BEAT

Biometrics Evaluation and Testing

http://www.beat-eu.org/

Funded under the 7th FP (Seventh Framework Programme)

Theme SEC-2011.5.1-1
[Evaluation of identification technologies, including Biometrics]

D4.6: Description of Metrics for the Evaluation of Vulnerabilities to Indirect Attacks

Due date: 28/02/2013 **Submission date:** 27/02/2013
Project start date: 01/03/2012 **Duration:** 48 months
WP Manager: Boris Leidner **Revision:** 1

Author(s): J. Galbally (UAM), J. Fierrez (UAM), Alain Merle (CEA-Leti), Ludovic Merrien (Morpho), Boris Leidner (Tuvit)

Project funded by the European Commission in the 7th Framework Programme (2008-2010)		
Dissemination Level		
PU	Public	Yes
RE	Restricted to a group specified by the consortium (includes Commission Services)	No
CO	Confidential, only for members of the consortium (includes Commission Services)	No

D4.6: Description of Metrics for the Evaluation of Vulnerabilities to Indirect Attacks

Abstract:

The objective of this deliverable is to propose a set of metrics which may enable the security experts to determine, in an objective and reproducible manner, the intrinsic risk posed by a given indirect attack. Furthermore, this group of risk factors, together with the vulnerability evaluation protocol described in the deliverable, are intended to constitute a supporting tool in order to fairly compare the threat represented by the different known indirect attacks identified in D4.2 and categorized according to the different biometric modalities considered in the BEAT project.

Thus, the inventory of known attacks described in D4.2, coherent with the use cases defined in the project (WP2), will serve as the baseline document to determine the set of risk factors (and their associated evaluation protocol) to be taken into account in order to estimate the danger posed by a certain indirect attack.

This deliverable will, in turn, be the starting point to determine an analogue set of metrics for the evaluation of direct attacks (D4.5). Also, the metrics and protocol described in the present deliverable will be of great help for the further development of the ongoing standards regarding the security evaluation of biometric systems (WP6).

It is very important to highlight that the present document focuses strictly on the evaluation of vulnerabilities of the biometric system on its own and not as part of a larger integrated security display where other non-biometric security measures (e.g., guard) specific of a given operational scenario can make certain biometric attacks unfeasible.

Contents

1 Introduction

The performance evaluation of biometric systems addressed in deliverable D3.3, is only one form of biometric testing that can be considered when performing an overall evaluation of a biometric application. Other tests include reliability, vulnerability and security, user acceptance or cost/benefit [17].

In particular, the need for independent, repeatable and consistent security assessment of biometric systems is evidenced by the generation of different security evaluation standards [4, 2, 6], the organization of competitions searching for new countermeasures against attacks [11], and the publication of numerous research works [13, 16, 5]. All these efforts stress the necessity of addressing the vulnerability evaluation of biometric systems from a rigorous and systematic perspective.

Due to the intrinsic statistical nature of biometric recognition, the evaluation of the security threats that affect them should be carried out in a similar fashion to that used in the performance assessment of the systems (see D3.3 for further details on this topic). Determining if a certain indirect attack (e.g., fraudulent access attempt using a hill-climbing attack) is or not feasible is not enough for a vulnerability evaluation. In order to estimate the robustness of a given biometric system to an indirect attack, it should be performed against a sufficiently large number of user accounts so that we may find out, from a statistical point of view and not just on a yes or no basis, *how* vulnerable to the indirect attack at hand is the system being tested.

In this scenario, we propose a set of metrics or risk factors to be considered in the evaluation of biometric systems vulnerabilities to indirect attacks and an associated systematic security evaluation protocol that can be applied regardless of the attack, system, or biometric trait being considered. The protocol includes a set of guidelines for the security analysis and for reporting the final results of the evaluation in a useful and meaningful manner for other researchers, evaluators and developers.

It is very important to highlight that the present document focuses strictly on the evaluation of vulnerabilities of the biometric system on its own and not as part of a larger integrated security display.

This means that, depending on the operating environment (e.g., place, application) where the biometric system will be deployed, certain vulnerabilities may not have to be considered due to the existence of other non-biometric security measures that make the attack unfeasible (e.g., the attacker needs physical access to the biometric system but it is unreachable as it is watched by a number of guards).

These application-specific factors (e.g., accessibility to the biometric system) will not be considered here as they are fully dependent on the operational context.

Ultimately, it is the security evaluator duty to decide which attacks to the biometric system have to be rated for a specific application, and how to take into account in the overall rating of the security system other non-biometric elements.

1.1 Attacks Classification

NOTE: Although an extended version of this section may be found in a similar form in the introduction of D4.2, for completion and in order to generate a self-contained document, we will also include here a brief summary of the basic concepts related to the categorization of attacks to biometric systems. For a more comprehensive description of these concepts we refer the reader to D4.2.

In Fig. 1 a diagram with the attack classification considered in the BEAT project is shown. Attacks that will be analyzed in the present document (indirect attacks) appear in grey. This classification is a result of the considerable effort that has been put over the past few years into the analysis of the possible security breaches that biometric systems may present [14, 1, 12, 3].

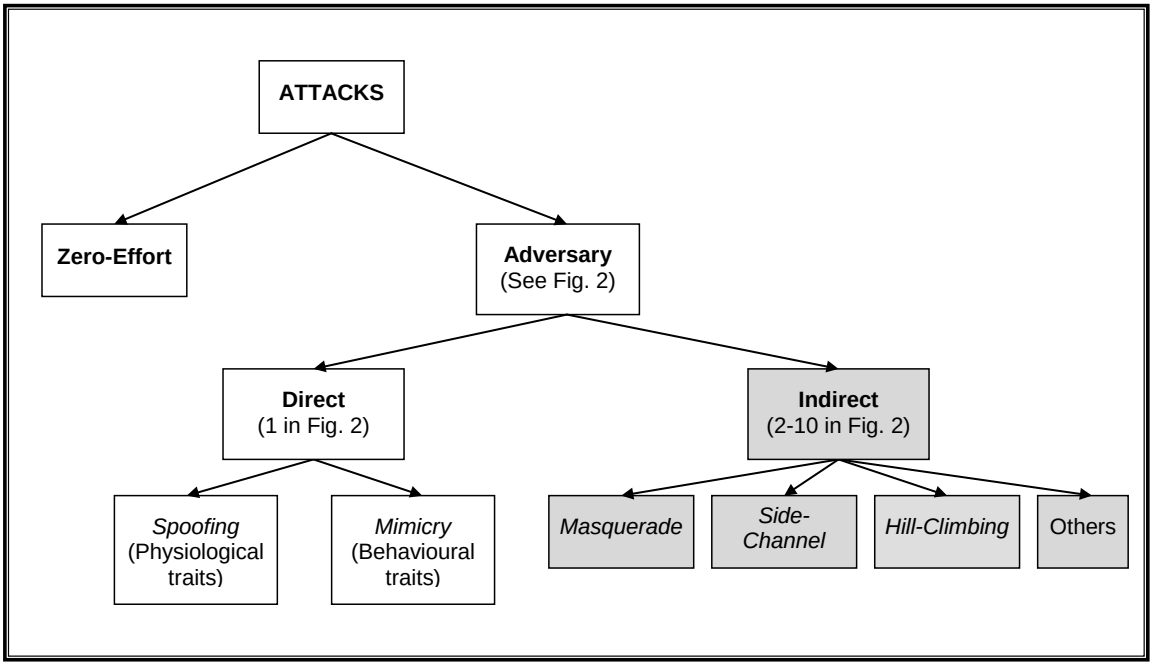

Figure 1: Classification of the attacks to a biometric system. Indirect attacks, that are the objective of the present document, are highlighted in grey.

As shown in Fig. 1, the attacks that can compromise the security provided by a biometric system may be categorized into two basic types [8]:

- *Zero-effort attacks*: also known as *intrinsic failure* [7]. This threat, impossible to prevent and present in all biometric systems, is derived from the fact that there is always a non-zero probability that two biometric samples coming from two different subjects are sufficiently alike to produce a positive match (the same way that there is a non-zero probability of guessing by chance a four digit PIN).

- *Adversary attacks*: this refers to the possibility that a malicious subject (attacker), enrolled or not to the application, tries to bypass the system interacting with it in a way for which it was not thought.

Adversary attacks have been systematically categorized in 10 classes by [13] depending on the point to which they are directed. The total 10 points of attack are depicted in Fig. 2. These adversary attacks can be grouped in direct and indirect attacks as follows (see Fig. 2):

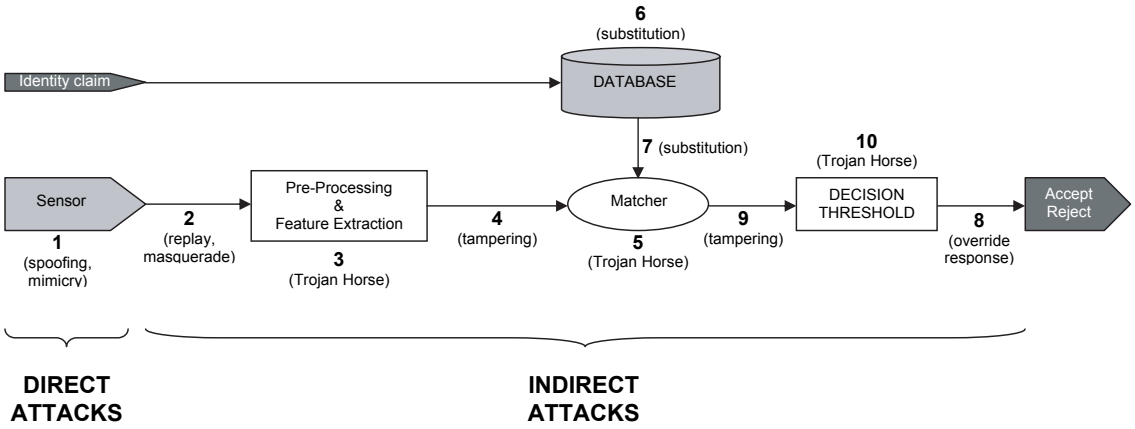

Figure 2: Architecture of an automated biometric verification system. Possible attack points are numbered from 1 to 10.

- **Direct attacks**. These threats correspond to type 1 in Fig. 2 and are aimed directly to the sensor trying to gain access to the system by impersonating a real user [15].

- **Indirect attacks**. This group includes all the remaining nine points of attack identified in Fig. 2, and are performed against some of the inner modules of the system (e.g., feature extractor or matcher).

  The *side-channel* attacks that appear in Fig. 1 refer to the possibility of attacking a biometric system using some measurable *side-channel* information such as the matching time, or the power consumed by the system in the matching process [5]. This type of information, which has already been used to successfully attack cryptographic security systems [9, 10], is in general easily accessible to a possible attacker and difficult to be manipulated or distorted by the system designer (in opposition to the similarity score used in traditional hill-climbing algorithms).

  In opposition to attacks at the sensor level, in the indirect attacks the intruder needs to have some additional information about the internal working of the recognition system and, in most cases, physical access to some of the application components (feature extractor, matcher, database, etc) is required.

The rest of the document is focused on the study of indirect attacks and on the proposal of a set of metrics and an associated evaluation protocol for the objective estimation of the vulnerabilities derived from this type of threats.

The deliverable is structured as follows. Some important concepts to understand the deliverable are defined in Sect. 2. The proposed metrics for the evaluation of indirect attacks are presented in Sect. 3 and the associated protocol is described in Sect. 4. The final summary of the deliverable appears in Sect.5.

2 Definitions

In the following, we define some important concepts which are key to understand the rest of the document:

- **Metrics**. Here we will consider a metric as any factor, not necessarily objectively quantifiable, which has a key impact in the danger posed by a given attack. This way, metrics include, but are not restricted to, measurable parameters such as the number of successful access attempts.

- **Normal Operation Scenario (NOS)**. This is the working scenario for which biometric systems are designed. Users interact with the system in the usual way, thus the two possible types of access attempts are defined as follows: *Genuine access attempt*, the user tries to access his account using his own real biometric trait; *Impostor access attempt* (also referred to as zero-effort attack), the user tries to access a different individual's account using his own real biometric trait.

- **Attacking Scenario (AS)**. In this case the user (from now on, attacker) tries to break the system by interacting with it in a way which differs from the NOS. Therefore, in this scenario, genuine and impostor access attempts should be redefined on a case by case basis (for each attack).

- **Verification Rates**. As already described in deliverable D3.3, the verification performance of biometric systems is usually expressed in terms of their False Acceptance Rate (FAR), False Rejection Rate (FRR) and the related Equal Error Rate (EER). These parameters are defined for the normal operation mode and reflect the system performance in this scenario. Under an attacking scenario, the standard definitions given for the FAR and FRR are not valid (as both impostor and genuine attempts also change). This means that these two metrics should not be used to evaluate attacks as it would lead to confusion.

  Therefore, in the present document, FAR and FRR are *only* used in the context of the system Normal Operation Scenario.

- **Account**. In the document this term refers to the enrolled biometric template/model of a legitimate user which is used as reference to be matched against the test samples.

- **Identification phase of an attack**. Corresponds to the effort required to create the attack, and to demonstrate that it can be successfully applied to the biometric system at hand (including setting up or building any necessary test equipment). The demonstration that the attack can be successfully applied needs to consider any difficulties in expanding a result shown in the laboratory to create a useful attack. One of the outputs from Identification could be a script that gives a step-by-step description of how to carry out the attack. This script is assumed to be used in the exploitation part.

- **Exploitation phase of an attack**. Corresponds to achieving the attack on an instance of the biometric system using the analysis and techniques defined in the identification part of an attack. It could be assumed that a different attacker carries out the exploitation, the technique (and relevant background information) could be available for the exploitation in the form of a script or set of instructions defined during the identification of the attack. This type of script is assumed to identify the necessary equipment and, for example, mathematical techniques used in the analysis. This means that the final ratings for some of the metrics specified in Sect. 3 (i.e., time, proficiency or system knowledge required) will sometimes be lower for exploitation than for identification.

3 Metrics for the Evaluation of Indirect Attacks

The objective evaluation of the performance of an attack (i.e., danger or risk posed to a system) is a very difficult and challenging problem as it depends on multiple non-independent factors. Here we will present a number of general metrics, common to any type of attack, that should be considered in order to compare the vulnerability of a given biometric system to different indirect attacks. In Sect. 4 an associated protocol that permits the estimation of these metrics is also defined.

Although, as mentioned above, certain dependencies may be drawn among risk factors and a closed classification is not possible, we will distinguish three groups of metrics according to the agent they are related to, namely: system-related metrics, attacker-related metrics, and attack-related metrics.

In order to correctly interpret and use this document there are a number of important notices that should be taken into account:

- It is very important to highlight that, due to their nature, the evaluation of many of the metrics defined here rely on the subjective perception of a security assessment expert who will ultimately be responsible for the overall rating of the attack.

- Therefore, this document should be taken as a supporting tool that intends to homogenize as much as possible the very difficult task of vulnerability rating, and which is thought for experts with a large experience in the field (who can accurately interpret its general guidelines).

- For each of the metrics, the document identifies a number "danger-levels" or "danger-ratings". These ratings are given for reference as a guidance to evaluators, but are not a closed set. Depending on the particular characteristics of the attack or the biometric system being evaluated, other new levels or sub-levels may be defined if considered necessary.

- It is also important to notice that for certain attacks, and in the frame of a specific evaluation, it may be interesting or even necessary to distinguish between two different phases: identification and exploitation (please see Sect. 2 for a definition of each phase). In each of these phases the ratings given to each of the metrics identified below may vary. Again, it is the evaluators task to identify, for each particular case, if the distinction between phases is required and if the ratings for the attack change.

- Some of the metrics identified below are highly dependent on the operating point of the system (defined by the FA and FR rates), therefore they should always be reported together with these verification rates (see Sect. 4 for further details).

- In an overall evaluation of a whole security display (of which the biometric system may just be a small component), there may be certain environmental-specific factors that also affect the vulnerability assessment of the biometric system. However,

as these factors are fully dependent on the particular implementation of the whole system and are very difficult to generalize, they will not be considered here.

3.1 System-related metrics

Attack # (see Fig. 2)	Knowledge	Suggested Rating
Type 2	Sample format	Public
Type 3	Feature extractor implementation	Critical
Type 4	Template format	Restricted
Type 5	Matcher implementation	Critical
Type 6	Template format	Restricted
Type 7	Template format	Restricted
Type 8	Response code	Restricted
Type 9	Score range	Critical
Type 10	Score range	Critical

Table 1: Typical knowledge required to perform each of the indirect attacks identified in Fig. 2. Tentative rating given (public, restricted, confidential or critical). To be taken just as an example which should be evaluated on a case by case basis.

System knowledge required. This metric refers to the amount of knowledge of the biometric system required to perform the attack.

For instance in an indirect attack of type 2 to the input of the feature extractor (see Fig. 1) the attacker will need to know the format of the acquired sample (e.g., in a fingerprint system the image format of the sample, its size and resolution). This information is in many cases publicly available at the website of the sensor manufacturer. However, for an indirect attack of type 4 to the input of the matcher, the attacker will need to know the specific format of the biometric templates (what information is extracted from the sample and how it is stored). This information is usually very difficult to obtain as it is not shared by companies.

Although it should be evaluated in a case by case basis, in table 1 we give, as reference, a non-exhaustive list of the usual knowledge required to perform the different types of indirect attacks shown in Fig. 1. Also, a tentative rating for this information is given. The danger-levels identified for this metric are:

- Public: information which is fairly easy to obtain (e.g., on the web).
- Restricted: information which is only shared by the developer and organizations which are using the system, usually under a non-disclosure agreement.
- Confidential: information which is only available within the organization that develops the system and is in no case shared outside it.

- Critical: it refers to information which is only available to certain people or groups within the organization which develops the system.

Special attention should be paid in this point to possible countermeasures that may be implemented in the system and wether it is necessary or not to have knowledge of their existence in order to be successful in a given attack.

Also to be noticed that countermeasures may not fully protect the system against an attack but can exponentially increase the time needed to perform it. Therefore, making the attack unfeasible in practice (see the entry "time" in Sect. 3.3)

Availability. This metric takes into account how easy/difficult it would be for an eventual attacker to acquire or to have access to a copy of the biometric system in order to prepare, develop, or carry out the attack. A suggested rating for this metric is:

- Public: The system is publicly available (e.g., on-line) and may be installed in your own facilities (e.g., a biometric SDK).

- Restricted: The system is accessible for the public but it is very difficult to get or to take with you (e.g., an ATM with a biometric system installed).

- Private: The system is only accessible to certain authorized people (e.g., access control to a restricted area of a company).

3.2 Attacker-related metrics

Proficiency. This metric refers to the level of proficiency required by the attacker and the general knowledge that he possesses, not specific of the system being attacked. A suggested rating for this metric is:

- Layman: no real expertise needed, any person with a regular level of education is capable of performing the attack.

- Proficient: some advanced knowledge in certain specific topics (e.g., optimization algorithms) is required. Good knowledge of the state-of-the-art of attacks. The person is capable of adapting known algorithms to his needs.

- Expert: a specific preparation in multiple areas such as pattern recognition, computer vision or optimization is needed in order to carry out the attack. The person is capable of generating his own new attacking algorithms.

- Multiple experts: the attack needs the collaboration of several people with high level of expertise in different fields (e.g., electronics, cryptanalysis, physics, etc.)

3.3 Attack-related metrics

Time. Amount of time needed by the attack (including its preparation and execution) to break the system. This metric is strongly related to the *Efficiency* (defined below) and to the countermeasures that the system may have integrated (see *knowledge required* in Sect. 3.2).

For the rating of this particular metric it may be useful to distinguish between the *identification* and the *exploitation* of an attack:

A suggested rating for this metric is:

- Low: less than one day.
- Medium: less than one week.
- Large: more than one week.

It should be noted that certain attacks may be considered to be unfeasible (i.e., the system is resistant to them) if the amount of time required to carry them out is too large.

Equipment. This refers to the type of equipment required to perform the attack. This includes the biometric databases used (if any). A suggested rating for this metric is:

- Standard: equipment which is affordable, easy to obtain and simple to operate (e.g., computer, video cameras or mobile phones). In the case of biometric databases it would refer to publicly available ones (or datasets generated synthetically).
- Specialized: this refers to fairly expensive equipment, not available in standard markets and which require of some specific formation to be used (e.g., spectrum analyzer). In the case of biometric databases it would refer to datasets with restricted and limited access or which are specifically captured by the attacker.
- Multiple specialized: in this case more than one specialized equipment is required to perform different parts of the attack.

Success Rate (SR). It is the expected probability that the attack breaks a given account. It is computed as the ratio between the accounts broken by the attack A_b, and the total accounts attacked A_T, that is:

$$\mathrm{SR} = A_b/A_T. \tag{1}$$

This metric gives an estimation of how dangerous it is a particular attack for a given biometric system: the higher the SR the bigger the threat.

A suggested rating for this metric is (numerical values are given in percentage):

- Low danger: SR < 1.

Type	Metric	Suggested Rating
System-Related	System Knowledge	Public, Restricted, Confidential, Critical
	Availability	Public, Restricted, Private
Attacker-Related	Proficiency	Layman, Proficient, Expert, Multiple experts
Attack-Related	Time	Low, Medium, Large
	Equipment	Standard, Specialized, Multiple specialized
	Success Rate (SR)	Low, Medium, High (danger)
	Efficiency ($\mathrm{E_{ff}}$)	Slow, Medium, Fast, Very Fast

Table 2: Summary of the proposed metrics for the evaluation of the vulnerabilities of biometric systems against indirect attacks.

- Medium danger: $1 < \mathrm{SR} < 10$.
- High danger: $\mathrm{SR} > 10$.

Efficiency ($\mathrm{E_{ff}}$). It indicates the *average* number of *matchings* needed by the attack to break an account. It is defined as:

$$\mathrm{E_{ff}} = \frac{A_b}{\sum_{i=1}^{A_b} n_i}, \tag{2}$$

where n_i is the number of comparisons computed to break each of the bypassed accounts. Note that it is computed in terms of the number of matchings or comparisons performed, and not in terms of the number of iterations carried out by the attack (should it be an iterative algorithm), as in each iteration more than one matching might be computed.

This parameter gives an estimation of how easy it is for the attack to break into the system in terms of speed: the higher the $\mathrm{E_{ff}}$ the faster the attack.

This metric has a deep impact on the overall time required to perform an attack.

A suggested rating for this metric is (numerical values are given in percentage):

- Slow: $\mathrm{E_{ff}} > 500$.
- Medium: $100 < \mathrm{E_{ff}} < 500$.
- Fast: $10 < \mathrm{E_{ff}} < 100$.
- Very fast: $\mathrm{E_{ff}} < 10$.

In Table 2 we present a summary of the metrics identified in this section for the objective evaluation of the vulnerabilities of biometric systems against indirect attacks. The metrics are divided into three groups following the same classification used in Sect. 3: System-related, attacker-related and attack-related. The suggested rating proposed for each metric is also provided.

4 Vulnerabilities Evaluation Protocol

In this section, we define a systematic security evaluation protocol for biometric systems that can be applied regardless of the attack, system, or biometric trait being considered. The protocol includes a set of guidelines for the security assessment of biometric systems and for reporting the results of the evaluation in a useful and meaningful manner. In particular, the protocol is divided into two separate stages (performance and security evaluations) with a number of different steps to be followed.

Performance evaluation. Regardless of the error rates claimed by the vendor (usually computed on small self-acquired datasets), an independent performance evaluation in the Normal Operation Scenario (NOS) should always be the starting point for a posterior security assessment of the system.

As mentioned in Sect. 3 some of the metrics defined in this document (e.g., specially the Success Rate (SR) and Efficiency (E_{ff})) are highly dependent on the FA and FR rates of the system. The performance evaluation will permit to determine how good the system is and, more important, the operating points where it will be attacked. Furthermore, defining the operating points will enable to compare, in a more fair manner, the vulnerabilities of different systems to the same attack (i.e., we can determine for a given FAR or FRR which of them is less/more robust to the attacking approach).

Therefore, any security or vulnerability evaluation of a biometric system should always be performed for a pair: Biometric system - Operating point. If either element (system or operating point) is changed, a new vulnerability assessment should be carried out.

We refer the reader to Deliverable D3.3 for a set of metrics, best practices and procedures for biometric performance evaluation. However, we may highlight here two key factors to any performance evaluation:

1. Database selection. A number of useful biometric databases for the different modalities considered in the BEAT project are given in deliverable D3.6.

2. Protocol definition. It should be clearly stated the genuine and impostor access attempts carried out during the performance evaluation in order to reach the reported error rates. In general it is better to follow fixed protocols. See deliverable D3.6 for a more formal definition of performance evaluation protocols (the reader can also find in D3.6 a number of them for largely used biometric databases.)

In case that a solid independent performance evaluation has already been carried out by a third party, the results may be used as input for the security evaluation (thus omitting our own performance assessment).

However, in this case, specific details about the performance evaluation considered should be given as well as a proper justification for its use.

Security evaluation.

1. Description of the biometric system that will be evaluated.

2. Description of the attack (see Fig. 1 for a general classification) for which we want to determine the vulnerability of the biometric system. This description must contain the parts of the system that are targeted by the attacker (e.g., template, algorithm, matching score...) and the goal of the attack.

3. Description of the **equipment** required to perform it.

4. Description of the attacker **proficiency**.

5. Description of the **knowledge** about the system under evaluation required by the attacker.

6. Execution of the vulnerability evaluation in the defined operating points (in the previously executed performance evaluation), paying special attention to the computation of the **Success Rate** and **Efficiency** of the attack (defined in Sect. 3).

7. Account for the **time** required to perform the attack (after a certain time, an attack can be considered as not feasible).

Finally, the overall rating of the attack should take into account the partial ratings of the metrics defined in Sect. 3 and should always be reported together with the FAR and FRR for which it was carried out.

5 Summary

The main objective of the document was to set a common framework so that the vulnerabilities of different biometric systems to different indirect attacks may be compared in an objective and quantitative way. To this end, the deliverable has presented different metrics to be considered in the evaluation of biometric indirect attacks, together with an associated protocol to be followed for the estimation of the different risk factors. Certain guidelines to report the results in a useful and meaningful manner for other researchers, evaluators and developers have also been given.

This deliverable will serve as starting point to determine an analogue set of metrics for the evaluation of direct attacks (D4.5). The metrics and protocol described in the present deliverable will be of great help for the further development of the ongoing standards regarding the security evaluation of biometric systems (WP6).

References

[1] A. Adler. *Handbook of biometrics*, chapter Biometric system security, pages 381–402. Springer, 2008.

[2] BEM. Biometric Evaluation Methodology. v1.0, 2002.

[3] I. Buhan and P. Hartel. The state of the art in abuse of biometrics. Technical report, University of Twente, 2005.

[4] CC. Common Criteria for Information Technology Security Evaluation. v3.1, 2006. Available on-line at http://www.commoncriteriaportal.org/.

[5] J. Galbally, J. Fierrez, and J. Ortega-Garcia. Bayesian hill-climbing attack and its application to signature verification. In *Proc. IAPR International Conference on Biometrics (ICB)*, pages 386–395. Springer LNCS-4642, 2007.

[6] ISO/IEC 19792. ISO/IEC 19792:2009, information technology - security techniques - security evaluation of biometrics., 2009.

[7] A. K. Jain, K. Nandakumar, and A. Nagar. Biometric template security. *EURASIP Journal on Advances in Signal Processing, Special Issue on Biometrics*, 2008.

[8] A. K. Jain, A. Ross, and S. Pankanti. Biometrics: a tool for information security. *IEEE Trans. on Information Forensics and Security*, 1(2):125–143, 2006.

[9] P. Kocher. Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems. In *Proc. 16th ICCAC*, pages 104–113. LNCS 1109, 1995.

[10] P. Kocher, J. Jaffe, and B. Jun. Differential power analysis. In *Proc. Crypto 99*. LNCS 1666, 1999.

[11] LivDet, 2009. http://prag.diee.unica.it/LivDet09/.

[12] K. A. Nixon, V. Animale, and R. K. Rowe. *Handbook of biometrics*, chapter Spoof detection schemes, pages 403–423. Springer, 2008.

[13] N. Ratha, J. H. Connell, and R. M. Bolle. An analysis of minutiae matching strength. In *Proc. IAPR Audio- and Video- Based Person Authentication (AVBPA)*, pages 223–228. Springer LNCS-2091, 2001.

[14] N. K. Ratha, J. H. Connell, and R. M. Bolle. Enhancing security and privacy in biometrics-based authentication sytems. *IBM Systems Journal*, 40:614–634, 2001.

[15] S. Schuckers. Spoofing and anti-spoofing measures. *Information Security Technical Report*, 7:56–62, 2002.

[16] U. Uludag and A. Jain. Attacks on biometric systems: a case study in fingerprints. In *Proc. SPIE Seganography and Watermarking of Multimedia Contents VI*, volume 5306, pages 622–633, 2004.

[17] J. Wayman, A. Jain, D. Maltoni, and D. Maio. *Biometric systems. Technology, design and performance evaluation*. Springer, 2005.