target system

Table 1. The identified assets of a generic biometric system

3.2. Expression of security needs

After describing the target system and identifying its assets, the next step consists of identifying the security requirements that will contribute to the risk assessment process. These identified requirements are also used during the risk reduction process (a perspective step of this work). As any IT system, the security requirements should include classical properties in terms of confidentiality (C), integrity (I) and availability (D). In addition, the security requirements of biometric systems should also contain the authenticity (A) property. This property is defined as the fact of

ensuring that the user presenting the biometric raw data is who he/she claims to be.

3.3. Risk analysis

Risk analysis is considered as a key factor to be taking into account during the development of any IT system. It consists of two steps: identifying the possible threats or events that could have a harmful impact, followed by a risk estimation step. Several works exist in the literature to the risk analysis of an IT system and they are generally divided into two approaches: quantitative or qualitative approaches. A comparison study of both approaches and their advantages and limitations is presented by Arthur Rot [8]. The proposed method is quantitative and based on the notion of risk factors. The choice of the quantitative is mainly retained to its easiness in evaluating and comparing biometric systems, and also it is more exploitable lately during the risk reduction process. A risk factor, for each identified threat and vulnerability, is considered as an indicator of its importance. The computation of risk factors in the presented method is given in both Sections 3.3.1 (identified threats) and 3.3.2 (retained vulnerabilities).

3.3.1 Risk factor computation of the identified threats

In order to compute the risk factors of the identified threats, we use a quantitative approach based on the multi-criteria analysis (MCA). More generally speaking, we use two criteria for the risk factor computation of each identified threat ($risk\ factor = f_1 \times f_2$):

- **Impact (f_1):** represents the impact of the threat in terms of criticality. It is defined between 0 and 10 (the highest score 10 corresponds to a critical attack). This factor is arbitrary fixed due to the four security requirements (confidentiality, integrity, availability and authenticity) presented in Section 3.2. In this work, we penalize the impact (f_1) of threats affecting the confidentiality property more, since such kind of threats affect the privacy and civil liberties of legitimate users.
- **Easiness (f_2):** represents the easiness to make a successful attack. It is defined between 0 and 10 (the lowest score 0 corresponds to an impossible attack, while the highest score 10 corresponds to an easy attack). This factor is arbitrary fixed using two types of informations: first, the weakness of the target system (*e.g.*, weakness related to its architecture), second, the cost in terms of specific equipments and required expertise to implement the attack.

3.3.2 Risk factor computation of the vulnerabilities

For the three retained system overall vulnerabilities (see Section 4.2), we use a set of rules for the risk factors computation process as depicted in Table 2. For the system performance vulnerability, we multiply by 2 since a biometric system providing a performance measure (such as the EER, AUC, *etc.*) more than or equal to 50% is not usable. For such systems, we put then its risk factor for the highest score 100. For the quality aspect, we define four rules according to whether the system implements quality checks during the enrollment step. For the templates database protection, we also define a set of rules according to whether the system implements protection mechanisms (such as encryption schemes, cancelable techniques, *etc.*).

Point	Rules	Risk factor
9	Sufficient panel of users	$2 \times \Theta$
10	- Multiple captures with quality assessment	0
	- One capture with quality assessment	40
	- Multiple captures without quality assessment	60
	- One capture without quality assessment	100
11	- Secure database and local storage	0
	- Secure database and central storage	40
	- Unsecure database and local storage	60
	- Unsecure database and central storage	100

Table 2. General scheme of risk computation for the system overall vulnerabilities. The value Θ illustrates the system overall performance such as the Equal Error Rate (EER)

3.4. Security index

The overall security level of a biometric system, is typically made up of several areas of variable risks. If any of these areas are omitted during the evaluation process, then an unreliable result will be concluded. At this time, such kind of evaluation is considered as a complicated task since the number of actors involved within the process is important. Therefore, an agreed methodology for illustrating the overall system security of a biometric system by an index would facilitate the evaluation and the comparison of such systems [9]. Towards this goal, we use the notion of the area under curve of the curve resulting from the retained risk factors to compute the security index of the target system. It is calculated using the trapezoid rule. The main benefit of using this approach is it permits to take into account all the risks of a biometric system and their relationships in the processing chain. The security index of the target system is then defined as follows:

$$\text{Index} = \alpha \left(1 - \frac{AUC(f(x))}{AUC(g(x))}\right) = \alpha \left(1 - \frac{\int_1^n f(x)\,\mathrm{d}x}{\int_1^n g(x)\,\mathrm{d}x}\right) \quad (1)$$

where α =100, $n = r + s$ with r the number of locations of possible attacks in a generic biometric system and s the number of the retained system overall vulnerabilities (in our case, $r = 8$ and $s = 3$); f(x) is the curve resulting from the set of risk factors retained from the n points (the maximal risk factor is retained from each point); and g(x) is the curve resulting from a set of the highest risk factors we can have from each point (according to our model, they are equal to

100). The use of the security index in comparing and evaluating biometric systems is used as follows: the more the index is near 100%, the better is the robustness of the target system against attacks.

4. Common threats and vulnerabilities of biometric systems

We present in this section a synopsis of the database of common threats and vulnerabilities of biometric systems. The presented database is collected due to the results of desk research, and take into account the known threats presented in previous works (such as those presented in [2, 10]). The database followed also the concerns and the recommendations presented by the International Organization for Standardization ISO/IEC FCD 19792. Our main objective here is to present an enhanced and unified knowledge base of threats and vulnerabilities to be used by the community in biometrics. We present in Section 4.1 a synopsis (one threat per point as an illustration) of the threats of a generic biometric system, while in Section 4.2 the retained system overall vulnerabilities.

4.1. System threats

The presented threats are related to the locations of possible attacks in a generic biometric system as illustrated in Figure 1. Each threat is presented as the following form: "Description" (D) which define the threat, and "Affect" (A) describes which couples (*security requirement* on *asset*) will be affected in the case of a successful attack. This representation allows us to compute the risk factor of each identified threat during the evaluation process (see Section 3.3.1). In other words, the "Affect" information permits us to compute the "Impact" criterion ($\mathbf{f}_1$) of each identified threat according to the security requirements presented in Section 3.2. The on-line platform contains a total of 19 threats, the number of threats on each identified point is given between two brackets.

Point 1. Sensor (6)

$\mathbf{A}_{11}$

- D: The attacker presents a fake biometric data to the sensor (*e.g.*, prosthetic fingers created out of latex). Such kind of attack is known by spoofing.
- A: Authenticity on I_DECISION.

Points 2 and 4. Transmission channels (5)

$\mathbf{A}_{241}$

- D: The attacker intercepts an authorized biometric sample from a communication channel in order to be replayed (replay attack), bypassing the biometric sensor, at another time for gaining access.
- A: Confidentiality on I_DATA_BIO; Authenticity on I_DECISION.

Points 3 and 5. Software components (1)

$\mathbf{A}_{351}$

- D: Biometric system components may be replaced with a Trojan horse program that functions according to its designers' specifications.
- A: Confidentiality on I_DATA_BIO; Confidentiality on I_TEMPLATE; Availability on F_EXTRACTION; Availability on F_MATCHER.

Point 6. Template database (2)

$\mathbf{A}_{61}$

- D: The attacker illegally reads the biometric templates.
- A: Confidentiality on I_TEMPLATE; Authenticity on I_DECISION.

Point 7. Transmission channel (3)

$\mathbf{A}_{71}$

- D: The attacker reads biometric templates from a communication channel in order to be replayed (replay attack).
- A: Confidentiality on I_TEMPLATE; Authenticity on I_DECISION.

Point 8. Transmission channel (2)

$\mathbf{A}_{81}$

- D: The attacker alters the transported information (yes or no) in order to deny access of a legitimate user, or even allow access to an impostor.
- A: Integrity on I_DECISION; Authenticity on I_DECISION.

4.2. System overall vulnerabilities

Point 9. Performance limitations

By contrast to traditional authentication methods based on "what we know" or "what we own" (0% comparison error), biometric systems are subject to errors such as False Acceptance Rate (FAR) and False Rejection Rate (FRR). This inaccuracy illustrated by statistical rates would have potential implications regarding the level of security provided by a biometric system. Doddington *et al.* [11] assigns users into four categories: sheep, lambs, goats and wolves. The sheep correspond to users who are easily recognized (contribute to a low FRR). The lambs correspond to users who are easy to imitate (contribute to a high FAR). The goats represent users who are difficult to recognize (contribute to a high FRR). The wolves represent users who have the capability to spoof the biometric characteristics of other users (contribute to a high FAR). A poor biometric in terms of performance, may be easily attacked by lambs and wolves users.

Point 10. Quality limitations during the enrollment process

The quality of the acquired biometric samples is considered as an important factor during the enrollment process. It is a generic organizational point of view in the deployment of the biometric system. The absence of a quality test increases the possibility of enrolling authorized users with

weak templates. Such templates increase the probability of success of zero-effort impostor, hill-climbing and brute force attempts [12].

Point 11. Protection schemes of the biometric templates database
The use of biometric systems presents concerns in terms of privacy. The fact of storing biometric data in a central database is considered as a violation of civil liberties. Biometric template security is becoming a major concern in biometrics field since, unlike traditional systems (*e.g.*, password-based solutions), compromised templates cannot be revoked and reissued.

5. Security tool

5.1. Overview and key benefits

The aim of the presented security platform is twofold. First, it provides biometrics community an assessment tool towards the security evaluation of biometric systems. As argued before, such kind of tool should be used by an independent party in order to avoid biased assessment results. Second, it aims to enhance the presented database of common threats and vulnerabilities of biometric systems based on researchers feedbacks. Such kind of databases is useful since it could be exploited by the evaluators in other (quantitative or qualitative) assessment methods. A snapshot of the tool is given in Figure 2.

Figure 2. A snapshot of the on-line evaluation platform

5.2. Architecture and functionality

The security evaluation platform provides three levels of users: evaluator, contributor and administrator level. The *evaluator level*, allows researchers to easily assess their developed systems using the on-line evaluation platform. The *contributor level*, provides the contributors dedicated pages to send to us their suggestions and recommendations in order to enhance the platform. It mainly concerns their feedbacks towards enhancing the presented database (*e.g.*, adding new threats) and the implemented security assessment method. The *administrator level*, allows us to manage and to keep up-to-date the on-line platform (the presented database, risk assessment method, ergonomic interface) based on contributors feedbacks. The platform functionalities are defined as follows: In order to use the platform, a user account (login & password) is created. Then, the user chooses the modality of its target system. After choosing the modality, a list of questions for the identified threats and a set of rules for the system overall vulnerabilities (Sections 4.1 and 4.2, respectively) is presented related to the chosen modality. For the list of requested questions, the evaluator has to rate each question according to a ten-point Likert-type scale. This representation allows us to compute the "Easiness" criterion ($\mathbf{f}_2$) of each identified threat. For the "Impact" criterion ($\mathbf{f}_1$), it is automatically rated and managed by the platform according to the security requirements presented in Section 3.2. In the presented method, we have more penalized the identified threats affecting the "confidentiality" security requirement factor, since it is related to the privacy issues of the legitimate users. After rating all the requested questions, the result of the security analysis is displayed on a dedicated webpage, or even downloadable as a PDF result file (or latex file). The result file contains a description of the possible threats and vulnerabilities of the target system, a radar presentation of the highest risk factor obtained on each assessment point (according to our model, 11 assessment points), and the security index illustrating the overall system robustness of the target system against attacks. An example of the use of the presented platform on a keystroke dynamics system [13] is presented Section 5.3. In addition, the common database of threats and vulnerabilities is also downloadable as a file, which allow researchers to analyze their systems using other security assessment methods (quantitative or qualitative).

5.3. Practical results

A keystroke dynamics system [13] has been evaluated using the presented security evaluation platform. Table 3 presents the security analysis of the target system. For the "Impact" and "Easiness" criteria ($\mathbf{f}_1$ and $\mathbf{f}_2$, respectively), we have put the symbol "-" in the last three lines since the corresponding risk factors are computed according to the set of rules presented in Table 2. For the sensor assessment (point 1), we have identified three threats such as A_{16} threat defined by:
- D: The attacker physically destroy the biometric sensor.
- A: Availability on M_SENSOR.

For this threat, the "Impact" criterion ($\mathbf{f}_1$) is automatically rated by the platform to the value 2 since such kind of threat does not affect the "confidentiality" property. For the

"Easiness" criterion ($\mathbf{f}_2$), we have rated (using the ten-point Likert-type scale) at 10, since there is no physical protection of the keyboard. Using the computed risk factors and Equation 1, the security index of the target system is equals to 56.7%. This index shows that the target system is vulnerable against attacks. In addition to this index, the comparison of biometric systems should take into account the 11 assessment points in order to achieve a better comparison accuracy. This comparison may be easily done by a radar presentation which compares the highest risk factor of each assessment point.

Point	Attack	C	I	D	A	f_1	f_2	Risk
1	A_{14}				×	6	2	12
	A_{16}			×		2	10	20
	A_{15}	×			×	8	3	24
2	A_{245}			×		2	6	12
	A_{243}		×			2	6	12
	A_{242}			×		2	10	20
	A_{244}				×	6	4	24
	A_{241}	×			×	8	6	48
3	A_{351}	×		×		8	6	48
5	A_{351}	×		×		8	6	48
6	A_{62}		×	×		8	4	32
	A_{61}	×			×	8	6	48
7	A_{72}		×			2	6	12
	A_{73}			×		2	10	20
	A_{71}	×			×	8	6	48
8	A_{82}			×		2	10	20
	A_{81}		×		×	6	6	36
9	Performance				×	-	-	35.02
10	Multiple captures without quality assessment				×	-	-	60
11	Insecure database and central storage	×	×	×	×	-	-	100

Table 3. Security analysis of the target system

6. Conclusion and perspectives

The evaluation of biometric systems is a major challenge in biometric research field. Despite the existing evaluation works (databases, competitions and platforms), few are the works dedicated to the security evaluation of biometric systems. Moreover, none platform exists towards the security evaluation of such systems. Nowadays, the security evaluation is considered as a complicated task since the number of actors involved (users behavior, softwares and hardwares) within the biometric process is important. However, an agreed security tool to the security evaluation of biometric systems would be important in order to quantify the benefits of new systems. Towards this goal, we have presented in this paper an on-line evolutive platform to the security evaluation of biometric systems. The platform implements a quantitative-based security assessment method to allow easily the evaluation and comparison of biometric systems. We have also presented a database of common threats and vulnerabilities of biometric systems which may be used by other researchers to quantify their developed systems in a quantitative or qualitative way. We have shown the benefits of the presented platform using a keystroke dynamics system.

For the perspective, many works should be done in order to enhance the presented database of common threats and vulnerabilities of biometric systems (which is one of the main utility of the on-line platform). A list of countermeasures for each modality would be identified to the risk reduction purpose. Finally, the main inconvenience of the presented platform is that it is based on evaluator estimation to compute the "Easiness" criterion ($\mathbf{f}_2$). Hence, it would be useful that the estimation of this criterion to be done automatically by the platform.

References

[1] N. K. Ratha, J. H. Connell, and R. M. Bolle, "An analysis of minutiae matching strength," in *Audio- and Video-Based Biometric Person Authentication*, pp. 223–228, 2001.

[2] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, *Handbook of Fingerprint Recognition*. Springer-Verlag, 2003.

[3] ISO/IEC FCD 19792, "Information technology – security techniques – security evaluation of biometrics," 2008.

[4] C. Dimitriadis and D. Polemi, "Application of multi-criteria analysis for the creation of a risk assessment knowledgebase for biometric systems," in *international conference on biometric authentication (ICB)*, vol. 3072, pp. 724–730, 2004.

[5] B. Schneier, "Attack trees," *Dr. Dobb's Journ. of Softw. Tools*, 1999.

[6] V. Matyás and Z. Ríha, "Biometric authentication - security and usability," in *Proceedings of the IFIP TC6/TC11 Sixth Joint Working Conference on Communications and Multimedia Security*, pp. 227–239, 2002.

[7] "Expression des besoins et identification des objectifs de sécurité (EBIOS)," tech. rep., L'Agence nationale de la scurit des systmes d'information (ANSSI), 2004.

[8] A. Rot, "IT risk assessment: Quantitative and qualitative approach," in *the World Congress on Engineering and Computer Science (WCECS)*, pp. 1–6, 2008.

[9] J. Ashbourn, "Vulnerability with regard to biometric systems." http://www.eetimes.com/, 2010.

[10] C. Roberts, "Biometric attack vectors and defences," *Computers & Security*, 2007.

[11] G. Doddington, W. Liggett, A. Martin, M. Przybocki, and D. Reynolds, "Sheep, goats, lambs and wolves: A statistical analysis of speaker performance in the NIST 1998 speaker recognition evaluation," in *International Conference on Spoken Language Processing (ICSLP)*, pp. 1–4, 1998.

[12] U. Uludag and A. K. Jain, "Attacks on biometric systems: A case study in fingerprints," in *Proc. SPIE-EI 2004, Security, Seganography and Watermarking of Multimedia Contents VI*, vol. 5306, pp. 622–633, 2004.

[13] R. Giot, M. E. Abed, and C. Rosenberger, "Greyc keystroke : a benchmark for keystroke dynamics biometric systems," in *IEEE Third International Conference on Biometrics : Theory, Applications and Systems (BTAS)*, pp. 1–6, 2009.