Supporting Document Guidance

Characterizing Attacks to Fingerprint Verification Mechanisms

2011

Version 3.0

CCDB-2008-09-002

Foreword

This is a supporting document, intended to complement the Common Criteria and the Common Evaluation Methodology for Information Technology Security Evaluation.

Supporting documents may be “Guidance Documents”, that highlight specific approaches and application of the standard to areas where no mutual recognition of its application is required, and as such, are not of normative nature, or “Mandatory Technical Documents”, whose application is mandatory for evaluations whose scope is covered by that of the supporting document. The usage of the latter class is not only mandatory, but certificates issued as a result of their application are recognized under the CCRA.

Technical Editor: National Cryptologic Centre (CCN, Centro Criptológico Nacional).

Document History:	V1.0 December 2009 (initial supporting document version)
Document History:	V2.0 December 2010 (revised supporting document version by CCN according to the comments and feedback received from German BSI and French ANSSI)

General purpose:

The present document provides guidance about attack methods to be considered in the evaluation of TOEs with fingerprint verification mechanisms. The document also helps the standardization of the security rating for this type of mechanisms, and to this end, the attack methods provide guidelines as well as examples for the attack rating.

Field of special use: Biometric based Devices and Mechanisms.

Acknowledgments*:*

This work is the result of the collaboration of the Spanish National Cryptologic Centre (CCN) and the Biometric Recognition Group - ATVS of the Autonomous University of Madrid (UAM).

Table of Contents

ACRONYMS

ATE – Tests Class

AVA_VAN – Vulnerability Assessment class _ Vulnerability Analysis

CB – Certification Body

CC – Common Criteria

CEM – Common Evaluation Methodology

DET – Detection Error Tradeoff

EER – Equal Error Rate

FAR – False Acceptance Rate

FMR – False Match Rate

FNMR – False Non Match Rate

FRR – False Rejection Rate

IT – Information Technology

MoC – Match-on-Card

PCB – Printed Circuit Board

ROC – Receiver Operating Characteristic

SF – Security Functionalities

SoC – Storage-on-Card

SR – Success Rate

TOE – Target of Evaluation

TSF – TOE Security Functionality

EXECUTIVE SUMMARY

Authentication and access control mechanisms to modern networked and computer systems are experimenting a very rapid evolution process where the traditional verification methods based on something that *you know* or something that *you have* are being complemented with more sophisticated mechanisms based on something that *you are*. This way, identity verification biometric devices are being incorporated into the security market. In particular, fingerprint is the biometric modality with a higher acceptance among manufacturers and vendors thanks to its high discriminative capacity and accuracy.

In spite of the advantages that biometric systems present over traditional security systems they are not free from possible external attacks which can jeopardize restricted information. Thus, it is of utmost importance to have a common benchmark in which to evaluate the security capabilities of the new biometric technology in comparison with other existing and tested security methods.

In the present document the CEM terminology is applied to fingerprint based recognition products, providing some guidance as to which attack methods have to be considered in the evaluation of TOEs with fingerprint verification mechanisms. The document also helps the standardization of the security rating of this type of mechanisms, and to this end, the attack methods provide guidelines as well as examples for the attack rating.

The document does not pretend to be a detailed methodology on how attacks are executed and just gives some general indications on how the attacks should be rated according to the CEM evaluation guidelines. Thus, implied in the application of this document is that the laboratory conducting the evaluation has the expertise and skill to select the appropriate attack methods and is able to perform them adequately or to subcontract special tasks.

In this point, it is also necessary to highlight the importance of the operational environment and other verification mechanisms complementing the full TOE authentication functionality. Thus the rating examples provided in this document have to be understood as general ideas focused on how to characterize aspects of the attack rating related to the fingerprint mechanisms. Evaluators can use these general guidelines to extrapolate the fingerprint factors described here to other real-life verification functions. In general these functions include also other traditional mechanisms based in something that *you know or have*, or even more they include security mechanisms like access control counters and so on forth. In other words, the examples in this document are focused on fingerprint mechanisms, and it is an evaluator task to use them to characterize complex security functionalities in real TOEs.

Additionally the fast evolution of this type of technology requires using this guidance always complemented with an evaluator review of other references in the status of the art, in order to update new information or factors that could be relevant for the rating examples.

1 Introduction

1.1 Motivation

Attack methods for the product range of fingerprint verification mechanisms cover diverse fields of expertise such as pattern recognition, informatics and cryptography. The use of these different types of expertise for attacks is complex. Also the quick evolution and change related to this kind of biometric technology is a handicap. Thus it is very difficult to ensure *status of the art* coverage of the whole range of attacks. Ideally the experts in security and security testing of a defined product range in IT would come together, pool their knowledge and compose a list of test methods representing the status of the art.

This document describes the most typical attacks on fingerprint verification mechanisms and serves two main purposes:

- It provides guidance as to which attack methods have to be considered in a fingerprint-related product evaluation. By describing the key factors of these methods, both a vulnerability assessment and penetration testing can be achieved in evaluations.

- The document also helps the standardization of the security rating of fingerprint verification mechanisms. To this end, the attack methods provide guidelines as well as examples for the attack rating.

1.2 Attack Potential and CEM versions used

All the skills and tools required to carry out the different attacks presented in this document, have been defined in the terminology of the **CEM v3.1** methodology document.

The separation between the Identification and the Exploitation of an attack can be very useful for many of the attacks carried out against fingerprint-related TOEs. Thus, in the present document we follow the definitions given in the **CEM v2.3** document to distinguish between both scenarios.

The ratings of the practical examples are computed according to the potential tables of **Version 3.1** and are given both for the Exploitation and the Identification scenarios. The final rating of a given attack is the sum of identification and exploitation cost (in terms of CEM 3.1 ratings).

The ratings for each attack potential factor come directly from CEM v3.1 Annex B.4 as shown by Table 1, but the final ratings of vulnerabilities and TOE resistance are described by the ad hoc Table 2 defined here for the fingerprint TOEs subject of this document.

Factor	Value
Elapsed Time	
<= one day	0
<= one week	1
<= two weeks	2
<= one month	4
<= two months	7
<= three months	10
<= four months	13
<= five months	15
<= six months	17
> six months	19
Expertise	
Layman	0
Proficient	3*(1)
Expert	6
Multiple experts	8
Knowledge of TOE	
Public	0
Restricted	3
Sensitive	7
Critical	11
Window of Opportunity	
Unnecessary / unlimited access	0
Easy	1
Moderate	4
Difficult	10
None	**(2)
Equipment	
Standard	0
Specialized	4(3)
Bespoke	7
Multiple bespoke	9

(1) When several proficient persons are required to complete the attack path, the resulting level of expertise still remains "proficient" (which leads to a 3 rating).
(2) Indicates that the attack path is not exploitable due to other measures in the intended operational environment of the TOE.
(3) If clearly different test benches consisting of specialized equipment are required for distinct steps of an attack, this should be rated as bespoke.

Table 1. Calculation of attack potential

Values	Attack potential for the whole attack	TOE resistant to attackers with attack potential of	Meets assurance components	Failure of components
<20	Basic	No rating		AVA_VAN.1 AVA_VAN.2 AVA_VAN.3 AVA_VAN.4 AVA_VAN.5
20-27	Enhanced-Basic	Basic	AVA_VAN.1 AVA_VAN.2	AVA_VAN.3 AVA_VAN.4 AVA_VAN.5
28-34	Moderate	Enhanced-Basic	AVA_VAN.1 AVA_VAN.2 AVA_VAN.3	AVA_VAN.4 AVA_VAN.5
35-42	High	Moderate	AVA_VAN.1 AVA_VAN.2 AVA_VAN.3 AVA_VAN.4	AVA_VAN.5
>42	Beyond high	High	AVA_VAN.1 AVA_VAN.2 AVA_VAN.3 AVA_VAN.4 AVA_VAN.5	

Table 2. Ratings of vulnerabilities and TOE resistance

In the document, the Identification and Exploitation of the attack are considered as follows:

Identification: corresponds to the effort required to create the attack, and to demonstrate that it can be successfully applied to the TOE (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: corresponds to achieving the attack on an instance of the TOE using the analysis and techniques defined in the identification part of an attack. 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 elapsed time, expertise and TOE knowledge ratings for exploitation will sometimes be lower for exploitation than for identification. For example, it is assumed that the script identifies such things as the physical point at which to apply a

brute force attack, and hence in the exploitation phase the attacker does not have to spend significant time to find the correct point at which to apply the attack. Furthermore, this same information may also reduce the exploitation requirement to one of time measurement, whereas the identification phase may have required reverse engineering of hardware or software information from power data – hence the expertise requirement may be reduced. Throughout the document the ratings given for the exploitation phase are computed assuming the ***worst case scenario*** (for different attack possibilities the one that leads to a lower rating is chosen).

1.3 Attack Information Template

Section: "Description of Attack"

Gives a short description of the purpose and method of the attack.

Section: "Effect of Attack"

Contains a more detailed attack description, and how to recognize the success of this attack. This may include variations of a basic attack.

Section: "Impact on TOE"

Examples of how the attack may result in an exploitable vulnerability in the TOE. This description is in terms of issues that would need to be notified to a user or developer (of other products that would use the TOE). This will also explain the motivation for carrying out this attack.

Section: "Characteristics of the Attack"

Factors that make the attack difficult/easy to carry out or to be applied to a real TOE.

Skills and tools required to carry out the attack, in the terminology of the CEM v3.1 methodology document.

References to books, papers, standards or methods where appropriate. This list of references will probably not be complete – more techniques are used in labs than are published – but they may give an understanding of the basics of the attack or attack techniques.

This part gives an agreed set of attacks (or attack variants) which should be considered as "obvious attacks".

Section: "Examples of Attack Potential Ratings"

These examples illustrate in more detail what is behind the different attack methods. The presentation of these ratings helps to come to consistent results when interpreting the potential table between different evaluation teams among Schemes.

The rating examples provided in these sections have to be seen as simple concepts focused on how to characterize aspects of the attack rating related to fingerprint mechanisms. These

general guidelines can be useful for evaluators to extrapolate the key concepts considered here to complex/real authentication functions. They are not absolute ratings, just examples to illustrate the relevant CEM potential factors related to the biometric idiosyncrasy of fingerprint mechanisms.

IMPORTANT NOTE: Please be aware that the example ratings for the attack methods in chapter 2 strongly depend on the condition that a certain attack is not yet published because most of the rating points are given for the identification phase (i.e., should the method be already published the attacker would have the knowledge he was supposed to gain at the identification phase, thus lowering the rating of the attack).

1.4 Scope of this Document

This document addresses the product range of TOEs including fingerprint verification mechanisms. It refines the CEM for this product range concerning the aspects of class AVA (Vulnerability Assessment).

As will be explained in Sect. 1.5, fingerprint, and in general biometric technology, presents two different modes of operation: *identification* and *verification*. In *identification* a biometric sample is matched against a set of templates or previously recorded references (i.e., it is a 1-to-N pattern-matching problem). On the other hand, *verification* applications solve a 1-to-1 pattern-matching to decide if the sample presented to the system corresponds to a specific template or reference (i.e., verify or validate a claimed identity).

This supporting document is focused on *verification mechanisms* based on fingerprint biometric technologies. Identification applications -in general- are restricted to domains related with forensic science and to support the operation of police corps. Although verification and identification systems share a common background the attack methods and vulnerabilities to be considered in a security evaluation will differ to some extent. The attack methods specific of identification applications should be the subject of a different supporting document.

The term *mechanisms* is used to refer strictly to the purely biometric-based modules of the whole security *system*, which may comprise other devices or parts (e.g., firewalls, encryption, etc.) that will not be considered in the present document.

For the planning of the vulnerability assessment and penetration testing, the document provides guidance as to which attack methods should be considered for fingerprint verification mechanisms. The examples give an indication of what is regarded as *status of the art*.

IMPORTANT NOTE: "Status of the art" is not static and may change over the time. The list does not claim to be complete but describes only a set of all possible attacks. This type of TOEs rapidly change, thus this list should be considered together with an additional review of other references, in order to include new information in the status of the art that could be important for the ratings.

So it should be noted that:

- The presented guidance is a minimum set of methods that have to be considered. For special applications and products there may exist attacks that are not specially mentioned here.

- Not all methods will be applicable for every product. It is in the responsibility of the Evaluation Laboratories and the Certification Body to select the appropriate methods.

For each evaluation it has to be decided which of the attack methods are applicable for the product under evaluation and how the attacks should be best implemented. It might be possible to exclude some attacks just by considering specific properties of the TOE (such as its use or operational environment).

Implied in the application of this list is that the laboratory conducting the evaluation has the expertise and skill to select the appropriate attack methods and is able to perform them adequately or to subcontract special tasks.

The examples in the document also give guidance about how the attack potential was decided. Even if the attacks performed for another TOE do not exactly match the examples, evaluators should be able to build an equivalent rating.

NOTE: Even though the examples sometimes consider commonly used countermeasures it is very important to note that the ratings given reflect only an average security level; but the real security level strongly depends on the implementation, thus there may also be other countermeasures that are not considered here. In consequence, the ratings for any particular evaluation may be different from the examples given.

It must also be noted that, in general, the attack potential ratings estimated in real evaluations would be computed over complete authentication functions in the TSF (TOE Security Functionality) that may include further security methods apart from those specific of the biometric technology (e.g. blocking-account countermeasures). Thus, the potential ratings presented in some examples do not belong to the isolated biometric component but to some composed authentication function as a whole. To be noticed that it is impossible to take into account all the possible external factors that may have an impact in a particular attack rating so it is the work of the evaluator to objectively and carefully examine the particularities of a given TOE.

It is also very important to emphasize that due to the statistic nature of biometric technology, we must distinguish between:

- ***Performance evaluation of the product***. Generally given in terms of its False Acceptance Rate (FAR) and False Rejection Rate (FRR). Both terms will be described in Sect. 1.5.1.

- ***Evaluation of a given attack***: Generally given in terms of its Success Rate (SR) and its Efficiency (E_{ff}). Both terms will be described in Sect. 1.5.2.

This disquisition is specially important in the computation of the elapsed time. In the rating examples of the present document we consider the time required for a realistic single attack, however, it has to be clearly stated that in order to carry out a proper evaluation, the FAR of the TOE given by the manufacturer should be first independently checked. This is necessary in order to fix an operating point (or a discrete set of them) where the manufacturer wants its product to be evaluated/certified, as the operating point fixes the resistance level of the system to external attacks which is directly related to the EAL of the certificate.

The verification of the product error rates is not a trivial task, which falls out of the scope of this document as it is not strictly part of the vulnerability tests but rather of the confirmation that the TSF operates according to its design descriptions (ATE class). In order to reach this objective (independent assessment of the performance of the TOE under normal operating conditions) the laboratories must have their own evaluation infrastructure (which includes large databases subdued to the personal data protection laws of each country). Furthermore, the FAR and FRR of a system are dependent on the database and the protocol used in their computation, thus, the manufacturer should give the evaluation laboratory very clear and detailed specifications of the experiments carried out to reach the claimed error rates. All these issues fall within the ATE class field (and not the AVA_VAN class which is the purpose of the present SP) and should be addressed on a complementary document.

It must be also emphasized that in the present document only those attacks which are specific of the biometric fingerprint based technology have been addressed. However, as a security aimed technology, fingerprint automatic recognition products are also exposed to the external attacks common to all security applications.

Furthermore, the document comprises the most typical and well known types of biometric-based attacks, which have been rated according to practical laboratory experiments. However, further laboratory experience is most valuable and will serve to complete, in future versions of the document, the set of examples given here with other analyzed attacks or countermeasures.

In order to restrict the number of attacking possibilities which largely depend on a great amount of external factors that may influence the success chances of a given attack, all the ratings and descriptions given in this document have been made under the assumption of the ***worst case scenario***. For instance, in the case of attacks with gummy fingers we will consider the existence of a "*golden fake*", manufactured with a specific material, which, once identified (in the identification phase), is able to break a given scanner/system with very few attempts for almost all the cases. Following the same principle, we will consider fingerprints as public data which can be obtained in a fairly easy manner. This way, again in the gummy fingers attacks, the rating will start when the attacker has already acquired (by some means) the fingerprint of the user.

The case of attacks involving direct threats to the legitimate user of a given system (e.g., access gained at gunpoint), or violent acts (e.g., attacking a fingerprint verification system with a dismembered finger), fall out of the scope of this document as this type of actions do not reflect the security level of a given technology, but rather depend on the willpower of the attacker and are not considered by the CC norm.

1.5 Description of the TOE

This document is directed to biometric mechanisms based on fingerprint verification. A biometric system is essentially a pattern recognition system that makes use of biometric traits (in this particular case fingerprint) to recognize individuals. The objective is to establish an identity based on '*who you are or what you produce'*, rather than by '*what you possess*' or '*what you know'*.

The digital representation of the characteristics or features of a biometric trait is known as *template*. Templates are stored in the system database through the enrolment or training process, which is depicted in Figure 1 (top). The database can either be centralized (this is the case of most biometric systems working at the moment), or distributed (as in Match-on-Card systems where each user carries the only copy of his template in a personal card). Once the users have been enrolled to the system, the recognition process can be performed in two modes:

- ***Identification***. In this mode, the question posed to the system is: is this person in the database?, the answer might be 'No' (the person is unknown to the system), or any of the registered identities in the database. In order to give the answer the system has to perform a "*one-to-many*" matching process, as it has to compare the input biometric to all the stored templates (Fig. 1, centre). In most practical cases, under the identification operation mode, the system usually returns, in a ranked manner, those identities that are more likely to be the searched person (i.e., those that have produced a higher similarity score), and then a human expert decides whether the subject is or not within that reduced group of people.

- ***Verification***. In this case what we want to know is if a person is really who she claims to be (i.e., is this person truly E. Nigma?). This way, under the verification mode (Fig. 1, bottom), the system performs a "one-to-one" matching process where the submitted biometric trait is compared to the enrolled pattern associated with the claimed identity, in order to determine if the subject is a client (the identity claim is accepted), or an impostor (the identity claim is rejected).

This document is focused on the security evaluation of fingerprint-based systems working under the verification mode. In this mode, the *clients* or *targets* are known to the system (through the enrolment process), whereas the *impostors* can potentially be the world population. The result of the comparison between the feature vector X (extracted from the biometric sample B provided by the user) and the template T_I corresponding to his/her claimed identity I is a similarity score s which is compared to a decision threshold. If the score is higher than the decision threshold, then the claim is accepted (client), otherwise the claim is rejected (impostor).

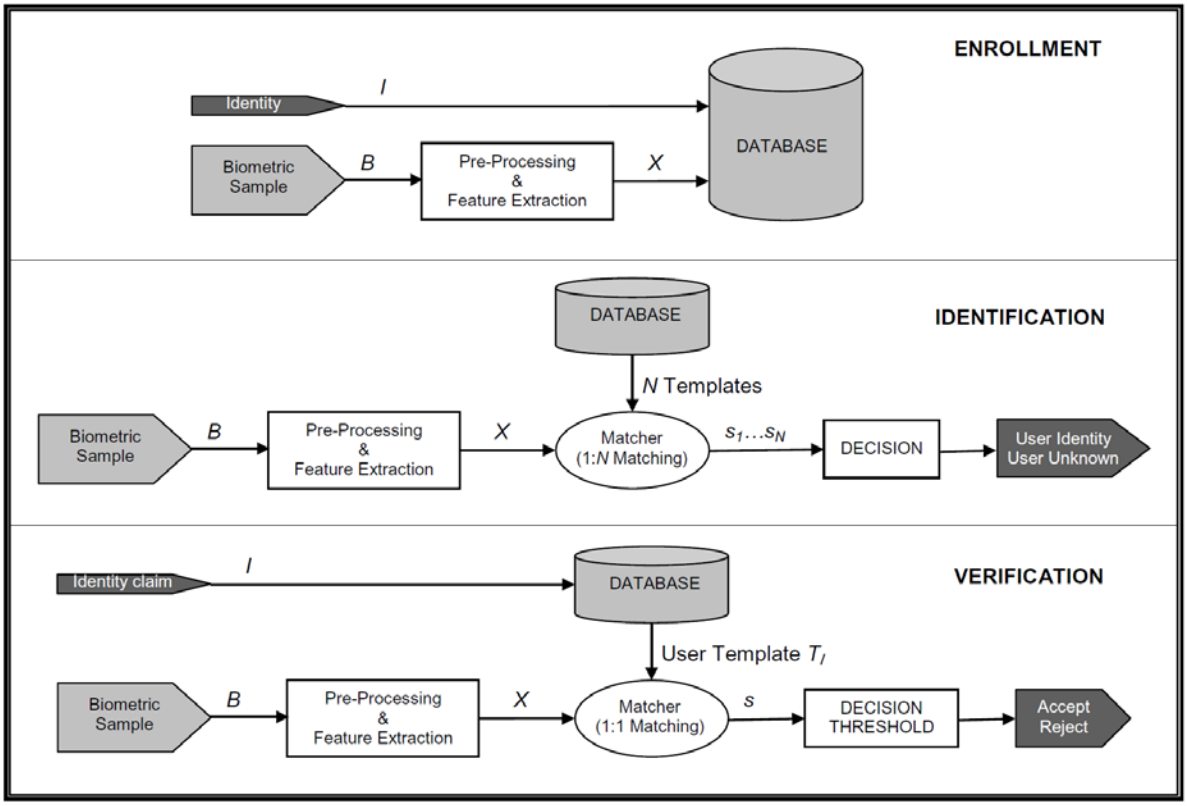

Figure 1: Diagrams of the typical modes of operation in a biometric system

1.5.1 Performance evaluation of verification systems

NOTE: as already explained in Sect. 1.4, the performance assessment of biometric systems constitutes a very wide field covering many different aspects of biometric recognition (including legal issues on personal data protection), which should be addressed on a different document. However, in spite of falling out of the scope of the present document, for completeness some basic concepts on the performance evaluation of biometric verification systems (strictly related to their vulnerability assessment) are included here.

The performance of biometric systems is estimated under normal operating conditions where the users try to access the system interacting with it in a straight forward manner. In opposition, security evaluations are carried out under attacking scenarios where an attacker tries to access (break) the system interacting with it using some type of approach or methodology for which the application was not thought. In the normal operation scenario of a verification biometric system two types of access attempts or claims of identity are defined:

- ***Genuine claim of identity***: a user making a truthful positive claim about identity in the system (the user truthfully claims to be him/herself, leading to a comparison of a sample with a truly matching template).

- ***Impostor claim of identity***: a user making a false positive claim about identity in the system (the user falsely claims to be someone else, leading to the comparison of a sample with a non-matching template).

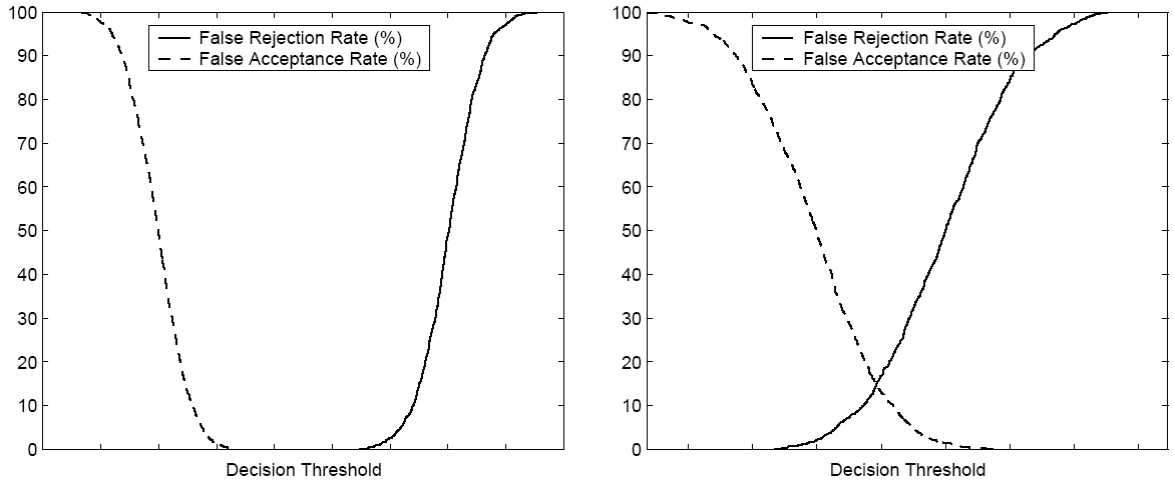

Figure 2: FA and FR curves for an ideal (left) and real (right) verification systems

Genuine attempts are also referred to as *client attempts*, while impostor attempts are also known as *zero-effort attempts*, and constitute the most basic form of attack to a biometric system.

Considering these two different types of access attempts (genuine and impostor) biometric verification can be considered as a detection task, involving a tradeoff between two types of errors:

- ***False Rejection (FR)***: occurring when a user making a genuine claim of identity is rejected by the system.

- ***False Acceptance (FA)***: taking place when a user making an impostor claim of identity is accepted into the system.

Although each type of error can be computed for a given decision threshold, a single performance level is inadequate to represent the full capabilities of the system. Therefore, the performance capabilities of verification systems have been traditionally shown in the form of FA and FR Rates versus the decision threshold, as depicted in Fig. 2 for an ideal system (left), and a real system (right). In order to estimate the FRR and FAR of a given system, a set of genuine and impostor matching scores (resulting respectively from genuine and impostor access attempts) have to be generated using the available biometric data.

Another commonly used graphical representation of the capabilities of an verification system, specially useful when comparing multiple systems, is the ROC (Receiver -or also Relative- Operating Characteristic) plot, in which FA Rate (FAR) versus FR Rate (FRR) is depicted for variable decision threshold. A variant of the ROC curve, the so-called DET (Detection Error Tradeoff) plot, is also commonly used. In this case, the use of a non-linear scale makes the comparison of competing systems easier. A comparison between ROC and DET curves for two hypothetical competing verification systems A and B is given in Fig. 3. A specific point is attained when FAR and FRR coincide, the so-called EER (Equal Error Rate). The global EER of a system can be easily detected by the intersection between the DET curve of the system and the diagonal line y = x.

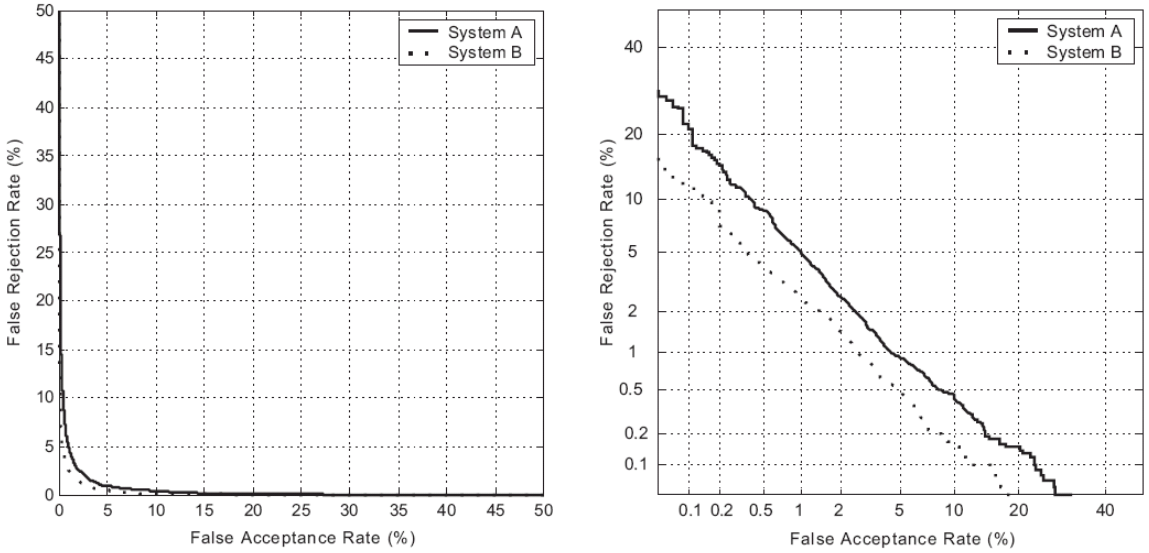

Figure 3: Example of verification performance with ROC (left) and DET curves (right)

The performance of biometric systems might also be measured in terms of the False Match Rate (FMR) and False Non Match Rate (FNMR), which are estimated in terms of the errors made when performing one *single* comparison of a submitted sample against a *single* enrolled template/model. These errors are defined to avoid ambiguity with systems allowing multiple access attempts or having multiple templates, and are generally not synonymous with FAR and FRR.

For instance, in a positive verification system allowing a maximum of three attempts to be matched to an enrolled template, a False Rejection will result with any combination of Failure-to-Acquire (i.e., the sample could not be acquire) and False Non Matches over the three attempts. A false acceptance will result if an image is acquired and falsely matched to an enrolled image on any of three attempts.

Although strictly not interchangeably, very commonly FAR and FRR are used instead of FMR and FNMR (single attempt errors). This is the case of the present document.

For further details on performance evaluation of biometric verification systems the reader is referred to:

> Mansfield and J. Wayman, "Best practices in testing and reporting performance of biometric devices," CESG Biometrics Working Group, Tech. Rep., August 2002. Available on-line at:
>
> (http://www.cesg.gov.uk/site/ast/biometrics/media/BestPractice.pdf).

1.5.2 Security evaluation of verification systems

Due to the intrinsic statistical nature of biometric verification systems, 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 Sect. 1.5.1). Determining if a certain attack is or not feasible, is in general not enough for a strict vulnerability evaluation. In order to estimate the robustness of a given biometric system to an attack, a large number of tests

should be carried out in order to find out, from a statistical point of view and not just on a yes or no basis, *how* vulnerable to the attack is the system being tested.

The security evaluation protocol reached from practical evaluation experiences and followed for the rating of the different attacks considered in the present document, is described next. The protocol includes a set of guidelines for the security analysis and reporting of the results in a useful and meaningful manner for other evaluators. In particular, the steps proposed for the systematic evaluation of biometric verification systems are:

1. Description of the attack for which we want to determine the vulnerability of the biometric system.
2. Description of the biometric system that will be evaluated.
3. Description of the information about the system under evaluation required to be known by the attacker.
4. Description of the database (if any) that will be used in the evaluation.
5. Description of the experimental protocol that will be followed in the evaluation.
6. Execution of an independent performance evaluation (see Sect. 1.5.1) of the system being tested. The performance evaluation will permit to determine if the system behaves according to the manufacturer specifications and, more important, the operating points where it will be evaluated (as the success chances of an attack are highly dependent on the FA and FR rates of the system). 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).
7. Execution of the vulnerability evaluation in the defined operating points, reporting the results in terms of (if possible) the *Success Rate* and *Efficiency* of the attack (defined next).

Two main parameters define the risk represented by an attack to a given biometric system (and therefore the vulnerability of the system to it):

- ***Success Rate***: 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 *Ab*, and the total accounts attacked *AT*, that is *SR = Ab/AT*. This parameter gives an estimation of how dangerous it is a particular attack for a given biometric system: the higher the *SR* the bigger the threat.

NOTE: a direct correlation may be drawn between the SR of an attack against a given biometric-based security system and other well-known attacks in different security fields. For instance, if we consider a system secured by a 4-digit PIN, it is straight forward to infer that, on average, 1 in every 10,000 accounts will be broken on the basis of a one random trial per account. Thus, the SR of the attack on this particular system would be SR=1/10,000. However, if the PIN was extended to 6 digits, then the success chances of such an attack would decrease to SR=1/1,000,000. Similarly, not all biometric-based security systems are equally vulnerable to a certain attack, and these differences are pointed out through the SR.

- ***Efficiency***: It indicates the average number of matchings needed by the attack to try to break an account. It is defined as $E_{ff} = \left(\sum_{i=1}^{A_b} n_i \right) \Big/ A_b$, where n_i is the number of comparisons needed to compromise each of the breakable accounts. This parameter gives an estimation of how easy it is for the attack to break into the system in terms of speed: the lower the E_{ff} the faster the attack.

With the term *account* we refer to the enrolled biometric template/model of a legitimate user which is used as reference to be matched against the test samples.

EXAMPLE: let us consider an attack carried out with gummy fingers against a system with 10 enrolled users (accounts). Let us assume that the attacker is able to break into 9 of those 10 accounts and that he needs 3 attempts to break into 4 of them, and 2 attempts to break the remaining 5 (one of the accounts is resistant to the attack). For this particular case: $SR = 9/10 = 0.9 = 90\%$ *and* $E_{ff} = \left[(4 \cdot 3) + (5 \cdot 2) \right] \big/ 9 = 2.44$ *matchings.*

Although the previous features constitute the way to model in a strict and statistical manner the vulnerability of a system to a given attack, in the frame of an AVA_VAN evaluation of the CC, it may not be necessary to compute these two parameters. Under the assumption of the worst case scenario, in which the ratings of the present document have been computed, if just one case is found in which the system is broken by a certain attacking approach, then the system fails that component (regardless of the *SR* and E_{ff} of the attack against the system). Thus, in the case of the previous example, if we were able to find a "golden fake" manufactured with a certain material (i.e., gelatine) which is able to break a few accounts (3-5) almost at the first attempt, then we may say that the system is vulnerable to the attack and that it fails that particular component (even if it were resistant to gummy fingers generated with many other materials: silicone, plasticine, glue...)

Similarly to the previous approach, when a countermeasure is introduced in a biometric system to reduce the risk of a particular attack (previously analyzed), it should be statistically evaluated considering two main parameters:

- ***Impact of the countermeasure in the system performance***. The inclusion of a particular countermeasure might change the FAR and FRR of a system, and these changes should be evaluated and reported (other performance indicators such as speed or computational efficiency might also change, and should also be considered).

- ***Performance of the countermeasure***, i.e. impact of the countermeasure in the SR and Efficiency of the attack.

1.5.3 Attacks to fingerprint verification systems

In Fig. 4 a diagram with the *biometric-based* attack classification that will be followed in this document is shown. The attacks that can compromise the security provided by a fingerprint verification system may be categorized into two basic types:

- ***Zero-effort attacks***: also known as *intrinsic failure*. 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 (fingerprint images) 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). This probability mainly depends on the system accuracy and on the biometric trait individuality. In this type of attacks the impostor uses the system in a normal and straight forward manner.

- ***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 (e.g., hacking an internal module, using a fake biometric trait, deliberately manipulating his biometric trait to avoid detection, etc.)

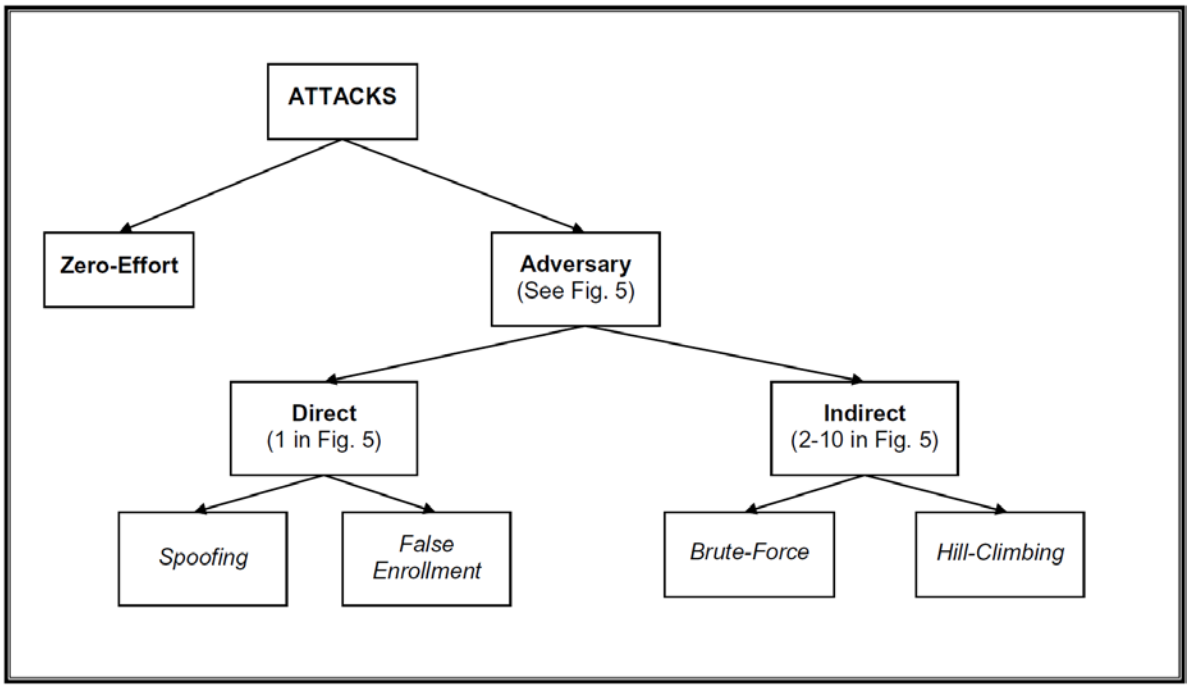

Figure 4: Classification of the *biometric-based* attacks against fingerprint verification systems considered in this document

As brute-force vulnerabilities are inherent to the statistical nature of biometric systems, the biometric community has focused in the study of adversary attacks, which have been systematically categorized in ten classes depending on the point to which they are directed (depicted in Fig. 5). These adversary attacks can be grouped in direct and indirect attacks as follows (see Fig. 5):

- ***Direct attacks***. These threats correspond to type 1 in Fig. 5 and are aimed directly to the sensor trying to gain access to the system by impersonating a real user. When they are executed against a biometric verification system working on a physiological trait (as is the case of fingerprints) they are also known as *spoofing* and try to enter the system by presenting a fake biometric trait or artefact (e.g., gummy finger) to the acquisition device, or by reactivating a latent fingerprint on the sensor. This type of approach can also be used to carry out a *false enrollment attack* using a fake imitation with the fingerprint impression of a different user. For completion we will

say here that in the case of biometric systems based on behavioural traits (e.g., signature, voice) this type of approaches are known as *mimicry*, where the attacker tries to break the system by imitating the legitimate user producing the so-called skilled forgeries.
It is worth noting that in this type of attacks no specific knowledge about the system is needed (matching algorithm used, feature extraction, feature vector format, etc.) Furthermore, the attack is carried out in the analogue domain, outside the digital limits of the system, so the digital protection mechanisms (digital signature, watermarking, etc.) cannot be used.

- ***Indirect attacks***. This group includes all the remaining nine points of attack identified in Fig. 5. Attacks 3, 5 and 10 might be carried out using a Trojan Horse that replaces the feature extractor, the matcher, or the decision threshold respectively, and outputs a feature vector, matching score, or final decision different from the original. In attack 6 the system database is manipulated (a template is changed, added or deleted) in order to gain access to the application (also known as *substitution* attack, it can also be executed as a type 7 attack between the database and the matcher). The remaining points of attack (2, 4, 7, 8 and 9) are thought to exploit possible weak points in the communication channels of the system, extracting, adding or changing information from them.
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.

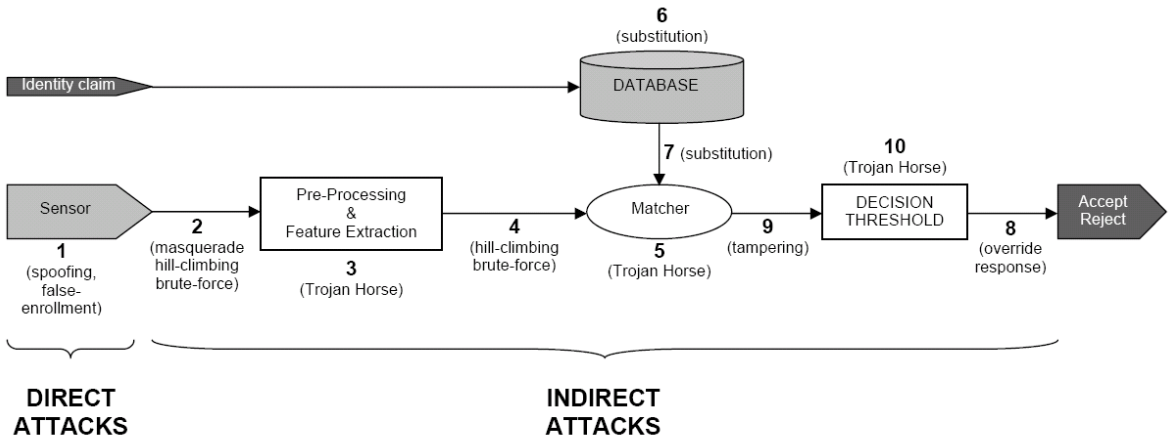

Figure 5: Possible adversary attack points to a fingerprint verification system as considered in the present document.

1.5.4 Match-on-Card (MoC) and Storage-on-Card (SoC) systems

Some of the attacks described in the present document, specially those which need the compromised template of a legitimate user (e.g., spoofing attacks starting from a template), are of special relevance in Match-on-Card (MoC) and Storage-on-Card (SoC) systems.

The majority of biometric systems in use today operate in a database environment. Whether it is a large-scale database such as US-VISIT or a small bank of biometrics stored on a server for logical access in an office, the solutions are based on networks that are vulnerable

to cyberattacks. Match-on-Card technology eliminates the need for the database by both storing and processing biometric data directly on a smartcard, providing a secure, privacy-enhancing biometric program with dynamic flexibility and scalability.

Match-on-Card technology elevates biometrics from a mere PIN replacement to an integral part of a secure and privacy-enhancing authentication solution. Match-on-Card technology takes biometric security and convenience one step further by performing the actual fingerprint match within the tamperproof environment of a smartcard. This removes the uncertainty of matching on a network-connected device, an external server, or a database, normally considered weak links in the security chain. It is important to emphasize the difference between Match-on-Card systems, where smartcards are used as storage and processing systems, and Storage-on-Card (also Template-on-Card) systems in which the cards only store the template and transfer it to an external system in order to carry out the matching.

The MoC technology was developed to meet the needs and demands of new markets such as national ID programs and travel documents. Match-on-Card is becoming an integral part of high-security smartcard-based biometric authentication in many diverse markets.

Although MoC systems present some very interesting features that make them more convenient in certain scenarios, they are not free from certain disadvantages. In a traditional biometric system, the processor power, the computer, has virtually no limits and the challenge for the algorithm is performance, speed, and effectiveness when it comes to processing huge amounts of biometric data. For a Match-on-Card implementation the challenges are different. The processor is in this case the small processor on the smartcard and the algorithm has to be optimized for very low processor performance and still deliver the security level and speed that is needed for the application and for practical usability. It should be emphasized, once more, that the definition of Match-on-Card is when the matching of the reference data with the verification data is performed on the smartcard, not when the smartcard is only used to store the reference data (template) on the card and transferred over to the computer to do the matching (Template-on-Card).

Furthermore, although in MoC systems communication channels are minimized (and thus cannot be intercepted), there still exists the possibility that the user's template is extracted in a fraudulent way from the smart card and used to attack the system (e.g., direct attack starting from a template).

2 Attack Methods

2.1 Direct Attacks

2.1.1 Description of the attack

These attacks try to illegally gain access to the biometric system presenting to the sensor a fake biometric fingerprint or, in the worst case, although it falls out of the scope of the present document, a dismembered one. Note that, although having some general information on the sensor will increase its success chances, in order to perform this attack no specific knowledge about the system functioning is needed (e.g., matching algorithm used, features extracted, template format, etc), hence its feasibility is higher than that of other attacks. Furthermore, since it operates in the analog domain, outside the digital limits of the biometric system, the digital protection mechanisms such as encryption, digital signature, hashing etc. are not applicable.

As mentioned above, in a traditional direct attack, the impostor makes (by some means) a fake gummy finger of the legitimate user's fingerprint and tries to access the system using the artifact (i.e., the matching is performed between the real enrolled template of the genuine user, and the image obtained from the fake fingerprint).

Although it is not considered in this document (as there are too many external factors not specifically related to the biometric system which may influence in its success chances), a different type of direct attack, known as "false enrollment", can be performed if the attacker uses the gummy finger to enroll to a system and then tries to access with that same fake fingerprint (i.e., the matching is performed between a fake enrolled template, and the image obtained from that same fake fingerprint). These attacks can be specially harmful if no countermeasures are provided in the enrollment stage, which is the case for many systems as the enrollment is commonly a supervised process (however, a thin transparent gummy finger attached to the fingertip would be very difficult to detect for a human supervisor).

2.1.2 Effect of the Attack

Three types of direct attacks can be distinguished depending on the information available to generate the gummy finger:

- *Residual prints*: this is the most basic and simple type of direct attack. Some sensors are sensitive to the print left on them after acquisition, which may be reactivated by very simple manipulations such as: gently breathing on the sensor, using an adhesive film, or even just placing a plastic bag with water on the scanner.

- *Direct attacks starting from a mould*: in this case the attacker has obtained by some means (probably with the cooperation of the legitimate user) a mould with the negative of the fingerprint (with plasticine or wax, for example). Then the final gummy finger is generated using for instance silicone or gelatin.

- *Direct attacks starting from a 2D image*: as already explained in this document we will rate the attacks under the assumption of the worst case scenario. For this reason we will consider fingerprints as public information which may always be obtained by some fairly easy method. Thus, for the ratings of this type of attacks we will not consider the process by which the attacker has obtained the 2D image of the fingerprint (e.g., lifting a latent fingerprint from a given surface) as this would just add too much uncertainty to the rating process.
  The most popular technique to go from the 2D image to the 3D negative of the fingerprint (mould) is to use a Printed Circuit Board (PCB). The 2D image is processed before using it to generate the negative of the fingerprint on a PCB. The PCB is then covered with silicone, gelatin, or some other material of similar characteristics in order to obtain the fingerprint imitation.
  A particular example of this type of attacks is the case in which the latent fingerprint has been left on the sensor surface. This fingerprint can be recovered and presented again to the sensor by just breathing on it, or placing a plastic bag with water on it (not feasible with sensors using sweeping technology). This case represents a nearly effortless attack against which external measures should be taken (e.g., automatically cleaning the sensor surface after each usage) and will not be further considered.

NOTE: although using PCBs is the most common technique to perform direct attacks starting from a 2D image, other methods which are not as effective but that do not require of specific knowledge or material for PCB manufacturing have also been described in some works (e.g., printing the image on a foil). These alternative schemes would require in a practical rating example a lower level of expertise and equipment than those attacks performed using PCBs.

- *Direct attacks starting from a minutiae template*: in this case the starting point of the attack is the stolen minutiae template of the genuine user (again, we will not take into account the process by which the attacker stole the template). The key step of the attack is the reconstruction from the minutiae template of a realistic fingerprint as similar as possible to the original image of the legitimate user. This process is extremely complex, as a matter of fact until very recently there was a widespread belief of the non-reversibility of fingerprint minutiae templates. Up to date there is only one work that has successfully challenged this belief under determined circumstances (basically enough number of available minutia points). Furthermore, even in the case of being able to reconstruct fingerprint images from its template, the attack requires a difficult task of reverse engineering to find out the template format (which can be encrypted) in order to distinguish the necessary information (location, angle and type of the minutiae) for the reconstruction process.
  Once a realistic fingerprint image has been reconstructed, the procedure is very similar to that used in the attacks starting from a 2D image: a PCB is used to generate the negative of the fingerprint, and then silicone, gelatin, or some other material of similar characteristics is used to obtain the fingerprint imitation.

2.1.3 Impact on TOE

The attack is directed against the sensor and is independent of the embedded software (i.e., it could be applied to any embedded software and is independent of software countermeasures).

The main impact of the attack is the fraudulent access to the information secured by the system.

The potential use of these techniques is very wide and has to be carefully considered in the context of each evaluation.

2.1.4 Characteristics of the Attack

One of the main advantages of this attack relies on its simplicity and the absence of any required technical knowledge. Only in the case of sensors with liveness detection countermeasures some more sophisticated procedure should be used, but even in that situation it is more a case of manual skill than of having a deep understanding of the biometric technology.

As mentioned before, in the attacks based on reactivating a latent fingerprint left on the sensor no specific knowledge (LAYMAN) or specific equipment (STANDARD) are needed, as the process may be as simple as breathing on the scanner's surface.

In the attacks starting from a mould a LAYMAN level of expertise is needed, while in the attacks starting from 2D image some basic knowledge on image processing is required, and, in the case of self-manufacturing the PCBs also some specific knowledge in the generation of PCBs is needed (although such PCBs can easily be obtained from third parties). Thus, under the worst case scenario assumption, a LAYMAN level of expertise from the CEM v3.1 potential tables can be used also in the latter case. For the case in which the attack starts from the compromised minutiae template of the legitimate user, the attacker also needs to have deep knowledge in pattern recognition, computer vision, and image processing in order to be able to reconstruct the fingerprint image from the minutiae information. EXPERT will be used as the rating for the level of expertise in this attack.

The equipment typically used for the direct attacks starting from a mould can be easily obtained, being in all cases of-the-shelf products (STANDARD):

- Generation of the mould for the negative of the fingerprint: materials such as plasticine, wax, etc.

- Generation of the gummy finger: materials such as latex, silicone, gelatine, etc.

In order to generate gummy fingers starting from a 2D fingerprint image the STANDARD or SPECIALIZED ratings may be used depending on whether we self-generate the PCBs or if we order them to specialized manufacturers:

- Digitalizing of images: standard scanner (STANDARD).

- Image processing: standard software such as photoshop (STANDARD). Depending on the quality of the images some further specific processing (e.g., using Matlab) might be needed.

- Generation of the negative of the fingerprint: specific equipment for the processing and generation of PCBs is needed (SPECIALIZED). If the PCBs are not self-manufactured then the rating can be reduced to STANDARD.

- Generation of the gummy finger: materials such as latex, silicone, gelatine, etc (STANDARD).

For the generation of gummy fingers starting from a minutiae template some specific equipment is needed, thus the SPECIALIZED rating from the potential tables should be used:

- Digitalizing of images: standard scanner (STANDARD).

- Software: specific computational software such as Matlab (SPECIALIZED) in order to accomplish the fingerprint image reconstruction process.

- Generation of the negative of the fingerprint: specific equipment for the processing and generation of PCBs is needed (SPECIALIZED). Again, the STANDARD rating may also be used in the worst case scenario were the PCBs are generated by some third party.

- Generation of the gummy finger: materials such as latex, modeling silicone, gelatine, etc (STANDARD).

Some detailed examples of these types of attacks can be found in:

- J. Galbally, J. Fierrez, J. D. Rodriguez-Gonzalez, F. Alonso-Fernandez, J. Ortega-Garcia, and M. Tapiador, "On the vulnerability of fingerprint verification systems to fake fingerprint attacks," in *Proc. IEEE of International Carnahan Conference on Security Technology*, vol. 1, 2006, pp. 130–136.

- T. van der Putte and J. Keuning, "Biometrical fingerprint recognition: don't get your fingers burned," in *IFIP*, 2000, pp. 289–303.

- T. Matsumoto, H. Matsumoto, K. Yamada, and S. Hoshino, "Impact of artificial gummy fingers on fingerprint systems," in *Proc. SPIE, Optical Security and Counterfeit Deterrence Techniques IV*, vol. 4677, 2002, pp. 275–289.

- L. Thalheim and J. Krissler, "Body check: biometric access protection devices and their programs put to the test," *ct magazine*, 2002.

- H. Kang, B. Lee, H. Kim, D. Shin, and J. Kim, "A study on performance evaluation of the liveness detection for various fingerprint sensor modules," in *Proc. of KES2003*, pp. 1245-1253,2003

- J. Galbally, R. Cappelli, A. Lumini, G. Gonzalez-de-Rivera, D. Maltoni, J. Fierrez, J. Ortega-Garcia and D. Maio, "An Evaluation of Direct Attacks Using Fake Fingers Generated from ISO Templates", *Pattern Recognition Letters*, Vol 31, pp. 725-732, 2010.

2.1.5 Example: direct attack based on a residual print on the sensor

The objective of the attack is to illegally gain access to the system through the reactivation of a latent fingerprint left on the sensor surface.

Step 0. Reactivation of the latent fingerprint: Different tricks may be adopted for this purpose, among them: gently breathe on the sensor, use an adhesive film, or place a plastic bag with water on the scanner.

NOTE: this first step is developed on the IDENTIFICATION of the attack, while in EXPLOTATION the method to reactivate the fingerprint is known.

Step 1. Exploitation of the latent fingerprint: in this phase we assume that the attacker has already found the way to trigger the residual print (in step 0) and here this method is used to access the system.

For this particular case, we refer the reader to performance evaluation comparative studies.

Source	L. Thalheim and J. Krissler, "Body check: biometric access protection devices and their programs put to the test," *ct magazine*, 2002.	
General parameters	System:	Minutiae based
	Operating point:	High security
	Sensor:	Capacitive

Rating example 1. *Direct attack using a residual print left on the sensor surface.*

For this example we assume a simple fingerprint minutiae based system, working with an capacitive sensor and with no countermeasures.

We will consider that the amount of time needed to identify the right method to reactivate the latent fingerprint can take around 2 days.

In the exploitation scenario we assume that the attacker already has the knowledge to reactivate the residual print in a fast and reliable way. Since there is no restriction in the number of access attempts, and the attacker only needs physical access to the sensor (normal operation mode of the system), we consider that less than one day should be enough to generate the gummy finger and perform the attack trials.

Factor	Comment	Identification	Exploitation
Elapsed Time	In identification, time needed to identify the "golden fake". In exploitation only time required to use the golden fake.	< 2 days (0)	< 1 days (0)
Expertise	The manual work required for the generation of the gummy fingers does not need any type of special skill.	Layman (0)	Layman (0)
Knowledge of TOE	We only need to know the type of sensor used in the system. Information which can be obtained at simple sight.	Public (0)	Public (0)
Window of opportunity	The attack does not require any kind of opportunity to be carried out and there is very small risk of being detected during the access to the TOE.	Unlimited (0)	Unlimited (0)
Equipment	The required material for the attack can be easily obtained.	Standard (0)	Standard (0)
Total		**0**	**0**
FINAL RATING		**0**	

Table 3

Given the resulting sum, 0, the attack potential required to carry out a successful attack is BASIC, so the TOE is resistant to attackers with attack potential of NO RATING (it falls below that considered to be Basic). It fails all components AVA_VAN.1-5.

2.1.6 Example: direct attack starting from a mould

The objective of the attack is to illegally gain access to the system through the presentation to the sensor of a gummy finger generated from a mould of the fingerprint of the legitimate user.

Step 0. Generation of the mould: get the user to place his finger on the material used to generate the negative of the gummy finger (wax, plasticine…). This step is specified here for clarity but will not be taken into account in the rating of the attack, as it is highly dependent on multiple external factors to the system, very difficult to quantize objectively, and which do not reflect the robustness of the TOE to the attacking scheme.

Step 1. Generation of the gummy finger: Different materials should be tried in order to find out which of them is more suitable to bypass the scanner (golden fake).

NOTE: these first two steps are developed on the IDENTIFICATION of the attack, while in EXPLOTATION the method to generate the gummy fingers is known and thus the time needed for the attack is smaller.

Step 2. Exploitation of the gummy finger: place the gummy finger on the sensor. In general if the system uses a capacitive or a thermal sensor the process to get the application to acquire an image is more difficult than when using an optical sensor. In any case the process can be anywhere from easy (e.g., we gain access on the first attempt), to impossible (e.g., the system consistently rejects the gummy fingers).

NOTE: in this case, and even considering the worst case scenario and the existence of a "golden fake", the attacker may need to perform several tries in order to access the system (e.g., due to different alignments or rotation angles of the finger). This would affect the E_{ff} of the attack and may be accounted for in the ratings of the attack changing the value of the "window of opportunity" (i.e., needing more attempts will narrow the window of opportunity). It is a task of the evaluation laboratory to take into account this E_{ff} of the attack (which may vary greatly from one case study to another) and reflect it on the final rating.

A case study for a particular evaluation scenario is given below:

Source	J. Galbally, J. Fierrez, F. Alonso-Fernandez and M. Martinez-Diaz, "Evaluation of direct attacks to fingerrprint verification systems", *Journal of Telecommunication Systems, Special Issue of Biometrics Systems and Applications*, 2010.	
General parameters	System:	Minutiae based
	Operating point:	FAR=0.1%
	Sensor:	Optical
	Material fake fingers:	Silicone

Rating example 1. *Direct attack starting from a mould, without countermeasures.*

For this example we assume a simple fingerprint minutiae based system, working with an optical sensor and with no countermeasures, in particular:

- No liveness-detection methods (for an indication on how this countermeasure might affect the rating of the attack we refer the reader to rating example 1 in Sect. 2.1.7).
- No use of multimodality (combination of more than one biometric trait).
- No limit in the number of access attempts (for an indication on how this countermeasure might affect the rating of the attack we refer the reader to rating examples 1 and 2 in Sect. 2.2.7).

NOTE: although here we will consider an unlimited access to the TOE, in real scenarios the window of opportunity might change depending of the operating environment of the system.

From our experience we consider that the amount of time needed to identify the right material to generate the gummy fingers that can fool a given scanner ("golden fake") following the process described above, and all the subsequent necessary tests, would take around 1 week.

In the exploitation scenario we assume that the attacker already has the knowledge to generate the gummy fingers in a fast and reliable way and that he only needs a couple of days to generate them and to access the TOE in order to carry out the attack. Since there is no restriction in the number of access attempts, and the attacker only needs physical access to the sensor (normal operation mode of the system), we consider that less than three days should be enough to generate the gummy finger and perform the attack trials.

Factor	Comment	Identification	Exploitation
Elapsed Time	In identification, time needed to identify the "golden fake". In exploitation only time required to use the golden fake.	< 1 week (1)	< 3 days (0)
Expertise	The manual work required for the generation of the gummy fingers does not need any type of special skill.	Layman (0)	Layman (0)
Knowledge of TOE	We only need to know the type of sensor used in the system. Information which can be obtained at simple sight.	Public (0)	Public (0)
Window of opportunity	The attack does not require any kind of opportunity to be carried out and there is very small risk of being detected during the access to the TOE.	Unlimited (0)	Unlimited (0)
Equipment	The required material for the attack can be easily obtained.	Standard (0)	Standard (0)
Total		**1**	**0**
FINAL RATING		**1**	

Table 4

Given the resulting sum, 1, the attack potential required to carry out a successful attack is BASIC, so the TOE is resistant to attackers with attack potential of NO RATING (it falls below that considered to be Basic). It fails all components AVA_VAN.1-5.

Rating example 2*. Direct attack starting from a mould, with liveness detection countermeasures.*

For this rating example we will consider the same attack as in the previous case (direct attack starting from a mould), but against a system with efficient liveness detection countermeasures.

For this case, identifying the material and the way to manufacture the golden fake that will break the system almost in all cases can take up to 2 weeks of the time of some PROFICIENT person which is largely familiar with the process of generating all kind of fake fingers and who is able to identify the specific properties of a given scanner. However, once the golden fake has been found, it is easy to replicate the process and so the level of expertise required by the attacker in the exploitation phase is LAYMAN.

At the same time we will consider that, being a high security product, the vendor will restrict its distribution only to institutions (not to individuals). This way, the knowledge of TOE will change from public to RESTRICTED, and the window of opportunity for the identification phase will raise from unlimited to MODERATE.

Factor	Comment	Identification	Exploitation
Elapsed Time	In identification, time needed to identify the "golden fake". In exploitation only time required to use the golden fake.	< 2 weeks (2)	< 1 day (0)
Expertise	The manual work required for the identification of the golden fake needs some skill.	Proficient (3)	Layman (0)
Knowledge of TOE	We need some specific information about the scanner in order to identify the golden fake.	< Restricted (2)	Public (0)
Window of opportunity	Restricted distribution of the TOE to institutions (no distribution to individuals).	< Moderate (3)	Unlimited (0)
Equipment	The required material for the attack can be easily obtained.	Standard (0)	Standard (0)
Total		**10**	**0**
FINAL RATING		**10**	

Table 5

Given the resulting sum, 10, the attack potential required to carry out a successful attack is BASIC, so the TOE is resistant to attackers with attack potential of NO RATING (it falls below that considered to be Basic). It fails all components AVA_VAN.1-5.

Rating example 3*. Direct attack starting from a mould, with highly efficient liveness detection countermeasures.*

Next, we give a possible example of the minimum expected performance of the liveness detection countermeasures in order for the system to have the BASIC rating.

In this case the process to identify the golden fake would take between two weeks and a month and it would require a PROFICIENT person in the generation of gummy fingers both in the identification and the exploitation phase.

Furthermore, the attacker would need to have access to SENSITIVE information (regarding the liveness detection approach embedded in the scanner) in order to be able to generate the golden fake, and he would have restricted access to the TOE in the identification phase. Thus, the window of opportunity will be rated as DIFFICULT in identification and EASY in exploitation (as it is expected that even with the golden fake more than one or two attempts will be needed, or even more than one gummy finger will have to be manufactured).

Factor	Comment	Identification	Exploitation
Elapsed Time	In identification, time needed to identify the "golden fake". In exploitation only time required to use the golden fake.	< 1 month (4)	< 1 day (0)
Expertise	The manual work required for the identification of the golden fake needs some skill both in identification and exploitation.	Proficient (3)	Proficient (3)
Knowledge of TOE	We need specific information about the scanner in order to identify the golden fake.	< Sensitive (5)	Public (0)
Window of opportunity	Restricted distribution of the TOE to institutions (no distribution to individuals). Several attempts needed in exploitation under a semi supervised protocol.	< Difficult (6)	Easy (1)
Equipment	The required material for the attack can be easily obtained.	Standard (0)	Standard (0)
Total		**18**	**4**
FINAL RATING		**22**	

Table 6

Given the resulting sum, 22, the attack potential required to carry out a successful attack is ENHANCED BASIC, so the TOE is resistant to attackers with attack potential of BASIC. It fails all components AVA_VAN.3-5.

2.1.7 Example: direct attack starting from 2D fingerprint image

The objective of the attack is to illegally gain access to the system through the presentation to the sensor of a gummy finger generated from a 2D fingerprint image which has been previously obtained by any means (e.g., lifting a latent fingerprint).

Step 0. Recovery of the 2D image. Just for clarity and as an example, we will consider here the case of the 2D image being recovered from a latent fingerprint which is lifted using some standard forensic material. This step is specified here for clarity but ***it is not*** taken into account in the rating of the attack, as it is highly dependent on multiple external factors to the system, very difficult to quantize objectively, and which do not reflect the robustness of the TOE to the attacking scheme.

Step 1. Image processing. The resulting image has to be processed in order to recover badly defined areas, to enhance ridges and valleys, and last to invert ridges and valleys.

Step 2. Generation of the negative. The processed image is then used to generate a PCB where the circuit lines are the fingerprint valleys.

Step 3. Generation of the gummy finger. Different materials should be tried in order to find out which of them is more suitable to bypass the scanner (golden fake).

These first three steps are developed on the IDENTIFICATION of the attack, while in EXPLOITATION the method to generate the "golden gummy fingers" is known and thus the time needed for the attack is smaller.

Step 4. Exploitation of the gummy finger. Place the gummy finger on the sensor so that the fake fingerprint image is acquired.

This process is slightly more difficult than that carried out for a direct attack starting from a mould as we have to deal with the generation of PCBs. In the case of self-manufacturing the PCBs we need some specialized material, equipment and knowledge. However, there are companies specialized in generating PCBs on demand for a low price (in this latter case only STANDARD material would be required).

A case study for a particular evaluation scenario is given below:

Source	J. Galbally, J. Fierrez, F. Alonso-Fernandez and M. Martinez-Diaz, "Evaluation of direct attacks to fingerrprint verification systems", *Journal of Telecommunication Systems, Special Issue of Biometrics Systems and Applications*, 2010.	
General parameters	System:	Ridge-based
	Operating point:	FAR=0.1%
	Sensor:	Capacitive
	Material fake fingers:	Silicone

Rating example 1. *Direct attack starting from a 2D image, with liveness detection*

For this example we consider a simple fingerprint minutiae based system, working with an optical sensor and with a liveness detection method based on skin distortion.

The generation of gummy fingers using PCBs is more time consuming than starting from a mould. In addition, the liveness detection countermeasure has an effectiveness of over 80%, which means that 4 out of 5 attempts of accessing the system with a gummy finger will be directly repelled by the system (until the golden fake is found). Thus, the elapsed time to carry out the attack in IDENTIFICATION is somewhat higher than in the case of starting the attack from a mould and no liveness detection embedded in the sensor. Once the golden fake is identified (EXPLOITAITION), all ratings remain the same.

For this particular example we will consider no restriction in the distribution of the TOE and no limit to its access.

Factor	Comment	Identification	Exploitation
Elapsed Time	In identification, time needed to identify the "golden fake". In exploitation only time required to use the golden fake.	< 2 weeks (2)	< 1 day (0)
Expertise	The manual work required for the identification of the golden fake needs some skill.	Proficient (3)	Layman (0)
Knowledge of TOE	We only need to know the basic characteristics of sensor used in the system. Information which can be easily obtained from the manufacturer.	Public (0)	Public (0)
Window of opportunity	The attack does not require any kind of opportunity to be carried out and there is very small risk of being detected during the access to the TOE.	Unlimited (0)	Unlimited (0)
Equipment	The required material for the attack can be easily obtained (assuming that the PCBs are generated elsewhere).	Standard (0)	Standard (0)
Total		**5**	**0**
FINAL RATING		**5**	

Table 7

Given the resulting sum, 5, the attack potential required to carry out a successful attack is BASIC, so the TOE is resistant to attackers with attack potential of NO RATING (it falls below that considered to be Basic). It fails all components AVA_VAN.1-5.

2.1.8 Example: direct attack starting from a minutiae template

The steps to be carried out for this attack are:

Step 0. Obtaining the minutiae template. This step is specified here for clarity but ***it is not*** taken into account in the rating of the attack, as it is highly dependent on multiple external factors to the system, very difficult to quantize objectively, and which do not reflect the robustness of the TOE to the attacking scheme.

Step 1. Development of a fingerprint reconstruction software. As expressed above, this task requires a high level of expertise and will take a great amount of time (more than six months).

Step 2. Finding the template format. Before the software can be used, we have to find the way in which the different minutiae parameters (location, angle and type) are stored in the

template. This task can be anywhere from easy (the template follows a known standard with no encryption), to very difficult (encrypted proprietary template).

Step 3. Fingerprint image reconstruction. Once the information is available in an understandable format it can be passed to the reconstruction software to generate the fingerprint image.

The rest of the actions are those described in the direct attack starting from a 2D image (section 2.1.6), which are:

Step 4. Generation of the negative. The reconstructed image is then used to generate a PCB where the circuit lines are the fingerprint valleys.

Step 5. Generation of the gummy finger. Different materials should be tried in order to find out which of them is more suitable to bypass the scanner (golden fake).

Step 6. Exploitation of the gummy finger. Place the gummy finger on the sensor so that the fake fingerprint image is acquired.

Again, several gummy fingers will have to be generated using different materials in the identification phase in order to find the golden fake that is able to bypass the system.

A case study for a particular evaluation scenario is given below:

Source	J. Galbally, R. Cappelli, A. Lumini, G. Gonzalez-de-Rivera, D. Maltoni, J. Fierrez, J. Ortega-Garcia and D. Maio, "An Evaluation of Direct Attacks Using Fake Fingers Generated from ISO Templates", *Pattern Recognition Letters*, Vol 31, pp. 725-732, 2010.	
General parameters	System:	ISO miutiae-based
	Operating point:	FAR=0.1%
	Sensor:	Optical
	Material fake fingers:	Silicone

Rating example 1. *Direct attack starting from a minutiae template, without countermeasures*

We will consider a minutiae based system working with unencryted standard ISO templates (knowledge of TOE both in identification and exploitation PUBLIC).

In identification the development of an automatic fingerprint reconstruction software is extremely costly and difficult, so the time is estimated in more than 6 months. In exploitation, once the reconstruction software is available and the golden fake has been identified, the time needed to carry out the attack is less than one day.

In order to develop the reconstruction software the attacker needs to have deep knowledge in pattern recognition, computer vision, and image processing in order to be able to reconstruct the fingerprint image from the minutiae information. EXPERT will be used as the rating for the level of expertise in this attack (IDENTIFICATION). In exploitation, once the software is available, no specific expertise is needed.

Factor	Comment	Identification	Exploitation
Elapsed Time	On the basis of the previous estimations.	> 6 months (19)	< 1 day (0)
Expertise	In identification large experience in pattern recognition techniques and in image processing is needed. For exploitation no specific knowledge is needed.	Expert (6)	Layman (0)
Knowledge of TOE	No information of TOE is needed for the attack.	Public (0)	Public (0)
Window of opportunity	Both in Identification and Exploitation there are no access limitations to the TOE.	Unlimited (0)	Unlimited (0)
Equipment	The required material for the attack can be easily obtained (assuming that the PCBs are generated elsewhere).	Standard (0)	Standard (0)
Total		**25**	**0**
FINAL RATING		**25**	

Table 8

Given the resulting sum, 25, the attack potential required to carry out a successful attack is ENHANCED BASIC, so the TOE is resistant to attackers with a BASIC attack potential. It fails component AVA_VAN.3-5.

2.2 Brute Force indirect attacks

2.2.1 Description of the attack

These attacks try to illegally gain access to the biometric system with a succession of *zero-effort* attempts, that is, presenting multiple fingerprints to the feature extractor (images) or to the matcher (templates). The fingerprint images can either be real (i.e., captured with a fingerprint sensor) or synthetic (i.e., generated with specific software). To carry out this attack we need physical access to the TOE in order to insert the images/templates, as well as some knowledge about the functioning of the system: sensor used and resolution of the images, information stored (minutiae, ridge pattern…), format of the stored data, etc.

2.2.2 Effect of the Attack

Two types of brute force attacks can be distinguished depending on the module of the biometric system to which they are directed:

- *Brute Force attacks to the feature extractor*: the attack tries to exploit the False Acceptance Rate (FAR) intrinsic to any biometric system by presenting multiple fingerprint images to the feature extractor input. The images can either be real (acquired with a compatible sensor to the one used in the system) or synthetic (generated with specific software). Thus, the attack requires physical access to the feature extractor, and some specific knowledge about the images used: size and resolution.

- *Brute Force attacks to the matcher*: in this case the attacker tries to exploit the FAR of the system by presenting multiple fingerprint templates to the matcher input. These attacks require physical access to the matcher and specific knowledge about the information stored (e.g., minutiae, the ridge pattern), and how this information is stored in the templates (i.e., format of the feature vector).

2.2.3 Impact on TOE

The attack is directed against the feature extractor or the matcher of the system and the main impact is the fraudulent access to the information secured by the TOE.

2.2.4 Characteristics of the Attack

This type of attack requires physical manipulation of the system, thus the window of opportunity in which to be executed is significantly narrower than in the direct attacks case, thus an EASY/MODERATE rate will be used in the following examples.

In addition, a higher level of knowledge of the TOE is required, as the attacker needs to know the size and resolution of the fingerprint images in the case of directing the attack to the input of the feature extractor, and the template format when accessing to the matcher input.

These attacks require specific equipment in order to locate the matcher and feature extractor inputs, and to enable a communication path between this point and a device (PC, mobile phone, PDA, etc.) from which to launch the attacks.

Furthermore, in the case of attacking the feature extractor with real images, we would need a fingerprint database large enough (hundreds of users) in order to be successful.

Further details about this attack can be found in:

- M. Martinez-Diaz, J. Fierrez, F. Alonso-Fernandez, J. Ortega-Garcia, and J. A. Sigüenza, “Hill-climbing and brute force attacks on biometric systems: a case study in match-on-card fingerprint verification,” in *Proc. IEEE of International Carnahan Conference on Security Technology*, 2006, pp. 151–159.

- U. Uludag and A. K. Jain, "Attacks on biometric systems: a case study in fingerprints," in *Proc. SPIE*, vol. 5306, no. 4, 2004, pp. 622–633.

2.2.5 Example: Brute Force attack to the feature extractor input

The typical steps to be carried out in order to successfully perform this type of attacks are:

Step 0. Acquisition of the database. Before the attack is carried out a large fingerprint database has to be obtained. The time and effort required for this task may vary greatly depending on whether the database is acquired (we collect a new database), purchased (we buy an existing database), or generated (we generate a database of synthetic fingerprints). Although this step has necessarily to be accomplished before carrying out the attack, it does not constitute a measure of the system vulnerability, but rather, of the attacker's ability to fulfill the task. Furthermore, the effort and time needed to acquire the database will be largely dependant on external factors very difficult to assess in an objective way. Thus, this step ***is not*** taken into account in the IDENTIFICATION or the EXPLOITATION of the attack, and we will assume the attacker has already obtained such a database.
The database image must match in size and resolution those used by the system. This means that the knowledge of the TOE required to carry out this attack is higher than in the direct attack case. However, these two parameters (size and resolution) are given by all sensor vendors, so the TOE information required will be rated as PUBLIC.

NOTE: many initiatives have been undertaken either with private or public funding in order to collect biometric databases which comprise fingerprint images from multiple users. However, biometric data is sensitive personal data and thus, all available databases are normally distributed to other institutions only for research purposes, and cannot be used with other objectives. Under these conditions, the purchase of a real fingerprint database is not a trivial task for non academic institutions.

Step 1. Gaining physical access to the system. The attacker has to find the way of having physical access over a determined period of time to the input of the feature extractor in order to insert the fingerprint images.

This step may include reverse engineering and is specially critical in the IDENTIFICATION of the attack. It may require the access to more than one sample of the TOE (which affects the rating of the window of opportunity in the IDENTIFICATION phase). It has a significant impact in the total time needed for the attack, and in the level of expertise of the attacker (needs some experience in hardware handling, and will be rated as PROFICIENT).

In EXPLOITATION we only need access to one sample of the TOE and the knowledge needed about its hardware structure is not very deep. The impact of this step in the elapsed time computation is small as we assume the attacker already knows where the input of the feature extractor is (located in identification) so its level of expertise can be rated as PROFICIENT.
Step 2. Automating the tests. In order to conduct this attack we need to be able to run automatic tests, which can be achieved with specific equipment to enable the communication between the attack launching device and the input of the feature extractor. Thus, we will rate the equipment needed as SPECIALIZED.

For this particular case, we refer the reader to performance evaluation comparative studies.

Source R. Cappelli, D. Maio, D. Maltoni, J. L. Wayman and A. K. Jain, "Performance evaluation of fingerprint verification systems", IEEE Trans. On Pattern Analysis and Machine Intelligence, vol 28, pp. 3-18, 2004

***Rating example 1**. Real images without countermeasures.*

We will assume that the system is operating at: FAR=0.1%, and FRR=2%. In IDENTIFICATION we will assume that the time needed by a PROFICIENT person to identify the input of the feature extractor considering that he only has PUBLIC information about the TOE is around 1 month. As well, we will consider that to do this the attacker needs to have access to some restricted information of the TOE.

Both in IDENTIFICATION and EXPLOITATION we will assume permanent physical access to the TOE and no countermeasures. In average an attacker should accomplish 1/FAR=1000 access attempts in order to break a given account, which means that, for an average 3 seconds per attempt, the elapsed time in the attack would be around 1 hour.

Factor	Comment	Identification	Exploitation
Elapsed Time	On the basis of the previous assumptions.	< 1 month (4)	< 2 hours (0)
Expertise	In identification and exploitation some experience in hardware manipulation is needed.	Proficient (3)	Proficient (3)
Knowledge of TOE	Only basic characteristics of the sensor are needed: size and resolution of the fingerprint images.	Public (0)	Public (0)
Window of opportunity	In identification we need multiple TOE samples (<10) but there are no restrictions to the access. In Exploitation the access to the TOE is restricted.	Easy/Moderate (3)	Easy/Moderate (3)
Equipment	We need specific inspection equipment to find the feature extractor input, connected to an electronic device in order to launch the attack.	Specialized (4)	Specialized (4)
Total		**14**	**10**
FINAL RATING		**24**	

Table 9

Given the resulting sum, 24, the attack potential required to carry out a successful attack is ENHANCED BASIC, so the TOE is resistant to attackers with a BASIC attack potential. It fails components AVA_VAN.3-5.

***Rating example 2**. Real images with countermeasures.*

We will assume that the system is operating at: FAR=0.1%, and FRR=2%, and that there is a blocking-account countermeasure for the EXPLOITATION of the attack.

In IDENTIFICATION the time required to carry out the attack is computed the same way as in example 1.

In EXPLOITATION we will compute the attack elapsed time considering that the attacker already possesses the database. In this case every user can make up to 3 attempts before the account is locked for 1 hour. In average the attacker should accomplish 1/FAR=1000 access attempts, and he can make 3 attempts every 60 minutes, that means the elapsed time for the attack is over 13 days (assuming that the attacker has permanent physical access to the TOE). A more realistic situation would be non-permanent access to the TOE, just 1/3 of the time, which would imply an attack duration of 39 days. This last estimation will be used in the EXPLOITATION attack potential rating.

Factor	Comment	Identification	Exploitation
Elapsed Time	On the basis of the previous estimations.	<1 month (4)	< 2 months (7)
Expertise	In identification and exploitation some experience in hardware manipulation is needed.	Proficient (3)	Proficient (3)
Knowledge of TOE	Only the basic characteristics of the sensor used in the system are needed: size and resolution of the fingerprint images (which can be easily obtained from the manufacturer).	Public (0)	Public (0)
Window of opportunity	In identification we need access to multiple TOE samples (<10) but there are no restrictions to temporal access. In Exploitation there is difficult access to the TOE.	Easy/Moderate (3)	Easy/Moderate (3)
Equipment	We need specific inspection equipment to find the feature extractor input, connected to an electronic device in order to launch the attack.	Specialized (4)	Specialized (4)
Total		**14**	**17**
FINAL RATING		**31**	

Table 10

Given the resulting sum, 34, the attack potential required to carry out a successful attack is MODERATE, so the TOE is resistant to attackers with a ENHANCED BASIC attack potential. It fails components AVA_VAN.4-5.

Rating example 3*. Synthetic images with countermeasures.*

In this case the database used in the attacks will comprise synthetic fingerprint images. To generate these images there are two possibilities:

- Develop a proprietary system capable of producing realistic fingerprint images, which would require a level of expertise and an amount of time not rated in the CEM potential tables. This would require an EXPERT in pattern recognition and image processing and it would take over 6 months.
- Obtain a software package which can generate synthetic fingerprint images. Following the assumption of the worst case scenario this will be the case rated in the examples.

NOTE: there is only one reported software of these characteristics, the SFinGe (Synthetic Fingerprint Generator), which is only distributed to institutions under a signed agreement.

The system operating point and the rest of the parameters involved in the elapsed time computation are the same as the ones considered in the rating example 2. Just to be noticed that synthetic images usually present a worse recognition rate than real samples, so it is expected that this attack will need more attempts to gain access to the system than that carried out with real images (the exploitation time was estimated in 39 days). In any case, considering an exploitation time inferior to 2 months is a reasonable assumption.

Factor	Comment	Identification	Exploitation
Elapsed Time	On the basis of the previous estimations.	<1 month (4)	< 2 months (7)
Expertise	In identification and exploitation some experience in hardware manipulation is needed.	Proficient (3)	Proficient (3)
Knowledge of TOE	Only the basic characteristics of sensor used in the system are needed: size and resolution of the fingerprint images (which can be easily obtained from the manufacturer).	Public (0)	Public (0)
Window of opportunity	In identification we need access to multiple TOE samples (<10) but there are no restrictions to temporal access. In Exploitation there is difficult access to the TOE.	Easy/Moderate (3)	Easy/Moderate (3)
Equipment	We need specific inspection equipment to find the feature extractor input, connected to a standard PC in order to launch the attack.	Specialized (4)	Specialized (4)
Total		**14**	**17**
FINAL RATING		**31**	

Table 11

Given the resulting sum, 31, the attack potential required to carry out a successful attack is MODERATE, so the TOE is resistant to attackers with an ENHANCED BASIC attack potential. It fails components AVA_VAN.4-5.

2.2.6 Example: Brute Force attack to the matcher input

In this case the attack is performed using as input randomly generated templates (created according to the format of real templates), so that there is no need to obtain a database of fingerprint images (step 0 in the attacks directed to the input of the feature extractor). However, the knowledge of the TOE required is deeper, as the attacker needs to know the information that is stored by the system, and the format in which that information is stored. This information may follow a fingerprint standard (e.g., ISO 19794-2:2005) in which case the knowledge of the TOE would be PUBLIC (rating taken in the examples), or can be proprietary of the manufacturing company in which case the knowledge of the TOE would be rated as RESTRICTED.

The steps to be carried out in order to successfully accomplish this attack are:

Step 1. Gaining physical access to the system. The attacker has to find the way of having physical access over a determined period of time to the input of the matcher in order to insert the fingerprint templates.

This step may include reverse engineering and is specially critical in the IDENTIFICATION of the attack. It may require the access to more than one sample of the TOE (which affects the rating of the window of opportunity in the IDENTIFICATION phase). It has a significant impact in the total time needed for the attack, and in the level of expertise of the attacker (needs experience in hardware handling).

In EXPLOITATION we only need access to one sample of the TOE and the knowledge needed about its hardware structure is not very deep. The impact of this step in the elapsed time computation is small as we assume the attacker already knows where the input of the feature extractor is (located in identification).

Step 2. Automating the tests. In order to conduct this attack we need to be able to run automatic tests, which can be achieved with specific equipment to enable the communication between the attack launching device and the input of the matcher. In this step the randomly generated templates are inserted in the system where they are compared with the feature vector of the account under attack. The attack continues until one of the templates gives a higher score than the fixed threshold and access is granted.

For this particular case we refer the reader to performance evaluation comparative studies.

Source

R. Cappelli, D. Maio, D. Maltoni, J. L. Wayman and A. K. Jain, "Performance evaluation of fingerprint verification systems", IEEE Trans. On Pattern Analysis and Machine Intelligence, vol 28, pp. 3-18, 2004.

Rating example 1. *Brute force attack to the matcher input, with countermeasures*

We will consider the same example as in the case of the brute force attack to the input of the feature extractor. Again the system operating point will be FAR=0.1%, FRR=2%, and will permit 3 invalid access attempts before the account is blocked for 1 hour.

In this case, the most time consuming task in IDENTIFICATION is the physical manipulation of the TOE in order to find the location of the matcher input. As in the previous example we will consider 4 weeks as a fair estimation for the accomplishment of this task for a PROFICIENT attacker with PUBLIC information about the TOE. Again, in IDENTIFICATION we assume that the countermeasures are not active and that we have permanent access to different samples of the TOE. As well, for this particular case we will assume that the system works with templates that follow a publicly available standard (i.e., the knowledge of the TOE is PUBLIC).

In EXPLOITATION, based on the previous calculations (rating example 2 of section 2.2.5), the elapsed time for the attack would be around 39 days, assuming that the attacker has clear instructions as how to perform the attack (location of the input feature extractor, communication between system and attack launching device, etc.)

This long attack duration entails that the window of opportunity in the exploitation scenario is rated as EASY/MODERATE. In identification we have permanent access to the TOE but due to the necessary hardware manipulation we will most likely need more than 1 sample, thus the window of opportunity is also rated as EASY/MODERATE.

Factor	**Comment**	**Identification**	**Exploitation**
Elapsed Time	On the basis of the previous estimations.	< 1 month (4)	< 2 months (7)
Expertise	In identification large experience in hardware manipulation is needed. For exploitation just some average knowledge is required.	Proficient (3)	Proficient (3)
Knowledge of TOE	We need specific information about the templates format. In this example we assume the system uses a publicly available standard	Public (0)	Public (0)
Window of opportunity	In identification we need access to multiple TOE samples (<10) but there are no restrictions to temporal access. In Exploitation there is difficult access to the TOE.	Easy/Moderate (3)	Easy/Moderate (3)
Equipment	We need specific inspection equipment to find the matcher input, connected to a standard PC in order to launch the attack.	Specialized (4)	Specialized (4)
Total		**14**	**17**
FINAL RATING		**31**	

Table 12

Given the resulting sum, 31, the attack potential required to carry out a successful attack is MODERATE, so the TOE is resistant to attackers with a ENHANCED BASIC attack potential. It fails component AVA_VAN.4-5.

2.3 Hill-Climbing indirect attacks

2.3.1 Description of the attack

Hill-climbing attacks try to gain access to biometric systems inserting random templates to the input of the matcher and, according to the score generated, iteratively changing the feature vectors until the system returns a positive verification. Although the main idea behind all hill-climbing algorithms is the same, the difference between them lies in the way that the templates are modified. In the case of fingerprint based systems two main approaches have to be considered: hill-climbing on systems working with non-fixed feature vectors (e.g., systems based on minutiae), and hill-climbing on applications with fixed length templates (e.g., systems based on the ridge pattern). In Fig. 1 we show a diagram of a generic hill-climbing algorithm.

Using an algorithm capable of reconstructing the fingerprint image from its feature vector, the hill-climbing algorithm can be directed to the input of the feature vector. Thus, the attack is simplified as the intruder would not need to know the template format of the system. Both examples (hill-climbing attacks directed to the input of the matcher and to the input of the feature extractor) are considered in Sects. 2.3.5 and 2.3.6 respectively.

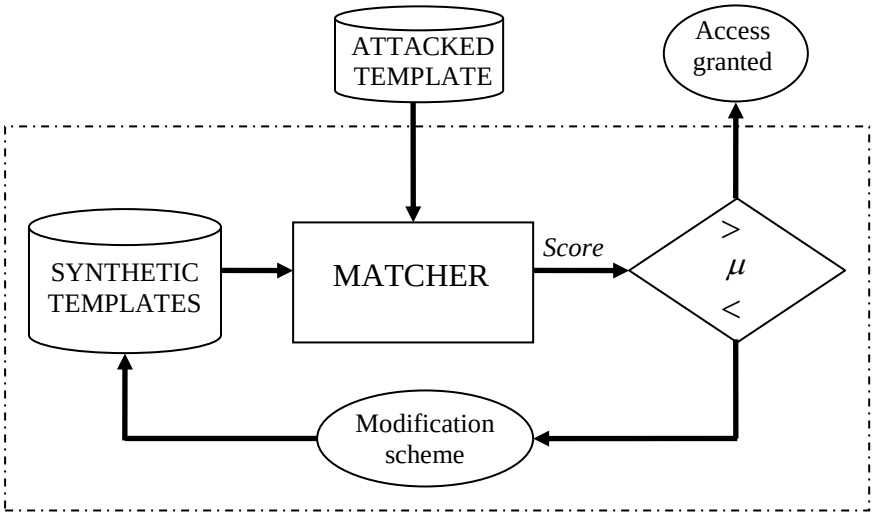

Figure 6. Diagram of a general hill-climbing algorithm

2.3.2 Effect of the Attack

When considering fingerprint based biometric systems, two types of hill-climbing algorithms can be distinguished depending on the fingerprint information stored in the templates and, subsequently, in the strategy followed by the algorithm to modify those templates:

- *Hill-climbing attacks against minutiae based systems*. Feature vectors are length variant depending on the number of minutia points stored. In this case the most used and studied hill-climbing algorithm was proposed in:

  U. Uludag and A. K. Jain, "Attacks on biometric systems: a case study in fingerprints," in *Proc. SPIE*, vol. 5306, no. 4, 2004, pp. 622–633.

- *Hill-climbing attacks against systems based on the ridge pattern*. In this case feature vectors have a fixed length which permits the usage of more general hill-climbing approaches, for example the one based on Bayesian adaptation described in.

  J. Galbally, J. Fierrez, and J. Ortega-Garcia, "Bayesian hill-climbing attack and its application to signature verification," in *Proc. International Conference on Biometrics*, 2007, Springer LNCS-4642, pp. 386-395.

Although the second algorithm is more general and can be applied to attack biometric systems based on other traits (with fixed length feature vectors), it needs a small fingerprint database in order to be initialized which can be not always easy to obtain.

2.3.3 Impact on TOE

The attack is directed against the feature extractor or the matcher of the system and the main impact is the fraudulent access to the information secured by the TOE.

2.3.4 Characteristics of the Attack

All the main characteristics and requirements of this type of attacks are very similar to those of the brute force attacks:

- Narrow window of opportunity due to the required physical manipulation of the TOE.

- High level of knowledge of the TOE when directing the attack to the input of the feature extractor (template format).

- A significant high level of expertise (some experience in hardware handling, rated as PROFICIENT) in the IDENTIFICATION scenario in order to locate the input and

output of the matcher. For EXPLOITATION we assume that those two points are known and so the level of expertise is somewhat lower (but still rated as PROFICIENT as a layman rating would fall short.)

- Specific equipment required to locate all the physical points necessary to carry out the attack. This task is specially critical in the IDENTIFICATION phase and may increase substantially the time required for the attack.

The most important differences between the hill-climbing and brute force attacks in terms of the evaluated factors in the CEM potential tables are:

- No database of real fingerprints is needed, with the subsequent gain in the time required for the attack.

- In the hill-climbing attack we need access no only to the input of the matcher or feature extractor, but also to the output of the matcher, which implies a considerable increase in the amount of time needed to identify the physical access points (IDENTIFICATION of the attack).

Further details about this type of attacks can be found in:

- M. Martinez-Diaz, J. Fierrez, F. Alonso-Fernandez, J. Ortega-Garcia, and J. A. Sigenza, "Hill-climbing and brute force attacks on biometric systems: a case study in match-on-card fingerprint verification," in *Proc. IEEE of International Carnahan Conference on Security Technology*, 2006, pp. 151–159.

- U. Uludag and A. K. Jain, "Attacks on biometric systems: a case study in fingerprints," in *Proc. SPIE*, vol. 5306, no. 4, 2004, pp. 622–633.

- J. Galbally, J. Fierrez, and J. Ortega-Garcia, "Bayesian hill-climbing attack and its application to signature verification," in *Proc. International Conference on Biometrics*, 2007, Springer LNCS-4642, pp. 386-395.

2.3.5 Example: hill-climbing attack to the matcher input

The steps to be carried out for this attack are analog to those required in the brute force attack to the matcher input:

Step 1. Gaining physical access to the system. The attacker has to find the way of having physical access over a determined period of time to the input of the matcher (in order to insert the fingerprint templates) and to the output of the matcher (in order to have the necessary feedback to execute the hill-climbing algorithm).

In this case there are two different physical points to be located (input and output of the matcher) which means that the number of TOE samples and the time required for this task in IDENTIFICATION will be bigger than in the brute force attacks (with its subsequent impact in the rating of the elapsed time and of the window of opportunity).

In EXPLOITATION the resources needed for both attacks (brute force and hill climbing) in terms of time, expertise and equipment are very similar.

Step 2. Recovering the score. Having access to the matcher output does not necessarily mean that we have access to the score, as this may be encrypted or protected by some other mean. In this case, recovering the score may not be an easy task and may require some side channel measure such as the power consumption (Differential Power Analysis, DPA), or the time (time analysis). This step also has an impact in the elapsed time (specially in IDENTIFICATION).

Step 3. Automating the tests. In order to conduct this attack we need to be able to run automatic tests, which can be achieved with specific equipment to enable the communication between the launching device and the input and output of the matcher. In this step the randomly generated templates are inserted in the system where they are compared with the feature vector of the account under attack. The resulting score is used by the hill climbing algorithm (executed on an electronic device) to modify the templates in an iterative process. The attack continues until one of the templates gives a higher score than the fixed threshold and access is granted.

A case study for a particular evaluation scenario is given below:

Source	M. Martinez-Diaz, J. Fierrez, F. Alonso-Fernandez, J. Ortega-Garcia, and J. A. Sigenza, "Hill-climbing and brute force attacks on biometric systems: a case study in match-on-card fingerprint verification," in *Proc. IEEE of International Carnahan Conference on Security Technology*, 2006, pp. 151–159.	
General parameters	System:	Minutiae-based MoC
	Operating point:	FAR=0.16%
	Sensor:	Optical
	Algorithm:	Hill-climbing minutiae specific

Rating example 1. *Hill-climbing attack to the matcher input, with countermeasures (score quantization).*

For this example we will consider a minutiae based system, operating at FAR=0.1% and FRR=2%. The considered fingerprint verification system has a countermeasure against hill-climbing attacks consisting of *score quantization*. These type of attack protection approaches try to avoid the threat by increasing the score step (e.g., instead of giving the scores in steps of 0.1, giving them in steps of 1) so that the hill-climbing algorithm does not get the necessary feedback to iteratively increase the similarity measure (the attack cannot take advantage of small increases in the output of the matcher).

We will assume that without any countermeasure the hill-climbing attack would be successful in half of the iterations of a brute force attack, but that the mentioned quantization of scores makes it 100 times slower (i.e., needs 50 times more attempts than a brute force attack). This means that, on average, we need to execute 50,000 attack iterations, taking 15 seconds as the average duration of each iteration the attack would gain access to the system in around 9 days.

In this case, the two access points (input and output of the matcher) to the TOE have to be located. Furthermore, in case that the raw score is protected it will have to be obtained by some alternative mean: Differential Power Analysis (DPA), time analysis, etc. We will assume between 1 and 2 months as a fair estimation for the completion of these steps.

Factor	Comment	Identification	Exploitation
Elapsed Time	On the basis of the previous estimations.	< 2 months (5)	< 2 weeks (2)
Expertise	Experience in hardware manipulation is needed.	Proficient (3)	Proficient (3)
Knowledge of TOE	We will assume that the templates follow a standard (public information)	Public (0)	Public (0)
Window of opportunity	In identification we need access to multiple TOE samples (<20) but there are no restrictions to temporal access. In Exploitation there is difficult access to the TOE, for less than two weeks.	Moderate (4)	Moderate/Difficult (5)
Equipment	We need specific inspection equipment to find the matcher input and output, connected to an electronic device in order to launch the attack.	Specialized (4)	Specialized (4)
Total		**16**	**14**
FINAL RATING		**30**	

Table 13

Given the resulting sum, 30, the attack potential required to carry out a successful attack is MODERATE, so the TOE is resistant to attackers with a ENHANCED-BASIC attack potential. It fails component AVA_VAN.4-5.

Rating example 2*. Hill-climbing attack to the matcher input, with countermeasures (account blocking).*

For this example we will consider a system based on the ridge pattern working with fixed length feature vectors. The operating point is: FAR=0.1%, FRR=2%, and it has incorporated a countermeasure in order to fight multiple-attempt attacks which blocks the account for 1 hour after 3 unsuccessful access attempts.

Due to the characteristics of the fingerprint verification system (fixed length feature vectors), it has to be attacked with the hill-climbing algorithm based on Bayesian adaptation. This attack needs a small database (around 20 subjects) to be initialized, which would take around 2 weeks to be acquired. This is just stated here for clarity but it will not be considered in the ratings as it does not reflect directly the robustness of the TOE against

the attack and there are many external factors that may influence this time estimation and that cannot be taken into account here.

Again in IDENTIFICATION we will assume that the location of the two access physical points (input and output of the matcher), and recovering the score from some easily measurable parameter (power consumption, time), takes the intruder from 1 to 2 months.

We will assume that the attack succeeds in half of the iterations needed by a brute force attack (i.e., 500 attempts), hence, the time needed for its completion will be around 7 days under the assumption of permanent physical access to the system which is only realistic in the IDENTIFICATION of the attack. For EXPLOITATION we will consider that the attacker can access the TOE only 1/3 of the time, thus the total time of the attack will be 21 days.

In this case we will assume that the template format used by the system is proprietary (it does not follow any known standard). This way, in the identification phase the attacker will need to have access to RESTRICTED information, while in exploitation this information is already known (disclosed in the previous phase) and will be treated as PUBLIC.

Factor	**Comment**	**Identification**	**Exploitation**
Elapsed Time	On the basis of the previous estimations.	< 2 months (5)	< 1 month (3)
Expertise	Experience in hardware manipulation is needed both for identification and exploitation.	Proficient (3)	Proficient (3)
Knowledge of TOE	We need specific information about the templates format in identification.	Restricted (3)	Public (0)
Window of opportunity	In identification we need access to multiple TOE samples (<20) but there are no restrictions to temporal access. In Exploitation there is difficult access to the TOE, for less than three weeks.	Moderate (4)	Moderate/Difficult (5)
Equipment	We need specific inspection equipment to find the feature extractor input, connected to an electronic device in order to launch the attack.	Specialized (4)	Specialized (4)
Total		**19**	**15**
FINAL RATING		**34**	

Table 14

Given the resulting sum, 34, the attack potential required to carry out a successful attack is MODERATE, so the TOE is resistant to attackers with a ENHANCED_BASIC attack potential. It fails component AVA_VAN.4-5.

2.3.6 Example: hill-climbing attack to the feature extractor input

When directed to the feature extractor the hill-climbing algorithm is analog to the ones described in Sect. 2.3.5, with the only difference that instead of inserting the templates to the matcher, we reconstruct the fingerprint image from the feature vector and we present it to the input of the feature extractor. This attack can only be performed on minutiae based systems and is significantly slower than the one directed to the matcher input (the reconstruction process takes some non negligible time). On the other hand it does not need any specific information about the TOE (the template format is not needed). The steps to be carried out for this attack are:

Step 1. Development of the fingerprint reconstruction software. In order to perform this type of attack the intruder must be able to reconstruct a realistic fingerprint image from its template (this was also the case in the direct attacks starting from a stolen minutiae template Sect. 2.1.7). This is an extremely difficult task that up to date can only be done with minutiae based templates. The development of such a system would take a great amount of time and would require a very high level of expertise on the fingerprint trait, on pattern recognition algorithms and on image processing (EXPERT rating). This step will only be taken into account in the IDENTIFICATION of the attack, for EXPLOITATION we will assume the attacker has already obtained (by any means) the fingerprint reconstruction software.

NOTE: only one efficient system capable of reconstructing realistic fingerprints from its minutiae templates has been reported in literature:

> R. Cappelli, A. Lumini, D. Maio, and D. Maltoni, "Fingerprint image reconstruction from standard templates," *IEEE Trans. on Pattern Analysis and Machine Intelligence*, vol. 29, pp. 1489–1503, 2007.

The next three steps are very similar to the ones carried out in the attack directed to the input of the matcher and we will only point out the differences:

Step 2. Gaining physical access to the system. In this case the two physical points to be located are the feature extractor input and the matcher output. Again the time elapsed in this task will only be considered in IDENTIFICATION. In order to find the location of the two points we need some expertise in hardware handling, both in identification and exploitation (PROFICIENT rating).

Step 3. Recovering the score. Having access to the matcher output does not necessarily mean that we have access to the score, as this may be encrypted or protected by some other mean. In this case, recovering the score may not be an easy task and may require some side channel measure such as the power consumption (Differential Power Analysis, DPA), or the time (time analysis). This step also has an impact in the elapsed time (specially in IDENTIFICATION).

Step 4. Automating the tests. In this attack the intruder inserts in the system (feature extractor input) the reconstructed fingerprint images (and not the templates). The rest of the algorithm remains unaltered: the resulting score is used by the hill climbing algorithm to modify the template, which is again used to generate a new fingerprint image. The iterative

process continues until one of the images gives a higher score than the fixed threshold and access is granted.

A case study for a particular evaluation scenario is given below:

Source	M. Martinez-Diaz, J. Fierrez, F. Alonso-Fernandez, J. Ortega-Garcia, and J. A. Sigenza, "Hill-climbing and brute force attacks on biometric systems: a case study in match-on-card fingerprint verification," in *Proc. IEEE of International Carnahan Conference on Security Technology*, 2006, pp. 151–159.	
General parameters	System:	Minutiae-based
	Operating point:	FAR=0.1%
	Sensor:	Optical
	Algorithm:	Hill-climbing minutiae specific

Rating example 1. *Hill-climbing attack to the feature extractor input, with countermeasures (score quantization).*

For this example we will consider the same system as in the rating example 1 of the hill-climbing attacks directed to the matcher input. So its basic characteristics are:

- Minutiae based, working at FAR=0.1%, FRR=2%.
- Countermeasure using quantization of scores.

Assuming the worst case scenario, we will consider that the attacker is able to obtain the reconstruction software from a third party and does not have to develop it by himself. In this case in IDENTIFICATION we will take 2 months as the time needed to find the two physical access points of the system (input of the feature extractor and output of the matcher), and to recover the score from side channel measures (e.g., power consumption, time).

Both for EXPLOITATION and IDENTIFICATION, the attacker needs to have some experience in hardware handling (level of expertise PROFICIENT). The knowledge of the TOE needed is very basic, just the size and resolution of the images used.

To compute the elapsed time of the attack in EXPLOITATION we will assume that the hill-climbing attack would typically access the system in half of the attempts of a brute force attack (i.e., 500 iterations). However, the quantization of the scores makes it 100 times slower (i.e., 50000 iterations). We will assume that the attacker does not have permanent access to the TOE, just 1/3 of the time, and that, as a result of the reconstruction process, an iteration takes around 20 seconds. With this premises, the expected execution time of the attack would be around 35 days (i.e., less than two months in the CEM ratings).

Factor	Comment	Identification	Exploitation
Elapsed Time	On the basis of the previous estimations.	< 2 months (5)	< 2 months (5)
Expertise	In identification and exploitation experience in hardware manipulation is needed.	Proficient (3)	Proficient (3)
Knowledge of TOE	Only the basic characteristics of the sensor used in the system are needed.	Public (0)	Public (0)
Window of opportunity	In identification we need access to multiple TOE samples (<20) but there are no restrictions to temporal access. In Exploitation there is difficult access to the TOE for less than two weeks.	Moderate (4)	Moderate/Difficult (5)
Equipment	We need specific inspection equipment to find the feature extractor input, connected to an electronic device in order to launch the attack.	Specialized (4)	Specialized (4)
Total		**16**	**17**
FINAL RATING		**33**	

Table 15

Given the resulting sum, 33, the attack potential required to carry out a successful attack is MODERATE, so the TOE is resistant to attackers with a ENHANCED_BASIC attack potential. It fails components AVA_VAN.4-5.