2009

Defeating biometric fingerprint systems: An applied testing methodology

David J. Brooks

Brooks, D. J. (2009). Defeating biometric fingerprint systems: An applied testing methodology. In D. M. Cook (Ed.)., *Proceedings of the 2nd Australian Security and Intelligence Conference, Kings Hotel, Perth, Western Australia, 1-3 December, 2009*. (pp. 1-9).

Defeating biometric fingerprint systems: An applied testing methodology

David J. Brooks
Security Research Centre (SECAU)
School of Computer and Security Science
Edith Cowan University, Australia.

Abstract

Biometric access control systems are becoming more common and may be considered high-security, due to their ability to identify and validate that the person is who they purport to be. Therefore, such biometric systems are often installed into critical infrastructure facilities as a means to gain high security protection. To date, there has been considerable research into the effectiveness of biometric devices to recognise valid users and reject invalid users, and to develop standards for interoperability. However, biometric systems are vulnerable to many categories of attack and there has been restricted research into such defeat vulnerabilities.

This article presents an approach that applied a defeat evaluation methodology to three high-security biometric fingerprint readers. Defeat testing included both physical and technical integrity testing, considering zero-effort to adversarial complex attacks. Physical defeat testing resulted in the attackers being able to gain entry into the internal circuitry of all three readers, with two readers having their tampers bypassed and access gained to the output relay door locks. Technical integrity testing resulted in one of the readers being defeated with an enrolled 2-dimensioal fingerprint spoof and one reader being spoofed by a 3-dimensional fingerprint overlay, with all live finger monitor being defeated. These results indicated a number of significant vulnerabilities in the three biometric readers, raising concern with such systems being applied within critical infrastructure.

Keywords
Biometrics, fingerprint, defeat evaluation, spoofing, vulnerabilities, critical infrastructure

INTRODUCTION

Biometric evaluation has, in general, considered the ability of such capture devices to deny valid users or accept invalid users, referred to as False Rejection Rate (FRR) and False Acceptance Rate (FAR). Much of the research and testing has focused on these measures of biometric access control systems, with limited consideration of system vulnerabilities (Dunstone and Poulton, 2008). Biometric systems, due to their measure of a person's physiological characteristics, may be considered to provide high security access control. Such a view was taken by the Australian Federal Government, with their allocation of $182 million to deploy such systems at the borders (Wilson, 2007). In addition, such systems are finding their way into many diverse access control solutions, to improve performance, delivery greater returns and extend applications (Crozier & Cochrane, 2009). For many critical infrastructure or high security installations, the ability of the access control system to provide a robust and reliable system is paramount. However, system factors such as FRR may not be as much of an issue in higher security environments.

There are many groups working on biometric systems, for example the Biometric Working Group, the International Biometric Foundation, the International Organisation for Standardisation Committee and in 2008, the US Government released a recommended registry of biometric standards (Moradoff, 2009, pp. 17-18). Nevertheless, such groups are in general considering biometric interoperability, based on developing standards and not necessarily considering vulnerabilities of such systems. As Mansfield and Wayman stated when considering biometric performance testing, there are many possibly more important testing including vulnerability and security evaluation (2002, p.1).

This article presents a methodology for the evaluation of biometric fingerprint systems, with a focus on defeat evaluation suitable for high security and critical infrastructure facilities. Biometric fingerprint were chosen as they are considered the most common form of biometric reader. Three commercially available *high security* biometric fingerprint systems were tested for a sponsoring Federal Government agency using this applied method. Such evaluation methodology was considered important, for example the Biometric Institute agenda is to test the claims of biometric manufacturers and produce a vulnerability assessment program (Crozier & Cochrane, 2009).

BIOMETRIC ACCESS CONTROL SYSTEMS

Biometric systems comprise of many techniques to extract, process and compare biometric characteristics. According to Johnson (2004), there are two classes of biometric characteristics, namely physical (physiological) and behavioural; with these classes divided into such methods as voice recognition through to iris scanning (Smith, 2006). Within a security context, biometric may be considered the highest level of validation, based on the principle of *something you have* (card, token), *something you know* (password) and *something you are* (biometric). As these stages are applied (Figure 1), alone or as multiple identifiers, the view is that the system becomes more secure as "biometric

characteristics is the true identifier of a person" (Smith, 2006, p. 624). However, this may not be the case when considering such issues as false acceptance rate and other system vulnerabilities.

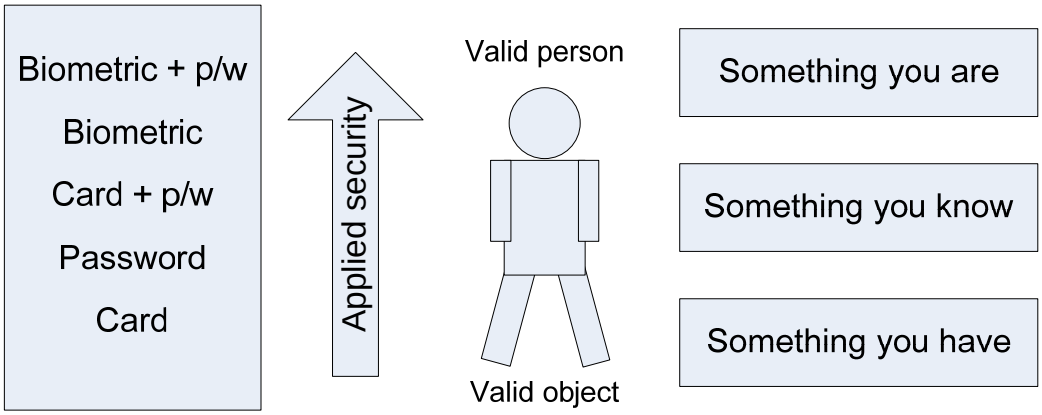

Figure 1 Levels of security access control

BIOMETRIC VULNERABILITIES

Biometric access systems may be vulnerable to two different categories of attack, namely *zero-effort attack* or *adversary attack* (Jain, Ross et al., 2006). With a zero-effort attack the biometric traits of the attacker may be similar to a valid user, resulting in false acceptance (FAR) by the system. There may be a possibility that valid user templates stored in the systems database can be similar to that of the imposter, given the variance designed or defined into such systems. In an adversary attack, the attacker can imitate a valid system user by using physical or digital artefacts belonging to the user. The attacker can also change their biometric traits to match those of the system user.

In addition, there are other types of system attacks; circumvention, repudiation, collusion, coercion and denial of service. Circumvention is where the attacker may gain access into the system beyond that of the data collection plenum, peruse and modify these sensitive data (Jain, Ross et al., 2005). Repudiation is where an employee gains entry into the system and sensitive data, from which there may be circumvention by attacker (Rejman-Greene, 2001). Collusion is where the super-user modifies the system parameters to allow an attack to gain access to the system (Jain, Ross et al., 2006). Coercion is where the attacker threatens or blackmails an employee to grant him or her access to the system (Jain, Ross et al., 2006). Finally, denial of service is where the attacker floods the system with requests, which will overwhelm the system resources and deny the valid user access (Uludag and Jain, 2004).

These types of attack may be demonstrated within a systems approach (Figure 2), where up to eight attack points (Table 1) may be considered.

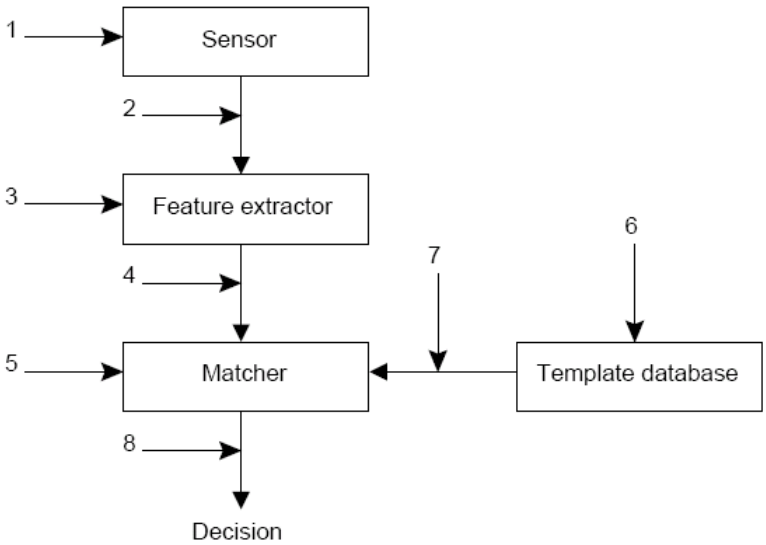

Figure 2 Generic biometric system attack points
(Uludag, 2006)

Attack points	System components	Attack procedure
1	Sensor	Verification attack 2D or 3D
2	Data transmission	Data capture, injection, replay
3	Feature extraction	Fake data
4	Feature transmission	Fake data injection
5	Template matching	Template sensitivity
6	Database	Manipulated database
7	Data transmission	Manipulated data injection
8	Authentication	Matching data overridden or altered

Table 1 *Biometric system attack points*
(Uludag cited in Smith, 2007)

In support, biometric vulnerabilities may have to consider three interrelated factors of the computing infrastructure, the human operators of the system and the specific biometric system (Dunstone and Poulton, 2008). The primary aim of defeat testing is to identify vulnerabilities in such systems and exploit these vulnerabilities. Such a view was supported by Smith (2007), who stated that such defeat testing seeks to exploit design and operational weaknesses in security systems to penetrate the security barriers.

EVALUATION METHODOLOGY

The evaluation methodology applied a priori testing approach, which considered reliability, validity and testing scope. These three aspects were considered to be core principles during evaluation, an aspect raised by previous authors (Jones and Smith, 2005; Smith, 2007). *Reliability* ensures that tests are conducted in such a way that results are repeatable, given the same variables and environmental conditions. *Validity* ensures that tests should be based on a careful selection and isolation of independent variables, with the use of a control variable. In addition, that test's do evaluate what they assert to test. *Testing scope* includes simple to complex physical and technological attacks, resulting in an understanding of the systems vulnerabilities. Testing, in general, did not include attacks that were outside the scope of the device; such as attacks on external input/output devices, interfaces or communications.

A number of discrete steps were taken within the evaluation methodology (Figure 3), comprising of evaluation mapping, commercial evaluation, performance testing, defeat testing and resulting final report. These steps commenced with documenting a defined approach to evaluation, ensuring priori testing criteria and that proceeding stages are mapped. An approach that according to Jhistarry and Frayssines is the first stage in formulating such evaluation strategies (2004). On completion of this first stage, the sponsoring agent's approval was gained to proceed to testing.

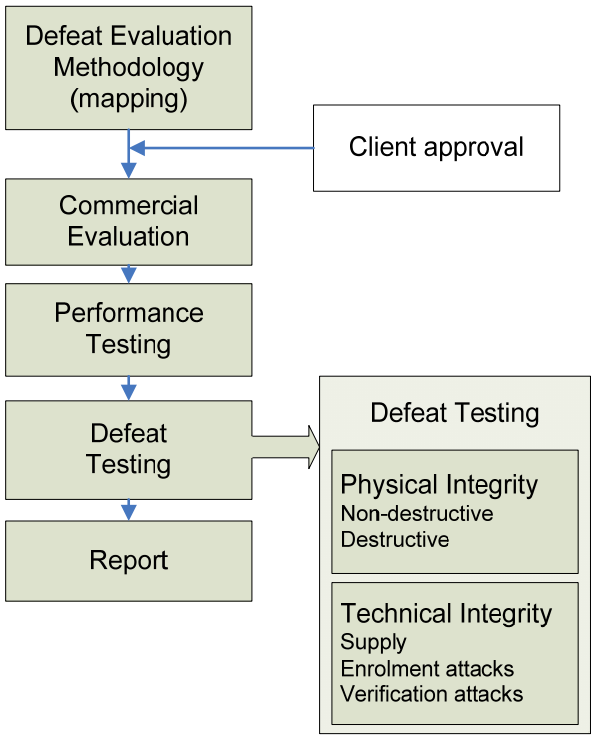

Figure 3 Biometrics defeat evaluation methodology

Commercial evaluation reviewed the robustness of manufacturer, supplier and logistics across all Australian states and territories. Reviews of national and international standards that may be applied to the test item were considered, with any past testing sourced.

Performance testing applied environmental testing on the device, with the prime intent to ensure compliance to manufacturer's stated specifications. In addition, environmental testing included inclement weather, user interface issues, environmental noise, etc. With the biometric fingerprint systems the FRR and FAR - with a restricted population size - were applied, considering the defeat evaluation of zero-effort attack and with such conditions divided into three categories of false acceptance analysis, non-ideal user conditions and non-ideal interface conditions. The user interface testing was, where possible, a quantitative investigation into the device's ability to accept *all* users under a range of non-ideal conditions.

Defeat testing was the main consideration within the evaluation and attempted to use both physical and technical adversary attacks against the device. These attacks included spoofing the device's detection capability in an attempt to identify vulnerabilities. Physical integrity tested both non-destructive and destructive structural integrity, access to enclosure, etc. Technical integrity tested the power supply, the device's underlying technology, tamper capability, etc. The evaluation was concluded with a comprehensive technical report of the testing results submitted to the sponsoring agency.

DEFEAT EVALUATION

The evaluation of the device attempted to discover vulnerabilities that may allow an intruder to bypass the device without triggering an alarm. The evaluation is categorised as:

- *Physical integrity*: to determine the item's physical resistance and vulnerabilities to attacks by covert and overt force.
- *Technical integrity*: to determine the item's technical resistance and vulnerabilities to bypass attempts using both zero-effect attacks and adversary technological attacks.

Physical Integrity

Physical integrity considered both non-destructive or covert attacks, and destructive attacks attempting to gain access into the device. Both approaches sought to evaluation the device's physical protection against such low level technical attacks, noting system vulnerabilities.

Non-Destructive Access to Item Interior

Non-destructive evaluation examined the ease (or delay) involved in removing the device's cover or otherwise opening the item's enclosure to gain access to its interior. Methods considered techniques that did not damage the device or show external tampering, maintaining a degree of covert access. Testing considered whether it was useful to the intruder to access the interior of the device and if such an attack was possible without triggering an alarm. The use of laboratory tools such as fine-blade screwdrivers, Allen and star keys, razorblades and such were used in this test.

Destructive Access to Item Interior

Destructive evaluation examined the ease (or delay) involved in gaining access to the device's interior using methods that may cause both superficial or destruction damage, such as forcibly removing the device from its mounting or piercing the device's enclosure. If the device had any sensors present to detect such an event, this was noted and attempts applied to defeat such anti-tamper devices. Testing included, but was not limited to, practices such as hammer strikes, prying and drilling. The assessment included a subjective discussion of the quality of casing and connecting hardware. The destructive testing used laboratory tools such as large screwdrivers, hammers, drill and drill bits.

Technical Integrity

With the creation of a *key*, biometric readers assume that every fingerprint presented is a credential unique to that user. If anyone can present a credential that the system considers valid, the system is essentially defeated and this constitutes a systemic failure to reliably authenticate users. Failure may be simple or complex adversarial attacks. The attacker may imitate a valid user by using the physical or digital artefact belonging to that valid user. The attacker may also change their biometric traits to match those of the system user. Technical attacks considered the ability of the device to resist artificial methods of defeat, including supply attacks, enrolment attacks and verification attacks.

Supply Voltage Testing

The supply voltage was tested to simulate both high and low voltage supply and likely effects this may have had on the device (Figure 4).

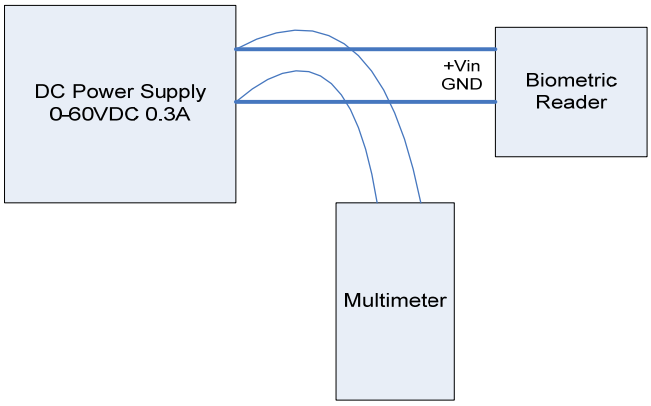

Figure 4 Supply voltage evaluation test

Commencing from the manufacturers specified voltage; the evaluation increased or decreased the device's supply voltage by 2V increments. During each change in voltage, ten-fingers were presented for validation and any effect noted.

Attack Analysis

These tests examined the device's ability to resist adversary attacks of a deliberate and sophisticated nature, divided into two categories of enrolment and verification attacks.

Enrolment attacks: attacks that attempted to undermine the principles and inherent security benefits of biometric systems by enrolling any of the artificial fingerprint types used in the verification attack testing. Due to the intent to consider defeat evaluation, enrolment tests were not applied.

Verification attacks: attacks that attempted to gain access during verification by using an artificial replication of a legitimately enrolled fingerprint. Verification attacks applied artificial replication methods, including both 2-dimensional types such as photocopies and photographs in various formats and media (Table 2; Figure 5), and 3-dimensional types such as residual prints on scanning platen, artificially constructed fingers and fingerprint overlays (Figure 6) on live fingers.

Photocopy	Photograph

Black and white paper	Greyscale paper
Greyscale paper	Colour paper
Colour paper	Colour transparency
Colour transparency	Colour paper with depressed print
Water misting with above	Water misting with above

Table 2 Two-*dimensional attack mediums*

Figure 5 Artificial 2-dimensinal depressed fingerprints

2-dimensional attacks: Several verification attacks with 2-dimensional images were attempted. The images were placed onto the platen 10 times, to see if the device would read the images. If the image was read, another 20 tries were conducted to ensure a proper read and rejection had been made. In addition, water misting was incorporated to replicate *live finger* monitoring.

The above adversary attack method was repeated with 3-dimensional medium. Artificial 3-dimensinal fingers and finger overlays (Figure 6) were made from different substances, primarily Gelatine poured into various moulds such as moulding plastic or etched circuit boards. This technique followed past testers (Mansumoto, Matsumoto, Yamada, & Hoshino, 2002), who published their artificial fingerprint spoofing methods.

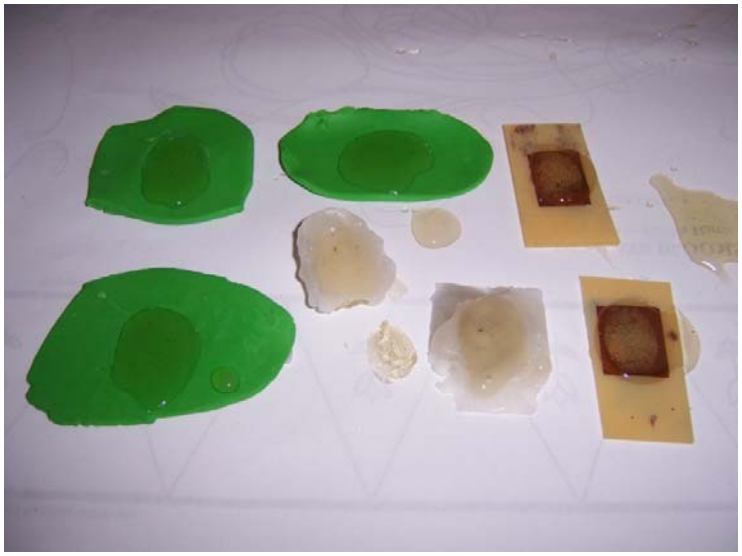

Figure 6 Replicated 3-dimensinal finger overlays

APPLIED DEFEAT EVALUATION

The defeat evaluation methodology was applied to three *high quality* biometric fingerprint devices. Each item was supplied from different manufacturers and with various image scanning and capture techniques.

Biometric fingerprint reader one

The first biometric fingerprint reader device was supplied in two discrete components, namely the Platen Reader and Secure Input/output board. The platen used a Radio Frequency (RF) ultrasonic sensing device, contained within a metal housing. Image data captured from the sensing device is encrypted to the Secure Input/output board. The Input/output board contains the power supply input, reader interface, output relay and door open output.

Biometric fingerprint reader two

The second biometric fingerprint reader was supplied as one complete stand-alone device, which contained the biometric platen, RFID reader, externally LCD display, 12-button keyboard and internal circuitry attached to the metal chassis and hardened plastic cover. The fingerprint scanning platen operated through an optical sensor.

Biometric fingerprint reader three

The third biometric fingerprint reader was supplied as a complete device, which contained the biometric platen, RFID reader and internal circuitry attached to the metal chassis and hardened plastic cover. The fingerprint scanning platen operated through an optical sensor.

RESULTS

The following defeat vulnerability results were obtained from the three biometric fingerprint devices.

Physical integrity and vulnerabilities

Evaluation comprised of both non-destructive and destructive testing. Simple physical attempts were made to pry the device casing from their mounts using a large screw driver. Various parts of the device were subjected to physical attacks, with a focus around the key fixing points. Attempts were made to crack or break the devices casings from its mount, using a medium weighted hammer and with various parts of the readers attacked. In general, 2 of the 3 devices proved to be robust in their ability to resist such brute force attacks. However, one of the devices could have its cover prised off with a screwdriver. Moreover, all three device's internal circuitry could be easily accessed with the use of common fixings. In one case, there was no cover tamper fitted. With the other two devices, the cover's anti-tampers could be bypassed with limited technical capability.

In two of the three devices, once access to the internal circuitry was possible this exposed the door release circuits. These circuits could be easily bypassed to active the door release, allowing door access. The third device came in two discrete components - platen reader and secure input/output board – with the door relay circuitry contained within this second component.

Technical integrity and vulnerabilities

Technical integrity evaluation included a number of 2-dimensional, 3-dimensional and multipoint attacks, leading to a number of vulnerabilities.

All three of the devices, when combined with water misting, would attempt a read of a 2-dimensional replicated finger. This misting approach also resulted in 2 of the 3 readers having a denial-of-service when water pooled. Nevertheless, none of the three items could be defeated with 2-dimensional replicated fingers. However, one of the readers allowed a replicated image to be enrolled and then read.

While the fake 3-dimensonal fingers would trigger a read condition in all devices, only one of the three devices resulted in a false acceptance condition. The use of fake 3-dimensional finger overlays, on a live finger, proved to be the most effective method (Figure 7). In addition, this approach could prove to be the most covert, as such manufactured overlays were discrete and could be fixed to the attacker's finger.

Figure 7 3-dimensional replicated fingerprint overlays

All the devices suffered some degree of random false acceptance read (FAR); however, due to the irregular nature of these FAR these were not repeatable. Nevertheless, when considering the relatively restricted number of test reads and testers applied during the study, the devices FAR's were of some concern.

CONCLUSION

The article has presented a defeat evaluation methodology for the testing of biometric systems, applied against three *high* security fingerprint reader devices. The evaluation methodology proposed a five stage process, with testing comprising of a commercial evaluation, performance testing and finally, defeat testing. Defeat testing was the prime focus of this evaluation, dividing this stage into both physical integrity and technical integrity. Defeat testing attempted to seek and examine vulnerabilities within the biometric devices.

Each tested biometric fingerprint reader device had some degree of vulnerability, with some of these being quite simple physical security failures. Physical defeat testing demonstrated that attackers were able to gain entry into the internal circuitry of all three readers, with two readers having their tampers bypassed and access to the output door relays. Technical integrity testing demonstrated that one of the readers could be defeated with an enrolled 2-dimensioal spoof and one reader could be spoofed by a 3-dimensional false fingerprint overlay, with all *live finger* monitoring being spoofed.

The article has shown that biometric systems, although considered *high security*, can be defeated using various techniques. Therefore such systems, however technology driven, should be considered one component within a holistic critical infrastructure security environment, with layers of deterrence, detection, delay, response and recovery.

REFERENCES

Crozier, R., & Cochrane, N. (2009). *Biometrics: the ultimate security?* Retrieved August 6, 2009, from http://www.crn.com.au/Tools/Print.aspx/CIID=149591

Dunstone, T., & G. Poulton (2008). *Biometrics vulnerabilities: a principled assessment methodology*, Sydney: Biometrics Institute Ltd.

Jain, A. K., Ross, A., & Pankanti, S. (2006). Biometrics: a tool for information security. *IEEE Transactions on Information Forensics and Security, 1*(2), 125-143.

Jain, A. K., Ross, A., & Uludag, U. (2005). *Biometric Template Security: Challenges and Solutions*. Proceedings of European Signal Processing Conference (EUSIPCO), Antalya, Turkey.

Jhistarry, S., & Frayssines, B. (2004). *Technical test methodology*. Unpublished manuscript, Perth: Edith Cowan University.

Jones, D. E. L., & Smith, C. L. (2005). The development of a model for the testing and evaluation of security equipment within Australian Standard / New Zealand Standard AS/NZS4360:2004 - risk management. *Recent Advances in Counter-Terrorism Technology and Infrastructure Protection*.

Mansfield, A. J., & Wayman, J. L. (2002). *Best practices in testing and reporting performance of biometric devices* Teddington: National Physical Laboratory.

Rejman-Greene, M. (2001). Biometrics - real identities for a virtual world. *BT Technology Journal 19*(3): 115-121.

Smith, C. (2006). Trends in the development of security technology. In M. Gill. (Ed.), *The Handbook of Security*. Basingstoke: Palgrave Macmillian Ltd, 610-628.

Smith, C. (2007). The evaluation of security systems: Testing biometrics and intelligent imaging systems. *The 6th International Workshop for Applied PKC (IWAAP2007)*.

Uludag, U. (2006). *Graduate psychology: Secure biometrics systems*. Michigan: Michigan State University.

Uludag, U., & Jain, A. K. (2004). Attacks on biometric systems: a case study in fingerprints. *Proceedings of the SPIE-EI 2004*, San Jose.

Wilson, D. (2007). Australian biometrics and global surveillance. *International Criminal Justice Review, 17*(3), 207-219.

COPYRIGHT