Risk Analysis of Biometric Systems

Christos K. Dimitriadis[1], Prof. Despina Polemi[2]

[1] Expertnet SA, 244 Kifisias Av., 15231 Athens, Greece

[2] University of Piraeus, 80 A. Dimitriou, 18534 Piraeus, Greece

Abstract: This paper, presents a risk analysis knowledgebase, which aims to enhance existing risk analysis methodologies and tools, by adding the capability of analyzing the risk of the biometric component of an information system. The knowledgebase was created by applying the Multi-Criteria Analysis methodology to the results of research in the security aspect of biometric technologies. The result is a set of vulnerabilities, risk factors and countermeasures for biometric systems.

1 Introduction

A main security weakness of password and token-based authentication mechanisms, is the fact that knowledge, as well as the possession of an item, does not distinguish a person uniquely. Modern biometric technologies provide enhanced security levels by introducing a new dimension in the authentication process called "proof by property". However, the design and deployment of a security architecture incorporating biometric technologies hides many pitfalls, which when underestimated can lead to major security weaknesses. International security standards, such as ISO/IEC 17799, "IT – Code of practice for information security management" and COBIT: "Control Objectives for Information and related Technology", provide the general guidelines and principles for correctly deploying a security architecture, both indicating as a very important aspect, the conduct of risk analysis. Regardless of the risk analysis methodology deployed, it is a common practice to utilize a database of common risks and countermeasures (called knowledgebase) for assuring the effectiveness of the process [4]. Such knowledgebases, are sources of expertise regarding security issues for the various components of information systems, assuring that no risks will be missed and adequate countermeasures will be proposed during the process. Despite the existence of biometric-specific standards and best practices, such as ANSI X9.84 "Biometric Information Management and Security" and Best Practices in Testing and Reporting Performance of Biometric Devices [1], there are no detailed knowledgebases for assisting the risk analysis process, as far as biometrics are concerned.

This paper, presents a risk analysis knowledgebase, which aims to enhance existing risk analysis methodologies and tools, by adding the capability of analyzing the risk of the biometric component of the system. Part of this work is the author's contribution to the EC project BIOSEC [20]. The authors would like to thank the EC for

K. Dimitriadis C. and Polemi D. (2004).
Risk Analysis of Biometric Systems.
In *Proceedings of the 2nd International Workshop on Security in Information Systems*, pages 23-32
DOI: 10.5220/0002650100230032

funding BIOSEC, as well as the BIOSEC partners. The remainder of the paper is organized in the following main sections:

- Methodology (general approach and multi-criteria analysis): Describing the methodology followed for building the knowledgebase.
- Biometric risk analysis Knowledgebase (BK): Containing the knowledgebase of vulnerabilities and risk factors of biometric systems, as well as the countermeasures for risk reduction.

2 Methodology: General Approach

In order to ensure applicability and easy integration of BK, to the widest possible risk analysis methodologies and tools, a general risk analysis model [2][3], which is implemented by most of the standard methodologies, was studied. This model is comprised of the following steps:

1. Asset identification,
2. Threat identification (defining as threat, an event that can potentially cause undesirable effects),
3. Vulnerability identification (defining as vulnerability, a security weakness of the system),
4. Risk identification (defining as risk, the probability that a particular threat will exploit a particular vulnerability),
5. Identification of countermeasures for risk reduction.

The first two steps (asset and threat identification) are covered sufficiently by standard risk analysis methodologies without the need of a specialized BK.

The third step (vulnerability identification) revealed the emerging need for the development of a catalogue of vulnerabilities for biometric systems. The catalogue acted as a foundation stone of BK and was populated by conducting:

- Extensive desk research on known or possible attacks against various biometric technologies
- Penetration tests on biometric systems in a dedicated lab
- Interviews with experts in the field

The forth step (risk identification), depends on the risk analysis methodology. Most standard risk analysis methodologies rely on the combination of existing knowledge with information extracted from questionnaires and interviews [5][6]. Other methodologies and tools [7] utilize predetermined risk scores for each identified vulnerability, based on the estimation of experts who studied the likelihood of occurrence of vulnerability exploits. For the creation of BK, a quantitative approach was chosen, calculating a risk factor for each vulnerability. The risk factor is an indicator of the importance of the vulnerability and the sum of all risk factors provides the total risk factor of the biometric component of the information system under review. In order to calculate the risk factor and provide an objective evaluation of each vulnerability a standard methodology called Multi-Criteria Analysis (MCA) was deployed.

The last step (identification of countermeasures for risk reduction), indicated the need for identifying countermeasures for reducing the risk. The countermeasures

were identified as an extension of the research conducted for identifying vulnerabilities and was also based on the conduct of tests, desk research and interaction with experts in the field of security and biometrics.

The final form of BK, is a set of vulnerabilities followed by the corresponding risk factors and countermeasures. In the case of vulnerabilities, which are applicable to all biometric technologies, common risk factors were calculated. In the opposite case of technology-specific vulnerabilities, individual risk factors were calculated for fingerprint, iris, face and voice biometrics.

3 Methodology: Application of Multi-criteria Analysis (MCA)

Multi-Criteria Analysis (MCA) [8][18] is a method to evaluate different alternatives (currently biometric vulnerabilities) and to determine an order of ranking of these alternatives. MCA takes into account that some specific criteria should be more influential in the determination of the ranking between alternatives. This is accomplished by the attachment of weighing factors to the different criteria. The following MCA steps were followed for evaluating biometric vulnerabilities:

1. Criteria selection: a number of criteria were selected, which were considered as the most important for evaluating vulnerabilities and which influence their probability of occurrence. These are:
- C1: Difficulty to exploit in terms of technical expertise required and complexity.
- C2: Effectiveness (in terms of level of exposure to threats - binding the vulnerability with the threat).
- C3: Cost in terms of special equipment required.

2. Input of the scores: For each vulnerability a score was calculated per criterion. The score was calculated after processing results from the desk research, biometric lab tests and interviews. The scores were based on a common quantitative scale (from 1-10). In more detail:
- C1: The highest score (10) represents the lowest difficulty.
- C2: The highest score (10) represents the highest effectiveness.
- C3: The highest score (10) represents the lowest cost.

3. Attachment of the weighing factors: The next step in the MCA process involved the prioritization of the criteria by the assignment of different rankings or weights. A weighing factor was attached to each criterion, after studying security incidents and attack profiles. The first three steps of MCA are presented in figure 1:

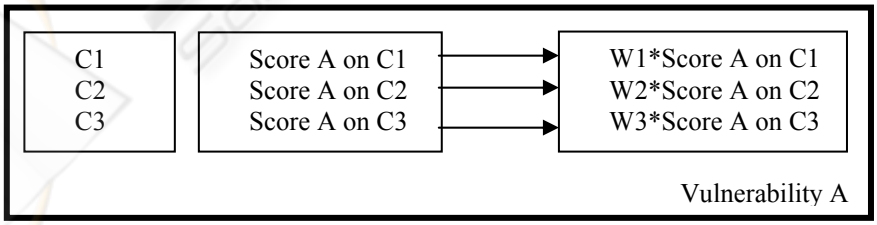

Fig. 1. The first three steps of MCA: criteria *C1*, *C2*, *C3*, *scores* and attached *weighing factors*

4. Ranking of the vulnerabilities: a simple method was deployed - the injunction MCA method. This method multiplies the scores of the criteria with the correspondent weighing factors and calculates for every vulnerability the sum of these products, as shown in the following figure.

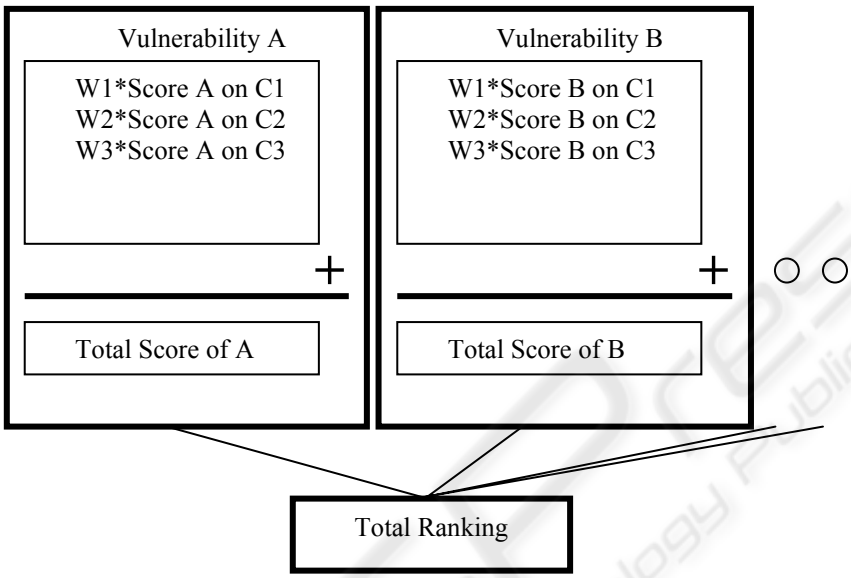

Fig. 2. *Ranking* of *vulnerabilities*. Calculations according to the injunction MCA method

The result is the total score per vulnerability and correspondent ranking. The vulnerability with the highest total score is the highest in ranking and most dangerous.

4 Biometric Risk Analysis Knowledgebase

This section is comprised of two sub-sections. The first one presents the identified vulnerabilities and countermeasures, while the second one presents a comprehensive form of BK, including vulnerabilities, risk factors and countermeasures.

4.1 Description of Vulnerabilities

This sub-section provides a short description of the identified catalogue of vulnerabilities of biometric systems, followed by proposed countermeasures for risk reduction.

- Spoofing – Mimicry – Artefacts: Poor biometric implementations are vulnerable to spoofing and mimicry attacks. An artificial finger made of commercially available

silicon or gelatin, can deceive a fingerprint biometric sensor [9][10]. The procedure for materializing this attack is consisted of three steps. The first step is capturing a fingerprint (e.g. from a glass, a door handle or with the user's consent). The second step is creating the artefact, which is a procedure that lasts from a few hours, to a few days maximum. The final step is using the artefact to access the system. The use of pictures, masks, voice recordings or speech synthesis tools is possible to deceive iris, face, and voice recognition systems. As a countermeasure, it must ensured that vitality detection features, which conduct an extra measurement of one or more attributes, such as the relative dielectric constant, the conductivity, the heartbeat, the temperature, the blood pressure, the detection of vitality under the epidermis, or the spontaneous dilation and constriction of the pupil or eye movement, are integrated in the biometric device. If these features are not present, compensating controls must be applied, such as the deployment of multimodal biometrics (e.g. combination of face and lips movement recognition), or the implementation of interactive techniques (e.g. the request for the user to say a specific phrase, or place 3 fingers in a certain order on the sensor).

- Server side - Fake templates: Server based architectures, where the biometric templates are stored centrally, inherit the vulnerabilities of such systems [14]. A possible attack can be realized when the impostor inserts his template in the system under someone else's name. Distributed architectures (e.g. template storage in a smart card) should be preferred. In that case, the template is stored in a tamper resistant memory module that is write-once and erased or destroyed if its content is altered, resisting to this type of attack. When this scenario is not an option, strong security controls must protect the server, including encryption of the templates, system and network security controls (firewalls, intrusion detection and prevention mechanisms) and a strong security policy followed by detailed procedures based on international standards.
- Communication links: Data could be captured from the communication channel, between the various components of a biometric system [14], such as: the sensor and the feature extractor, the feature extractor and the matching algorithm or the matching algorithm and the application, in order to be replayed at another time for gaining access. This is also called electronic impersonation. An effective countermeasure is the integration of the various parts of the system into a hardware security module, or generally the elimination of the transmission of the biometric template. An example of such a module is the biometric smart card, that has a fingerprint sensor and the matching mechanism embedded in it, confining the template to a secure environment. Similar security levels are addressed in integrated terminal devices, such as PDAs or mobile phones. If this is not an option, challenge and response is another approach for addressing this vulnerability. An additional control is the introduction of a rule to discard a signal when it is identical to the stored template or to the last measurement that was conducted.
- Cross system: The utilization of the template in two or more applications with different security levels (i.e. convenience applications and security applications) tends to equalize these security levels, by decreasing the higher security level to the lower one - if a template is compromised in one application, it can be used for gaining access to the other. A countermeasure, depending on the criticality of the application, is the deployment of custom encoding algorithms in order to ensure

the creation of custom templates per user. Another option is the combination of existing biometric encoding algorithms with one-way hash functions for ensuring that the templates produced for a specific user in the specific system, are unique. In that case, special care should be given to the calibration of the system, because very strong non-invertible functions lower the system's accuracy, due to the fact that the matcher, must deal with the measurement variations, in the transformed space [11]. This feature, also provides the ability of revocation to the system in the case that an impostor compromises a template.

- Component alteration: A possible attack can be realized with a Trojan Horse on the feature extractor, the matching algorithm or the decision algorithm of the system, acting as a manipulator of each component's output. Security controls should be defined, such as write-once memory units that host the feature extraction program and the matching algorithm, as well as the integration of the system to a hardware security module. Additional controls include the development of a strong security policy controlling the operation of the system, in order to protect it from exposure to manipulating attempts.
- Enrolment, administration and system use: Poor enrolment, system administration and system use procedures, expose the biometric system. During the enrolment phase, raw biometric data and biometric templates can be compromised and databases can be altered or filled with imprecise user data. Poor system administration procedures, in addition to the above, might lead to altered system configuration files, with decreased FAR, making false acceptance easier, thus security weaker. Similarly, a user might exceed his/her authority, threatening the system. Detailed procedures for user enrolment, system administration and use should be defined, based on international standards and best practices. Controls should be defined, as extensions of the system's security policy, forcing for example segregation of duties, job rotation procedures, logging facilities, alteration or anomaly detection mechanisms.
- Noise and power loss: Off-limit power fluctuation or flooding of a biometric sensor with noise data - for example flashing light on an optical sensor, changing the temperature or humidity of the fingerprint sensor, spraying materials on the surface of a sensor or vibrating the sensor outside its limits - might cause the biometric device to fail. The design of the security policy, should include those security controls that will make the system environment as controlled as possible. These controls depend on the nature of the application.
- Power and timing analysis: Capturing the power consumption of a chip can reveal the software code running on the chip, even the actual command [12][13]. Simple Power Analysis and Differential Power Analysis techniques are deployed for such purposes and are capable for breaking cryptographic algorithms such as DES, by using statistical software. The same strategy can be followed, for breaking the matching mechanism of the biometric system or revealing the biometric template. The secret key or biometric template will appear as the peaks of a diagram projecting the result of applying the appropriate software to the power consumption measurement. Timing attacks are similar and measure the processing time instead of the power consumption. As countermeasure, it should be ensured that all necessary technology controls are in place. These include the use of micro controllers with lower power consumption and noise generators for power blurring. Regarding tim-

ing attacks, the algorithm and program code have to be designed as time-neutral. These technological countermeasures must be included in the biometric system either it is a smart card based architecture or not.

- Residual characteristic: The residual biometric characteristic of a user on the sensor may be sufficient to allow access to an impostor (e.g. a fingerprint the sensor). The attack is realized on a fingerprint sensor with a residual fingerprint from the previous measurement, by pressing a thin plastic bag of warm water on the sensor, by breathing on the sensor or by using dust with graphite, attaching a tape to the dust and pressing the sensor [14]. The last technique is the most effective one. Even when a specific rule in the login algorithm is in place, for declining the exact same measurement, repositioning the tape to provide a slightly different input would deceive the system. A technology assessment should be conducted. Non-optical types of fingerprint sensors are resistant to this vulnerability. In general, deploying interactive authentication in an adequate control for this type of risk.
- Similar template - Similar characteristics: A user having a similar template or a similar characteristic with a legitimate one, might deceive the system, especially in identification applications, where one to many template comparisons are conducted. The maturity of the encoding algorithm, in terms of producing unique outputs from different inputs, as well the FAR of the biometric device should be studied. For security applications the biometric system should be calibrated in order to have reduced FAR (indicative value FAR<0,001%). The maturity of the algorithm can be assured by the deployment of certified products or independently tested products based on [1].
- Brute force: This type of attack is based on trial and error practices [16][17]. The impostor is attempting continuously to enter the system, by sending incrementally increased matching data to the matching function until a successful score is accomplished. This method is most effective in systems that implement identification rather than verification, since the biometric measurement is compared to a great number of templates, making the system weaker (as the number of users increases), due to the increased probability of the existence of similar templates or characteristics among the population. Biometrics however are more resistant to this attack, than traditional systems, since the impostor has to find a way to insert the trial data to the system, thus combine this vulnerability with one of those described above. As a countermeasure, it should be ensured that traditional controls are in place, such as the automatic locking of the user's account after a specific number of attempts, as well as the application of verification instead of identification if possible.

4.2 Comprehensive Form of BK

MCA, was applied step by step for each identified vulnerability. Criteria C1 (difficulty to exploit) and C3 (cost) were assigned with higher weighing factors (equal to 3) than C2 (effectiveness - weighing factor equal to 1), reflecting the most common attack profiles and following the observation that attackers test vulnerability exploits when they are easy to exploit and inexpensive, considering effectiveness at a latter stage [19].

The results of MCA were transformed to percentages (risk factors). Each risk factor indicates the increase of the risk level, in the case that the vulnerability is applicable to the system under review and no countermeasure is taken to address it. The sum of all risk factors provides the total risk factor of the biometric component of the information system under review. The risk factors were individually produced in the cases of vulnerabilities that were specific for each biometric technology. Null scores are translated to non-applicability of the vulnerability to a specific biometric technology. The vulnerabilities, risk factors and countermeasures comprise the comprehensive form of BK(fingerprint: Fi, iris: Ir, face: Fa, voice: V).

Table 1. : Comprehensive form of BK. *Vulnerabilities*, *risk factors* and *countermeasures*

Vulnerability	**Risk Factor (%)**				**CM No.**
	Fi	Ir	Fa	V	
1. Spoofing – mimicry - artefacts	11	10	12	14	i, ii, iii
2. Server side - Fake templates	16				iv, v
3. Communication links	11				Vi
4. Cross system	9				vii
5. Component alteration	11				iv, vi
6. Enrolment, administration and system use	19				iv
7. Noise and power loss	4	4	4	6	iv
8. Power and timing analysis	4				viii
9. Residual characteristic	7	0	0	0	iii, ix
10. Similar template - Similar characteristics	2	2	6	6	ix, x
11. Brute force (verification applications)	4				xi
Countermeasures					
i. Vitality detection.					
ii. Multimodal architecture.					
iii. Interactive authentication.					
iv. Well-implemented security policy according to standards.					
v. Storage of the template in a secure medium.					
vi. System integration into a hardware security module.					
vii. Custom biometric encoding algorithms – hash functions.					
viii. Noise generators, low power consumption chips and specific software design.					
ix. Technology assessment.					
x. Calibration review.					
xi. Traditional controls - account lock after a number of attempts.					

In order to clarify the figures presented in the table, the calculation of the risk factor for the power and timing analysis vulnerability is presented below as an example:

1. Desk research, tests and interviews, defined timing analysis attacks, as difficult to implement (special expertise is required - score on C1=1), effective (score on C2=8) and expensive also (specific equipment is required - score on C3=1).

2. The scores were multiplied with the weighing factor of each criterion, providing a total score of 14.
3. After calculating the total score for each vulnerability, the maximum total score of all vulnerabilities was calculated - it belonged to the case of voice biometrics.
4. All scores were transformed to percentages of the maximum total score of all vulnerabilities. This action was performed, in order to achieve a maximum of 100% when all vulnerabilities are present and at the same time preserve a common denominator for all vulnerabilities. This resulted the risk factor of the power and timing analysis vulnerability to be 4%.

The role of BK during risk analysis depends on the methodology deployed. The main functions are the identification of those vulnerabilities that are applicable to the system under review, after consulting the vulnerability description sub-section, the calculation of the total risk factor, by adding the percentages of each identified vulnerability, utilizing the comprehensive form of BK and the proposal – implementation of countermeasures for risk reduction.

5 Conclusions

The main conclusions of the research conducted, are the following: Special care should be given to user enrolment, system administration and use, implementing as a mandatory control, concrete security policies and procedures based on international standards. Server-based architectures, where templates are stored centrally, heavily increase the risk level of the system, uncovering the demanding need for encryption and strong intrusion prevention, detection and response countermeasures. Vitality detection was also identified as a demanding need, which can be relatively compensated by interactive authentication techniques or multi-modal biometrics. The restriction of the biometric template to a hardware security module and the elimination of the template submission over communication links and networks, addresses a great number of vulnerabilities and reduces the total risk factor significantly. Horizontal results between the four different biometric technologies were also derived and made visible in the comprehensive form of BK, including the high distinctiveness of fingerprint and iris characteristics, reducing the similar characteristic vulnerability. These results however, are strictly related with security, under the specified criteria and should not be confused with results on biometric system performance, or applicability testing. The conduct of risk analysis is a significant step towards the creation of security architectures, which promote the advantages of biometric systems in a risk-proof manner.

References

1. Wayman, J.L., Mansfield, A.J.: Best practices of testing and reporting performance of biometric devices. http://www.cesg.gov.uk/site/ast/biometrics/media/BestPractice.pdf. (2002)
2. Certified Information Systems Auditor Manual. Information Systems Audit and Control Association (2003)

3. Peltier, T.R.: Information Security Risk Analysis. CRC press LLC USA (2001)
4. King, M., Dalton, C., Osmanoglu, T.: Security Architecture. RSA press USA (2001)
5. Operationally Critical Threat, Asset, and Vulnerability Evaluation method (OCTAVE). http://www.cert.org/octave
6. CCTA Risk Analysis and Management Method (CRAMM). http://www.cramm.com.
7. Consultative, Objective and Bi-functional Risk Analysis (COBRA). http://www.security-risk-analysis.com/introcob.htm
8. Multi-Criteria Analysis manual. http://www.odpm.gov.uk
9. Matsumoto, T., Matsumoto, H., Yamada, K., Hoshino, S.: Impact of artificial fingers on fingerprint systems. Proceedings of SPIE, Vol. 4677. Yokohama (2002)
10. Van der Putte, T., Keuning, J.: Biometrical fingerprint recognition – don't get your fingers burned. IFIP TC8/WG8.8 Fourth Working Conference on Smart Card Research and Advanced Applications. Kluwer Academic Publishers. (2000) 289-303
11. Sudan, M., Jules, A.:A fuzzy Vault Scheme. IEEE Internation Symposium on Information Theory. IEEE Press Lausanne Switzerland (2002) 408
12. Gandolfi, K., Mourtel, C., Olivier, F.: Electromagnetic Analysis: Concrete Results. Lecture Notes in Computer Science, Vol. 2162. Springer-Verlag (2001) 251-261
13. Kocher, P., Jaffe, J., Jun, B.: Introduction to Differential Power Analysis and Related Attacks. http://www.cryptography.com/technology/dpa/DPATechnicalInfo.PDF. (1998)
14. IST-1999-20078 Business environment of biometrics involved in e-commerce. http://expertnet.net.gr/bee (2002)
15. Prabhakar, S., Pankanti, S., Jain, A.: Biometric Recognition Security and Privacy Concerns. IEEE Security and Privacy, March /April (2003) 33-42
16. Bolle, R.M., Connell, J.H., Ratha, N.K.: Biometric perils and patches. Pattern Recognition, Vol. 35, no. 12 (2002) 2727-2738
17. Smith, R.: The biometric Dilemma. Secure Computing (2002)
18. Pardalos, P., Siskos, Y., Zopounidis, C.: Advances in Multicriteria Analysis. Kluwer Academic Publishers Dordrecht Hardbound (1995)
19. Know your enemy series. The Honeynet project. http://www.honeynet.org
20. IST-2002-001766 Biometrics and Security – BIOSEC. http://biosec.tid.es