A False Rejection Oriented Threat Model for the Design of Biometric Authentication Systems

Ileana Buhan, Asker Bazen, Pieter Hartel, and Raymond Veldhuis

University of Twente, Faculty of Electrical Engineering,
PO 217, 7500AE Enschede, 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 air-and seaports, banks, military installations, etc. 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 [1]. Watch lists are mainly used in ports 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 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 [15]. 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.

We propose 3W trees (Who, hoW, What) 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. A similar approach is taken

D. Zhang and A.K. Jain (Eds.): ICB 2006, LNCS 3832, pp. 728–736, 2005.

by de Cock et al. in [3], when modeling threats for security tokens in web applications. Our method is more concrete than other methods 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 points of vulnerability in biometric authentication systems. The extended architecture of a biometric authentication system is presented in Section 3. Section 4 describes 3W trees the method proposed for identifying *false rejection* attacks and in Section 5 we apply this 3W tree to the *Terrorist Watch List* and to the *Smart Gun*. The last section concludes and suggests further work.

2 Related Work

Like all security systems, biometric systems are vulnerable to attacks [7, 12]. One specific attack consists of presenting fake inputs such as false fingerprints [4] to a biometric system. To analyze such threats systematically various threat models have been developed. 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) [8], the U.S. Government Biometric Verification Mode Protection Profile for Medium Robustness Environments (USGovPP) [10] and Information Technology-Security techniques -A Framework for Evaluation and Testing of Biometric Technology (ITSstand) [5]. In the sequel we refer to these three protection profiles and the ITSstand simply as “the standards”.

In many ways, the standards are similar. In particular, they do not make a clear distinction between a *false rejection* and a *false acceptance* attack. A total of 48 distinct threats are identified 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 with both *false rejection* and *false acceptance* threats.

It is difficult to compare threats amongst the four standards. 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 channel tampering . In *ITSstand* tampering and bypassing is mentioned when describing the same threat while BDPP explicitly mentions the T.BYPASS threat.

ITSstand is the most complete in identifying *false rejection* threats, it identifies the largest number (8) of such rejections (See [5] [threats 8.4, 10.2, 11.2, 13.1, 13.3, 14.1, 14.3, 15.1]). However, only threat 13.3 is a clear false rejection. All the others are “catch all” threats. There are three tamper related threats: one related to hardware tampering (13.1), one related to software tampering (14.1) and one for channel tampering (15.1). These threats are general, not specifying the exact point in the system that is vulnerable, or the circumstances that make the system vulnerable to attack. The method of attack is also not clear, all that is said is that hardware can be tampered with, bypassed or deactivated. These threats lack the exact how and where. The key idea of our 3W tree is that it provides the missing how and where to the analyst.

Attack trees offer a related method of analyzing attacks [14]. 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. 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 does not provide much guidance.

Bolle et al. [13] 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.

3 Biometric Authentication Generic System Architecture

Ratha et al. [12] 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, as illustrated in Fig. 1.

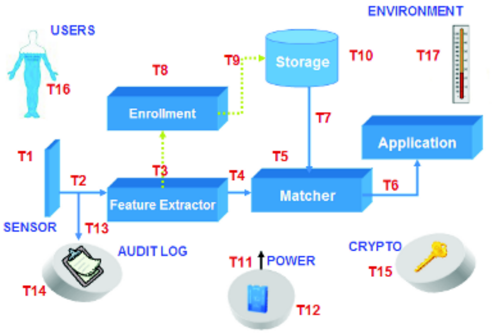

Fig. 1. General view of a Biometric Authentication System showing 17 points of attack

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 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:

(a) *Cryptography,* for ensuring 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*, T.CRYPT_ATTACK and T.CRYPTO_COMPROMISE in *USGovPP*.

(b) *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*.

(c) *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*.

(d) *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* 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 and in *ITSstand* they are labeled as: 8.1, 8.2, 8.3 and 8.4. Other threats are T.FAILSECURE, T.DEGRADE presented in *DoDPP*.

This concludes the extension of the architecture of Ratha et al. [13], by adding 7 components that could influence the performance and security of a biometric system.

4 3W Trees

The attack classifications from the standards are too coarse. For example threat T.UNDETECT in *BDPP* says: *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.* Nothing is said about the type of attack except that it is undetected and that the result can be either a false acceptance or a false rejection. To solve this problem we propose a more detailed analysis using 3W trees to give concrete insights in potential attacks, without burdening the analyst with irrelevant detail.

Three relevant grounds of distinctions are identified in the general security taxonomies in the literature, namely the *who*, the *how* and the *what*. We use each of these grounds of distinction at different levels of the 3W tree (*Fig.* 2).

The first level of the 3W tree is a classical *who* taxonomy from the attacker's position relative to the system [9]. Attackers are divided in three classes. *Class I* attackers or *external* attackers, lack knowledge about the system and have moderately sophisticated

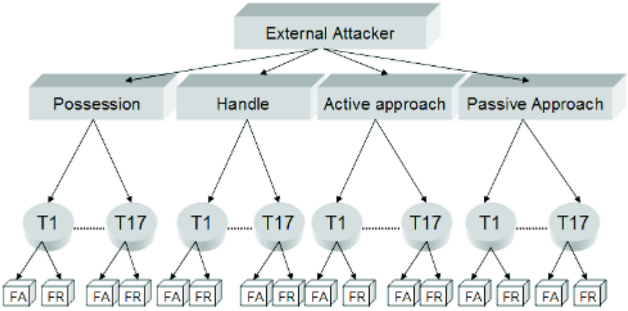

Fig. 2. 3W tree of attacks on biometric systems. T1-T17 are points of attack shown in Fig. 1.

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.

As a second level the 3W tree we use the Rae and Wildman taxonomy for secure devices [11]. This is a *how* taxonomy:

- *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 :

$$\textit{passive approach} \subset \textit{active approach} \subset \textit{handle} \subset \textit{possession}$$

The third level of the 3W tree , the *what*, deals with the threats our system might be subject to. For a description of the first 10 attacks T1-T10 we refer the reader to the Bolle et al. [13]. In addition to threats T1-T10 of Bolle et al. [13] we identify threats T11-T17:

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.

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*.

This concludes the presentation of the 3W tree for identifying attacks on a general biometric authentication system in the design phase, which allows us to classify known attacks and to identify the possibility of new attacks in a systematic manner. This is the subject of the next section.

5 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*.
- $i \in \{1..17\}$ indicates 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 *Scenario:* name of the evaluated scenario.
I *Tactics:* describe a possibility to realize this attack.
I *Name:* the name of the attack in the literature or a link to a paper that describes this attack (if known).
II *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.
II *Knowledge:* lists the knowledge that an intruder must have to launch the attack. The categories are: *common sense, high school education, expert.*
II *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 *Countermeasures:* some notes on how this attack might be prevented, or how at least to diminish its consequence.

Below we present two examples, showing that analysis based on the 3W tree leads to asking relevant questions about threats on biometric authentication systems. In the Technical Report version of this paper all $4 \times 17 = 68$ threats are analyzed [2]. From 68 possible threats, 13 are considered serious threats. From these 13 threats, 6 have are likely to occur and 12 have major consequences for the integrity of the device.

Example 1: Smart Gun 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 a gun should recognize all members of a police patrol, and that wearing gloves should not affect the operation. The PO4R attack, shown in Table 1 is a tamper attack. All standards mention tamper attacks but do not detail the point in the system where the tampering might occur. However, a tamper attack is relatively easy to perform and the consequences are high: the gun is not working. By

Table 1. *PO4R Scenario in the Smart Gun application*

I. Scenario	Can an attacker in the *possession* situation attack the communication channel between the feature extractor and the matcher in order to produce a *false rejection*?
I. Tactics	Physically breaking the channel is the most obvious choice. To destroy wires/connections inside the electronic device we have the following possibilities: exposing the object to extreme values of pressure, temperature etc. and at some point the mechanical connections will break.
I. Name	Physical tampering.
II. Damage	High. If the template extractor is out of order the gun will not work correctly.
II. Knowledge	Expert. The attacker must know how to open the gun and which device is the template extractor and then reassemble the gun.
II. Occurrence	Medium. The result of such an attack is a gun that is not working properly in the hands of the rightful user. If he wants to harm the user there are other ways in which he has more control over what is happening. (i.e pulling a knife)
III. Counter measures	A seal on the gun handle seems to be most appropriate. The seal must ensure that even if the attacker can open the gun, resealing the device would be easily detectable. It should be possible to discover the details of such an attack from an audit log.

pointing out the specific points of attack, our analysis, suggests that a seal is needed on the gun handle where the electronics are located. A tamper evident seal would indicate the police officer whether the integrity of the weapon has been violated.

Example 2: Terrorist Watch Lists are used to detect terrorists while traveling. Applications like this are usually installed at airports, seaports, main railway stations etc. Peo-

Table 2. *AA1R Scenario in Terrorist Watch List Application*

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 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..

ple who want to travel are checked against a central database with potentially dangerous persons. There are at least two ways to 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 2. We could not find any mention of this attack in the literature. Again, our 3W tree helps to ask the right question during the analysis.

6 Conclusions

Existing biometric protection profiles and standards by and large define the same set of attacks. However, their focus is mainly on *false acceptance* attacks. Attacks that result in a false acceptance or false rejection are often put in the same class. Threats that could only lead to a *false rejection* are largely ignored.

In new 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 advantage of the 3W tree is that (1) its fosters a systematic approach to threat analysis, (2) allows asking concrete questions, and (3) does not burden the analysis with irrelevant detail. Analyzing a 3W tree helps us to develop scenarios. For evaluating and describing scenarios we propose a model consisting of: *tactics, name, consequence, estimated knowledge, estimated probability, countermeasure.* In two detailed examples we identify appropriate countermeasures to attacks. For the smart gun example we argue that there must be a seal on the gun handle to protect the electronics inside the gun. For the terrorist watch list we argue that the camera should be positioned in a way that would prevent a light beam to be reflected on the camera. The main advantage of the 3W tree is that relevant threats are identified.

This research is supported by Technology Foundation STW. We thank Jeroen Doumen and Ruud van Munster for their comments on the paper.

References

1. 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.
2. I. Buhan and P. Hartel. The state of the art in abuse of biometrics. Technical report to appear, Centre for Telematics and Information Technology, Univ. of Twente, The Netherlands, June 2005.
3. D. De Cock, K. Wouters, D. Schellekens, D. Singelee, and B. Preneel. Threat modelling for security tokens in web applications. In D. Chadwick and B. Preneel, editors, *8th IFIP TC-6 TC-11 Conference on Communications and Multimedia Security*, pages 131–144, Lake Windermere, England, Sep 2004. Springer-Verlag, Berlin.

4. 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.
5. 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.
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. 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.
8. 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.
9. 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.
10. 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.
11. 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.
12. 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.
13. 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.
14. B. Schneier. Attack trees: Modeling security threats. *Dr. Dobb's Journal [on-line: www.ddj.com]*, 1999.
15. 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.