On security evaluation of fingerprint recognition systems

Olaf Henniger, Dirk Scheuermann, and Thomas Kniess
Fraunhofer Institute for Secure Information Technology, Germany

Abstract. This paper discusses the methodology for evaluating the security of fingerprint recognition systems. For keeping track of the multitude of potential vulnerabilities an attack tree is used. Only potential vulnerabilities specific to fingerprint verification systems are considered. The attack tree is truncated where the efforts required for a successful attack (the attack potential) can be estimated. The attack potential of the parent nodes is the aggregation of the attack potentials of the child nodes.

1 Introduction

Biometric methods can increase the binding of authentication processes to persons provided they are themselves sufficiently secure [1]. Security evaluations by independent third-party testing laboratories are needed for building confidence in the security of IT products. For some applications (e.g. legally binding electronic signatures), a security evaluation based on officially recognized criteria like the Common Criteria for IT security evaluation [2] is even legally required [3].

Only few biometric products have attained a security certificate and, if so, then only on the low Evaluation Assurance Level EAL2 [4][5][6][7][8]. Even though some guidance on security evaluations of biometric systems [9][10][11] and several protection profiles for biometric systems [12][13][14][15][16][17] have already been developed, there remain open issues concerning the security evaluation of biometric systems. The assurance components within the Common Criteria that require clarification in the context of biometric systems are those related to vulnerability analysis. A methodical vulnerability analysis requires that the evaluator identifies a list of potential vulnerabilities in the Target of Evaluation (TOE) and conducts corresponding penetration tests to determine the TOE's resistance to attacks with a certain attack potential. The attack potential essentially corresponds to the minimum effort required to create and successfully carry out an attack [18]. The higher the attackers' motivation (value of the asset), the higher efforts they may exert.

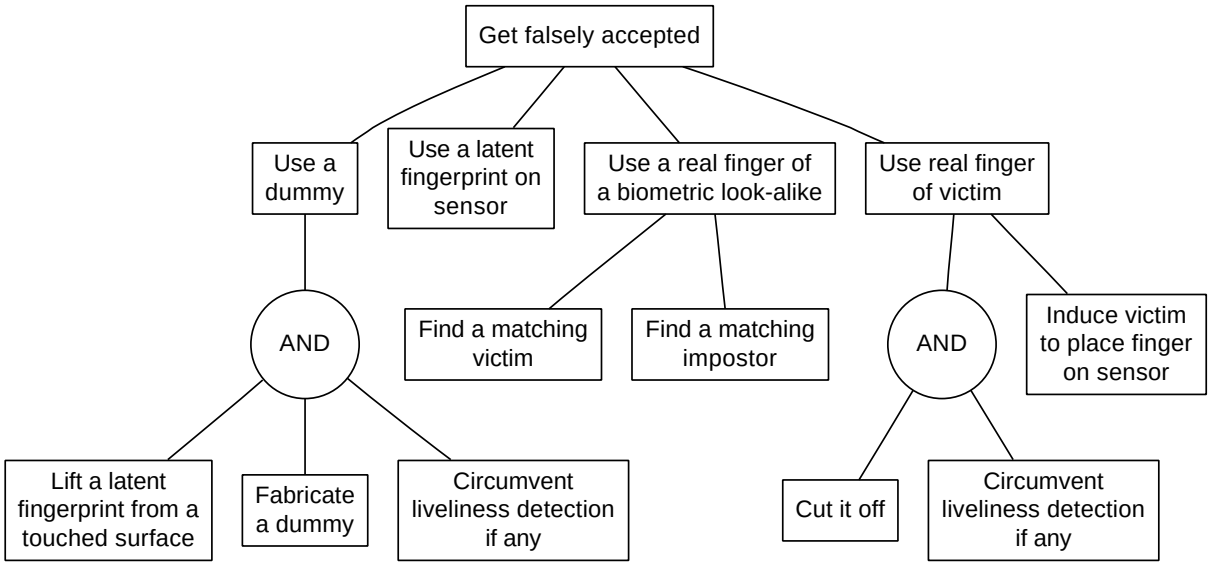
This paper focuses on analysing vulnerabilities specific to biometric systems, in particular fingerprint recognition systems: their fraud resistance and recognition accuracy. After analysing vulnerabilities in fingerprint recognition (Section 2), the assessment of attack potentials based on attack trees is considered (Section 3). This is based on hands-on experience in fabricating fingerprint dummies gained at Fraunhofer SIT.

2 Potential vulnerabilities in fingerprint recognition systems

The potential vulnerabilities are structured using attack trees [19][20]. The root of an attack tree represents the goal of an attack. Child nodes represent subgoals that could satisfy the parent attack goal. Child nodes may have children themselves. The tree is truncated where the efforts required for a successful attack can be estimated. If a node is labelled with a logical AND operator, all its children need to be achieved to achieve the superior goal. Otherwise, an attack goal can be achieved by achieving any one of its subgoals (logical OR relation).

Figure 1 shows part of the attack tree for a positive-claim fingerprint verification system. As we would like to compare the particular strengths and weaknesses of biometric methods with that of other user authentication methods such as PINs and passwords, here we consider only potential threats specific to biometric systems. In the same way as stored PINs and passwords should not be readable and alterable, we also assume that the stored biometric reference cannot be read or altered by attackers. In a security evaluation of a real system, of course, it should be checked whether such assumptions hold.

Figure 1 Attack tree for fingerprint verification systems



A main threat to the assets protected by a biometric system is that of an impostor impersonating another person who is enrolled and gaining access to the protected assets. An attacker may also attempt to masquerade as another person by use of a fingerprint dummy made e.g. from gelatin.

3 Assessment of attack potentials

3.1 Overview

The required attack potential is estimated for the leaf nodes of the attack tree. For higher attack goals, the individual attack potentials of their child nodes can be combined using the tree logic: If an attack goal requires a conjunction of attacks (i.e. AND relationship), the combined attack potential is taken to be the highest of the attack potentials associated with the contributing attack steps. If an attack goal can be achieved using any one of a number of

attacks (i.e. OR relationship), then the combined attack potential is taken to be the lowest of the attack potentials for the attack options. A system is only as secure as its "weakest link".

The following factors are considered during attack potential evaluation [18]:

- Time taken by an attacker to identify a vulnerability, to develop an attack method, and to mount the attack;
- Specialist technical expertise required;
- Knowledge of the TOE required;
- Window of opportunity required to access the TOE;
- IT hardware/software or other equipment required to identify and exploit the vulnerability.

Table 1 (based on [18]) identifies the factors and associates numeric values with each level. Intermediate values to those in the table can also be chosen.

Table 1 Rating of aspects of attack potential

Factor	**Level**	**Value**
Elapsed time	≤ 1 day	0
	≤ 1 week	1
	≤ 1 month	4
	≤ 3 months	10
	≤ 6 months	17
	> 6 months	19
	not practical	∞
Expertise	Layman	0
	Proficient	3
	Expert	6
	Multiple experts	8
Knowledge of TOE	Public	0
	Restricted	3
	Sensitive	7
	Critical	11
Window of opportunity	Unnecessary/unlimited	0
	Easy	1
	Moderate	4
	Difficult	10
	None	∞
Equipment	Standard	0
	Specialized	4
	Bespoke	7
	Multiple bespoke	9

To determine the attack potential for an attack, sum up the appropriate values for the factors from Table 1 and apply Table 2 [18] to map the sum to the attack potential. Note that once vulnerabilities have been identified and exploited, they may be exploited repeatedly with less effort than for the first time. Both phases, identification of vulnerabilities and their exploitation, are considered in conjunction.

Table 2 Rating of attack potential

Values	Attack potential required to identify and exploit vulnerability
0–9	Basic
10–13	Enhanced-Basic
14–19	Moderate
20–24	High
≥ 25	Beyond High

3.2 Relationship to risk assessment

The attack potential has an impact on the risk associated with an attack. The risk is a function of the severity of a successful attack (i.e. loss for the stakeholders) and the frequency of successful attacks [19]. It may be hard to exactly quantify all factors influencing the risk of an attack. However, the relative severity and frequency of successful attacks can be assessed, allowing a ranking of attacks based on their relative risk.

Assuming that each attack that is possible will be carried out by someone, the relative frequency of successful attacks depends on the attack potential that the TOE is able to withstand. A low attack potential corresponds to a high frequency of successful attacks since many possible attackers will have the necessary attack potential. Conversely, a high attack potential suggests a low frequency of successful attacks since the number of attackers with the necessary attack potential is expected to be comparatively small.

3.3 Attack potential for fabricating dummies

Fingerprint dummies for spoofing fingerprint recognition systems can be fabricated from different materials [21]. Depending on the sensor technology, the dummies need to imitate certain physical characteristics of fingers measured by fingerprint sensors in order to allow an attacker to successfully spoof the sensors:

- For attacking optical sensors, the material just needs to deliver an optical image of the ridges and valleys of the finger.
- For attacking capacitive sensors, where the sensor and the finger surface represent the plates of a capacitor, the material also needs to imitate some characteristic electrical properties of finger surfaces.
- For attacking e-field sensors, which do not only measure features of the surface but also electrical properties of deeper regions of the finger skin, care must be taken to imitate not only the surface of the finger but also its deeper regions.
- For attacking thermal sensors, which measure the temperature differences between touched and non-touched locations on the sensor surface and hence create a thermal image of the finger ridges and valleys, the material needs to be able to imitate thermal features of a finger surface, i.e. to transmit a sufficient amount of thermal energy to the sensor surface.

Fraunhofer SIT gained hands-on experience in fabricating dummies based on existing fingerprint images out of a database. The fingerprint images are used for the production of moulds (negative forms) by exposing photo-reactive polymer plates to UV light through transparencies carrying these images. The locations exposed to the UV light get hardened.

The locations that are not exposed can be washed out with water. These moulds are used to produce fingerprint dummies of different materials. Three different materials were tested: Wax, gelatin and material for dental casts. Among the materials tested, gelatin turns out to be the most generally usable material being able to spoof almost all sensors. Nevertheless, some sensor/software combinations can be spoofed more easily with other materials that do not work at all for the other sensors. Modifications with the aid of powder and flexible plastic films sometimes increase, but sometimes diminish the success rates.

The test outcome is that spoofing fingerprint sensors with the aid of fingerprint dummies is generally possible with a relatively low attack potential under certain technical preconditions (availability of usable images, liveliness detection deactivated if any). With liveliness detection deactivated, for all tested sensor technologies, from given fingerprint images matching dummies could be fabricated. Nevertheless, it becomes obvious that there is no attack method working for all fingerprint recognition systems as not for all sensor types the same materials work out. Furthermore, an attacker who has successfully fabricated a fingerprint dummy does not own a means for breaking the system once and forever, but may eventually need to re-invest the efforts since some dummy materials become useless after some time.

In summary, the attack potential for fabricating fingerprint dummies from given fingerprint images may be rated as basic (cf. Table 3). Dummies can be fabricated within less than one week. Proficient expertise is needed for fabricating the dummies. Public knowledge is sufficient for knowing how to fabricate and use the dummies. The window of opportunity may be considered unnecessary/unlimited. Some specialized equipment (e.g. the different materials) is needed.

Table 3 Attack potential estimate for fabricating fingerprint dummies

Attack	Elapsed time	Expertise	Knowledge of TOE	Window of opportunity	Equipment	Required attack potential	
						Sum	Rating
Fabricate a dummy from a given fingerprint image	1	3	0	0	4	8	Basic

Each sensor technology and each individual fingerprint comparison algorithm needs to be tested separately since the attack possibilities, although similar in the general amount of effort needed, appear to be quite different. Furthermore, it turns out that the optimisation of sensor technologies may lead to a higher fake resistance since specific attacks do not work any more. Since the test outcome also differs between several comparison algorithms used with the same sensor and the same dummy, it is obvious that the fake resistance of a fingerprint recognition system may also be increased by an optimisation of the software.

3.4 Attack potential for circumventing liveliness detection

Some fingerprint recognition systems have liveliness detection (or spoof detection) measures incorporated [22]. Often, these measures are effective only as long as the attacker does not know their functional principle and are kept secret as intellectual property. Hence, expertise and knowledge of the TOE are key factors for circumventing the liveliness detection: An attacker with little knowledge of the TOE needs a lot of effort to find out how to circumvent the liveliness detection while an insider knowing the functional principle may circumvent it

within a short time. An attacker either needs to produce a fingerprint dummy imitating the liveliness features or to manipulate the sensor in a way that the liveliness detection is deactivated. Some special equipment may be needed. The window of opportunity is easy to get if the sensor is unattended. In total, we consider the attack potential for circumventing liveliness detection as high (cf. Table 4): Effective liveliness detection should deliver sufficient protection against attackers with a moderate attack potential, though it may help little against insiders, e.g. persons involved in developing and manufacturing fingerprint sensors. Whether or not this is the case in practice should be subject to further studies.

Table 4 Attack potential estimate for circumventing liveliness detection

Attack	Elapsed time	Expertise	Knowledge of TOE	Window of opportunity	Equipment	Required attack potential	
						Sum	Rating
Circumvent liveliness detection	4	6	7	1	4	22	High

3.5 Attack potential for lifting latent fingerprints from surfaces

Unlike PINs (Personal Identification Numbers) and passwords, fingerprints are not secret. They can be lifted from surfaces touched by the victim of the attack. Once a usable image has been obtained, fingerprint dummies may be fabricated as described in Section 3.2. However, if the victim is not cooperative, obtaining latent fingerprints of sufficient quality is not that easy. This may be the only rescue left if the liveliness detection can be spoofed and the fingerprint recognition system accepts dummies. One critical key factor is the limited window of opportunity to get a usable image. Additional technical equipment is then needed to enhance the image quality, but not more specialized than the other equipment for fabricating the dummies. If the attacker is able to obtain a good image, less effort is needed for enhancing the image quality. If the image quality is poor, a more extensive use of professional image processing equipment and more time are needed. In total, we consider the attack potential for lifting latent fingerprints from surfaces as moderate. This should be subject to further studies. A summary of our attack potential estimates is given in Table 5.

Table 5 Attack potential estimate for lifting a latent fingerprint from a touched surface

Attack	Elapsed time	Expertise	Knowledge of TOE	Window of opportunity	Equipment	Required attack potential	
						Sum	Rating
Lift a latent fingerprint from a touched surface	0	3	0	10	1	14	Moderate

3.6 Attack potential for getting falsely accepted as a biometric look-alike

Attempts to get falsely accepted by a fingerprint verification system as a biometric look-alike of somebody else are referred to as zero-effort impostor attempts [23]. Zero-effort impostor attempts do not require expertise or knowledge of the TOE. In case of unattended one-factor authentication, the window of opportunity is easy to get. The attack potential for such an

attack is related to the system's false accept rate (FAR), i.e. the proportion of impostor attempts falsely declared to match the biometric reference within a permitted number of attempts [23]. In order to prevent brute-force attacks on the biometric reference of a single person, the number of permitted retries should be limited, e.g. to five retries.

The resistance of a TOE security function to direct attacks (i.e. not to bypassing, deactivating, corrupting, etc.) was referred to as Strength of Function (SOF) in older versions of the Common Criteria. Several attempts to define fixed mappings between FAR and SOF of a biometric system have been made (e.g. in [9] and in working drafts of [11]), but did not find universal approval because they did not reflect all strengths and weaknesses of biometric systems. [24] requires a FAR of 10^{-6} for commensurate security with that of PINs or passwords. If the presentation of a biometric characteristic does not take longer than entering a PIN, then the FAR should not be higher than the probability of guessing PIN or password. However, measuring such a low FAR with statistical significance is hardly feasible. The assessment should in some way take the stronger binding of biometric characteristics to persons (compared to that of PINs or passwords) into account [25].

Since the biometric characteristics of different persons are independent from each other, the probability of being falsely accepted is independent from the number of persons whom the attacker has already failed to impersonate. The elapsed time till getting falsely accepted as somebody else is proportional to the number $N = \log_{(1-\mathrm{FAR})}(1 - 0.95)$ of

- persons an attacker needs to try to impersonate until being falsely accepted with 95% probability or
- attackers that have to team up with each other to have a 95% chance of impersonating a particular person.

Assume the decision threshold of a biometric system is chosen such that FAR = $5 \cdot 10^{-4}$. This is attainable at an acceptable false reject rate (FRR) [26], i.e. proportion of genuine attempts falsely declared not to match the biometric reference within a permitted number of attempts [23]. How many different persons must the attacker try to impersonate in order to be falsely accepted with 95% probability as one of the persons? The attacker would have to try to impersonate 5,990 different persons in order to have 95% confidence to be falsely accepted once within the allowed number of attempts. This risk may be acceptable if the fingerprint recognition is part of a multi-factor authentication, e.g. in combination with a smart card (stealing so many cards should be difficult).

Table 6 shows an attack-potential estimate for getting falsely accepted using a real finger of a biometric look-alike. The values depend on the FAR of the TOE.

Table 6 Attack potential estimate for using a real finger of a biometric look-alike

Attack	Elapsed time	Expertise	Knowledge of TOE	Window of opportunity	Equipment	Required attack potential	
						Sum	Rating
Use a real finger of a biometric look-alike	13–19	0	0	1	0	14–20	Moderate – High

3.7 Attack potential for other attacks

Attackers may chop off a victim's finger to get round a fingerprint recognition system used e.g. for disarming a car's immobilizer [1]. This attack is rather easy and highlights the need for effective liveliness detection and for other countermeasures such as multi-factor authentication. It also highlights the need for risk assessment: The deployment of a biometric system adds the users' limbs to the assets requiring protection and puts them at risk.

Attackers may also try to activate a latent fingerprint on the sensor to work like a real finger by enforcing light, heat or moisture effects. The attack potentials for these attacks should be subject to further studies.

3.8 Attack potential summary

Our attack potential estimates are based on the following assumptions: The person impersonated by an attacker does not cooperate with the attacker. The attackers do not come into possession of databases linking fingerprints and identities of victims. The number of permitted retries is limited to prevent brute-force attacks on the biometric reference of a single person.

The essential elements for using a fingerprint dummy are (1) lifting a latent fingerprint from a touched surface, (2) fabricating a dummy from a fingerprint image, and (3) circumventing liveliness detection. The attack potential for using a fingerprint dummy is as high as that of the hardest essential element. Given a moderate attack potential for lifting a latent fingerprint from a touched surface, a basic attack potential for fabricating a dummy from a given fingerprint image, and a high attack potential for circumventing liveliness detection, the attack potential for using a fingerprint dummy is high if there is liveliness detection and moderate if there is no effective liveliness detection.

4 Summary

Biometric methods may replace knowledge-based user authentication methods in many application fields, provided that their recognition accuracy and attack resistance can be demonstrated to be sufficiently high. Their strengths lie in freeing users from the burden of recalling PINs or passwords from memory and in increasing the binding of authentication processes to persons. However, the security of biometric systems may be broken by faking biometric characteristics using e.g. fingerprint dummies, and even during normal use, occasional false acceptances and false rejections cannot be completely avoided.

Quantifying the security of a biometric system and comparing it with that of a PIN or password is difficult and requires taking all strengths and weaknesses into account. Attack trees help to keep track of the plethora of possible attacks. The attack potential of direct and indirect attacks that fingerprint recognition systems should be able to withstand is classified based on the efforts necessary for completing these attacks. More experiments and a wide consensus on the attack potential assessment are needed. The basic ideas of the described approach are also applicable to the security evaluation of other biometric systems.

References

[1] Prabhakar, S., Pankanti, S., and Jain, A.K. (2003). Biometric recognition: Security and privacy concerns. *IEEE Security & Privacy*. March/April 2003, pp. 33–42

[2] International Standard ISO/IEC 15408. *Information technology – Security techniques – Evaluation criteria for IT security*.

[3] German government (2001). *Ordinance on electronic signatures*.

[4] Canadian Communications Security Establishment (2001). *EAL2 certification report for Bioscrypt™ Enterprise for NT logon version 2.1.3*. Certification Report 383-4-8.

[5] Australian Defence Signals Directorate (2003). *EAL2 certification report for Iridian Technologies KnoWho authentication server and private ID*. Certification Report 2003/31.

[6] TÜViT (2005). *EAL2 certification report for authentication engine of VOICE.TRUST server version 4.1.2.0*. Certification Report TUVIT-DSZ-CC-9224.

[7] German Federal Office for Information Security (2008). *EAL2 certification report for VoiceIdent Unit 2.0 from Deutsche Telekom*. Certification Report BSI-DSZ-CC-0469-2008.

[8] German Federal Office for Information Security (2008). *EAL2 certification report for PalmSecure SDK Version 24 Premium from Fujitsu Ltd*. Certification Report BSI-DSZ-CC-0511-2008.

[9] Common Criteria Biometric Evaluation Methodology Working Group (2002). *Biometric evaluation methodology*. Version 1.0.

[10] Australian Biometrics Institute (2008). *Biometric vulnerability: A principled assessment methodology*. White paper.

[11] International Standard ISO/IEC 19792. *Information technology – Security techniques – Security evaluation of biometrics*.

[12] UK CESG (2001). *Biometric device protection profile (BDPP)*. Draft issue 0.82.

[13] U.S. Information Assurance Directorate (2007). *U.S. government biometric verification mode protection profile for basic robustness environments*. Version 1.1.

[14] U.S. Information Assurance Directorate (2007). *U.S. government biometric verification mode protection profile for medium robustness environments*. Version 1.1.

[15] German Federal Office for Information Security (2008). *Biometric verification mechanisms protection profile (BVMPP)*. Common Criteria Protection Profile BSI-CC-PP-0043.

[16] German Federal Office for Information Security (2010). *Fingerprint spoof detection protection profile based on organizational security policies (FSDPP_OSP)*. Common Criteria Protection Profile BSI-CC-PP-0062.

[17] German Federal Office for Information Security (2010). *Fingerprint spoof detection protection profile (FSDPP)*. Common Criteria Protection Profile BSI-CC-PP-0063.

[18] International Standard ISO/IEC 18045. *Information technology – Security techniques – Methodology for IT security evaluation*.

[19] Schneier, B. *Secrets and lies – Digital security in a networked world*. New York: Wiley, 2000

[20] Speicher, D. *Vulnerability analysis of biometric systems using attack trees*. Master's Problem Report, West Virginia University, 2006

[21] Matsumoto, T., Matsumoto, H., Yamada, K., and Hoshino, S. (2002). Impact of artificial gummy fingers on fingerprint systems. In van Renesse, R.L. (ed.), *Optical Security and Counterfeit Deterrence Techniques IV*, Proc. SPIE vol. 4677, pp. 275–289.

[22] Sandström, M. (2004). *Liveness detection in fingerprint recognition systems*. M.Sc. Thesis. Linköping University, 2004.

[23] International Standard ISO/IEC 19795-1. *Information technology – Biometric performance testing and reporting – Part 1: Principles and framework*.

[24] NIST (2001). *Security requirements for cryptographic modules*. Federal Information Processing Standards Publication FIPS PUB 140-2.

[25] Statham, P. (2005). Threat analysis – How can we compare different authentication methods? In *Biometric Consortium Conference*, Arlington, VA, USA, 2005.

[26] Cappelli, R., Maio, D., Maltoni, D., Wayman, J.L., and Jain, A.K. (2006). Performance evaluation of fingerprint verification systems. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 28, no. 1, January 2006, pp. 3–18

[27] Kent, J. (2005). *Malaysia car thieves steal finger*. BBC News, Kuala Lumpur, 31 March 2005, http://news.bbc.co.uk/2/hi/asia-pacific/4396831.stm