The State of the Art in Abuse of Biometrics

Ileana Buhan,Pieter Hartel

University of Twente, The Netherlands

Abstract. For applications like Terrorist Watch Lists and Smart Guns, a false rejection is more critical than a false acceptance. In this paper a new threat model focusing on false rejections is presented, and the "standard" architecture of a biometric system is extended by adding components like crypto, audit logging, power, and environment to increase the analytic power of the threat model. Our threat model gives new insight into false rejection attacks, emphasizing the role of an external attacker. The threat model is intended to be used during the design of a system.

1 Introduction.

Biometric authentication systems are used to identify people, or to verify the claimed identity of registered users when entering a protected perimeter. Typical application domains include airports, banks, military installations, etc. Bolle et al. [18] identifies 9 threats that plague biometric systems. Their opinion is that many questions about how to make biometric authentication work without creating additional security loopholes remain unanswered and that little work is being done presently in this area. Our paper contributes to filling this gap.
For most of these systems the main threat is an authorized user gaining access to the system. This is called a *false acceptance* threat.
Currently, new applications that have a completely different threat model are emerging. For example, *Terrorist Watch List* applications and *Smart Guns* applications are characterized by the fact that a false rejection could lead to life threatening situations.
Terrorist watch list applications currently use facial recognition or fingerprint recognition [2]. Watch lists are mainly used in airports to identify terrorists. For this application, the main threat is a *false rejection* which means that a potential terrorist on the list is not recognized. A *false acceptance* results in a convenience problem, since legitimate subjects are denied access and their identity needs to be examined more carefully to get access.
Smart guns [23] are weapons that will fire only when operated by the rightful owner. Such guns are intended to reduce casualties among police officers whose guns are taken during a struggle. The most promising biometric for this application is grip pattern recognition [23]. Again, a *false rejection* is the most serious threat as this would result in a police officer not being able to use the weapon when necessary. For a police officer to trust his gun the *false reject rate* must be below 10^{-4}, which is the accepted failure rate for police weapons in use.

Contribution We propose 3W trees (Who, What, hoW tree) for identifying false rejection threats to biometric security systems. Analysis based on a 3W tree leads

to concrete questions regarding the security of the system. Questions raised by other methods (e.g. attack trees) do not lead to the same level of specific questions. Our method is more concrete than other, because we make explicit assumptions about the generic architecture of the system, thus exposing all main components in the architecture that are vulnerable to attack. Our method is not less general than other methods because other architectural assumptions can be plugged in easily. Our method is intended to be used as a design aid.
Section 2 is an overview of threat models presented in the area of biometric authentication systems. The extended architecture of a biometric authentication system and the state of the art regarding attacks on each component is presented in Section 3. Section 4 is an introduction to security taxonomies. Section 5 describes 3W trees the method proposed for identifying attacks. Section 6 maps 3W trees threats to threat models identified in the literature.
In Section 7 we apply the 3W tree to the *Smart Gun*. Section 8 is about Terrorist Watch List with an example of an attack identified using the 3W tree. Conclusions are presented in last section.

2 Industry best practices: The Standards

This section describes standards that address threats to biometric devices. Like all security systems, biometric systems are vulnerable to attacks [8,17]. An example of such an attack consists of presenting fake inputs such as false fingerprints [3] to a biometric system. To analyze such threats systematically various threat models have been developed.

In the following we discuss the most important models: the Biometric Device Protection Profile (BDPP) [6], the Department of Defense & Federal Biometric System Protection Profile for Medium Robustness Environments (DoDPP) [9], the U.S. Government Biometric Verification Mode Protection Profile for Medium Robustness Environments (USGovPP) [14] and Information Technology-Security techniques -A Framework for Evaluation and Testing of Biometric Technology (ITSStand) [4].

In the sequel we refer to these three protection profiles and the *ITSStand* simply as "the standards". Threats and vulnerabilities identified in "the standards" are described and compared.

In September 2001 the UK Government Biometrics Working Group issued *BDPP*. *BDPP* specifies functional and assurance requirements applicable to commercially available Biometric Devices that are used to identify or verify previously enrolled individuals for entry to a portal. The portal protects assets such as data, equipment, people. The *BDPP* includes requirements concerning the connection between individual and the Biometric Device, the connection between the Biometric Device and the portal and supports policies for verification, identification, auditing and integrity. The Biometric Device is not assumed to be of a particular type. Any particular Biometric Device that meets the requirements in the operational environment may be evaluated.

In March 2002 *DoDPP* was published.

This protection profile specifies the minimum functional and assurance security requirements for biometric systems employed by the U.S. Department of Defense (DoD) and Federal Agencies to provide identification and authentication allowing access control to physical facilities as well as to information systems in medium robustness environments.

The requirements section of this protection profile specifies a need to encrypt biometric templates. Specifically, all biometric templates must be encrypted while in transit and storage.

In November 2003, The Biometrics Management Office and National Security Agency sponsored a new Protection Profile, *USGovPP*.

USGovPP targets biometric products operating in verification mode and specifies the minimum functional and assurance security requirements that have to be met in order to provide authentication allowing physical and logical access control to facilities as well as to information systems in medium robustness environments.

The same year, 2003 Deutsches Institut für Normung e.V. from Berlin issued the draft of the ISO standard, *ITSStand*.

ITSStand specifies security evaluation and testing of biometric algorithms, component systems and additional relevant elements of biometric technology. A generic framework is stated that enables the adaptation of testing and evaluation processes (procedures) for different environments, applications, algorithms and privacy related security conditions for biometric technology. In this document security, reliability and privacy aspects are explicitly addressed.

2.1 Threat model -general assumptions

In the following assumptions made by the standards are presented. They describe the environment in which the biometric authentication system will be used. The assumptions are important for motivating the threat model presented in these documents.

BDPP

This Protection Profile states 5 assumptions regarding the operating environment including physical, personnel and connectivity issues. These assumptions are:

A.PORTAL The biometric device is intended to be used for identifying or verifying the identity of, regular users for entry to a portal.

A.FALLBACK It is assumed that any alternative or fallback verification/identification system, used when the biometric system is not in operation, offers adequate protection of the assets. The security of the fallback system is outside the scope of the evaluation.

A.ROLES Administrator, operator and regular user roles are defined in this Protection Profile. Depending on the application, 2 or more individuals may fulfill a single role; alternatively 2 or more roles may be fulfilled by a single individual. In each case the characteristics applicable to roles are assumed to be transferred to the individual or individuals filling the roles.

A.NOEVIL Administrators are assumed to be non-hostile and trusted to perform all their duties in a competent manner.

A.USERTMPL It is assumed that, if users supply their own biometric template (e.g. stored on a smartcard), measures exist to protect the authenticity and integrity of the template.

A.PORTAL states the intended usage of the system, namely whether the system will be used for verification or identification or both. A.FALLBACK is a “fail secure ” assumption which says that there should be other means by which the assets can be protected if the biometric system is not in operation. A.ROLES identify three types of users: administrator, operator and regular user. However, the distinction between roles is not clearly stated. A.NOEVIL rules out threats posed by hostile or incompetent administrators. The authors make the observation that administrators are not assumed to be incapable of human error. Assumption A.USERTMPL is called the “Connectivity assumption” and states that templates need to be protected. Proof of template authenticity is required. Template quality has an influence on the systems performance and on the security on the biometric system.

DoDPP The assumptions made about the intended usage of the system A.PORTAL, the TOE operating environment A.NOEVIL, A.ROLES and the “Connectivity Assumption”, A.USERTMPL are the only assumptions made by the authors and they a re exactly as defined in the Biometric Device Protection Profile.

USGovPP This Protection Profile makes three assumptions about the specific conditions that are assumed to exist in the TOE environment. They are as follows:

A.ENROLLMENTAPPROVAL It is assumed that sites follow appropriate procedures for validating the identity of enrolled individuals.

A.NOGENERALPURPOSE There are no general-purpose computing or storage repository capabilities (e.g., compilers, editors, or user applications) available on the TOE.

A.OPERATINGRANGE The TOE is placed in an environment that does not exceed its normal operating range (e.g., temperature, humidity) as defined by the vendor.

It is of paramount importance to ensure the authenticity of the enrolled individual states the A.ENROLLMENTAPPROVAL assumption. Nothing is said about the integrity of the templates. A.NOGENERALASSUMPTION says that the biometric authentication device should be implemented on a dedicated device and the environment in which the device will be used should not decrease the performance recommends A.OPERATINGRANGE assumption.
The *ITSStand* makes no assumptions about the biometric device environment. Table 1 contains the assumptions made in the standards.

BDPP Number	**DoDPP**	**USGovPP**	**ISOStand**
A.PORTAL	A.PORTAL	-	-
A.FALLBACK		-	-
A.ROLES	A.ROLES	-	-
A.NOEVIL	A.NOEVIL	-	-
A.USERTMPL	A.USERTMPL	-	-
		A.ENROLLMENTSPPROVAL	-
		A.NOGENERALPUPOSE	-
		A.OPERATINGRANGE	-

Table 1. *Assumptions made in the standards.*

2.2 Summary

The standards are based on largely disjunct sets of assumptions. In our own threat model we will take the entire set of assumptions into account, omitting those that are not relevant to false rejection sensitive biometric applications.

3 Biometric Authentication Generic System Architecture

Figure 1 presents the components and the points of vulnerability of a general biometric system as presented by Ratha et al. [17], who provide a systematic analysis of different points of attack in a biometric authentication system. Their analysis is based on a generic architecture of a biometric system. The components

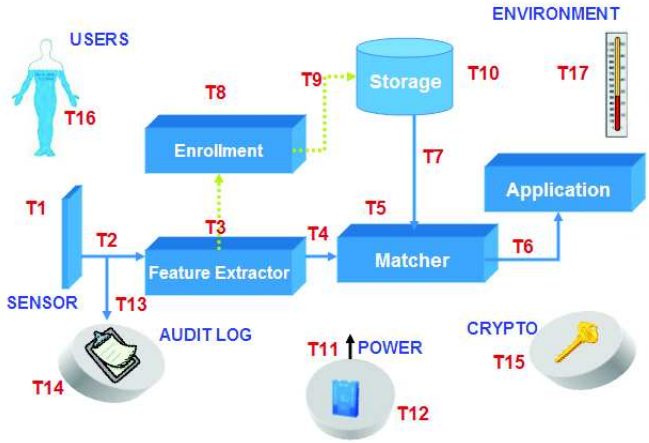

Fig. 1. General view of a Biometric Authentication System showing 17 points of attack.

of that architecture are:

(a) The *input device* or *sensor* used for the acquisition of the biometric sample.
(b) The *feature extractor* that builds a digital representation from the raw biometric sample.
(c) The *matcher* that calculates the similarity between two biometric samples.
(d) The *application* for which the authentication is done.
(e) The *storage* where template and other information, like user name are stored.
(f) The *channels* in which information is transmitted between the components of the system.
(g) The *enrollment* when the system is trained. During enrollment samples are collected, calculating the feature vector and storing this information in the database.

Each of the components as well as the connecting channels are potential targets of attack. Comparing these targets of attack to the threats identified in the standards, see section 6, we discovered some threats that do not have a corresponding target of attack in the architecture. For example in the architecture nothing is mentioned about the power that makes the electric equipment work. Cutting the power to the system will make the system fail. Therefore, we extend the generic biometric architecture to include the following components also shown in *figure* 1:

(h) *Audit*, important actions need to be recorded for later analysis. In the case of the *Smart Gun* application it is particularly important to have a record

of which user fired the gun at what time. The auditing process itself can be subject to an attack for example T.AUDIT_COMPROMISE, *DoDPP*, see table 3.

(i) *Cryptography,* to ensure the authenticity and integrity of data stored and transmitted on channels. The standards identify threats related to cryptography as follows; T.CRYPT_ATTK in *DoDPP*, see table 3, T.CRYPT_ATTACK and
T.CRYPTO_COMPROMISE in *USGovPP*, see table 4.

(j) *Power,* is a major concern especially when the biometric device is portable. For example, replacing the power source might restart the application causing the biometric system to enter an unknown or unstable state. This attack is related to threat T.POWER in *BDPP*, *DoDPP*, *ITSstand*, and T.UNKOWNSTATE in *USGovPP*, see table 4.

(k) *Environment and users,* this is general but we also include in this category: operating parameters such as temperature, humidity, etc. Threats related to users identified in the standards are T.BADUSER, T.BADADMIN, T.BADOPER in *BDPP*, see table 2 and *DoDPP* (T.BADOPER is not present in that document), USGovPP does not contain T.BADUSER and T.BADOPER but it contains two threats related to a bad administrator, namely T.ADMIN_ERROR and T.ADMIN_ROGUE, see table 4 and in *ITSstand* they are labelled as: 8.1, 8.2, 8.3 and 8.4, see table 5. Other threats are T.FAILSECURE, T.DEGRADE presented in *DoDPP*, see table 3.

Having identified the components of the generic authentication architecture, we now list the specific threats possible for this type of architecture.

T1 is a threat resulting from attacking the input device or the sensor. The most serious threat on a biometric system is presenting a fake biometric [17]. The fabrication of something analogous to a real user is called a *Synthetic Biometric Feature Attack*. This attack can be implemented with or without tampering with the sensor.

T2 is the resubmission of a previously stored biometric signal in the channel between the sensor and the template extractor (replay attack).

T3 is a feature extractor threat, for example at a given time or under some specific conditions a *Trojan Horse* may produce a pre-selected feature.

T4 is an attack on the communication channel between the feature extractor and the matcher. For example, inserting a previously recorded signal into the communication channel.

T5 is again a *Trojan Horse* attack. This time the target is the matcher, which is forced to produce a high or low match on.

T6 consists of overriding the output of the matcher and thus bypassing the entire authentication process. The output of the matcher module could be forced to be either a match or a non-match.

T7 is another channel attack on the communication between the (central or distributed) database and the authentication system. The templates stored in the database are sent to the matcher through a channel, which is attacked to change the representation before it reaches the matcher.

T8 is an attack on the enrollment center. The enrollment and the authentication process have similarities in the sense that they are both implementations of an authentication protocol, and therefore enrollment is vulnerable to attack points T1, . . . , T6.

T9 is an attack on the channel from the enrollment center to the database. Control of this channel allows an attacker to override the (biometric) representation that is sent from enrolment to the biometric database.

T10 attacks the database itself. This could result in corrupted templates, denial of service to the person associated with corrupted template or authorization of a fraudulent individual.

In addition to threats **T1-T10** of Bolle et al. [18] we identify threats **T11-T17** that influence the performance and security of a biometric system:

T11 The channel that links the power source to the system is destroyed.

T12 The power source of the system is tampered with.

T13 An attacker may prevent future audit records from being recorded by attacking the channel that transports the audit information.

T14 Audit records may be deleted or modified, thus masking an intruder action.

T15 Security functions may be defeated through cryptanalysis on encrypted data, i.e. compromise of the cryptographic mechanisms.

T16 Users, regardless of the role that they play in the system, can compromise the security functions.

T17 The environment (temperature, humidity, lighting, etc.) and extensive usage can degrade the security function of the system

In our opinion, threats T1-T13 should be addressed by security mechanisms and threats T14-T17 should be addressed by operational security procedures.

In the next sections we describe in more detail attacks particular to each component of the architecture.

3.1 Attacking the input device/sensor

Each time a user is authenticated a sample of her biometric data is collected. Depending on the type of biometric, the input device has various forms. The acquisition devices used vary from cameras (video, single-image, infrared), scanners (optical, silicon, ultrasound, touchless), audio devices (microphone, telephone), desktop peripherals (keyboard, keypad, signature tablet) etc., according to the feature extracted. It is important to understand the device limitations to assess the risk of attacks.

One general requirement is that the input device must be consistent over time. Some systems include automatic quality control features in the sensors and can detect poor quality signals that otherwise increase the false reject rate. Technical information on the most common biometric sensors can be found in Gonan [5].

The most serious threat on an input device is presenting a fake biometric [17]. The fabrication of something analogous to a real user is called a *Synthetic Biometric Feature Attack*. Some biometrics are harder to forge: iris, retinal scan, face thermogram while others are easier to forge: voice print, face, hand written signature [7]. Fingerprint biometric authentication systems are also easy to bypass [3]. Bolle et al. [18] evaluate the inherent strength of fingerprint-based authentication scheme. That is the probability that a brute force attack at point T4 at *Figure 1* will succeed in matching a given stored template.

When cost is not an issue, to the attacker, all biometrics can be, and probably will be, the subject of a synthetic feature attack. The difficulty of such an attack depends on the implementation of a specific system [18].

We have to keep in mind that biometrics are unique identifiers, but they are not secrets [20]. The system must somehow be able to verify that the biometrics came from the person at the time of verification. *Liveness* determination verifies that a biometric sample is coming from a living person [16].
The synthetic feature biometric attack can be implemented as a *coercive*, *impersonation* or *replay attack* with more or less tampering with the sensor [18].
A *coercive attack* is an attack where the legitimate user's biometric data is presented in an illegitimate scenario. For example the attacker physically forces a genuine user to identify herself to an authentication system or after the physical removal from the rightful owner [18]. Designers have to think how to counter such attacks, for example by installing security cameras at ATM's.
An *impersonation attack* involves changing one's appearance so that the measured biometrics match an authorized individual. Examples of biometrics that can easily be the subject of this kind of attack are face, voice or signature. Multimodal biometrics reduces the exposure to an impersonation attack (particularly if the system is checking for consistency between the multiple biometrics).
A *replay attack* involves the re-presentation of previously recorded biometric data. This is the simplest attack possible against a biometric system. For example record someone's voice, or take a picture of a person and present it to a face recognition biometric system (favorite subject of movies with thefts). Current research tries to eliminate this kind of attack. For example face recognition systems try to detect the three - dimensionality of the face presented to the camera.
Some characteristics change slowly over time and biometric systems may employ *adaptation* in order to keep the stored reference template in step with those changes. *Renewal* is the re-enrollment of a user by provision of a new enrollment template for that individual. The interval of renewal of a particular biometric is best to be evaluated before the system is deployed in order to schedule the activities that have to do with maintenance.

3.2 Attacking the feature extractor

The feature extractor transforms raw biometric data read by the sensor into an electronic signal suitable for further processing. The transformation depends on the type of biometric sample of the feature extractor. Matyas et al. [11] identify the relevant processing steps as:

- A quality analysis on the input signal to determine whether it is suitable to use or not. If the signal fails the quality tests it is rejected and the user may supply another sample.
- A filter may be applied to the signal to remove noise or information that is not necessary for the matching step.
- The signal may be normalized in some way. For example an image can be adjusted to standard levels of brightness and contrast.

Gonon [5] mentions that the three main factors that should be taken into account when handling biometric data at this stage are:

- The acquisition time of the test data.
- The processing time and complexity of the feature or template extraction
- The ability of the score function to perform direct scoring on incoming data or the need to gather all data before scoring. Gonon refers to these approaches as online and offline/batch processing.

The different existing algorithmic strategies for scoring biometric data can be categorized into two types of processing:

- Template matching or *offline matching*: a template is constructed after all test data are gathered and the stored templates are compared.
- Scoring over a stream of feature vectors or *online matching*: while test data are acquired, feature vectors are constructed and sent to the matcher for scoring.

A *Trojan Horse* attack on the feature vector, produces at a given time or under some specific condition a pre-selected feature. Much care must be taken during the employment of the system to avoid this.

Stored templates can be protected by encryption. Data transmitted between the capture device and the rest of the system could also be protected by cryptography. But here, unique session keys would be necessary (e.g. through time-stamping) to prevent data being replayed successfully. If the stolen template is used, then liveness testing could be used to ensure that the biometric is actually being submitted by a person.

Transformations e.g. cryptography can be applied on the feature vector only if the time element is not critical or the equipment can process data fast enough. Template transformation techniques have been developed to circumvent the compromise of a template by the legitimate substitution of the transformed version of the template for matching against a similarly transformed feature vector. This is called in the literature *cancellable biometrics* [16]. This is an intentional, repeatable distortion of a biometric signal based on a chosen transform. The biometric signal is distorted in the same fashion at each presentation, that is, during enrollment and for every subsequent authentication. This technique has been developed to protect the privacy of the individual and to permit the reutilization of a biometric sample even after the biometric feature has been stolen.

3.3 Attacking the Matcher

The matching-scoring module measures the similarity of a test sample with a template. Biometric samples are compared through pattern recognition techniques obtained from two samples of real world biometric data, which are never the same because of noise and distortion in the acquisition process.

The result of a matching decision is a score s which is a numeric value indicating how close the sample and the template match. This score is used by the authentication protocol to arrive at a decision based on a threshold T: if $s > T$ then the samples match otherwise if $s \leq T$, the matcher decides that the samples don't match. The threshold T is tuned by the system designer's through a process of training and testing to achieve acceptable values for FAR and FRR.

The reliability of the score is influenced by the variability in sampling process and the variation from sensor to sensor. The similarity score is equal to one only if two biometric samples are copies of each other. This is called a *perfect match*.

Some systems perform adaptation to keep the enrollment templates up-to-date with gradually changing biometric characteristics for the user.

Again a *Trojan Horse* attack is possible, this time the target is the matcher, which can be forced to produce a high or low match score and thereby to manipulate the match decision [18].

3.4 Attacking the Database

The database maintains the templates of the enrolled users. It may contain one or more templates. The database can be local or central depending on the architecture of the application. One problem when enrolling a new user is to make sure that there are no duplicates that might confuse the system. Another issue is database integrity. Bolle et al. in [18] define database integrity as

how well the database reflects the true data on the biometric sampling.

The process of checking the database integrity and purging the detected duplicates is called *database consolidation*.
A possible threat is the unauthorized modification of one or more template representations in the database. Another threat to take into account is *the double enroll error attack* that refers, as the name suggest at re-enrolling a user under a different name.
Another possibility is a privacy attack - an attack of the confidentiality of the authentication system.
The protection of the database is important because the final authentication system is only as secure as its enrollment database.

3.5 Channel attacks

Channels provide the ability to transfer information between input device, feature extractor, matcher and database. The system components that are communicating may be local or remote. Communication can be realized using different transmission media. *Figure 1* shows that from 10 possible threats on a generic biometric system 5 are channel attacks. This emphasizes the importance of addressing channel attacks. The *Connectivity assumption*[9] states that biometric templates must be protected during transmission between the biometric subsystems for example by cryptographic means.

3.6 Power attacks

By cutting the power to the system an attacker can make the system fail. Depending on the power source connected to the system batteries or electricity attacks may be different. Restarting the system after a power loss can result in an unstable system.

3.7 Crypto Compromise

Cryptanalysis on encrypted data or brute force attacks may help an attacker gain unauthorized access. If code or data associated with cryptographic functions can be accessed inappropriately by a process or user the cryptographic mechanisms and the data protected by those mechanisms may be viewed, modified or deleted.

3.8 Audit log Compromise

Audit log compromise is not a direct attack on the system, but an inadequate collection of audit data with the intention to hide the traces of an attack on the system.

3.9 Environmental and User related threats

A user may cause harm to a system intentionally or unintentionally. For example an administrator may incorrectly install or configure the biometric system, the result being an ineffective mechanism. Even if the administrators intentions are not malicious he may become so as mentioned by T.ADMINROGUE in table 4. Non-hostile administrators (unintentionally or under coercion) could incorrectly modify user privileges or matching threshold or enrolls an unauthorized user. An other threat is that an impostor may acquire administrator privileges as stated by threat 8.1 in table 5.
An attacker may cause failure of the biometric system by exposing the authentication device to conditions outside its normal operating range. The conditions refer to temperature, humidity, light, etc.

3.10 Other attacks

Further attacks that can be conducted on biometric systems:

Hill climbing attack: This attack is described in by Bolle et. all [18]. The biometric sample is slightly modified and then submitted to the algorithm repeatedly. The output score of the current biometric sample is observed. If the score is greater than the previous output score the changes applied on the biometric sample are preserved. The goal is to achieve the match threshold. When the attacker has no information on the legitimate user's biometric data this is the most suitable attack on electronic systems.
This attack can be prevented if repeated trials are not allowed. According to Ulugad et al. [22] this type of attack can be cast as an attack in point T2 or point T4 in *figure* 1. When hill-climbing is applied as a T2 attack (before the feature extractor), the information about the template format (which is essential for a T4 attack) is not necessary.
Swamping attack : Tries to exploit weakness in the algorithm to obtain matches for incorrect data. For example for a fingerprint system the attacker might try to submit a print with a lot of minutiae hoping that the threshold number N of them will match the stored template. The weakness in the algorithm is that it accepts such a representation. [18]
Piggy-back attack : The attacker tries to gain physical or logical access simultaneously with a legitimate user.[18]

3.11 Summary

Biometric systems have a lot of weak points. Most likely, attacks occur during the live verification phase. An attack during the *Enrollment Procedure* is less expected, because this operation can take place in a secured environment, the focus of our analysis are smart guns and terrorist watch lists in both of which enrollment is supervised by trusted personnel. However, a successful attack during the enrollment phase will have a devastating effect.
By comparison, attacks made during the *Live Verification Procedure* will be most likely, so the effect of these attacks should be limited. The devices are carried

around (police officers) or placed in public places (terrorist watch lists), some of their parts, i.e. the sensors can be bought in order to be intensively studied.
Biometrics, like other protection mechanisms, are influenced by environmental conditions which can cause surprises. Dirt or unreliable lighting conditions all take their toll. Some systems, like speech recognition are vulnerable to alcohol intake and stress [1].
We have to find out which are, and to what extent, external factors can influence the way our system operates. In the case of grip patterns RSI, stress and physical condition might affect the performance of the system.
Bolle et al. [18] say that biometrics is not considered much in the security literature and that there are many questions in how to make biometric authentication work without creating additional security loopholes.
In this section we presented an extended architecture of a biometric system. We discussed particular threats to each component in the architecture. We related this threats to possible attacks from the standards. In the next section a structure for the attacks will be provided.

4 An introduction to security attack taxonomies

There are many general security taxonomies in the literature. They classify attacks based on one or more grounds of distinction. Some taxonomies group attacks using similar grounds of distinction, but use different classes. For example, both *Neumann and Parker's SRI Computer Abuse Methods and Models* and *Jayaram and Morse's Network Security Architectures* refer to misuse techniques,[10], but the Neumann classification identifies classes like: *external, hardware misuse, masquerading, pest programs, bypasses, active misuse, passive misuse, inactive misuse, indirect misuse* while Jayaram and Morse's taxonomy identifies only 5 different classes i.e. *physical, system weak spots, malignant programs, access rights and communication based*. Other taxonomies view attacks from totally different angles, for example *Anderson's Penetration Matrix*[10] has three types of penetrators: *external, internal and misfeasance* while *Knight's Vulnerability Taxonomy*[10] defines a vulnerability as having five parts (*Fault, Severity, Authentication, Tactic, Consequence*). Each part is defined according to a different taxonomy. None of these classifications pay special attention to biometrics. It is a difficult task, in our opinion, to identify the most adequate taxonomy that a security architect should use for evaluating the risks associated with the system that she is trying to protect. However during our research for suitable taxonomies we observed that computer security taxonomies can themselves be classified. We propose to use this meta-classification to assist in identifying a proper threat model.

Our meta-classification will prove to be useful in choosing, the right taxonomy or if there is no appropriate taxonomy at least provide a guidance to the process of building a new one.

Atomic taxonomies classify attacks based on one 'fundamentum divisionis' or 'ground of distinction'.

The main grounds of distinctions used are:

- *The who*. Is used by taxonomies that classify attacks according to various characteristics of the attacker. Anderson's Penetration Matrix, [10] covers the types of penetrators, based on whether they are authorized to use a resource, Abraham et al. [10] identify three classes of 'adversary' relative to the attackers position into the system, Rae and Wildman [15] assemble a structured taxonomy of attacks as a basis for defining the access required by an attacker, and there are others for which the motivation or the skill required to mount a successful attack, is taken into account.
- *The how*. A considerable number of taxonomies group attacks on 'modus operandi' or attack methods used during an attack. Neumann and Parker, [10] identify 9 distinct procedures of conducting an attack like *external, hardware misuse, masquerading, pest programs, bypasses, active misuse, passive misuse, inactive misuse, indirect misuse*. Later, Lindqvist and Jonsson [10] extend the work of Neumann and Parker, refining the classification allowing the number of classes the increase from 9 to 26. For example the *hardware misuse* class is decomposed in *logical scavenging, eavesdropping, interference, physical attack, physical removal* and *masquerading* is broken down in *impersonation, piggybacking attacks, spoofing attacks and network weaving*. Lindqvist and Jonsson also introduce the concept of dimension of an attack that states that for every intrusion technique there is an intrusion result. Jayaram and Morse's develop a *taxonomy of security threats to networks*

and the classes identified are *physical, system weak spots, malign programs, access rights, communication based*. We notice that some classes as *malign programs* overlap *pest programs* in Neumann and Parker's taxonomy, but the *communication* based class is new. Other taxonomies of this type are extensively covered in D. Lought's PhD thesis [10], who also lists the similarities between taxonomies.

– *The what*. Taxonomies of this type have as ground of division the flaw exploited. Howard's CERT Taxonomy distinguishes three types of flaws *implementation vulnerability, design vulnerability, configuration vulnerability*. Other taxonomies identify a vulnerability as belonging to one of the following categories of attack: *specification weakness, implementation weakness, brute force attack*. One of the most interesting taxonomies proposed is Knight's Vulnerability Taxonomy [10]. He defines a vulnerability as being a quintuple of the form (*fault, severity, authentication, tactic, consequence*). In 1976 Stanford Research Institute collected 355 security breaching incidents and divided them into 7 violation categories [10].

Each atomic taxonomy represents only one dimension of the attack. An attack is rarely caused by a single flaw in a system and is rather a function of different characteristics of the system. Therefore we propose to use one taxonomy from each of the identified classes(who, how and what). This offers the possibility of identifying a broad range of attacks. Combining a taxonomy from each of these classes creates a nested taxonomy, which we called the *3W tree* (What,hoW, Who). *Process oriented taxonomies* take one step further compared to *atomic taxonomies* and view an attack as a process. We see the extension of 3W trees to cover processes as future work.

So, we are now ready to organize the area of biometric security taxonomies and to see how attacks can be viewed from different angles. Our goal is to identify as many relevant attacks as possible, from all the points of view while maintaining a comprehensive structure (the 3W tree). Our contribution is the identification of grounds of distinction used in the classification of the security computer taxonomies and in the use of 3W trees to analyze threats to biometric systems.

4.1 Summary

We divide taxonomies of attacks in security computer in three classes based on the ground of division used: the who, the how, the what. Among taxonomies studied we could not find one that could give us the assurance that all the relevant threats are indeed identified and which help in developing the threat model for a biometric authentication system.

5 3W trees

A 3W tree is a structure that combines three taxonomies (from different classes) in a nested manner.
The first level of the our 3W tree, *figure* 2 is a classical *who* taxonomy from the attacker's position relative to the system [13]. Attackers are divided in three classes. *Class I* attackers or *external* attackers, lack knowledge about the system and have moderately sophisticated equipment. *Class II* attackers or *internal* attackers are knowledgeable insiders, which are highly educated and have access to most parts of the system. *Class III* attackers are funded organization with ample resources that are able to assemble teams and design sophisticated attacks. It is widely acknowledged that there is no protection against class III attackers. The general opinion is that a system is considered secure if it can withstand class I and class II attackers.
In this paper we address only single points of attack even though attacks usually mean controlling more points in the system.
A 3W tree is intended as a design aid; therefore we focus on external attacker.

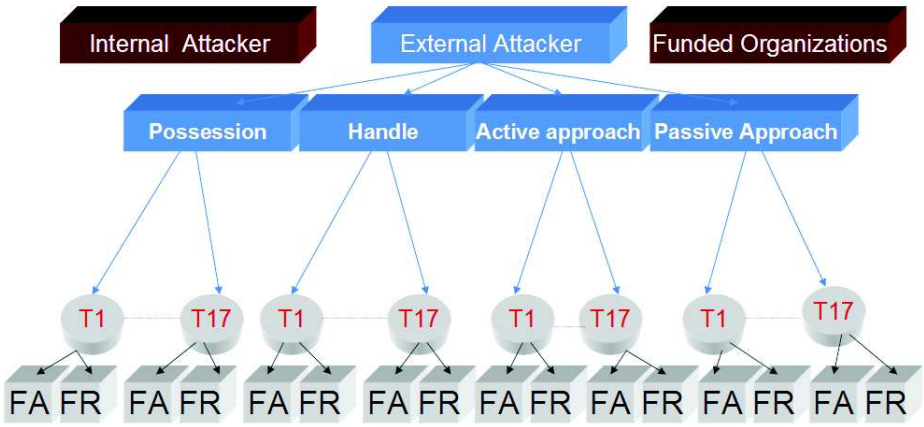

Fig. 2. 3W tree of attacks on biometric systems. T1-T17 are points of attack shown in *figure* 1.

As a second level in the 3W tree we use the Rae and Wildman taxonomy for secure devices [15]. This is a *how* taxonomy. The next paragraph paraphrases Rae and Wildman:

- *passive approach*, the attacker may be in the proximity of the device, but cannot touch the device;
- *active approach*, the attacker can interfere with the device (e.g. over a network) and transmit data to the device from either an insecure or a secure domain.
- *handles* the device physically, but cannot break tamper evident seals on the device;

– *possesses* the device i.e. can open the device and break tamper evident seals with impunity;

The classes presented are related to one another. *Possessing* the device means that the attacker can *handle* the device and of course may *approach* the device. This relationship can be formalized as :
passive approach $\subset$ *active approach* $\subset$ *handle* $\subset$ *possession*

The third level of the 3W tree, the *what*, deals with the threats our system might be subject to.
The relevant threats T1-T17 are listed in section 3.
Finally, in keeping with our observation made earlier about the increasing importance of studying *false rejections* we add as a fourth layer the distinction between *false acceptance* and *false rejection*. What makes our layered taxonomy biometric specific is that: (1) the points of vulnerability T1-T17 refer to a Biometric System and (2) we consider two specific effects of each attack: a *false acceptance* or a *false rejection*.
An observation is that portable biometric devices are likely to be attacked in *possession* and *handle* situation so there must be some methods to ensure the physical integrity and robustness of such devices. Fixed biometric devices are more likely to be attacked by *passive approach* and *active approach* means.
For constructing a 3W tree one can choose any taxonomy from the identified classes. The way in which they are nested must not be necessary the one presented in this document. Another issue is that of the architecture of the system. If one knows that his system is more specific, some threats can be eliminated. Other layers might be added as needed.

5.1 External Attack Scenarios

A scenario is a path in the 3W tree of *figure* 2. A scenario is named as xiy where:
– $x \in \{PA, AA, HA, PO\}$, PA stands for *passive approach*, AA stands for *active approach*, HA stands for *handle* and PO for *possession*.
– $i \in \{1..17\}$ indicating threat Ti.
– $y \in \{A, R\}$, where A means an attack leading to a *false acceptance* attack and R means an attack leading to a *false rejection* attack.

Each path in the tree corresponds to a threat that has to be evaluated. For example, scenario PO1A identifies the following: in the possession situation (denoted by the letters PO), threat $T1$ (presenting a fake biometric/tampering with the sensor) to obtain a false acceptance (A).
To describe and evaluate scenarios we use the following attributes:

I. Description:
- *Scenario:* name of the evaluated scenario.
- *Tactics:* describe a possibility to realize this attack.
- *Name:* the name of the attack in the literature or a link to a paper that describes this attack (if known).

II. Evaluation:
- *Damage:* the estimated consequence of the attack for the device. The possibilities are: *minor*, *moderate*, *major*. An attack with minor consequences will temporarily damage the device. A moderate consequence attack will temporarily damage the device but it needs specialized personnel to repair it. An attack with major consequence will completely ruin the device, and the whole or parts of it need to be replaced.

- *Knowledge:* lists the knowledge that an intruder must have to launch the attack. The categories are: common sense, high school education, expert.
- *Occurrence:* an educated guess of the probability that such an attack occurs. The estimators are: *low* (unlikely to have such an attack), *medium* (it might happen), *high* (likely to happen).

III. Defense

- *Countermeasures:* some notes on how this attack might be prevented, or how at least to diminish its consequence.

Section 7 presents a complete case study in the case of the Smart Gun Application, where a 3W tree is applied to assess the most relevant false rejection threats.

5.2 Attacks trees and 3W trees

Attack trees offer a method of analyzing attacks [19]. The root of the tree is identified with the goal of compromising a system. The goals of the children of a node could be the compromise of a sub-system or a contribution thereof, and so on recursively. There are two types of nodes: the goal of an *and*-node depends on the goals of all its children, and the goal of the *or*-node depends on at least one of the children [12]. There are commercial tools to support analysis working with attack trees; for example the Secur*IT*ree tool from `http://www.amenaza.com/`.
The main advantage of attack trees is that they help the designer by visualizing possible attack scenarios. If there are many possible attacks, or if there are many components that are subject to attack, an attack tree may become large. In this case the vizualisation is ineffective. However by attacker profile based pruning, support tools allow the designer to focus on attacks relevant to specific attacker profiles. Another useful feature of the tools is that while constructing a tree the designer can document the changes and also the reason for changes made by annotating nodes. The main disadvantage of attack trees is that they provide only the choice between *and*-/*or*-nodes. This does only provides a low level way of breaking up a goal up into sub-goals. The general recommendation is to think hard, which, though important, does not provide much guidance.
Our 3W tree approach gives such guidance for two reasons: (1) we identify concrete points of attack in the generic architecture of the system under threat and (2) we focus on concrete questions such as what to attack, how to attack it and who the attacker is. The disadvantage of our 3W tree is that it has been developed specifically for a generic biometric authentication system. However, by replacing this architecture by another, generic architecture our 3W method could be deployed more widely.
To obtain the advantages of both methods, we propose to combine attack trees with 3W trees. At the top level, the 3W tree gives rise to concrete questions about the what, how and whom of an attack. To answer the question, we attach an attack tree to each leaf of the 3W tree. By constructing the attack tree for each leaf, the analyst is encouraged to answer the specific, focused question.
Attack trees, 3W trees and also the combination suffer from the disadvantage that node attributes (such as estimated Damage, or the likelihood of Occurrence) are typically educated guesses. Short of large scale experimentation with all kinds of attacks, there is no general method for providing accurate attribute values. However, assume that there are dependencies between attribute values. Then the

idea of using a model checker, such as proposed by Sheyner et al. [21], could be pursued to analyze 3W/attack trees. This would enable developers of 3W/attack trees to state and verify properties of the attack tree and its attributes. We leave this as future work.

5.3 Summary

In applications like *Terrorist Watch Lists* or *Smart Guns*, *false rejection* attacks are more important than *false acceptance* attacks. We propose 3W trees as a flexible tool to highlight *false rejection* or *false acceptance* attacks depending on the type of application. Our threat model gives new insight into false rejection attacks emphasizing the role of an external attacker.
The main purpose of a analysis using 3Wtree is that relevant threats are identified. Only after this step one can decide what the proper security measures are that need to be developed.

6 Comparison between threat models in the standards and the threat model from 3W trees

In the following we will try to map threats identified in the standards to the attacks identified in the 3W tree threat model. Only attacks from external users are discussed.
In tables 2, 3, 4 and 5 the "Attack Description" column attacks are presented as the authors of BDPP described them. The "3W tree Classification" column contains the same attack from our taxonomy and a possible scenario is presented in the "Motivation" column.
It is difficult to compare threats amongst the four standards even though the standards are similar. They are similar because they address the same threats and they are difficult to compare because for the same attack one identifies one threat while others identify more. For example, *BDPP* contains one T.TAMPER threat while *ITSStand* contains three tamper related threats: one for hardware tampering another for software or firmware tampering and one for channels. In *ITSStand* tampering and bypassing is mentioned when describing the same threat while *BDPP* explicitly mentions the T.BYPASS threat.
Also the standards do not make a clear distinction between a *false rejection* and a *false acceptance* attack.

6.1 Biometric Device Protection Profile threat vs. 3W-tree Classification

In table 2 the attacks presented in BDPP are mapped to the attacks that we identified in our taxonomy.

Table 2: *BDPP*

BDPP	Attack Description	3W tree Classification	Motivation
T.CASUAL	An impostor may make a zero-effort forgery attempt to impersonate an authorized user	$HA \left\{ \begin{matrix} 1 \\ 16 \end{matrix} \right\} A$	The intruder puts his hand on the gun and tries to shoot.
T.MIMIC	An impostor may be able to reproduce the biometric characteristics for the ID under attack by mimicry, e.g. changing his voice, forging a signature or hand contortions.	$HA \left\{ \begin{matrix} 1 \\ 16 \end{matrix} \right\} A$	The intruder tries to mimic the authorized users grip pattern by successive attempts.
T.ARTIFACT	An impostor may use an artificial biometric characteristic (e.g. artificial hand/fingerprint/life-size photograph, etc.) to gain access.	$HA1A$	An exoskeleton hand is used to shoot the gun.
T.RESIDUAL	The residual biometric image from a previous user may be sufficient to allow access to an impostor.	$\left\{ \begin{matrix} HA \\ PO \end{matrix} \right\} 1 \left\{ \begin{matrix} A \\ R \end{matrix} \right\}$	The sensor might be deceived to read the residual image of a authorized user, might be done by tampering with the sensor, thus allowing an attacker to fire the weapon.

T.BYPASS	An impostor may bypass the capture device or other parts of the biometric system	$PO \left\{ \begin{matrix} 2 \\ 4 \\ 6 \\ 7 \\ 9 \end{matrix} \right\} \left\{ \begin{matrix} A \\ R \end{matrix} \right\}$	This refers to all channel attacks. Channels are situated inside the gun thus, this attack can be carried out in possession situation.
T.UNDETECT	An undetected attack against the TOE security functions is mounted by an attacker, which eventually succeeds in either allowing illegal access to the portal, or denying access to authorized users.	$\left\{ \begin{matrix} PA \\ AA \\ HA \\ PO \end{matrix} \right\} i\, A$	The only thing that they mention about the attack is that is undetected. Is the first attack that results in denying access to authorized users.
T.POWER	A power loss results in failure of the Biometric System.	$\left\{ \begin{matrix} HA \\ PO \end{matrix} \right\} \left\{ \begin{matrix} 12 \\ 11 \end{matrix} \right\} R$	Sinking the gun in water may cause short circuits and heating the gun can make the batteries explode. This will result also in the destruction on other parts of the system.
T.NOISE	The Biometric Device or its connections are flooded with noise data causing improper functioning of the capture device or comparator, causing an individual to be erroneously allowed or denied entry to the portal	$PA \left\{ \begin{matrix} 2 \\ 3 \\ 4 \\ 6 \end{matrix} \right\} \{ R \}$	The attacker may use electromagnetic radiations to cause damage. In the case of the TAPgun an false acceptance attack is improbable in this situation.
T.TAMPER	An attacker may modify or otherwise alter the hardware components or the connections between them, or between the Biometric Device and the portal, thereby causing an individual to be erroneously allowed or denied entry to the portal.	$\left\{ \begin{matrix} HA \\ PO \end{matrix} \right\} i \left\{ \begin{matrix} A \\ R \end{matrix} \right\}$	This is very general. Every attack in handle and possess situation is in this category.
T.WEAKID	An impostor may direct an attack against a weak ID.	$HA \left\{ \begin{matrix} 10 \\ 16 \end{matrix} \right\} A$	This is not actually the description of an attack. It can be considered an initial step of an attack that would consist in choosing a particular gun to attack.
T.EVILTWIN	An impostor may attack a similar or a twinned biometric template	$HA \left\{ \begin{matrix} 10 \\ 16 \end{matrix} \right\} A$	First the attacker must find a similar ID that means that he must access to the template database and test similarities.
T.POORIMG	An impostor may direct attack against a noisy or null image	$HA \left\{ \begin{matrix} 10 \\ 16 \end{matrix} \right\} A$	It is the initial step, choosing the target, not the attack itself, also the attacker must know about a noisy or null image.

T.ILLENROL	An impostor may become illegally enrolled on the biometric system	$HA \left\{ \begin{matrix} 9 \\ 16 \end{matrix} \right\} A$	Very dangerous. It involves the complicity of another user the one that is in charge with the enrollment.
T.FAKETMPL	If a user supplies his own biometric template (e.g. stored in a smart card, such a card may be forged, containing the biometric template of an impostor)	$HA9A$	This attack implies the users cooperation and access to a attacker to enroll his biometric template in the database. We assume that the enrollment can be done in a secure environment.
T.BADUSER	A user attempts to exceed their authority.	$\left\{ \begin{matrix} PO \\ HA \\ AA \\ PA \end{matrix} \right\} 16 \left\{ \begin{matrix} A \\ R \end{matrix} \right\}$	A bad user may try to harm the system in any situation.
T.BADADM	A legitimate administrator may unintentionally misuse their authority.	$HA\ 16 \left\{ \begin{matrix} A \\ R \end{matrix} \right\}$	This threat is in contrast with assumption A.NOEVIL that states that an administrator will not misuse his authority.
T.BADOPER	A legitimate operator may intentionally or unintentionally compromise the security of the Biometric Device during routine maintenance.	$HA\ 16 \left\{ \begin{matrix} A \\ R \end{matrix} \right\}$	This is always a threat. The damage that an operator can do should be evaluated and procedures developed to thwart those threats.

6.2 Department of Defense Protection Profile vs. 3W-tree Classification

The threat model developed is similar to the one presented in the Biometric Device Protection Profile. The following threats are defined identically: T.CASUAL, T.MIMIC, T.ARTIFACT, T.WEAKID, T.BADADM, T.BYPASS, T.EVILTWIN, T.RESIDUAL, T.POORIMG, T.FAKETMPL, T.BADADM, T.BADUSER, T.POWER, T.NOISE, T.TAMPER, see table 2.
The T.ILLENROL and T.BADOPER threats are not present, but there are some new threats, see table 3 and the T.UNDETECT threat is differently defined.
Table 3 contains the mapping between threats identified in DoDPP vs. 3W tree threats.

Table 3: *DoDPP*

DoDPP	Attack Description	3W tree Classification	Motivation

T.FAILSECURE	An attacker may cause failure of the TOE security functions by exposing the TOE to conditions outside of its normal operating range, causing the TOE to enter a non-secure state	$HA\ 17 \left\{ \begin{matrix} A \\ R \end{matrix} \right\}$	Most false rejection attacks will try to make the device work outside its normal parameters.
T.DEGRADE	Installing and using the biometric system may degrade the security of the host IT environment.	$HA\ 17 \left\{ \begin{matrix} A \\ R \end{matrix} \right\}$	Using the device in an improper manner is the same as trying to cause a failure in a handle situation.
T.FARFRR	An improperly adjusted FAR or FRR may result in an unauthorized individual entering the portal or an authorized individual being denied.	$PO\ 5 \left\{ \begin{matrix} A \\ R \end{matrix} \right\}$	The matcher is attacked to produce an artificially high or low score.
T.REPLAY	An unauthorized user may capture a valid user's biometric authentication data as it is being transmitted between portions of the TOE or from where it is stored, and replay it at a later time to gain illicit access or used to attack an higher robustness system.	$PO \left\{ \begin{matrix} 2 \\ 4 \\ 6 \end{matrix} \right\} \{ A \}$	Biometric templates can be captured when they are transmitted between components of the system, that corresponds to channel attacks .
T.CRYPTATTK	An attacker may defeat security functions through a cryptographic functions employed in the biometric system	$\left\{ \begin{matrix} PO \\ HA \end{matrix} \right\} 15 \left\{ \begin{matrix} A \\ R \end{matrix} \right\}$	The A.USERTMPL assumption states that the authenticity and integrity of the templates should be ensured. This can be done only by cryptographic means and the points where we need to protect the templates are during transmission between components and at the place where they are stored

6.3 U.S. Government Protection Profile vs. 3W-tree Classification

Table 4 contains 20 threats. Even though the threat model has certain similarities with previous two, new threats in the design and testing phase of the biometric system are identified.

Table 4: *USGovPP*

USGovPP	Attack Description	3W tree Classification	Motivation
T.BYPASS	An attacker may bypass any component of the biometric product and gain unauthorized authentication.	$PO \left\{ \begin{matrix} 2 \\ 4 \\ 6 \end{matrix} \right\} A$	This threat is related to channels. Any channel attack is in this class.

T.CRYPTATTACK	An attacker may defeat security functions through a cryptographic attack against the algorithm, through cryptanalysis on encrypted data, or through a brute force attack and thereby gaining unauthorized authentication.	$\left\{ \begin{matrix} PO \\ HA \end{matrix} \right\} 15 \left\{ \begin{matrix} A \\ R \end{matrix} \right\}$	The first three attacks are channels attacks, when data is transmitted between components and the last attack is the cryptanalysis on the encrypted template.
T.CRYPTOCOMPROMISE	A malicious user or process may cause key, data or executable code associated with the cryptographic functionality to be inappropriately accessed(viewed, modified, or deleted), thus compromise the cryptographic mechanisms and the data protected by those mechanisms.	$\left\{ \begin{matrix} PO \\ HA \end{matrix} \right\} 15 \left\{ \begin{matrix} A \\ R \end{matrix} \right\}$	Trojan Horse attacks on the template extractor or matcher or cryptanalysis on the stored data
T.MIMIC	An attacker may masquerade as an enrolled user or presenting their biometric characteristics that is similar, or by reproducing the biometric characteristics that is similar or by reproducing the biometric template	$HA1A$	The intruder tries to mimic the authorized users grip pattern by successive attempts
T.REPLAY RESIDUAL-IMAGE	An attacker may attempt to "reuse" an authorized user's biometric residual characteristics (e.g., finger print left on capture device) to gain unauthorized access.	$PO \left\{ \begin{matrix} 2 \\ 4 \\ 6 \end{matrix} \right\} A$	Biometric templates can be captured when they are transmitted between components of the system, that corresponds to channel attacks.
T.RESIDUAL DATA	Residual biometric authentication data from a previous valid user if not cleared from memory may allow an attacker to gain unauthorized authentication.	$PO\ 5\ A$	A Trojan Horse is installed in the matcher that records valid user templates and replays them at a particular moment in time.
T.REFERENCE TEMPLATE	An attacker modifies or creates a biometric reference template in storage or transmission to/from storage to gain unauthorized authentication.	$PO \left\{ \begin{matrix} 7 \\ 10 \end{matrix} \right\} A$	The reference template stored in the device is attacked and an illegal template is introduced or a during transmission an illegal template is inserted.
T.TAMPER	An attacker may modify or otherwise alter the software and hardware components, the connections between them thereby gaining unauthorized authentication	$\left\{ \begin{matrix} HA \\ PO \end{matrix} \right\} \left\{ \begin{matrix} 1 \\ \vdots \\ 17 \end{matrix} \right\} \left\{ \begin{matrix} A \\ R \end{matrix} \right.$	This is very general. Every attack in handle and possess situation is in this category.

T.MALICIOUS TSFCOMPROMISE	A malicious user or process may cause TSF data or executable code to be inappropriately accessed(viewed, modified or deleted).	$PO\ 5 \left\{ \begin{matrix} A \\ R \end{matrix} \right\}$	TSF means Target Security Function and a possible attack is to modify the threshold value.
T.UNKNOWN STATE	When the TOE initially started or restarted after a failure, design flaws or improper configurations may cause the security state of the TOE to be unknown.	$HA\ 1 \left\{ \begin{matrix} A \\ R \end{matrix} \right\}$	The device is restarted after a failure by its user and in that case the unwanted behavior is that the device is not recognizing its user, then we have a false rejection attack. If the device is restarted by an attacker then the unwanted behavior is a false acceptance. Usually an attack have more than one step that is the recognition, other parts of the system are attacked.
T.ADMINERROR	An administrator may incorrectly install or configure the TOE resulting in ineffective security mechanisms.	$HA\ 16 \left\{ \begin{matrix} A \\ R \end{matrix} \right\}$	The administrator is responsible in this case.
T.ADMINROGUE	An administrator's intentions may become malicious resulting in user or TSF data being compromised.	$HA\ 16 \left\{ \begin{matrix} A \\ R \end{matrix} \right\}$	Internal attacker, other protection profiles have the A.NOEVIL assumption that eliminates this threat.
T.AUDIT COMPROMISE	A malicious user or process may view audit records, cause audit records to be lost or modified, or prevent future audit records from being recorded, thus masking a user's action.	$HA \left\{ \begin{matrix} 13 \\ 14 \end{matrix} \right\} \left\{ \begin{matrix} A \\ R \end{matrix} \right\}$	Very important threat. If possible the audit data might be stored in a tamper resistant device in an unsafe environment and then the data downloaded into a central repository.
T.FLAWED DESIGN	Unintentional or intentional errors in requirements specification or design of the TOE may occur, leading to flaws that may be exploited by a malicious user or program.	$\left\{ \begin{matrix} HA \\ PO \end{matrix} \right\} 16 \left\{ \begin{matrix} A \\ R \end{matrix} \right\}$	These errors are the most difficult to detect and if not detected in time the cost of these errors is high.
T.CORRUPTED IMPLEMENTATION	Unintentional or intentional errors in implementation of the TOE may occur, leading to flaws that may be exploited by a malicious user or program.	$\left\{ \begin{matrix} HA \\ PO \end{matrix} \right\} 16 \left\{ \begin{matrix} A \\ R \end{matrix} \right\}$	Trojan Horse that are intentionally introduced during implementation or buffer overflow attacks that are discovered by attacks.
T.POORTEST	Lack of an insufficient tests to demonstrate that all TOE security functions operate correctly (included in a fielded TOE) may result in incorrect TOE behavior being undiscovered thereby causing potential security vulnerabilities	$\left\{ \begin{matrix} HA \\ PO \end{matrix} \right\} 16 \left\{ \begin{matrix} A \\ R \end{matrix} \right\}$	Again insiders, people involved in the project development are not careful.

T.POOR_ ENROL-MENT	An attacker may direct an attack against a low quality reference template and gain unauthorized authentication.	$HA \left\{ \begin{matrix} 9 \\ 16 \end{matrix} \right\} \left\{ \begin{matrix} A \\ R \end{matrix} \right\}$	The attacker must find a low quality template, that means he must have access to inside information.
T.UNATTEND_ EDSESSION	An attacker may gain unauthorized access to an administrator's unattended session.	$\left\{ \begin{matrix} HA \\ PO \end{matrix} \right\} \left\{ \begin{matrix} 9 \\ 16 \end{matrix} \right\} \left\{ \begin{matrix} A \\ R \end{matrix} \right\}$	To have this result the system must have other weak points. This is the result of an attack, not the actual threat.
T.UNAUTHORIZED_ ACCESS	A user may gain access to administrative functions for which they are not authorized according to the TOE security policy.	$\left\{ \begin{matrix} HA \\ PO \end{matrix} \right\} \left\{ \begin{matrix} 9 \\ 16 \end{matrix} \right\} \left\{ \begin{matrix} A \\ R \end{matrix} \right\}$	Again, the result of an attack, other weak points must exist in the system.
T.UNIDENTIFIED ACTIONS	The administrator may fail to notice potential security violations, thus limiting the administrator's ability to identify and take actions against a possible security breach.	$\left\{ \begin{matrix} HA \\ PO \end{matrix} \right\} \left\{ \begin{matrix} 9 \\ 16 \end{matrix} \right\} \left\{ \begin{matrix} A \\ R \end{matrix} \right\}$	This the same as T.UNDETECTED threat in the other two Protection Profiles.

6.4 ISOStand vs. 3W-tree Classification

Table 5 lists all threats for *ITSStand*. In this standard a slightly different notation is used. The matcher is called the Capture subsystem and the feature extractor is called the Extraction subsystem. Another remark is that some threats are applicable to all points in the system.

Table 5: *ISO- Standard*

ISO Stand	Attack Description	3W Classification	Motivation
1.1	Impostor covertly captures a biometric sample from authorized user,e.g. record voice photograph face.	$PO2A$	The biometric sample can be captured outside the device environment or when an authorized sample is submitted for verification the signal transmitted on the channel is recorded.
1.2	Impostor steals a biometric sample from authorized user e.g. cut off authorized user finger, or install fake biometric readers to capture biometric sample.	$PO2A$	It is the same threat as 1.1 but here the impostor steals the biometric instead of covertly capturing the biometric.
1.3	Authorized user knowingly provides own biometric sample to impostor (collusion)	$HA \left\{ \begin{matrix} 1 \\ 16 \end{matrix} \right\} A$	This is not actually a false acceptance attack because the sample from the rightful user is used, but the purpose is to provide access to an impostor.

1.4	Authorized user modifies own biometric sample to facilitate an impostor attack(collusion)	$HA \left\{ \begin{matrix} 1 \\ 16 \end{matrix} \right\} A$	The user is weakening the system in order to produce a false acceptance.
2.1	Impostor presents own biometric sample in a zero-effort forgery attempt to impersonate (a) a randomly selected authorized user (for verification), (b)any authorized user (for identification), (c) a selected weak biometric template, or (d) an authorized user with a biometric sample similar to that of the impostor (e.g., a twin).	$HA \left\{ \begin{matrix} 1 \\ 16 \end{matrix} \right\} A$	The impostor is trying to produce a false acceptance by presenting something to the sensor.
2.2	Impostor modifies own behavior(e.g. voice, signature) or physiology (e.g. face, hand) in an attempt to impersonate (a) selected authorized user, or (b) a selected weak biometric template.	$HA1A$	The sensor is the target, the purpose is to produce a false acceptance.This is threat T.MIMIC.
2.3	Impostor presents an artificial biometric sample (e.g. fake fingerprint, voice recording) in an attempt to impersonate (a) a selected authorized user, or (b) a selected weak biometric template.	$HA1A$	The same threat, a different scenario. This the same as threat T.ARTIFACT.
2.4	Impostor presents a noisy, poor-quality, or null biometric sample in an effort to match a weak or regular-quality biometric template.	$HA1A$	The purpose is to produce a false acceptance by presenting a bad image to the sensor. The same as threat T.POORIMG.
2.5	Impostor utilizes a residual biometric image left on the biometric system (typically a latent fingerprint) in an attempt to impersonate the last authorized user	$HA1A$	The same as threat T.REDIDUAL.
2.6	Impostor presents own biometric sample after impostor's biometric template has been: (a)provided on a forged data carrier e.g. smart card; (b)placed in the biometric system's template storage database by illegal enrollment; (c)illegally added directly to storage database; or (d)illegally inserted directly into the comparison subsystem	$HA1A$	The same goal, but the attack is carried out in a different manner. The impostors biometric sample is already registered in the system when he tries to be falsely accepted.
2.7	Impostor mounts a hill-climbing or other repeated-attempt attack that is not detected via audit trails	$HA1A$	A false acceptance attack, but the is a brute-force type attack.

3.1	Impostor intercepts an authorized biometric sample during transmission between the Capture and Extraction subsystems	$PO2A$	The impostor is eavesdropping on the channel between the Capture and Extraction subsystem, the goal is to produce a false acceptance.
3.2	Impostor inserts an authorized biometric sample directly into the Extraction subsystem, thus bypassing the Capture subsystem.	$PO2A$	This is the second step in the attack, first the sample must be recorded and then replayed. This is threat T.REPLAY.
4.1	Impostor intercepts extracted biometric feature during transmission between the Extraction and Comparison subsystems.	$PO4A$	The impostor is recording the feature vector, not the raw biometric data as in case of threat 3.1.
4.2	Impostor inserts extracted biometric features directly into the Comparison subsystem.	$PO4A$	After he recorded a valid signal he will replay the recorded signal in order to obtain a false acceptance.
5.1	Authorized user presents a noisy, poor-quality, highly varying, or null biometric sample; or modifies own behavior; or presents an artificial sample, in an effort to enroll a weak biometric template.	$HA \left\{ \begin{matrix} 8 \\ 16 \end{matrix} \right\} A$	This is also a false acceptance attack because the purpose of the user is to facilitate an impostors actions. The same as threat T.BADUSER.
5.2	Unauthorized user is enrolled: (a) administrator error , e.g. credentials not properly checked; (b) authorized user template intercepted and replaced with impostor template during enrollment	$HA8A$ $PO16A$	The administrator is responsible for this threat. The systems security depends on the administrators carefulness.
6.1	Impostor's own biometric template is either (a)provided on a forged personal data carrier (e.g. smart card); or (b) illegally placed in the biometric system's template storage database [Either a new authorized user account created for the impostor, or the template of existing user replaced with impostor template.]	$PO10A$	The gun is opened and the memory where the template is stored is replaced with a new one which contains an impostor template.
6.2	Impostor steals the biometric template of an authorized user from template storage or from another biometric system	$PO \left\{ \begin{matrix} 10 \\ 16 \end{matrix} \right\} A$	The attacker opens the gun and extracts the template from memory
6.3	Attackers modifies or deletes biometric templates in storage.	$PO\ 10\ A$	In the impostor can delete a template than the rightful user of the gun might be rejected because there is nothing to match the newly submitted template.

6.4	Impostor intercepts an authorized biometric template during transmission between the Extraction and Template Storage subsystems	$PO7A$	An authorized biometric sample is recorded.
7.1	Impostor intercepts an authorized biometric template during transmission between the Template Storage and Comparison subsystems.	$PO7A$	A channel attack, the purpose is to record an authorized biometric template. This is the first step in the attack.
7.2	Impostor inserts own template directly into the Comparison subsystem	$PO7A$	After he completed attack 7.1 he can use the information recorded to produce a false acceptance.
8.1	A hostile authorized user or impostor may acquire administrator privileges through (a) non-biometric means, e.g. coercion, password, backup system, alternative authentication method, or exception handling procedure, or (b) biometric means as presented in this outline.	$\left\{ \begin{matrix} PO \\ HA \end{matrix} \right\} 16 \left\{ \begin{matrix} A \\ R \end{matrix} \right\}$	An internal user may acquire privileges through non-biometric or biometric means.
8.2	Non-hostile administrator (unintentionally or under coercion) or hostile authorized user or impostor who has acquired administrator privileges: (a) incorrectly modifies matching threshold, (b) incorrectly modifies user privileges, (c)allows unauthorized access to template storage (d) allows unauthorized modification of audit trail, (e)enrolls an unauthorized user	$\left\{ \begin{matrix} PO \\ HA \end{matrix} \right\} 16 \left\{ \begin{matrix} A \\ R \end{matrix} \right\}$	Administrators are humans so they will make mistakes it depends on the designers of the systems to limit the amount and the severity that an administrator can cause. The other threat, coercion of the administrator can be solved by non-biometric means.
8.3	Administrator fails to properly review and respond to audit trail anomalies	$\left\{ \begin{matrix} PO \\ HA \end{matrix} \right\} 16 \left\{ \begin{matrix} A \\ R \end{matrix} \right\}$	The administrator might be unexperienced or not careful.
8.4	Attacker modifies matching threshold.	$PO\,5 \left\{ \begin{matrix} A \\ R \end{matrix} \right\}$	The attacker tries to set a very low threshold in order to allow false acceptance, or set a high threshold to reject an authorized user.
9.1	Impostor authenticates as authorized user through non-biometric means, e.g. collusion, coercion, password, backup system, alternative authentication method or exception handling procedure	$\left\{ \begin{matrix} PO \\ HA \\ AA \\ PA \end{matrix} \right\} \left\{ \begin{matrix} 1 \\ \vdots \\ 17 \end{matrix} \right\} \left\{ \begin{matrix} A \\ R \end{matrix} \right\}$	If there exists such a system then this threat should be carefully considered. The impostor may use any weak points in the algorithm to authenticate himself.

10.1	Audit data collection inadequate to detect attacks (e.g. hill-climbing or other repeated-attempt attacks).	$\left\{\begin{matrix}PO\\HA\end{matrix}\right\}\left\{\begin{matrix}13\\14\end{matrix}\right\}\left\{\begin{matrix}A\\R\end{matrix}\right\}$	If possible the audit data might be stored in a tamper resistant device in an unsafe environment and then the data downloaded into a central repository.It is the same threat as T.AUDITCOMPROMISE.
10.2	Attacker modifies user identifier.	$\left\{\begin{matrix}PO\\HA\end{matrix}\right\}\left\{\begin{matrix}10\\15\end{matrix}\right\}\left\{\begin{matrix}A\\R\end{matrix}\right\}$	Internal attacker, he must get access to the central repository and make there the modifications
11.1	Attacker inserts appropriate "grant privileges" signal directly into portal, thus bypassing the entire biometric system	$PO6A$	The match decision signal is inserted in the channel thus bypassing the entire system.
11.2	Attacker cuts power to the system. Either (a) system fails in"open" or "insecure" mode allowing unauthorized access; or (b) system fails in "closed" or "secure" mode disallowing authorized access.	$\left\{\begin{matrix}PO\\HA\end{matrix}\right\}\left\{\begin{matrix}11\\12\end{matrix}\right\}R$	The same as T.POWER threat.
11.3	Attacker defeats backup system, alternative authentication method, or exception handling process: (a) during normal operation, or (b) after"secure" system failure	$PO6A$	The attacker bypasses the entire system
12.1	Attacker gains unauthorized access to privileges with the willing or unwilling aid (e.g. piggybacking, collusion, coercion) of an authorized user after the user has been authenticated.	$HA1A$	This is about unauthorized access so it is a false acceptance attack and nothing is said about disassembling the device.
12.2	User gains access to unauthorized privileges after privileges have been improperly modified.	$HA16A$	Same as T.BADUSER threat.
13.1	Attacker tampers, modifies, bypasses, or deactivates one or more hardware components.	$\left\{\begin{matrix}HA\\PO\end{matrix}\right\}\left\{\begin{matrix}1\\\vdots\\17\end{matrix}\right\}\{R\}$	The impostor can deactivate or tamper with hardware if he is in possession or handle situation.
13.2	Attacker exploits hardware "backdoor", design flaw, environmental conditions or failure modes.	$\left\{\begin{matrix}HA\\PO\end{matrix}\right\}\left\{\begin{matrix}1\\\vdots\\17\end{matrix}\right\}\left\{\begin{matrix}A\\R\end{matrix}\right\}$	The same as the previous one.

13.3	Attacker floods one or more hardware components with noise, (e.g. electromagnetic or acoustic energy).	$PA \left\{ \begin{matrix} 1 \\ \vdots \\ 17 \end{matrix} \right\} \left\{ \begin{matrix} A \\ R \end{matrix} \right\}$	This time the attacker do not need to make physical contact with the device, so he is not in possession or handle situation, he is an active attacker.
13.4	Impostor intercepts/inserts authorized biometric template from/to one or more hardware components.	$PO \left\{ \begin{matrix} 2 \\ 4 \\ 6 \end{matrix} \right\} A$	This is the classical T.REPLAY attack.
14.1	Attacker tampers, modifies, bypasses, or deactivate one or more software or firmware executables.	$PO \left\{ \begin{matrix} 3 \\ 5 \end{matrix} \right\} \left\{ \begin{matrix} A \\ R \end{matrix} \right\}$	Trojan Horse attack that produce a false rejection or a false acceptance attack.
14.2	Attacker exploits software or firmware "back-door", algorithm quirk, design flaw, or failure mode.	$PO \left\{ \begin{matrix} 3 \\ 5 \end{matrix} \right\} \left\{ \begin{matrix} A \\ R \end{matrix} \right\}$	The template extractor and the matcher are the components that are vulnerable to this threat.
14.3	A virus (or other malicious software is introduced into the system)	$PO \left\{ \begin{matrix} 3 \\ 5 \end{matrix} \right\} \left\{ \begin{matrix} A \\ R \end{matrix} \right\}$	The same as 14.2, but the database also might be subject to such an attack.
14.4	Impostor intercepts/inserts authorized biometric template from/to one or more software or firmware components	$PO \left\{ \begin{matrix} 2 \\ 4 \\ 6 \end{matrix} \right\} A$	Channel attacks, the same as T.REPLAY.
15.1	Attacker tampers, modifies, bypasses or deactivates one or more connections between components.	$PO \left\{ \begin{matrix} 2 \\ 4 \\ 6 \end{matrix} \right\} \left\{ \begin{matrix} A \\ R \end{matrix} \right\}$	The attacker can also destroy channels, not just insert signal in order to bypass different components.
15.2	Impostor intercepts or inserts authorized biometric sample or template as it is being transmitted between subsystems or components.	$PO \left\{ \begin{matrix} 2 \\ 4 \\ 6 \end{matrix} \right\} A$	The same as 14.4.

6.5 Summary

A total of 48 distinct threats are identified in the standards of which only 3 are *false rejection* threats. These are: (1) cutting the power to the system, (2) flooding

hardware components with noise and (3) exposing the device to environmental parameters that are outside its operating range. In addition, there are 12 “catch all” threats that include both *false rejection* and *false acceptance* threats. The threat models in these protection profiles are not *false acceptance* oriented and are therefor less not suitable for applications like *Smart Gun* or *Terrorist Watch List*.

7 Smart Gun Studies

7.1 Smart Gun intended use

Significant numbers of police weapons are lost or stolen. Each year several police officers die or are injured because their own weapons are used against them. The Smart Gun application is designed for a police force, which would like to render a weapon inoperative when it is captured by the assailant of a police officer. The requirements include that the gun should recognize all members of a police patrol, and that wearing gloves should not affect the operation.

7.2 Security Threat Scenario for smart gun

We defined the 3W tree to classify all attacks discussed earlier in the paper, with a specific focus on the smart gun. A *false rejection* attack in the case of the smart gun would not permit its user to fire the gun. A *false acceptance* attack would permit other persons than the owner of the gun to use it. As we mentioned before a false rejection attack is a more dramatic than a false acceptance attacks.
Finally, before analyzing the threats our system is subject to we make some realistic assumptions about the intended use of the T:

1. ***A.SG_ROLES*** *The biometric, subsystem of the smart gun is intended to verify the identity of its rightful user*
2. ***A.SG_NOEVIL*** *Administrators of the system (i.e police officers) are assumed to be non-hostile and trusted to perform all their duties in a competent manner*
3. ***A.SG_SEAL*** *Tampering with the seal(s) on the gun, which secure the feature extractor, matcher and all the communication channels, should be easy to detect and re-sealing should be hard to do.*
4. ***A.SG_SECENROLL*** *The enrollment procedure takes place in a secure environment (the police station)*
5. ***A.SG_TMPLLOAD*** *Templates can be loaded in a secure environment, before the officer takes his gun.*

Each of these assumption is motivated by the strict procedures to which police offices work. Under these assumptions we make the following observations:

A. *An external attacker can attack the system in points T1 to T6 (and not in T7-T10)* since only authorized personnel have access to the database and the enrollment center. We will address these threats in the "internal attackers case".

B. *False rejection attacks in a possession situation are no real threat*. This holds because of A.SM_SEAL. The attacker has to open the gun, tamper with parts of the system situated inside the gun, reseal the gun and return the gun to the owner. The owner should immediately be able to see if the seals have been broken.

C. *In a handle situation we have no successful false acceptance attack, except threat T1*. The attacker cannot open the gun so he has no access to the subsystems situated inside the gun.
D. *In the approach mode we have no obvious attacks*. The attacker is simply in proximity of the gun so he cannot touch it.
E. *In the case of an passive attacker false acceptance attacks are improbable*. This type of attack is possible but the reason for doing this would be of course, to fire the gun and is cumbersome to insert an electronic signal with some device in one hand and then simultaneously shoot the gun with the other hand.

Assumptions create the general environment for describing attack scenarios. Other assumptions may be added as a result of the analysis of attack scenarios.
In the next paragraph 9 attack scenarios are presented. If we don't make any assumptions the number of scenarios would have been bigger and some of attacks are redundant in the sense that they can be applied to more than one component of the system.
The threats identified are presented in Figure 1, 2 and possible scenarios leading to this threats are detailed in the next paragraph.

7.3 Scenarios

Scenario **PO1A**(**HA1A** is similar)

I. Description
   - *Tactics:* Produce an exoskeleton hand [1] that can reproduce a hand pressure pattern
   - *Name:* This attack is known in the literature as *physical spoofing*.

II. Evaluation
   - *Damage:* Minor.
   - *Knowledge:* Expert. Measure, record and store grip patterns. The raw pressure pattern has to be fed into the exoskeleton hand, so the intruder must have access to a exoskeleton hand and has to know how to use it.
   - *Occurrence:* Low. Recording grip pattern and feeding this data to an exoskeleton hand require specialized equipment. Even if its possible to reproduce the grip pattern manipulating the gun is cumbersome to use with such a hand.

III. Defense
   - *Countermeasures:* We have to ensure that the image coming directly from the sensor is authentic, using for example liveness testing and making sure that the signal cannot be recorded.

Scenario **PO1R**(the same goes for scenario **HA1R**)

I. Description
   - *Tactics:* Jam or break the sensor.

[1] http://human-factors.arc.nasa.gov/ihh/spatial/papers

- *Name:*Unknown

II. Evaluation
- *Damage:* Major.
- *Knowledge:* High school. Which part of the gun is the sensor and he needs to know how to destroy a sensor eventually without the damage being visible.
- *Occurrence:* High. It is easy to damage something that is not secure by a seal and is not tamper resistant.

III. Defense
- *Countermeasures:* The gun architecture should ensure that tampering with the sensor is obvious.

Scenario **PO2A**

I Description
- *Tactics:* The attacker records a correct biometric signal and then injects the signal just before using the gun.
- *Name:* Replay attack.

II. Evaluation
- *Damage:* Moderate.
- *Knowledge:* Expert. Measure, record and store the biometric of a legitimate user. If the attacker records the raw biometric then he must know the algorithm that produces the feature vector. The format of the feature vector and because the number of elements of the feature vector depends on the number of user registered to the system he also has to know this number. He also needs to figure out a way of injecting the signal just before the gun is fired.
- *Occurrence:* Low. The attack requires inside knowledge of the system, the number of enrollees, and technical skills: recording the biometric or injecting the electronic signal

III. Defense
- *Countermeasures:* Encrypted communication, challenge-response protocol, perfect-matching checking, time-stamping.

Scenario **PO3A**

I. Description
- *Tactics:* Trojan horse attack on the feature extractor, the attacker insert a piece of code at a certain point in time to produce a preselected feature, at that time the attacker is able to fire the gun. The most obvious choice would be to extract the stored template and replay-it at a certain moment.
- *Name:* Replay attack.

II. Evaluation
- *Damage:* Moderate.
- *Knowledge:* Expert. The attacker must have access to the algorithm that produces the feature extractor from the raw biometric data, at least some programming skills, and he must also know how to produce a valid feature vector for an illegitimate user.

- *Occurrence:* Medium. Trojan Horses are designed in the implementation phase that implies that the developers are not completely trustworthy.

III. Defense

III *Countermeasures:* The implementation of the algorithm must be carefully reviewed.

Scenario **PO4A**

I Description

- *Tactics:* An old biometric feature is injected on the communication channel between feature extractor and matcher.
- *Name:* hill-climbing attack. In [22] such an attack on fingerprint authentication systems is described.

II. Evaluation

- *Damage:* Moderate.
- *Knowledge:* Expert. This is a channel attack like the PO2A scenario and the knowledge required is approximately the same, except the signal is inserted between the feature extractor and the matcher.
- *Occurrence:* Low. The same motivation as for PO2A scenario.

III. Defense

III *Countermeasures:* If the feature extractor and matcher are on the same device this attack is not a real threat. If this is not possible then perfect match checking should be implemented. We have perfect matching when a biometric sample is identical to a previous submitted one.

Scenario **PO5A**

I. Description

- *Tactics:* The attacker manages to control the output of the algorithm on the matcher, by attaching a Trojan Horse or by a buffer overflow attack.
- *Name:* buffer overflow, Trojan Horse

II. Evaluation

- *Damage:* Moderate.
- *Knowledge:* Expert. The attacker must know how the system is deployed he has to guess the threshold and how to produce a buffer overflow or a Trojan Horse.
- *Occurrence:* Medium. The attacker must have detailed information on the system and technical skill, a lot of work to fire the gun, depends on his motivation.

III. Defense

- *Countermeasures:* Certification of the implementation.

Scenario **PO6A**

I. Evaluation

- *Tactics:* A fake matcher is inserted in the gun, that is a matcher that always return a yes.
- *Name:* could not find such an attack in the literature

II. Description
- *Damage:* Moderate.
- *Knowledge:* Expert. Must know how the system is deployed, how to produce a matcher that always produce a yes and of course how to replace the old matcher with the hacked one.
- *Occurrence:* Medium. In the literature this attack is not very popular and again a lot of work to make the gun work, but once the attack is successful the gun will work again and again like a regular gun.

III. Defense
- *Countermeasures:* Security by obscurity is not a good idea but it can deter occasional attackers.

Scenarios **HA2R, HA3R, HA4R, HA5R, HA6R**

I. Description
- *Tactics:* For jamming and/or physically breaking an electronic device (in the situation when the attacker can handle the gun) we have to fear mechanical damages that are not noticeable from the outside. A way to mechanically damage a device is to find the resonance frequency of that object and then applying vibrations/shocks of the resonance frequency to the object. This way, the maximum mechanical energy is absorbed by the object, thus producing maximum damage.
  To destroy wires/connections inside the electronic device we have the following possibilities: exposing the object to alternating high-low extreme values of pressure or temperature and at some point the mechanical connections will break. Violent shocks of any kinds are common for the gun, the amount of damage depending on the architecture.
  If the gun handle is made out of plastic then ultraviolet light can be used to erase any EEPROM memory inside.
  Another matter of concern are the batteries that will be used in the gun. Sinking the gun in water can cause short circuits and heating the gun can make the batteries explode.
- *Name:*Unknown. But an example is Napoleon's bridge.

II. Evaluation
- *Damage:* Moderate.
- *Knowledge:* High school. General knowledge on how to hack an electronic device, maybe an engineering degree, but some of the attacks can be carried out by anyone.
- *Occurrence:* High. Because it does not require a lot of effort and the impact is maximum

III. Defense
- *Countermeasures:* Tamper resistant architecture for the gun. Extensive testing.

Scenarios **AP2R, AP3R, AP4R, AP5R, AP6R**

I. Evaluation

- *Tactics:* Electromagnetic radiation induces currents in the metallic part of an electronic device. This can cause signal interference or damaging junctions of transistors by the avalanche effect. The amount of energy used is dependent on frequency (inversely proportional to the frequency). At relative medium frequencies a high power radio station antenna can be used to cause damage. An microwave oven can be also used (the frequency is in this case several order of magnitudes higher).
  Electrical damage can be created by applying external current through the gun (the gun can be simply connected to a power outlet). Nuclear radiation is in fact radiation of electrons which can lead to the same avalanche effect and crash the electronic device situated inside the gun.
- *Name:* Unknown

II. Evaluation
- *Damage:* Severe
- *Knowledge:* High school. Approximately the same as in the previous scenario, but this time a device must be used to produce the damage.
- *Occurrence:* Medium. The technical skills are slightly higher than in the previous case and the attacker needs additional equipment.

III. Defense
- *Countermeasures:* Study the manufacturer's specification on gun materials.

7.4 Summary

9 attack scenarios were found to be relevant for the Smart Gun application. These scenarios are ranked in table 7.4 according to their likelihood of occurrence and the damage produced to the device. The first ordering criterion is the estimated likelihood of occurrence. The higher the likelihood of occurrence, the more important it is to as to address that threat. The second criteria is the damage to the device. If the damage is minor it will be hard for the police officer to notice that his weapon was tampered with. The result is that false rejection threats are the major concern for this application and most probably attacks will occur in handle situation. The security architecture will take into account the obtained results.

8 Terrorist Watch List

Terrorist Watch Lists are used to detect terrorist while traveling. Applications like this are usually installed at airports, sea ports, main railway stations etc. People who want to travel are checked against a central database with potentially dangerous persons. There are at least two ways to

Scenario	Damage	Occurrence
$HA \left\{ \begin{matrix} 1 \\ 2 \\ 3 \\ 4 \\ 5 \\ 6 \end{matrix} \right\} R$	Major	High
$PO \left\{ \begin{matrix} 3 \\ 5 \\ 6 \end{matrix} \right\} R$	Moderate	Medium
$HA \left\{ \begin{matrix} 2 \\ 3 \\ 4 \\ 5 \\ 6 \end{matrix} \right\} R$	Major	Medium
$PO \left\{ \begin{matrix} 2 \\ 4 \end{matrix} \right\} R$	Moderate	Low
PO1A	Minor	Low
HA1A	Minor	Low

do the matching: using the name (which can easily be forged) or a biometric feature like face or fingerprint. We consider the case where the terrorist watch list is implemented using face recognition. The intended use is as follows: a camera is placed at a passport control point and before issuing the stamp the person is asked to look at the camera using a neutral expression. The officer in charge will check if the individual is acting as asked. We show that attacking the camera following an *active approach* is feasible, see table 6. We could not find any mention of this attack in the literature.

8.1 Summary

This application is similar to the *Smart Gun* because the false rejection threat is more critical than the false acceptance threat. We present only one scenario. Further work is needed to discover more relevant attack scenarios.

I. Scenario	Can an *active attacker* produce a false rejection by tampering with the input device (video camera)?
I. Tactics	An active attacker can interfere with the camera using mirrors to reflect sun light on the camera, affecting the quality of the image. The similarity between the newly acquired sample and stored biometric sample might then be below the threshold.
I. Name	Unknown.
II. Damage	Minor. The personnel in charge of supervising the cameras will eventually notice that something is wrong.
II. Knowledge	Common sense. Children play in school with watches projecting light on surfaces to annoy their teachers.
II. Occurrence	High. It is easy to perform such an attack from a safe distance. No special tools are required.
III. Countermeasures	To ensure that light beams cannot be projected on the camera. This can be done by carefully positioning the camera, detecting changes in lighting conditions,etc..

Table 6. *AA1R Scenario in Terrorist Watch List Application*

9 Conclusions

Biometric authentication systems are not as secure as most people think. Even though the investment in biometric systems have seen an explosive growth in the last years, few papers related to the security of biometric systems were published.

The threat model for most biometric systems is false acceptance oriented but this is not appropriate for the *Smart Gun* or *Terrorist Watch List* applications. For these application false rejection attacks are critical and can lead to life threatening situations.

Because the threat models in the literature do not consider false rejection extensively, we combine existing security taxonomies to build a realistic threat model that is false rejection centric. We divide taxonomies in three classes based on the ground of distinction used: *who* taxonomies in which some relationship between the attacker and the system is used to construct classes of attackers, *what* taxonomies where the target of the attack is used to construct different classes of threat and *how* taxonomies in which the methods used to conduct an attack are considered.

The result of this study is that none of the taxonomies studied guarantee that all relevant threats will be identified.

Therefore, we propose the 3W tree as a structure to combine these taxonomies.

The advantage of the 3W tree is that (1) it fosters a systematic approach to threat analysis, and (2) it allows asking concrete questions, and (3) it does not burden the analysis with irrelevant detail.

The completeness and the relevancy of the threats identified using the 3W tree depends on the system architecture to which they are applied. The generic architecture of a biometric system presented in the literature is not constructed with security in mind, because components like cryptography, audit logging, users and also other components like the power supply are missing. To address this problem we extend the generic architecture presented to contain these critical components.

Threats in existing standards are compared against 3W tree attack scenarios to see whether our threat model is complete. The results are promising: we are able to map all threats in the existing standards while preserving control on the capabilities of different attacker in attacking components of the biometric system.

We apply our method to the Smart Gun application considering only the external attacker, since only the architecture for the biometric system (the gun) is presently known. The result is that we can identify three major threats to our device which will be addressed in the security architecture requirements.

As future work we plan to design the architecture for the whole system and to address internal attacker threats. We plan to analyze the correctness of system architecture using formal methods.

Another future work is multipoint attacks. That is attacks that are applied on simultaneous points in the system to increase the chances of success of an attack. This is an important issue since most attacks are of this type.

Acknowledgements

This research is supported by Technology Foundation STW, applied Science Division of NWO and the technology program of the Ministry of Economic Affairs, The Netherlands.

References

1. R.J. Anderson. *Security Engineering: A guide to building dependable distributed systems*. John Wiley & Sons Inc, New York, 2001.
2. J. M. Bone and D. M. Blackburn. Biometrics for narcoterrorist watch list applications. Technical report, Crane Division, Naval Surface Warfare Center and DoD Counterdrug Technology Development Program Office, July 2003.
3. T. Van der Putte and J. Keuning. Biometrical fingerprint recognition: Don't get your fingers burned. *Smart Card Research and Advanced Applications, IFIPTC8/W68.8 Fourth Working Conference on Smart Card Reserch and Advanced Applications*, pages 289–303, Sep 2001.
4. Germany DIN-Deutsches Institut Fur Normung E.V., Berlin. Information technology - security techniques - a framework for security evaluation and testing of biometric technology. Technical Report ISO/IEC JTC 1/SC 27 N 3806, DIN - Deutsches Institut fur Normung e.V. Berlin, Germany, 2003.
5. G. Gonon. RFC draft material requiremets for biometrics. Technical Report INSPIRED-RFC-INR-002-R0.1, INRIA-Rennes/IRISA, Rennes, France, November 2004.
6. UK Government Biometrics Working Group. Biometric device protection profile (BDPP). Technical Report Draft Issue 0.82, UK Goverment Biometrics Working Group, 2001.
7. A. Jain, L. Hong, and S. Pankanti. Biometric identification. *CACM*, 43(2):90–98, Feb 2000.
8. A. K. Jain, S. Pankanti, S. Prabhakar, A. Ross, and J.L. Wayman. Biometrics: A grand challenge. *Proceedings of International Conference on Pattern Recognition*, Volume 2:935–942, 2004.
9. A. Kong, A. Griffith, D. Rhude, G. Bacon, and G. Shahs. Department of defense federal biometric system protection profile for medium robustness environments. Technical Report Technical Report Draft Version 0.02, U.S Department of Defense, 2002.
10. D.L. Lough. *A taxonomy of computer attacks with applications to wireless networks*. John Wiley & Sons Inc, New York, 2001.
11. S.M. Matyas and J. Stapleton. A biometric standard for information management and security. *Computer&Security*, 19(5):428–441, May 2000.
12. A. P. Moore, R.J. Ellison, and R.C. Linger. Attack modeling for information security and survivability. Technical report, CMU/SEI-2001-TN-001, 2001.
13. P.G. Neuman and D.B. Parker. A summary of computer misuse techniques. *12th National Computer Security Conference, Baltimor, MaryLand*, pages 396–407, 10-13 October 1989.
14. The Biometrics Management Office and National Security Agency. U.s. government biometric verification mode protection profile for medium robustness environments. Technical Report Version 1.0, The Biometrics Management Office and the National Security Agency, 2003.
15. A.J. Rae and L.P. Wildman. A taxonomy of attacks on secure devices. *Australian Information Warfare and IT Security, 20-21 November 2003, Australia*, pages 251–264, 2003.
16. N.K. Ratha, J.H. Connell, and R. M. Bolle. Enhancing security and privacy in biometric-based authentication systems. *IBM System Journal*, 40(3):614–634, 2001.

17. N.K. Ratha, J.H. Connell, and R.M. Bolle. Biometrics break-ins and band-aids. *Pattern Recognition Letters*, 24(13):2105–2113, Sep 2003.
18. R.M.Bolle, J.H. Connel, S. Pankanti, N.K.Ratha, and A.W. Senior. *Guide to Biometrics*. Springer-Verlag, 175, Fifth Avenue, New York ,NY 10010, USA, 2004.
19. B. Schneier. Attack trees: Modeling security threats. *Dr. Dobb's Journal [on-line: www.ddj.com]*, 1999.
20. B. Schneier. The uses and abuses of biometrics. *Communication of the ACM*, 42(8):136, Aug 1999.
21. O. Sheyner, J. Haines, S. Jha, R. Lippmann, and J.M. Wing. Automated generation and analysis of attack graph. *In Proc. of IEEE Symposium on Security and Privacy*, 2002.
22. U. Uludag and A. Jain. Attacks on biometric systems: A case study in fingerprints. *Proc. SPIE-EI 2004, Security, Steganography and Watermarking of Multimedia contents VI*, 2004.
23. R.N.J. Veldhuis, A. M. Bazen, J. Kauffman, and P. H. Hartel. Biometric verification based on grip-pattern recognition (invited paper). In E. J. Delp III and P. W. Wong, editors, *IS&T/SPIE 16th Annual Symp. on Electronic Imaging - Security, Steganography, and Watermarking of Multimedia Contents*, volume 5306, pages 634–641, San Jose, California, Jan 2004. SPIE – The Int. Society for Optical Engineering, Washington.