Towards the Security Evaluation of Biometric Authentication Systems

Mohamad El-Abed, Romain Giot, Baptiste Hemery, Christophe Rosenberger, Jean-Jacques Schwartzmann

Towards the Security Evaluation of Biometric Authentication Systems

Mohamad El-Abed, Romain Giot, Baptiste Hemery and Christophe Rosenberger
GREYC Laboratory
ENSICAEN – University of CAEN - CNRS
Caen, France
{mohamad.elabed, romain.giot, baptiste.hemery, christophe.rosenberger} @greyc.ensicaen.fr

Jean-Jacques Schwartzmann
Orange Labs
Caen, France
jeanjacques.schwartzmann@orange-ftgroup.com

***Abstract*—Despite the obvious advantages of biometric authentication systems over traditional security ones (based on tokens or passwords), they are vulnerable to attacks which may considerably decrease their security. In order to contribute in resolving such problematic, we propose a modality-independent evaluation methodology for the security evaluation of biometric systems. It is based on the use of a database of common threats and vulnerabilities of biometric systems, and the notion of risk factor. The proposed methodology produces a security index which characterizes the overall security level of biometric systems. We have applied it on two different biometric systems (one research laboratory implementation of keystroke dynamics and a commercial system for physical access control using fingerprints) for clarifying its benefits.**

Keywords- Biometrics; security evaluation; threat; vulnerability; risk factor.

I. INTRODUCTION

Biometric-based authentication methods constitute one of the most promising candidate for either replacing or enhancing traditional methods based on secret (*e.g.*, password) and/or token (*e.g.*, card). They have many applications [1]: border control, e-commerce… The main benefits of this technology [2] are to provide a better security and to facilitate the authentication process for a user. In spite of their numerous advantages, biometric systems present several drawbacks which may considerably decrease their security.

Ratha *et al.* [3] have identified eight possible attack points to biometric authentication systems as illustrated in Figure 2 (points 1 to 8): 1) involves presenting a fake biometric data to the sensor such as a dummy finger; 2) in a replay attack, an intercepted biometric data is submitted to the feature extractor bypassing the sensor; 3) the feature extractor is replaced with a Trojan horse program that functions according to its designer specifications; 4) in the fourth type of attack, genuine extracted features are replaced with other features selected by the attacker; 5) the matcher is replaced with a Trojan horse program; 6) involves attacks on the template database; 7) the templates can be altered or stolen during the transmission between the template database and the matcher; and 8) the matcher result (accept or reject) can be overridden by the attacker. Schneier [4] compares traditional security systems with biometric systems. The study presents several drawbacks of biometric systems including: i) the lack of secrecy: everybody knows our biometric traits such as iris and ii) the fact that a biometric trait cannot be replaced if it is compromised. Matloni *et al.* [5] described typical threats of a generic biometric authentication application: i) circumvention: an attacker gains access to a part of the system protected by the authentication application. In this case, the attacker may manipulate the data or even read them in an illegal way (*e.g.*, medical records of other users); ii) repudiation: a legitimate user may deny accessing the system. For example, a bank clerk modifies the financial records and later claims that his biometric data was stolen and denies that he is responsible; iii) contamination: an attacker illegally obtains biometric data of a genuine user and uses it to access the system (*e.g.*, lifting a latent fingerprint from a material surface); iv) collusion: a user having high privileges (*e.g.*, system administrator) illegally modifies system policy and rules and v) coercion: an attacker forces a legitimate user to access the system (*e.g.*, using iris to access ATM at a gunpoint). Moreover, as biometrics technology becomes more widely used in our daily life, the incentives of its misuse or attack will grow. Therefore, it is important that biometric systems be designed to withstand different sources of attacks on the system when employed in security-critical applications. Towards this goal, we propose in this paper a modality-independent evaluation methodology for the security evaluation of biometric systems. It is based on the use of a database of common threats and vulnerabilities resulting to the results of desk research and laboratory testing [6] [7]. The proposed methodology produces a security index which characterizes the overall security level of biometric systems. Such kind of evaluation is beneficial, since it allows easily (*i.e.*, in a quantitative way) to compare the security level of biometric systems.

The outline of the paper would be as follows. We present related previous research on security evaluation of biometrics in section II. Section III details the proposed method and the computation of the associated security

index. We present in section IV an illustration of the developed method on two different biometric systems (a research keystroke dynamics system and a commercial fingerprint embedded system). Section V gives a conclusion and some perspectives of this work.

II. BACKGROUND

The security evaluation of biometric systems is receiving more and more attention in biometrics community. The international standard ISO/IEC FCD 19792 [8] addresses the aspects of security evaluation of such systems. The report presents an overview of biometric systems vulnerabilities. In addition to the threats presented by Maltoni *et al.* [5], the report addresses a threat related to system performance and the quality of the acquired biometric characteristics during the enrollment. For example, a system having a high False Acceptance Rate (FAR), may be attacked by presenting several impostor attempts. If low images are accepted during the enrollment then the attacker may hope to break the system as in the case of noisy images. The report also argues that privacy issues (*e.g.*, access to the stored templates) should be taking into account within the evaluation process. The Common Criteria Biometric Evaluation Working Group [9] presents 15 threats that may need to be considered when evaluating biometric systems for vulnerabilities. Dimitriadis *et al.* [10] present a study for evaluating the security level of an access control system for stadiums based on biometric technologies. They present a list of 12 vulnerabilities of biometric systems. Their method quantifies a risk factor to each vulnerability. However, other threats and vulnerabilities should be take into account nowadays in order to enhance the reliability of the assessment method. Attack tree technique introduced by Schneier [11], 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. An example of its use for the security evaluation of fingerprint recognition systems is presented by Henniger *et al.* [12]. Matyás *et al.* [13] propose a security classification of biometric systems along similar lines to Common Criteria [9] and FIPS 140-1/2 [14]. 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

Existing works (such as Uludag *et al.* [2]) show the vulnerabilities of biometric systems which can considerably decrease their security. In order to be used in a reliable context, the security evaluation of biometric systems should be carefully taken into account when designing such systems. Jain *et al.* [1] categorize the fundamental barriers in biometrics into four main categories: (i) accuracy in terms of errors, (ii) usability in terms of acceptance, and (iii) security. On the other hand, the state-of-the-art shows that only few partial security analysis studies with relation to biometric authentication systems exist. Also, recently addressed vulnerabilities and threats [8] [15] should also be taken into account within the evaluation process. In order to contribute in enhancing the security evaluation of biometric systems, we propose a modality-independent evaluation methodology for the security evaluation of such systems. It is based on the use of a database of common threats and vulnerabilities of biometric systems resulting to the results of desk research and laboratory testing [6] [7], and the notion of risk factor. The proposed method produces a security index (between 0 and 100) for the overall system, which allows easily the comparison of biometric systems in term of security.

III. DEVELOPED METHOD

The security evaluation of biometric systems is generally divided into two complementary assessments [8]: 1) assessment of the biometric system (devices and algorithms) and 2) assessment of the environmental (for example, is the system is used indoor or outdoor?) and operational conditions (for example, tasks done by system administrators to ensure that the claimed identities during enrolment of the users are valid). The objective of this work is to define a type 1 assessment method for the security evaluation of biometric systems. We intend to develop a generic approach (*i.e.*, modality-independent) for quantifying the security level of a biometric system. The proposed methodology principle is illustrated in Figure 1: It takes the characteristics/architecture of a biometric system and produces, using a black box, a security index between 0 and 100 (the highest score 100 corresponds to a particularly unsecure system). The black box process works as follows: using a list of common threats/vulnerabilities and three predefined criteria (section III-B), a risk identification process is deployed in order to identify the list of threats and vulnerabilities of the intended biometric system. The security index of the system is then computed using its calculated risk factors.

The rest of this section is organized as follows. We present in section A the list of common threats and vulnerabilities of a generic biometric system. Section B presents the risk identification process deployed in order to produce a list of risks of the intended biometric system, and section C presents the security index computation of the intended system.

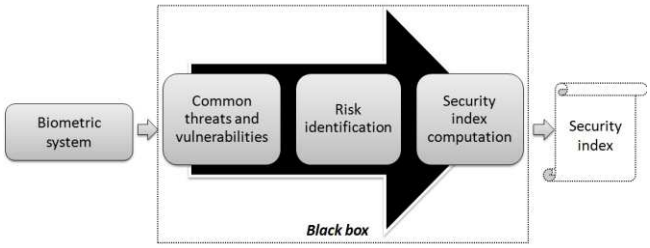

Figure 1. Methodology principle.

A. *Common threats and vulnerabilities of biometric systems*

We intend in this section to give a list of common threats and vulnerabilities of a generic biometric system. The proposed list was created to the results of desk research. It also noted threats and vulnerabilities that we found it valuable when collecting the GREYC-Kesytroke database [6], and during the usability study [7] of biometric systems. The list is based on an extended model to Ratha *et al.* [3] model as illustrated in Figure 2, and it is divided into two sets:

1) *Set I Architecture threats*

- **Sensor (location 1)**
  - Attacker presents a fake biometric data to the sensor (*e.g.*, prosthetic fingers created out of latex). Such kind of attack is called spoofing;
  - Attacker exploits the similarity due to blood relationship to gain access (*e.g.*, case of identical twins and biometric systems using specific modalities such as face and DNA);
  - Authorized users willingly provide their biometric sample to attacker;
  - Attacker provides own biometric sample as a zero-effort attempt to impersonate an authorized user;
  - Attacker modifies its own behavior (*e.g.*, voice) or physiology (*e.g.*, fingerprint) to impersonate a selected weak biometric template;
  - Attacker exploits a residual biometric image left on the sensor to impersonate the last authorized user.
- **Communication links (locations 2 and 4)**
  - Attacker reads an authorized biometric sample from a communication channel;
  - 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;
  - Attacker cuts the communication link in order to make the system unavailable to its intended authorized users (Denial of Service attack);
  - Attacker alters the transported information from a communication channel (Denial of Service attack);
  - Attacker attempts continuously to enter the system (known as hill-climbing attack), the input image/template is conveniently modified until a desired matching score is attained. The attempts are made, by injecting samples on the communication link, to the feature extractor input (image) [16] or the matcher input (template) [2].
- **Template database (location 6)**
  - Attacker modifies (adding/replacing) biometric templates from storage;
  - Attacker deletes biometric templates from storage;
  - Attacker steals the template database.
- **Communication link (location 7)**
  - Attacker reads biometric templates from a communication channel;
  - Attacker alters the transported information from a communication channel (Denial of Service attack).
- **Software modules (locations 3, 5 and 8)**
  - Biometric system components may be replaced with a Trojan horse program that functions according to its designers' specifications.

2) *Set II System overall vulnerabilities*

- **Performance limitations (point 9)**

By contrast to traditional authentication methods based on "what we know" or "what we own" (0% comparison error), biometric systems is 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.* [17] assigns users into four categories: i) sheep: users who are recognized easily (contribute to a low FRR) ii) lambs: users who are easy to imitate (contribute to a high FAR), iii) goats: users who are difficult to recognize (contribute to a high FRR) and iv) wolves: users who have the capability to spoof the biometric characteristics of other users (contribute to a high FAR). A poor biometric in term of performance, may be easily attacked by lambs, goats and wolves users. Therefore, it is important to take into consideration system performance within the evaluation process. To do so, we use the Half Total Error Rate (HTER) as a performance measure of the system. It is defined as:

$$HTER = \frac{FAR + FRR}{2} \qquad (1)$$

➢ **Quality limitations during enrollment (point 10)**

The quality of the acquired biometric samples is considered as an important factor during the enrollment process. 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 [2]. Therefore, we added this measure in the computation of the security index.

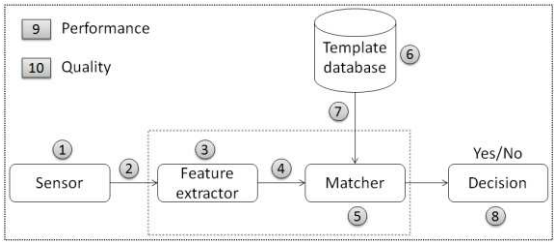

Figure 2. Proposed model (extended to Ratha *et al.* model [3]): vulnerability points in a general biometric system.

B. Risk identification

Risk identification is considered as a significant step towards the design of useful information technology systems. The objective of risk identification [18] is to identify risks that could affect the functionality of the intended biometric system. This step depends on the risk methodologies used. Most of the existing methods rely on the combination on knowledge extracted from questionnaires and interviews [19] [20]. Others [10] [21], use predefined risk factors for each identified vulnerability, based on the estimation of experts who studied the likelihood of occurrence of vulnerability exploits. A risk factor, for each identified threat and vulnerability, is considered as an indicator of its importance. According to the proposed model illustrated in Figure 2, the risk factors are calculated as follows:

1) Risk factors computation of the identified threats

In order to calculate the risk factor of each identified threat, we use a quantitative approach inspired from the Multi-Criteria Analysis (MCA) [22]. More specifically, we use three criteria to compute the risk factor of each identified threat (*risk score*=C_1*C_2*C_3):

- Effectiveness (C_1): represents the impact of the attack in term of criticality. It is defined between 0 and 10 (the highest score 10 corresponds to a heavy/danger attack);
- Easiness (C_2): represents the difficulty to exploit the vulnerability and make a successful attack. It is defined between 0 and 10 (0 corresponds to an impossible attack and the highest score 10 corresponds to an easy attack);
- Cheapness (C_3): represents the cost in terms of specific equipment required to make an attack. It is defined between 0 and 10 (the highest score 10 represents the lowest cost).

For each identified threat, the three predefined criteria are rated subjectively. An example of subjective-based rating is used in the security assessment tool COBRA [21], which rates its predefined criteria based on the estimation of experts who studied the likelihood of occurrence of vulnerability exploits.

2) Risk factors computation of system overall vulnerabilities

Table I illustrates a general scheme for the risk computation of system overall vulnerabilities (Section III-A set 2). For the system performance, we multiply by 2 since a biometric system providing a HTER more than or equal to 50% is not considered as important (for such systems, we put its risk factor to 1000). For the quality, we define four rules according to whether the system implements quality checks during the enrollment step.

C. Security index computation

The overall security level of a biometric system, is typically made up of several areas of variable risk. If any of these areas are omitting 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 of such systems [23]. In order to produce a security index for a biometric system, we use the notion of the Area Under Curve (AUC) of the curve resulting from the retained risk factors. It is calculated using the trapezoid rule. The main benefit of using this approach is it permits to take into account all vulnerabilities of a biometric system and their relationships in the processing chain. The security index is then defined as follows:

$$\frac{AUC\ (f(x))}{AUC\ (g(x))} * 100 = \frac{\int_1^n f(x)\,dx}{\int_1^n g(x)\,dx} * 100 \qquad (2)$$

where n = number of locations (according to our model, n is equal to 10); f (x) is the curve resulting from a set of risk factors retained from each location (the maximal risk factor is retained from each location); and g (x) is the curve resulting from a set of the highest risk factors we can have from each location (according to our model, they are equal to 1000).

IV. EXPERIMENTAL RESULTS

We have applied the proposed method on two different biometric systems. The first one is a keystroke dynamics application developed in our research laboratory [6]. The second one is a commercial fingerprint lock to manage physical access to the development room in our laboratory. The architecture and the main characteristics of the *keystroke dynamics system* are:

- The system implements a score-based method as presented in [24]. The system provides a Half Total Error Rate (HTER) equal to 10.1%;
- System architecture is not distributed (all system's components including template database are implemented within the same PC);
- There is no data protection neither encryption schemes applied on the template database;
- There is no quality check during enrollment phase;
- The PC used is connected to the Internet.

The architecture and the main characteristics of the *fingerprint lock system* are:

- The system provides a FAR of 0.0001% and a FRR of 0.1%. We believe, after a period of use (1 year), that these rates are optimistic (especially the FRR). Nevertheless, we did not modify them since this is not the main interest of the paper. The Half Total Error Rate (HTER) is then equal to 0.05%;
- There is no data protection neither encryption schemes applied on the template database, but it is physically protected;
- System architecture is not distributed (all system components including template database are implemented within the same material);
- The material is not connected to the Internet and there is no USB port;
- There is no quality check during enrollment phase;
- The material power supply is 4 * 1.5V AA batteries with a life span of 1-2 years.

Tables II and III represent an analysis of the keystroke dynamics and fingerprint lock systems, respectively. We put the mark "x" in the last two lines of both tables, since the risk factors of system overall vulnerabilities are not computed using the three predefined criteria (*i.e.*, they are computed according to the set of rules presented in Table I). The risk factors are computed subjectively according to the results of desk research and laboratory testing. For example, the three criteria for the "presentation of prosthetic fingers" threat to fingerprint lock system (table III, point 1) are subjectively rated as follows: for effectiveness criteria, we put 10 since if the attacker succeeds in presenting a fake finger, he will be allowed to access the room that contains costly materials; for easiness criteria, we put 8 since the system has a low FAR rate (we did not put lowest than 8 since the sensor does not integrate any module to detect fake fingers); for cheapness criteria, we put 9 since the materials/products required to make a fake are cheap. However, the evaluator may rates differently these criteria according to the intended system and its context of use. Figure 3 illustrates a comparative study (of the maximal value of risk factor at each location) between both systems. However, the evaluator may also compare other factors such as number of threats at location *i*. From Figure 3, we can conclude several results such as: fingerprint lock system is much more vulnerable at location 1 than the keystroke dynamics system, keystroke dynamics system is much more vulnerable at locations 2, 3, 5, 6, 7, 8 and 9 than fingerprint lock system, both systems are not vulnerable at location 4. Using equation 2, the security index (total risk) of keystroke dynamics system is equal to (47.91%), while for the fingerprint lock system it is equal to (7.34%). These security indexes show clearly that the overall security of keystroke system is less important than the fingerprint lock system against attacks. Because the fingerprint lock system is a black box, we cannot say a lot of things for different locations. Even if we have not presented security problems for these locations, an attacker could be able to find them, thanks to reverse engineering (hardware and software). However, the use of the commercial system in this study was taken as an illustration case for the comparison. More generally speaking, during the security evaluation process of an IT system, system designers should provide all the details/characteristics of the intended system for the evaluators.

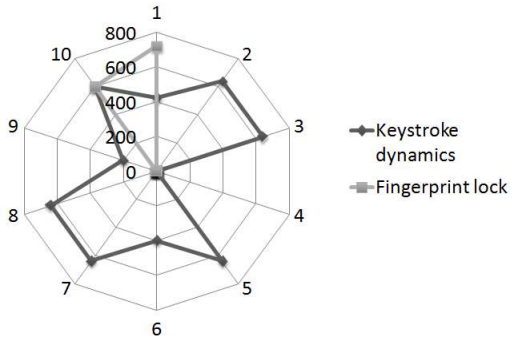

Figure 3. A comparative illustration of both systems among the 10 tested points in our model.

V. CONCLUSION AND PERSPECTIVES

The security evaluation of biometric systems is considered as an important factor to take into account when designing and evaluating them. Nowadays, such kind of evaluation is considered as a complicated task since the number of actors involved within the process is important. However, an

agreed methodology for illustrating the overall system security of a biometric system by an index would facilitate the evaluation of such systems [23]. Towards this goal, we present in this paper a modality-independent evaluation methodology for the security evaluation of biometric systems. It uses a database of common threats and vulnerabilities of biometric systems resulting to the results of desk research and laboratory testing [6] [7], and the notion of risk factor. The proposed method produces a security index (between 0 and 100, the highest score 100 corresponds to an unsecure system) which allows easily to compare the security level of biometric systems. We have applied it on two different biometric systems (the first one is based on morphological analysis and the other one on behavioral analysis) for clarifying its benefits.

For the perspectives, many efforts should be more done in order to extend the presented database of threats and vulnerabilities of a generic biometric system. We believe that this step is indispensable in order to take into account the future (*e.g.*, new modalities) biometric systems, and the new threats that will be identified by researchers and hackers. We intend to develop a web-based software embedding the known threats and vulnerabilities for each biometric modality that would be used for the scientific community. A list of countermeasures (such as liveness detection, cryptographic storage and transport…), for each modality, will be also embedded for risk reduction. In addition, the proposed method quantifies the biometric system (devices and algorithms) without taking into account the environmental and operational conditions of a biometric system. Therefore, we intend also to work on this complementary evaluation part.

TERMS AND DEFINITIONS

Attacker: The agent causing an attack (not necessarily human).
Vulnerability: A weakness in the system that can be exploited to violate its intended behavior.
Threat: A potential event that could compromise the security integrity of the system.
Enrollment: The process of collecting biometric samples from a person and the subsequent preparation and storage of biometric reference templates representing that person's identity.
False Acceptance Rate (FAR): Rate at which an impostor is accepted by an authentication system.
False Rejection Rate (FRR): Rate at which the authorized user is rejected from the system.
Half Total Error Rate (HTER): This error rate corresponds to the average of both FAR and FRR error rates.

ACKNOWLEDGMENT

The authors would like to thank the French Research Ministry for their financial support of this work.

REFERENCES

[1] A. K. Jain, S. Pankanti, S. Prabhakar, L. Hong, and A. Ross, "Biometrics: A grand challenge," *Pattern Recognition, International Conference*, 2004.
[2] 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*, 2004.
[3] N. K. Ratha, J. H. Connell, and R. M. Bolle, "An analysis of minutiae matching strength," in *Audio- and Video-Based Biometric Person Authentication*, 2001.
[4] B. Schneier, "Inside risks: the uses and abuses of biometrics," *Commun. ACM*, 1999.
[5] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, *Handbook of Fingerprint Recognition*. Springer-Verlag, 2003.
[6] R. Giot, M. El-Abed, and C. Rosenberger, "Greyc keystroke : a benchmark for keystroke dynamics biometric systems," in *BTAS*, 2009.
[7] M. El-Abed, R. Giot, B. Hemery, and C. Rosenberger, "A study of users' acceptance and satisfaction of biometric systems," in *ICCST*, 2010.
[8] "Information technology – security techniques –security evaluation of biometrics," Internation standard ISO/IEC FCD 19792, Tech. Rep., 2008.
[9] "Common criteria for information technology security evaluation," Tech. Rep., 1999.
[10] C. Dimitriadis and D. Polemi, "Application of multi-criteria analysis for the creation of a risk assessment knowledgebase for biometric systems," in *ICB*, 2004.
[11] B. Schneier, "Attack trees," *Dr. Dobb's Journ. of Softw. Tools*, 1999.
[12] O. Henniger, D. Scheuermann, and T. Kniess, "On security evaluation of fingerprint recognition systems," in *Internation Biometric Performance Testing Conference (IBPC)*, 2010.
[13] V. Matyás, Jr. and Z. Riha, "Biometric authentication - security and usability," in *Proceedings of the IFIP TC6/TC11 Sixth Joint Working Conference on Communications and Multimedia Security*, 2002.
[14] "Security requirements for cryptographic modules," National Institute of Standards and Technology (NIST), Tech. Rep., 2001.
[15] F. Abdullayeva, Y. Imamverdiyev, V. Musayev, and J. Wayman, "Analysis of security vulnerabilities in biometric systems," in *The second international Conference: Problems of Cybernetics and Informatics*, 2008.
[16] C. Soutar, "Biometric system security," http://www.bioscrypt.com/assets/security_soutar.pdf.
[17] 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 *ICSLP98*, 1998.
[18] G. Stoneburner, A. Goguen, and A. Feringa, "Risk management guide for information technology system," National Institute of Standards and Technology (NIST), Tech. Rep., 2002.
[19] C. Alberts, A. Dorofee, J. Stevens, and C. Woody, "Introduction to the OCTAVE approach," U.S. Department of Defense, Tech. Rep., 2003.
[20] Z. Yazar, "A qualitative risk analysis and management tool - CRAMM," SANS Institute, Tech. Rep., 2002.
[21] "Consultative, objective and bi-functional risk analysis (cobra)," http://www.security-risk-analysis.com/, 2010.
[22] "Multi-criteria analysis: a manual," Department for Communities and Local Government: London, Tech. Rep., 2009.
[23] J. Ashbourn, "Vulnerability with regard to biometric systems," http://www.eetimes.com/, 2010.
[24] S. Hocquet, J. Ramel, and H. Cardot, "User classification for keystroke dynamics authentication," in *ICB07*, 2007, pp. 531–539.

TABLE I. GENERAL SCHEME OF RISK COMPUTATION FOR THE SYSTEM OVERALL VULNERABILITIES.

Point	Description	Conditions	Risk factor
9	System performance	Sufficient panel of users	2 * 10 * HTER (limited to 1000)
10	Template quality during enrollment	▪ Multiple captures with quality assessment	0
		▪ One capture with quality assessment	400
		▪ Multiple captures without quality assessment	600
		▪ One capture without quality assessment	1000

TABLE II. SECURITY ANALYSIS OF THE KEYSTROKE DYNAMICS APPLICATION.

Point	Description	Effectiveness	Easiness	Cheapness	Risk factor
1	▪ attacker modifies own behavior to impersonate a weak template	10	1	10	100
	▪ zero-effort impostor attempt	10	1	10	100
	▪ artificial generation of key events	10	6	7	420
2	▪ cutting communication link	3	10	10	300
	▪ alteration of the transported key events (DoS)	7	6	8	336
	▪ injecting of key events (hill-climbing and brute-force attacks)	10	6	8	480
	▪ listening then replay of previous key events (events belonging to authorized users)	10	8	8	640
3	▪ modification of program in memory	10	8	8	640
5	▪ modification of program in memory	10	8	8	640
6	▪ reading the SQL database (privacy violation)	3	8	8	192
	▪ modification (suppressing) of the SQL database	8	5	8	320
	▪ modification (adding/replacing) of the SQL database	10	5	8	400
7	▪ listening to the template (privacy violation)	3	8	8	192
	▪ alteration of the transported template (DoS)	7	6	8	336
	▪ injecting of templates (hill-climbing and brute-force attacks)	10	6	8	480
	▪ listening then replay of previous templates	10	8	8	640
8	▪ modification of program in memory	10	8	8	640
9	system performance	X	X	X	202
10	multiple captures without quality assessment	X	X	X	600

TABLE III. SECURITY ANALYSIS OF THE FINGERPRINT LOCK SYSTEM.

Point	Description	Effectiveness	Easiness	Cheapness	Risk factor
1	▪ zero-effort impostor attempt	10	1	10	100
	▪ removing the battery (DoS)	4	8	10	320
	▪ exploitation of the residual biometric image left on the sensor	10	8	8	640
	▪ presentation of prosthetic fingers	10	8	9	720
9	system performance	X	X	X	1
10	multiple captures without quality assessment	X	X	X	600