11-30-2010

Assessing Vulnerabilities of Biometric Readers Using an Applied Defeat Evaluation Methodology

David Brooks
Edith Cowan University

DOI: 10.4225/75/579ec6e8099cb
3rd Australian Security and Intelligence Conference, Edith Cowan University, Perth Western Australia, 30th November 2010

Assessing Vulnerabilities of Biometric Readers Using an Applied Defeat Evaluation Methodology

David J. Brooks
secau – Security Research Centre
School of Computer and Security Science
Edith Cowan University
Perth, Western Australia
d.brooks@ecu.edu.au

Abstract

Access control systems using biometric identification readers are becoming common within critical infrastructure and other high security applications. There is a perception that biometric, due to their ability to identify and validate the user, are more secure. However, biometric systems are vulnerable to many categories of attack vectors and there has been restricted research into such defeat vulnerabilities.

This study expands on a past article (Brooks, 2009) that presented a defeat evaluation methodology applied to high-security biometric readers. The defeat methodology is represented, but applied to both fingerprint and back-of-hand biometric readers. Defeat evaluation included both physical and technical integrity testing, considering zero-effort to adversarial complex attacks. In addition, the evaluation considered the whole device and not just the biometric extraction and storage device.

The study found a number of common vulnerabilities in the various types of biometric readers. Vulnerabilities included the ability to spoof optical readers with another person's extracted print, use of inanimate objects to enrol and validate, defeat of live detection and the ability to by-pass the biometric reader. Optical sensors appeared the least secure, with capacitive the most secure. An awareness of the vulnerabilities and limitations of biometric readers need to be propagated, as such readers should not be considered high-security by default. As this study demonstrated, most of the readers had some inherent vulnerability that was not difficult to exploit, in particular, from an insider's perspective.

Keywords

Access control, biometric, defeat, evaluation, spoofing, vulnerabilities

INTRODUCTION

"Identical twins can fool some biometric systems:" (Peterson, 2000); however, defeating a biometric reader is far simpler than trying to coerce identical twins.

Biometrics systems are becoming far more common place today, being used in many parts of society. For example, biometric are now used in law enforcement to fingerprint suspects and for victim identification, national security in border control, workplace for time and attendance, retail and financial sectors (Peterson, 2000) and many other places for entry control and person validation, such as high-end motor vehicles, access to computers, etc. The use of biometrics within access control systems is thought to be the most secure form of access control (Khairallah, 2006) and today, biometric readers are used extensively in high security applications such as airport, ports, border crossings, government facilities and other such critical infrastructure.

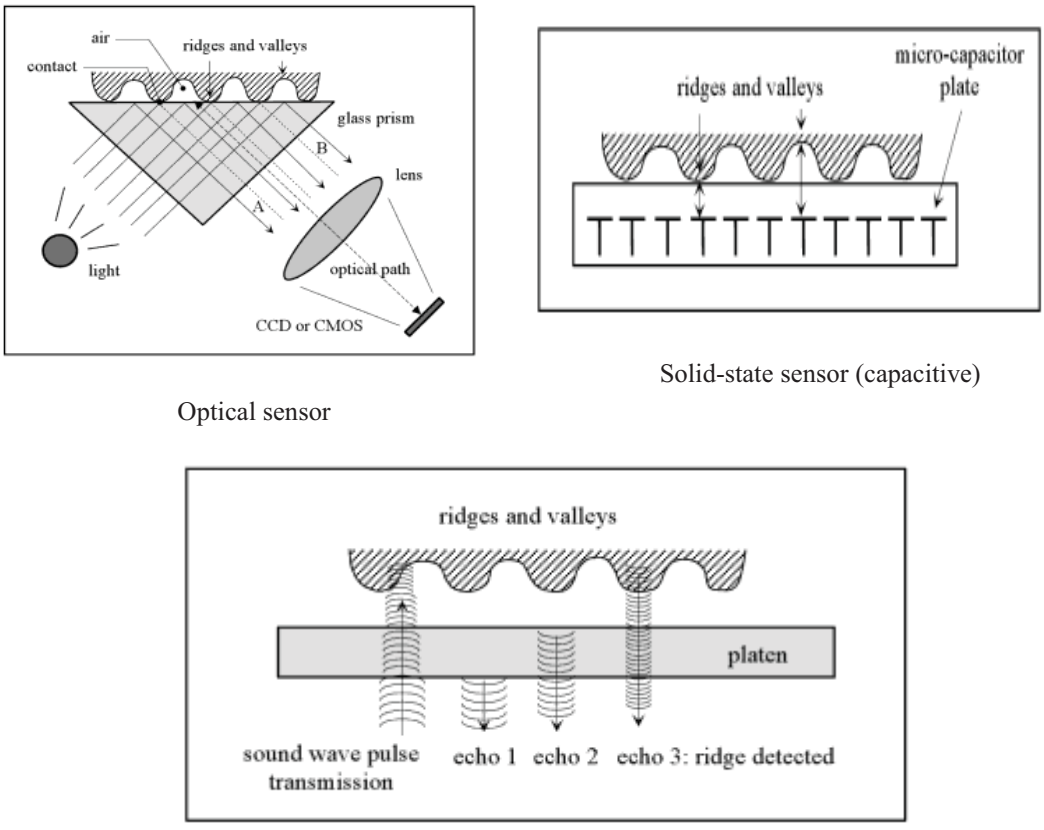
Although some suggest that there are privacy issues with biometric systems and its readers, 72 percent of Australians are willing to use fingerprint readers to protect themselves, their information and finances. What is interesting, is that 66 percent are willing to use an iris reader and 47 percent use a Vascular reader (Australia Security Magazine, 2008). Since the 1990s, there have are many factors driving the proliferation of biometric readers, being reduced cost, greater promotion of benefits, increasing reliability of such systems (Peterson, 2000), ease of use, greater portal speed, limited concern of privacy issues. However, past studies have demonstrated that biometric readers do suffer significant vulnerabilities (Uludag and Jain, 2004a; Crozier and Cochrane, 2009; Brooks, 2009).

This article puts forward an evaluation methodology (Brooks, 2009) for the defeat testing of biometric systems, whether the reader is fingerprint, back-of-hand or hand scanner. The methodology has been presented in the past; however, recent research has applied the methodology to additional types of biometric readers beyond the original applied fingerprint readers. The focus remains defeat evaluation, with the benchmark suitable for high

security and critical infrastructure facilities with an *insider* threat. A number of commercially available high security biometric fingerprint and back-of-hand systems were tested using this applied methodology. Such evaluation methodology is important, as supported by such groups as the Australian and New Zealand based Biometric Institute whose agenda is to test the claims of biometric manufacturers and produce a vulnerability assessment program (Crozier & Cochrane, 2009).

BIOMETRIC ACCESS CONTROL SYSTEMS

In general, biometric systems are becoming more reliable as readers, software and multipoint systems improve (Peterson, 2000). 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 to iris scanning (Smith, 2006). From a technical perspective, these can be further divided into their underlying principle, namely optical, solid-state and ultrasonic. These techniques are supported by the underlying principle that the sensor acquires the biometric image (Figure 1).



Optical sensor

Solid-state sensor (capacitive)

Ultrasonic sensor

Figure 1: Fingerprint reader sensors
(Maltoni, Jain & Prabhakar, 2009, p. 63)

Optical readers use a picture capture device in either the visible or infrared light spectrum to extract the biometric image. Solid-state readers use a platen made of many capacitive circuits, where the image is extracted from ridges or valleys that alter each electrical circuit. Finally, ultrasonic readers again use the ridges and valleys but extract the image using sound waves.

This study considered perhaps the most common of biometric readers, being those that are applied to the hand, either fingerprint or back-of-hand. The reason for this approach is that the hand and fingerprint has advantages, such as the demonstrated uniqueness of an individual fingerprint and their greater commercial popularity. For example, in over "140 years of fingerprint comparison worldwide, no two fingerprints have ever been found to be alike, not even those of identical twins" (Biometric Authentication, n.d.).

Why Biometrics are considered high security

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 this principle is applied (Figure 2), alone or as multiple identifier, the perception is that the security system becomes more secure. Such a view is held as "biometric characteristics is the true identifier of a person" (Smith, 2006, p. 624); however, taking such a theoretical approach with biometric system may and does lead to systems that are prone to attack through either technical or simple defeat through many of system and reader vulnerabilities (Brooks, 2009).

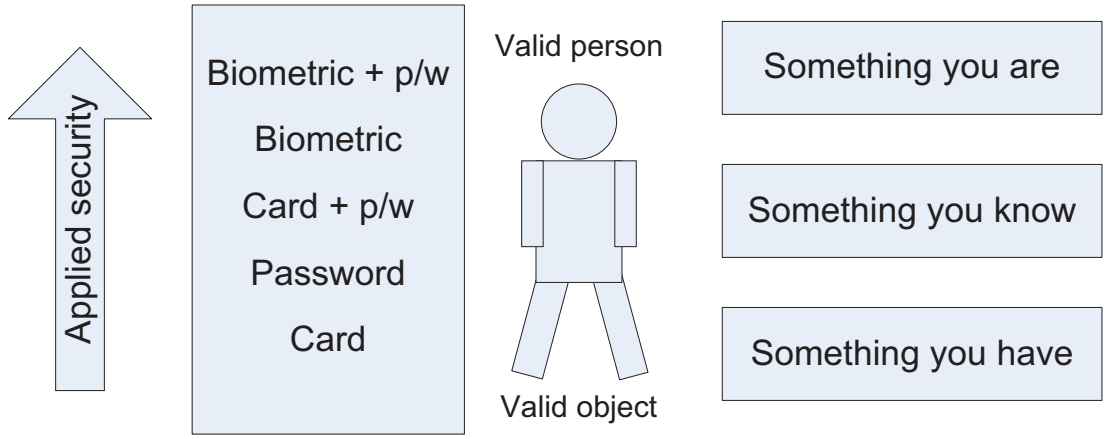


Figure 2 Access control: Perceived level of applied security
(Brooks, 2009)

Biometric vulnerabilities

Biometric access systems may be vulnerable to 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 and result in false acceptance (FAR). There may be a possibility that a valid user template stored in the system's database is similar enough to that of the imposter, given the variance designed or user defined into the systems. In an adversary attack, the attacker can imitate a valid system user by using physical or digital artefacts. 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 & Jain, 2004b).

These types of attack may be demonstrated within a systems approach (Figure 3), where up to eight attack points (Table 1) may be considered.

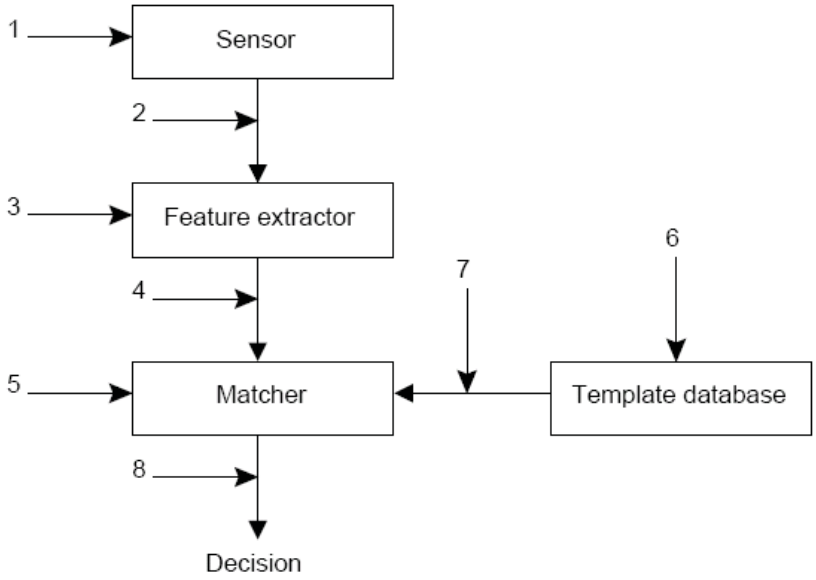


Figure 3 Generic biometric system attack points (Uludag, 2006)

Table 1
Biometric system attack points

Attack points	System components	Attack procedure
1	Sensor	Enrol and/or 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 default and sensitivity
6	Database	Manipulated database
7	Data transmission	Manipulated data injection
8	Authentication	Bypass system

(Adjusted from Uludag cited in Smith, 2007)

Attack methods against say the capacitive reader may include creating moisture around the sensor platen and using the latent fingerprint body residues. Another successful strategy may involve the application of a thin-walled water filled-plastic bag onto the sensor to reactivate the latent fingerprints (Thalheim, Krissler et al., 2002). Significant success in spoofing a variety of fingerprint readers using artificial gelatine fingerprint created from moulds of actual fingers achieving a success rate of between 68-100 percent and extracted prints achieved a 67 percent success rate (Matsumoto, Matsumoto et al., 2002). In addition, means of bypassing cheaper systems with an almost 100 percent success involved dusting graphite over the platen residues and stretching an adhesive strip over the latent prints while applying pressure (Thalheim, Krissler et al., 2002).

Nevertheless, biometric vulnerabilities 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). In high-security environments, this has to include the *insider* threat. The primary aim of defeat evaluation was 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. The approach taken in this study was to consider the biometric reader as a *Black-box*, unlike other evaluation methods that have evaluated only the biometric reader sensor. Such an approach better reflects the many attack points put forward by Uludag (2006).

BIOMETRIC EVALUATION

In general, biometric evaluation has only 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 and 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) and now, the IEEE Certified Professional (Institute of Electrical and Electronic Engineers, 2010). Nevertheless, such groups are in general considering biometric interoperability, based on national and international standards, and with bounded consideration of system vulnerabilities. As Mansfield and Wayman stated when considering biometric performance testing, there are many possibly more important testing including vulnerability and security evaluation (2002).

STUDY EVALUATION METHODOLOGY

This study applied a methodology that took a priori evaluation approach, which considered reliability, validity and testing scope (Brooks, 2009). These three aspects were considered to be core principles during evaluation, an aspect raised by previous authors (Jones and Smith, 2005; Smith, 2007). For example, *reliability* ensures that evaluation is conducted in such a way that results are repeatable, given the same variables and environmental conditions. *Validity* ensures that evaluation should be based on a careful selection and isolation of independent variables, with the use of a control variable. In addition, that the methodology evaluates what it assert to measure. Finally, the *testing scope* included simple to complex physical and technological attacks, resulting in an understanding of the systems vulnerabilities. Testing, in general, considered the biometric reader as a stand-alone device or *Black-box*. Therefore, data communications to external devices were not considered, only connectivity within the device itself.

A number of discrete steps were taken within the evaluation methodology (Figure 4), 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.

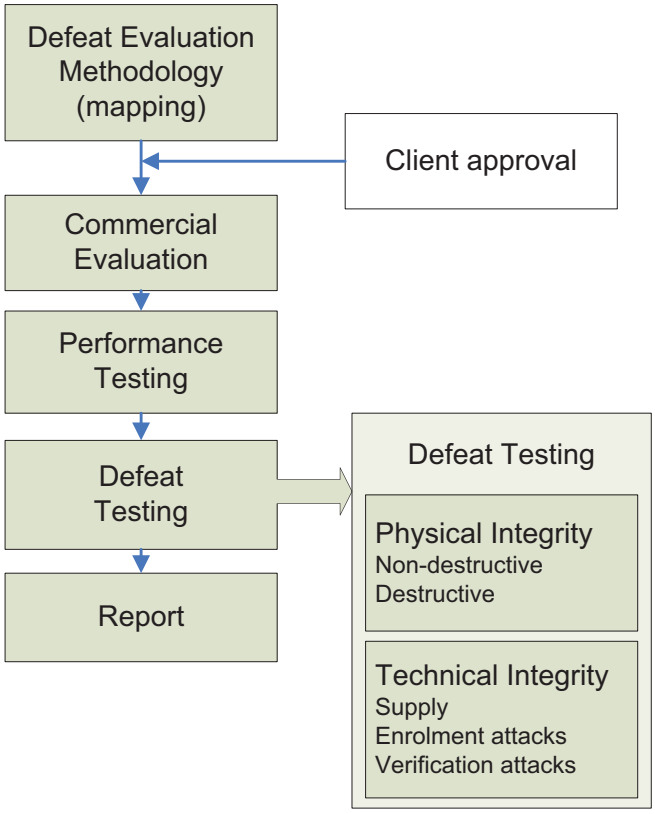


Figure 4 Biometrics defeat evaluation methodology
(Brooks, 2009)

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 sampling 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 evaluation was the main consideration within the testing and attempted to use both physical and technical adversary attacks. These attacks included spoofing the device's detection capability in an attempt to identify vulnerabilities. Physical integrity evaluated both non-destructive and destructive structural integrity, access to enclosure, fixings, etc. Technical integrity evaluated the power supply, the device's underlying technology, tamper capability, etc.

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 evaluate 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 evaluated to simulate both high and low voltage supply and likely effects this may have had on the device. 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 attempted to undermine the principles and inherent security benefits of biometric systems by enrolling any of the artificial objects used in the verification attack testing (Table 2).

Table 2
2-dimensional attack mediums

Artificial object	
Black and white paper	Colour transparency
Greyscale paper or cardboard	Water misting with above
Colour paper	

Verification attacks attempted to gain access during verification by using an artificial replication of a legitimately enrolled objects'. Verification attacks applied artificial replication methods, including both 2-

dimensional types such as photocopies and photographs in various formats and other medium (Figures 5 and 6). In addition, 3-dimensional types such as residual prints on scanning platen, artificially constructed fingers and fingerprint or hand overlays (Figure 7).

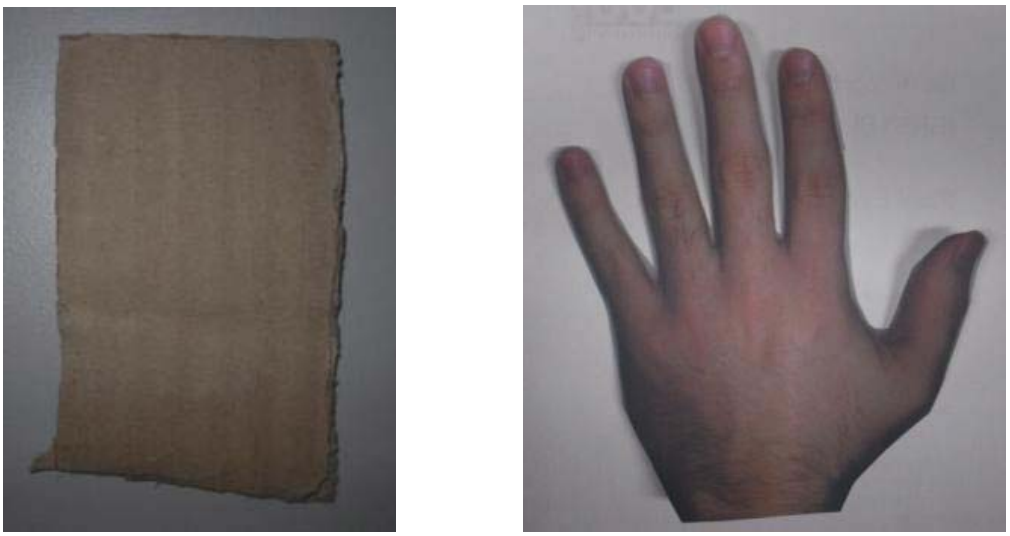


Figure 5 Inanimate 2-dimensinal object and back-of-hand scan (colour)

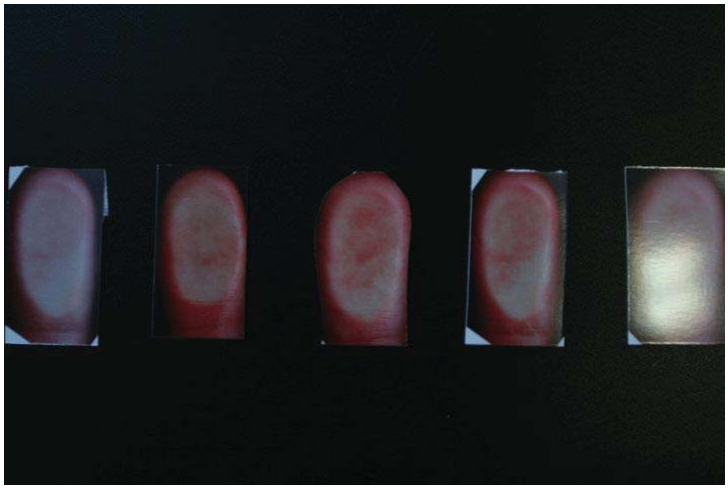


Figure 6 Artificial 2-dimensinal depressed fingerprints

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. Water misting comprised of spraying fine droplets of water onto the platen to moisten the artificial images.

The above adversary attack method was repeated with 3-dimensional medium. Artificial 3-dimensinal fingers, back-of-hand and finger overlays (Figure 7) were made from different substances, primarily Gelatine poured into various moulds such as moulding plastic or etched circuit boards. This technique followed past testers (Matsumoto, Matsumoto et al., 2002; Uludag and Jain, 2004a), who published their artificial fingerprint spoofing methods.

Figure 7 Replicated 3-dimensinal back-of-hand and fingerprint overlays

APPLIED DEFEAT EVALUATION

The evaluation methodology was applied to four *high-quality* biometric devices. Each item came from different manufacturers, and each used various image scanning and capture techniques. Three devices were fingerprint readers, with one using Radio Frequency (RF) ultrasonic sensing device and contained within a metal housing. The other two fingerprint readers used optical sensors. The fourth reader was a back-of-hand near-infrared optical sensor. Three of the readers used some form of live detection, either embedded into the platen or within the sensor algorithm. Two of the four readers used a remote sensor captured device and discrete control board. The control boards generally contained power supply input, sensor power, reader interface, output relay and door open output.

DEFEAT EVALUATION RESULTS

The following defeat vulnerability results were obtained from the various biometric readers.

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, three of the four devices proved to be robust in their ability to resist such brute force attacks. However, one of the devices could have its cover pried off with a screwdriver. Moreover, all four 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 three devices, the cover's anti-tampers could be bypassed with limited technical capability.

In two of the four 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. Two of the four devices came in two discrete components, with the sensor platen reader and control board separate. The control boards contained 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 fours devices would attempt to read 2-dimensional replicated objects, although some required water misting to simulate and by-pass the live detection. Misting also resulted in two of the four readers having a denial-of-service; nevertheless, none of the three fingerprint devices could be defeated with 2-dimensional replicate; however, the back-of-hand would both enrol and validate inanimate objects i.e., cardboard (see Figure 5). In addition, one of the fingerprint readers would allow a replicated image to be enrolled and then read.

The use of replicated 3-dimensional fingerprint overlays, when placed on a invalid live finger, proved to be the most effective defeat method (see 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. Replicated fingers and back-of-hands proved ineffective.

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

RECOMMENDATIONS

Biometric readers are considered high-security and are being placed in critical infrastructure environments based on this perception. However, high security application should consider not only the external threat, but more importantly, internal or insider threat. As many past security breaches have demonstrated, when systems fail they are generally supported by an insider. Therefore, biometric readers are not an access control system panacea that many believe. Within the context of the study, the following biometric reader recommendations are put forward:

Optical systems provided a simpler user experience, with clear directions and greater feedback from the device when in use. Nevertheless, optical systems, both fingerprint and back-of-hand, were the most vulnerability to both 2-dimensional and 2-dimensional spoofing attacks. The ultrasonic fingerprint reader appeared the most secure, validating other published research from Dunstone and Yager, who stated that capacitive fingerprint sensor was a significant improvement over earlier optical fingerprint sensor (2009).

The majority of the biometric readers suffered physical vulnerabilities with their enclosures, ability to by-pass anti-tampers, gain access to door control relays and in general, by-pass the whole access control biometric system. It is suggested that manufactures appear to focus their design energies on the sensor and user experience, neglecting the reader as a whole.

The biometric readers that used an external controller were in general less vulnerable to by-pass attack, as access to such aspects as door relays were removed. Nevertheless, this is subject to the controller being located within the secure area and within an appropriate anti-tamper proof enclosure. For example, one controller contained no anti-tamper device and the other controller's anti-tamper device could be easily defeated.

An awareness of the vulnerabilities and limitations of biometric readers need to be propagated. Biometric readers should not be considered high-security by default, as many suggests. As this study has demonstrated, most of the readers had some inherent vulnerability that was not difficult to exploit, in particular, from an insider's perspective.

LIMITATIONS

The study has to be considered within the context of a number of limitations. These limitations included a non-random sample size of biometric readers, restricted sample size from each image extraction technology and a relative small false acceptance rate (FAR) measure. Nevertheless, the biometric readers were considered *high-quality* devices that have been used in some critical infrastructure and high security environments.

CONCLUSION

The article has presented a defeat evaluation methodology for the testing of biometric systems, applied against four *high-security* readers. The evaluation methodology proposed a staged process, with testing comprising of a commercial evaluation, performance testing and finally, defeat testing. Defeat evaluation was the prime focus of this study, divided into both physical integrity and technical integrity. Defeat evaluation attempted to seek and examine vulnerabilities within the biometric devices, their sensor and the device as a whole.

Each tested biometric fingerprint reader device had some degree of vulnerability, with some of these being quite simple physical security failures. Physical defeat evaluation demonstrated that attackers were able to gain entry into the internal circuitry of all four readers, with two readers having their anti-tampers bypassed and access to the output door relays. Technical integrity testing demonstrated that two of the readers could be defeated with an

enrolled 2-dimensioal spoof and that these readers could also be spoofed by a 3-dimensional false reliant overlay, with all *live detection* being spoofed.

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

REFERENCES

Australia Security Magazine (2008). *ASM Headlines: More ID please*. Brisbane: Author.

Biometric Authentication. (n.d.). Biometric authentication: What method works best? Retrieved September, 28, 2009, from http://www.technovelgy.com/ct/Technology-Article.asp?ArtNum=16

Brooks, D. J. (2009). *Defeating biometric fingerprint systems: An applied testing methodology*. Proceedings of the 2nd Australian Security and Intelligence Conference, Perth, School of Computer and Security Science.

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

Dunstone, T., & Yager, N. (2009). *Biometric system and data analysis: Design, evaluation, and data mining*. Eveleigh, New South Wales: Springer.

Institute of Electrical and Electronic Engineers. (2010). IEEE Certified biometric professional. Retrieved August, 20, 2010, from www.ieeebiometricscertification.org

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

Jain, A. K., Ross, A., et al. (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*.

Khairallah, M. (2006). *Physical security systems handbook: The design and implementation of electronic security systems*. Oxford: Butterworth Heinemann.

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

Matsumoto, T., Matsumoto, H. et al. (2002). *Impact of artificial "gummy" fingers on fingerprint systems*. Proceedings of SPIE: Optical and Counterfeit Deterrence Techniques IV.

Peterson, J. K. (2000). *Understanding surveillance technologies: Spy devices, their origins and applications*. Boca Raton: CRC Press.

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. *The Handbook of Security*. M. Gill. 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).

Thalheim, L., Krissler, J., et al. (2002). Bodycheck: Biometric access protection devices and their programs put to the test. *C'T* (114).

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

Uludag, U., & Jain, A. K. (2004a). *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.