BIOMETRIC ATTACK VECTORS AND DEFENCES

Chris Roberts
September 2006

Table of Contents

Key Words

Biometric, identification, security, attack vector, threat, countermeasures, defences.

Abstract

Much has been reported on attempts to fool biometric sensors with false fingerprints, facial overlays and a myriad of other spoofing approaches. Other attack vectors on biometric systems have, however, had less prominence. This paper seeks to present a broader and more practical view of biometric system attack vectors, placing them in the context of a risk-based systems approach to security and outlining defences.

Introduction

Structure of this Paper

This paper contains the following:

- An introduction to the topic of biomentric attack vectors;
- A brief review of previous models and a suggested new approach;
- An outline of the risk context; and
- A description of defences and countermeasures.

Definitions

For the purposes of this paper an *attack vector* is defined as the channel, mechanism or path used by an attacker to conduct an attack or to attempt to circumvent system controls. A *threat* is the possibility of an attack. *Spoofing* is the presentation of an artefact, false data or a false biometric claiming to be legitimate, in an attempt to circumvent the biometric system controls. A system *vulnerability* is a design flaw or feature that creates a security weakness and presents an opportunity for attack or exploitation of the biometric system.

Problem Outline

The majority of reported biometric systems incidents are related to spoofing. While some attempts have been made to represent a more complete view of attack vectors, successive representational models have become increasingly complex with decreasing practical application. Practitioners and information security professionals will seek structured and practical representations that correlate with existing methods and approaches to risk and security management. This paper presents such an approach.

Preamble

Biometrics are increasingly being used for security and authentication purposes and this has generated considerable interest from many parts of the information technology community. There has also been a great deal of interest from those interested in examining and researching methods of circumventing and compromising biometric systems.

In common with all security systems, there have been attempts to circumvent biometric security since they were introduced. Designing secure systems can be challenging and it is important to assess the performance and security of any biometric system in order to identify and protect against threats, attacks and exploitable vulnerabilities. Security breaches are, most commonly, the result of an exploited vulnerability[1]. This includes poor physical security which continues to be an easily exploitable attack vector.

Often these vulnerabilities were not considered or had been discounted as implausible in systems design and management. It is, therefore, important to adopt a systems approach and assess *all* risks as failing to assess any one aspect can lead to a catastrophic failure of system security.

Biometric Spoofing History

An early report into fingerprint devices and their susceptibility to acceptance of "lifted" fingerprints or fake fingers, was published by Network Computing in 1998[2]. They found that four out of six devices tested were susceptible to fake finger attacks.

Further research was undertaken by Tsutomu Matsumoto who published a paper on "gummy" fingers in 2002[3]. In this research, finger sleeves were made from gelatine, designed to cover a fingertip and with a fingerprint on the outer surface. In testing, these had a high acceptance rate from fingerprint readers using optical or capacitive sensors. In addition, fake fingers could be enrolled in the system (68 to 100% acceptance).

In November 2002 c't magazine[4] published the results of the testing of a variety of biometric devices. A number of spoofing attacks were successful, as were "man-in-the-middle" attacks on datastreams. Tests were conducted on fingerprint, facial recognition and iris scan biometric devices. The facial recognition devices were spoofed by playing back a video of a person's face. Iris scanners were spoofed with a high resolution photograph of an iris held over a person's face and with a hole cut in the photograph to reveal a live pupil. Another method of spoofing iris scanners is to replay a high resolution digital image of the iris.

In August 2003, two German hackers claimed to have developed a technique using latent prints on the scanner and converting them to a latex fingerprint replacement, small enough to escape all but the most intense scrutiny[5]. This method uses graphite powder and tape to recover latent prints which are digitally photographed, and the image enhanced using graphics software. Where complete fingerprints are not available, the graphics software is used to compile a fingerprint from overlapping portions recovered from the scanner. The image is photo-etched to produce a three-dimensional reproduction of the fingerprint. This etch is then used to as a mould for the latex fingerprint.

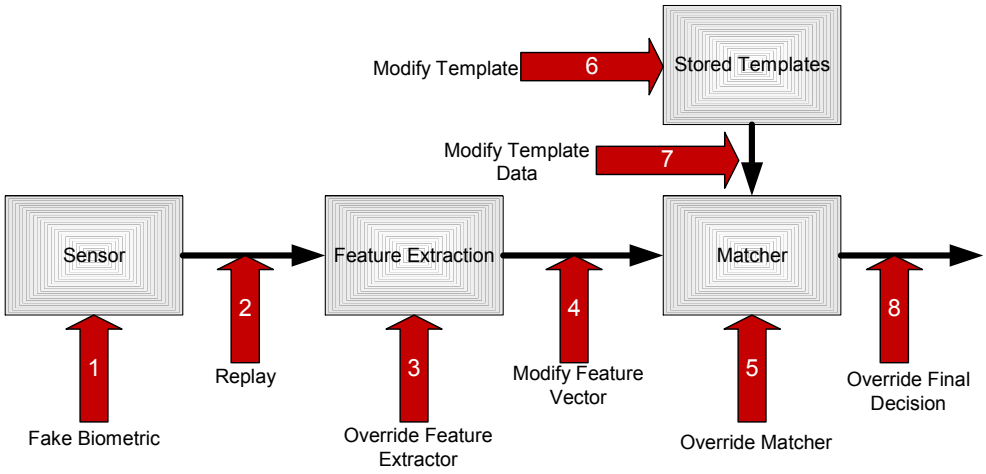
More recently (December 2005) research undertaken at Clarkson University revealed that it was possible to demonstrate a 90% false verification rate in the laboratory[6]. This included testing with digits from cadavers, fake plastic fingers, gelatine and modelling compounds. However, when "liveness" detection was integrated into the fingerprint readers, the false verification rate fell to less than 10% of the spoofed samples.

Much of the activity in spoofing biometric systems has, up until now, been confined to researchers. However, as biometric systems become more widespread, the incentives to misuse or attack biometric systems will grow. Understanding the nature and risk of such attacks it will become increasingly important to systems architects administrators and security managers.

Previous Models

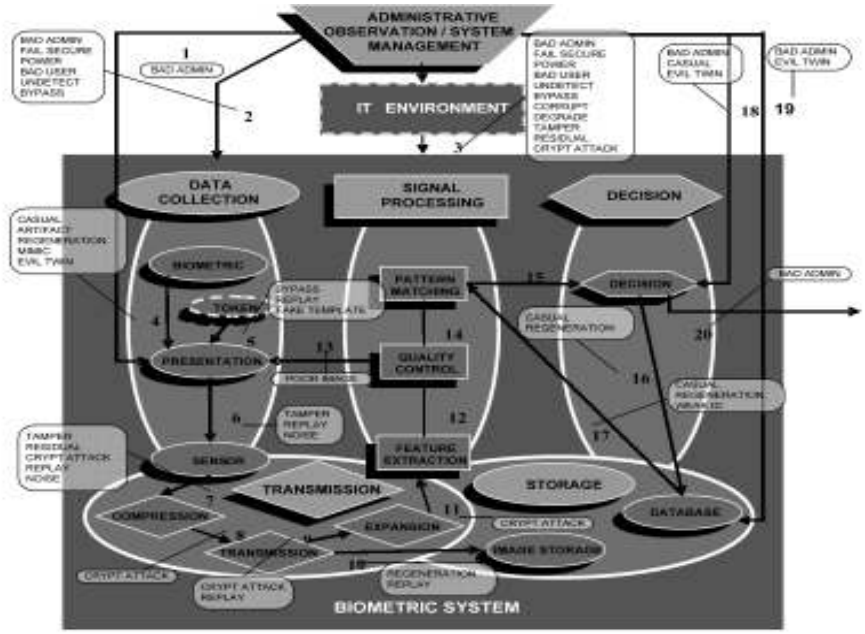
There are a number of points or vectors where a biometric system can be attacked. While the fake biometric attack has attracted the greatest publicity, other attacks require some form of access to the biometric processing systems and perhaps represent a more significant risk. Some of the early work by Ratha *et al*[7] identified eight possible points of attack, see Figure 1 below:

Figure 1: Ratha's Framework



Work by Jain *et al*[8] sought to refine this approach. Further work by Wayman[9] focused on technical testing of biometric devices and identified five subsystems, allowing a more refined analysis of potential attack vectors. Bartlow and Cukic[10,11] extended this research in a framework combining elements of previous work and adding three components: administrative supervision, IT environment and token presentation. The resultant framework identified 20 potential attack points with 22 vulnerability possibilities. See Figure 2 below:

Figure 2: Bartlow and Cukic Framework



A Practical View

Attempting to illustrate attack vectors using the frameworks referenced above presents considerable challenges due to the multi-dimensional nature of attacks. These models have become increasingly complex and consequently their utility for practitioners has been reduced.

These models have also not fully accommodated risk-based approaches adopted by many organisations. In order to simplify the analysis of risk of attacks on biometric systems, three dimensions are examined, each of which can be separately analysed for risk. Appropriate risk-reduction and countermeasures can then be selected to manage the risks identified. Finally the separate risk analyses can be merged to develop a system protection profile.

With adaptation, this approach may also be usefully applied to other technology systems, its utility not being confined to biometric systems.

Threat Dimensions

There are three key dimensions of systems attacks, each of which may require different treatment. These are:

- Threat agents;
- Threat vectors; and
- System vulnerabilities.

Given the complexity of interactions and the difficulty in illustrating all three dimensions in a single diagram, this paper presents each attack dimension separately. This approach assists in rationalising defences as countermeasures can then be grouped in several ways, thus facilitating system management. This approach also facilitates the assessment of risk associated with the threats and threat vectors.

Threat Agents

An attack is conducted by a *threat agent*, which is defined as an person who, intentionally or otherwise, seeks to compromise the biometric system. There are three categories of threat agents[12] which are listed below:

- Impostor: any person who, intentionally or otherwise, poses as an authorised user. The impostor may be an authorised or an unauthorised user.
- Attacker: any person or system attempting to compromise the biometric device or system. Motivation may include unauthorised entry or denial of service.
- Authorised users: any person or system authorised to use the biometric system but who may unintentionally compromise the biometric device or system. This category caters for unintentional and human error, such as an administrator error in configuring a system.

Threat agents generally have some degree of technical skill. At the lower end of the risk scale, threat agents may lack specific system knowledge and be poorly funded. A greater threat are the those skilled, knowledgeable and well-funded threat agents.

Understanding the types of threat agents can assist in developing effective protection measures. It is regularly demonstrated that authorised users and insiders pose as much, or more of a threat than unauthorised users. For example, the 2005 New Zealand Computer Crime and Security Survey reported that[13] of the organisations who had experienced incidents, 60% experienced incidents from *outside* the organisation but 70% experienced incidents originating from *inside* the organisation. Other surveys have reported similar observations[14]. These surveys do not differentiate the type of threat agents.

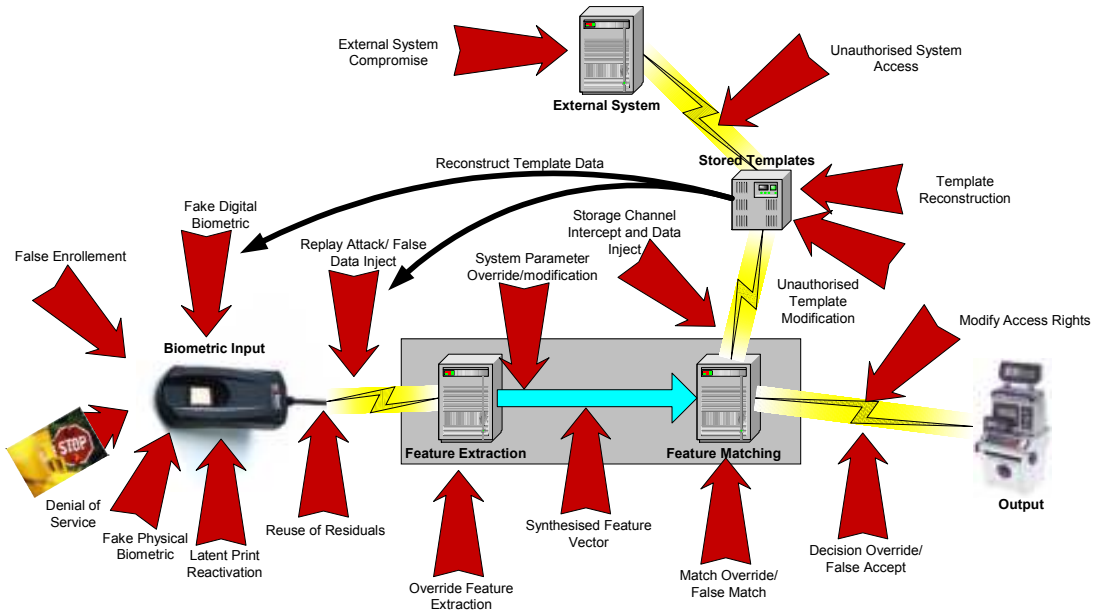
Collusion and Coercion

Associated with threat agents is collusion and coercion where legitimate users are pressured in some way, to provide their biometric and access privileges. This can range from social engineering and promises of payment or some other reward to threats of exposure to some real or imagined offence (blackmail). Often reputations can be irrepairably damaged by allegations, however unfounded, and this is a powerful weapon in coercion.

Threat Vectors

Threat vectors are the points at which a system can be attacked and are illustrated in Figure 3 below. This illustration of threat vectors has been adapted from the Biometric Device Protection Profile published by UK's CESG[15] and the Study Report on Biometrics in E-Authentication by INCITS[16]. Threat vectors are then individually described.

Figure 3: Threat Vectors



Denial of Service

Denial of Service (DoS) attacks are perhaps the crudest of threat vectors. They range from physical damage or power loss to system attacks designed to corrupt or incapacitate the biometric system. Introducing adverse environmental conditions such as heat, light and dust can degrade the performance of sensors and the quality of data. Other forms of attack, such as introducing electrical or radio frequency contamination can also adversely affect data quality. Specific examples may be the use of portable strobe lights against optical sensors, spillage of liquid on sensors and introducing large static electricity charges.

DoS attacks are generally "noisy" in that they are noticed quickly. In some cases, however, the intent is to have the attack noticed in order to create confusion and alarm and force the activation of alternative or exception handling procedures. Seldom used or exercised alternative or backup procedures will, almost inevitably, present greater opportunity for system compromise and are themselves a threat vector.

False Enrolment

The accuracy of the biometric data if founded on legitimate enrolments. If identity is faked, the enrolment data will be an accurate biometric of the individual but identity will be incorrectly matched. This threat vector is seen in other systems, for example, passport applications. Once registered, the system will validate a false identity, and with it any access privileges.

Fake Physical Biometric

Perhaps the threat vector that has the greatest prominence when biometric systems are discussed is spoofing or providing a fake physical biometric designed to circumvent the biometric system. The history of biometric spoofing has been outlined in the introduction to this paper.

This attack can be relatively easily conducted as little or no technical system knowledge is required. The materials for the creation of false biometrics are generally cheap and easily obtainable. Another factor is that these attacks are conducted at the point of entry to the system so many of the digital protection mechanisms, such as encryption and the use of digital signatures, are not effective. Many biometrics (including fingerprints, hand and iris) are subject to this form of attack.

The original biometric can be relatively easily obtained from many sources, with or without the permission and co-operation of the "owner" of that biometric. We leave extensive biometric traces, such as fingerprints and hand prints, on desks, doors, utensils and many other surfaces. Today's digital camera and digital recording technology has made the acquisition and processing of images and voice recordings a trivial task.

Fake Digital Biometric

A fake digital biometric can have two components outlined below:

- False data using commonly available biometric data such as digital facial images or digitised latent fingerprints. These are sometimes known as masquerade attacks.
- A replay of reference sets. A reference set replay attack takes place *inside* the biometric system and digital defences are more effective here. In addition, the attackers require knowledge of the biometric system and usually also require system access.

Latent Print Reactivation

This threat vector is peculiar to fingerprint and palm print scanners. The oils from sweat glands in the skin and residue from touching a variety of surfaces will leave a latent print on the surface of the biometric sensor. These latent prints can be copied or reactivated into readable prints through a range of techniques including powder, the fumes from cyanoacrylate glue, or placing a plastic bag contain warm water over the print.

Reuse of Residuals

Some biometric devices and systems may retain the last few biometrics extracted and templates used in local memory. If an attacker gains access to this data, they may be able to reuse it to provide a valid biometric. Clearing memory and prohibiting identical samples being used consecutively is an effective defence.

Replay Attacks/ False Data Inject

This category also covers man-in-the-middle attacks. Here the data related to the presentation of a biometric is captured and replayed. Alternatively a false data stream is injected between the sensor and the processing system. In most cases this will involve some physical tampering with the system. Where templates are stored on an RFID or proximity card, the data is likely to be unencrypted. This can facilitate the unauthorised collection of the data for later replay.

A replay attack is a two or three-stage process, first intercepting or copying the sensor transmission, then possibly modifying the data and finally replaying the signal. Transmission encryption adds a layer of complexity and is an effective defence as the captured signals may be difficult to identify and also must be decrypted, modified and then re-encrypted before replay. Decrypting and re-encrypting data may require the use of specialised tools and the possession of advanced technical skills.

This is also a threat vector for the injection of false data into the biometric system, bypassing the sensor. It is also possible the attacker will automate the intrusion, such as in a 'hill climbing" attack (see below).

Synthesised Feature Vector

A data stream representing a fake biometric is injected into the system. One approach to generating acceptable data is described as "hill climbing"[17,18] . This technique iteratively changes the false data, retaining only those changes that improve the score until an acceptable match score is generated and the biometric system accepts the false data. This technique requires access to the system's match scores and communication channels.

Override Feature Extraction

This attack interferes with the feature extraction routines to manipulate or provide false data for further processing. Alternatively, this attack can be used to disable a system and create a DoS attack. This is usually conducted through an attack on the software or firmware of the biometric system.

System Parameter Override/Modification

This threat vector modifies the FAR/FRR or other key system parameters. Adjustments to the system tolerances in feature matching, in particular the false acceptance rate (FAR), can result in system acceptance of poor quality or incorrect data. The US Department of Defense recommends an FAR no greater than 1 in 100,000 and a False Rejection Rate (FRR) no greater than 5 in 100[19] for their biometric systems.

Match Override/False Match

This threat vector could attack software, firmware or system configuration and parameters. Templates are generally unencrypted when undergoing feature comparison and are more susceptible to tampering. The matching decision could be overridden or ignored and replaced with a match. Authorised users are unlikely to notice any anomaly as the system may continue to provide them access.

Storage Channel Intercept and Data Inject

Perhaps the attack with the most significant consequences, this attack can compromise both the processing system and any data stored. If the attacker has system access, storage is an easier target as templates are smaller and the data sets less complex than unprocessed biometric data. Examples include the capture of a legitimate template for later use and the injection of a false template. This is an ideal entry point from which to conduct "hill climbing" attacks. Successful attacks usually require specific system and template knowledge.

Unauthorised Template Modification

Templates can be stored on the biometric reader or sensor, on an access card or token or within the biometric system itself. In this threat vector, unauthorised changes are made as templates are modified, replaced or added to the system. Adding an unauthorised template can circumvent any registration procedures and real (but unauthorised) biometrics can be presented and processed by the system alongside legitimate biometrics. A denial of service can be created by corrupting template data or associating users with a modified template. Finally, accidental corruption from a DoS attack, system malfunction or administrative error can also damage template integrity. Loss of template integrity can subvert the identification or authentication processes.

Template reconstruction

One aspect is similar to the synthesised feature vector attack where "hill climbing" techniques are used to generate acceptable data. Another form of a template reconstruction attack is scavenge file fragments from data storage. In both these situations, access to the data store is required.

Decision Override/False Accept

This is a form of bypass attack which ignores any processing and overrides the decision data or injects a false acceptance between the system and the end device (for example a door lock or a cash dispenser). In this case the decision criteria is *accept/accept* in all cases. This may involve some form of physical tampering.

Modify Access Rights

An unauthorised change to a user's access rights can create a DoS attack when rights are curtailed or alternatively breach security when rights are increased. It is generally achieved by obtaining system administrator rights to enable access to user privileges and other key system parameters and data.

System Interconnections

Interconnection with other systems presents at least two more threat vectors, unauthorised (external) system access and external system compromise. If the interconnected system is compromised, it provides an attack vector for the biometric system. Similarly the communication channel between the systems is open to threat. Often there is little control by the operators of the biometric system over the operation of the external system.

System Vulnerabilities

Defects in system design, architecture, production or implementation can all introduce vulnerabilities to biometric systems. In some cases "secondary" systems may be integrated into the biometric system and which, if compromised, could leave the biometric system open to exploitation or attack. There are five important areas where vulnerabilities may occur:

- Operating systems (server, workstation);
- Storage management systems (operating system and application);
- Biometric applications;
- Sensor software;
- Hardware/firmware.

Other key aspects that can be conveniently categorised here include:

- Operations management,
- Remote management (particularly of FAR/FRR parameters); and
- Systems configuration.

These system vulnerabilities are common to many technology systems and have been addressed in some detail in other discussions. It is important to recognise, however, that a system vulnerability can present opportunities for system compromise and the effects can be as equally debilitating as the threat vectors described above.

Defences

Risk-based Approach

While it is an axiom that defences should be selected for their effectiveness, the criteria for selection are much more difficult to determine. Risk assessment and management frameworks and approaches have been shown to be effective tools in this selection process. The threat dimensions described above are consistent with many of the accepted risk frameworks such as the AS/NZS 4360: *Risk Management* standard[20], the Treasury Board of Canada Secretariat's (TBS) *Integrated Risk Management Framework* (IRMF)[21] or the US National Institute of Standards and Technology's *Risk Management Guide for Information Technology Systems*[22].

The consideration of threats, in relation to risk, provides a threat model which can be used as the basis for architectural designs, information security policy enhancements and security testing plans. Risk analysis is becoming more important as:

- Interfaces are standardised;
- Specifications and standards become widely available;
- Threats to information systems increase;
- Consequences of system compromise increase; and
- Governance requirements are enhanced.

It is important to recognise that no system can be completely secure and no one single defensive mechanism will comprehensively protect a system. It is also important to recognise that few defensive systems are able to withstand sustained and determined attacks. A risk-based approach to defending systems will allow prudent and pragmatic measures to be identified and can also demonstrate good governance practices and a selection of complementary defences can effectively reduce risk to acceptable proportions.

The vulnerability/robustness ratio of a system can be determined by measuring residual risk, which is generally inversely proportional to the effectiveness of security measures applied.

Systems and Security Architecture

The two basic architectural decisions in biometric systems are the locations of the biometric matching operations and the template storage. Combined with systems elements, this provides 16 possible architectures[23]. There are also storage alternatives such as Network Attached Storage (NAS), Storage Area Networks (SAN) and other storage arrays. Adding these elements provides 20 possible architectures, each of which should be assessed for risk, threat, vulnerability and then appropriate defensive measures selected.

Table 1: Architectural Combinations

Storage Location	Matching Location
NAS/SAN/Storage Array	
Central/distributed (local server)	Server
Local workstation (client)	Local workstation (client)
Device (peripheral)	Device (peripheral)
On-Token	On-Token

Good practice incorporates proof of concept validation, prototyping and security testing to determine if the architecture and defensive measures selected will provide the required levels of residual risk in the biometric system.

Specific principles incorporated into architectural designs should include the use of "least privilege" and any design should also follow recognised good practice (see *Policy* below).

Defensive Measures

There are a number of defensive measures that can be taken to minimise the risk of the threat agents, threat vectors and vulnerabilities described above. As with many defensive measures, these are complementary and security should not rely on a single method. Defences can be grouped into six categories and within these groups there are several relevant defensive measures[24,25,26]. These are illustrated in Table 2 below:

Table 2: Defensive Measures

	Input device protection	Input data protection	System data protection	Data Storage	System tamper resistance	Secure communications
Challenge/Response	✓	✓	✓	✓	✓	✓
Randomising input biometric data		✓	✓		✓	
Retention of data		✓	✓		✓	
Liveness detection		✓	✓		✓	
Use of multiple biometrics		✓	✓		✓	
Use of multi-modal biometrics		✓	✓		✓	
Use of multi-factor authentication		✓	✓		✓	
Use of "soft" biometrics			✓		✓	
Signal and data integrity and identity		✓	✓	✓	✓	✓
Encryption and digital signatures		✓	✓	✓	✓	✓
Template integrity			✓	✓	✓	
Cancellable biometrics			✓	✓	✓	
Hardware integrity	✓	✓	✓	✓	✓	
Network hygiene	✓	✓	✓	✓	✓	✓
Physical security	✓	✓	✓	✓	✓	✓
Activity logging, policy & compliance checking	✓	✓	✓	✓	✓	✓

Challenge/Response

Challenge/response is a technique well-established in protective security. Many will recall or will have used the "Halt! Who goes there?" challenge with a password or pass phrase given in response to the challenge. Today we see this technique applied in many on-line transactions and interactions, such as Internet banking and with utility, credit card and retail organisations. Typically some private reference data is incorporated into the account or transaction set-up and is later used to verify account holders. A classic example is mother's maiden name, although this is well known and an essential piece of information for social engineers seeking to spoof identities.

Challenges can be issued in response to some other “trigger” such as liveness detection failures, lack of movement or changes during the biometric acquisition phase. In biometric systems, users can be challenged, for example, to repeat a particular phrase, blink their eyes, nod heads or present specific fingers to the sensor.

Challenge/response can not only be used between the user and the biometric system but also between components of the system. Sometimes described as mutual authentication, it can be an effective defence to replay and data injection attacks, particularly for remote sensors and data storage or other systems components which are separated geographically.

Randomising Input Biometric Data

A variation of challenge/response is where users are required to enroll multiple biometric samples, such as several fingerprints. Verification will then randomise the sample requested thus adding complexity to any attempt to circumvent the biometric authentication. Such systems may also require multiple biometrics for verification, again adding complexity as any such attempt to circumvent the biometric system will have to prepare several "target" biometrics. This will also assist in defeating attempts to reuse, for example, latent fingerprints on the fingerprint reader.

Retention of Data

Generally sensors are easier to physically access than other biometric system components and are thus more susceptible to attack. In addition, some sensors can store data and copies of templates locally, making them an attractive target.

In most biometric systems, image data is discarded after template generation. Retaining image data may provide a means of resolving spoof claims, although this adds system complexity in dealing with privacy and other storage protection challenges. Clearing data and data buffers is a defence against “man-in-the-middle” attacks and forces an impostor to create data that appears as a biometric sample to the naked eye as well as to the system.

Liveness Detection

A key defence to spoofing is “liveness” detection to ensure the biometric sample presented to the reader is from a live person and is not artificial or from a cadaver. Some liveness tests are based on autonomic responses and other can use a challenge/response construct such as blinking an eyelid on command. Liveness detection methods can be incorporated into the biometric reader or can be generated by a separate device. Detection methods include:

- Measurement of finger perspiration patterns;
- Pulse oximetry where pulse and blood oxygenation are measured by shining a beam of light through the finger tissue;
- Skin spectroscopy, which measures the absorption of light by tissue, fat, and blood and melanin pigment;
- Photonic and spectrographic measures incorporated into iris recognition;
- Thermal measurement;
- Head, face, eye and pupil movement;
- Synchronising lip movement with voice;
- 3-D feature information; and
- Printing (dot matrix) and print dye detection.

The use of 3-D feature information is considered to improve systems performance against pose and expression variations and changing environmental conditions, such as light and heat[27]. 3-D increases the complexity of the data set by incorporation of subtle variations, particularly in facial images, thus making spoofing extremely difficult. An added advantage is that liveness detection incorporates a non-repudiation element as the user has difficulty in denying that they presented the biometric where there is no evidence of system compromise.

Multiple Biometrics

Multiple biometrics increases processing time and adds a level of complexity if more than one biometric is required, for example, a fingerprint and an iris scan. Clearly it is much more difficult to spoof multiple and different biometrics. The requirement for multiple biometrics, however, also adds complexity to the authentication system with requirements, such as, multiple sensors.

Multi-Modal Biometrics

Multi-modal techniques are an evolution of multiple biometrics. They can operate using multiple representations of a single biometric or consolidation of multiple features into a new template. Most sensors today will take multiple readings, alternatively, multiple sensors can be used. Processing can range from simple averaging to weighted feature averaging in order to generate match scores. A third technique is to allow biometric sub-systems to individually generate match scores and use majority-voting.

Multi-modal biometrics can assist in improving data quality, precision and integrity, the improved accuracy thus defending against spoofing. It does, however, carry a computational overhead and adds complexity to biometric systems.

Multi-Factor Authentication

Again similar in concept to randomising data and the use of multiple biometrics, the use of multi-factor authentication, such as a requirement for smart cards, tokens, PINs and passwords, can provide a powerful deterrent to spoofing. It can, however, increase processing time and may reduce the convenience of biometric systems. An attempt to circumvent the biometric system would need both the biometric and the second authentication factor. Multi-factor authentication can be combined with a challenge/response mechanism, further increasing the complexity for any attacker.

“Soft” Biometrics

“Soft” biometrics are biometric characteristics which, in themselves, are not sufficiently distinctive to differentiate individuals but in combination provide sufficient data for accurate identification. Examples include age, gender, height, weight, ethnicity and distinctive markings (scars, marks and tattoos). These are the characteristics by which humans identify each other.

This is a defence against spoofing when use in combination with other biometrics. It may also improve systems performance by reducing search times in large biometric databases.

Signal and Data Integrity and Identity

An important component of system integrity is reliable data. Data generated at the sensor must be reliable and it should pass through the various stages of comparison and processing with integrity. This is a key defensive mechanism against replay and man-in-the-middle attacks.

Defensive techniques include:

- Time-stamping of the signal between the sensor and the rest of the system. Time stamping, when compared to system clocks or current time, may indicate the use of old or replayed data.
- Use of digital signatures.
- Use of steganography or data hiding[28]. This technique embeds critical data inside another data stream or embeds one biometric data inside another biometric data stream. Such data may include, for example, digital certificates.
- Use of data "watermarks"[29]. Again key authentication and verification data can be incorporated into the "watermark".
- Blocking matching attempts where false match thresholds or time periods are exceeded. For example, authorised users are unlikely to have high numbers of false matches in a given time period (with the majority in the morning and at lunch time). Setting limits on the number of attempted matches or number of failed attempts in a given time period, is an effective defence technique.

It is also important that related defensive measures, such as hardware integrity and encryption, are considered.

Cryptography and Digital Signatures

Encryption of data streams can be an effective defence against data interception and injects. Encryption of data "at rest", such as templates, can be an effective defence against data modification. Digital signatures also defend against data modification for both data in process and "at rest". Key management is an essential component in preserving the integrity of the encryption and digital signature systems. Encryption keys should be secured, preferably not on the biometric system.

Template Integrity

The ability to reconstruct biometrics from template data is a concern to privacy advocates and is a threat to template integrity. While many vendors view the template creation process as a one-way algorithm, researchers have shown it is possible to reconstruct sufficient elements from a template to constitute a recognisable biometric. Again "hill-climbing" techniques can be used to iteratively process template data in order to reconstruct a biometric[30].

A defence against hill-climbing techniques is the use of quantised match scores. This applies rounding techniques to match score calculations in order to minimise differences from small modifications to input images. It thus denies the hill-climbing attack sufficient useful data to identify match score improvements. Soutar[31] proposes limiting the precision of match scores to make hill-climbing attacks prohibitively time consuming. His research demonstrates unrestricted access to match score data enables a successful attack after a relatively small number of iterations. However, restricting the match score data allows recognition thresholds only after 10^{16} iterations. This technique limits the effectiveness of a hill-climbing attack.

Some researchers have demonstrated this defence can be defeated but requires extended access to the biometric system in order to be successful, thus increasing the risk of detection. For example, Adler[32] required 122 minutes to process 135,000 biometric comparisons on a PC. While attack techniques and computing power continue to improve, quantised match scores can, at the very least, introduce a significant delay to an attack.

Cancellable Biometrics

A characteristic of biometrics is that they are irreplaceable and once compromised, generally cannot be reused. A technique to allow reuse of original biometrics is described as cancellable biometrics[33]. This is a deliberate distortion based on a selected transform in which the presented biometric is distorted in the same way at each presentation. The transforms are designed to be non-invertible. Only the transformed data is stored and if this data is compromised, a new transform can be applied, thus replacing the original template.

Cancellable biometrics do not defend biometric systems against attack but will assist in recovery where templates or other biometric data have been compromised. Cancellable biometrics are, however, of little use where the original biometric or image has been compromised.

Hardware Integrity

This provides data validation linked to the originating sensor. It may include hardware device identification to generate a unique transaction identification and clearing of local sensor memory to avoid local storage of sensor data or templates. This can be combined with a challenge/response mechanism or even extended to mutual sensor/server authentication before communication is enabled. Ratha[34] *et al* proposed a pseudo-random challenge to the sensor, the response based on current sensor conditions such as pixel values at selected positions. The response is matched against the biometric data provided by the sensor. This is also a defence against replay attacks.

Network Hygiene

As with all technology, good network disciplines and hygiene are essential to the maintenance of system security. Many frameworks and best practice guides are available and apply equally to biometric as well as other technology systems. Examples include ITIL®[35], ISO 27005:2005[36] and COBIT®[37].

Physical Security

Many of the attack vectors described are more easily executed if the attacker has physical access to the biometric system. Physical security, as in many IT security systems, is often the cheapest and most effective deterrent to attempts to circumvent biometric systems. This ranges from physical restrictions to limit access to the biometric readers, to surveillance and guards. Supervised operation or the presence of guards can also defeat other attack types, such as coercion. The risk/reward considerations for attackers should also be factored into the use of physical security as the consequences of discovery and then detention (such as calling the local police), are a significant deterrent to sustained or physical attacks.

Regular inspection and cleaning of equipment is also important. Cleaning, for example, will not only sanitise the equipment for health reasons but also minimises the persistence of latent prints and may improve the performance of the sensor.

Physical security is a key defence in managing access to biometric systems and stored data, such as templates.

Other important physical protections includes items such as :

- Tamper switches on sensors and readers;
- Alarmed and locked panels for devices and communications interfaces (patch panels etc.);
- Protect cabling, in conduit if necessary. Pay particular attention to cabling in non-protected areas, such as ceiling or floor cavities;
- Monitored CCTV coverage for readers;
- Limited access to readers and sensors, including turnstiles or other forms of physical access control to limit numbers able to access sensors at any one time. This may assist in preventing "tail-gating" or " piggy-back" attacks where the biometric system is used to control access and entry.

Activity Logging

Where strong defensive measures are in place, determined attackers may conduct reconnaissance or run the attack over several days or even months, in order to gather sufficient information for a successful attack. Activity logging and pattern extraction can be a useful tool in identifying such reconnaissance or attacks.

In addition to activity logging and monitoring, biometric systems should monitor specific activities and related security events including:

- Communication errors from sensors and readers;
- False readings;
- Repeated failed authentication attempts.

Policy

Policy is the fundamental framework of security systems. It is a statement of expected behaviours in support of the organisation's objectives. Without a clearly defined security policy, organisations often lack direction, security measures are ineffective and perform below expectations[38] in relation to the security and integrity of their information systems.

Good policy, on the other hand, enhances security and will act as a deterrent to unwelcome, inappropriate and malicious behaviours.

There are several generally accepted standards and frameworks for the management of information security, issued by standards, professional and security organisations. These include:

- ISO 27001, *Information Security Management Systems*[39];
- BS 7799 Parts 1,2 & 3, *Information Security Management Systems*[40];
- ISO 15408, *Common Criteria*[41]
- Various NIST Computer Security Publications[42];
- COBIT®[43];
- IETF (RFC 2196, *Site Security Handbook*)[44];

Compliance Checking

Compliance checking and security assessments play a very important role in:

- Maintaining information systems security;
- Identifying and facilitating changes necessary to respond to rapidly changing technologies and threats.
- Demonstrating prudent governance of information systems; and
- Demonstrating compliance with legislation and regulation.

Good compliance systems support risk management systems and decision making. They have close correlation and are complementary to quality control systems. Some compliance tools, such as Nessus[45], can monitor technical compliance to assist in keeping systems current and patched against known vulnerabilities and also monitor systems against defined security policies.

In Conclusion

Much of the activity in spoofing biometric systems has, up until now, been confined to researchers. However, as the use of biometric systems become more widespread, the incentives to misuse biometric systems will also grow. The application of biometric systems in access control and authentication, coupled with uptake by the financial and banking sectors will undoubtedly see an increase in misuse and attacks on biometric systems.

This growth phenomena is not unique to biometrics and has been replicated in many other systems which seek to safeguard information and money.

An holistic approach should be taken when considering any biometric system. It is also important to ensure security is incorporated into the design and architecture from inception. This assists in properly understanding risks and appropriately selecting and implementing defences, in order to avoid those embarrassing and costly security breaches.

The approach presented in this paper accommodates organisational requirements to undertake risk-based analyses and systems security. It is a practical approach to the difficulty of analysing a multi-dimensional threat environment by allowing separate analysis of threat agents, threat vectors and system vulnerability. These separate analysis then draw together system defences, selected for their risk reduction properties, to produce a demonstrably risk-based system protection profile.

Endnotes

[1] Enhancing security and privacy in biometrics-based authentication systems N. K. Ratha, J. H. Connell, R. M. Bolle, IBM Systems Journal, Vol 40, No 3, 2001, http://domino.research.ibm.com/tchjr/journalindex.nsf/a3807c5b4823c53f85256561006324be/dd12e71773f23bcb85256bfa00685d76?OpenDocument

[2] Six Biometric Devices Point The Finger At Security, David Wills and Mike Lees, Network Computing, June 1, 1998, http://www.networkcomputing.com/910/910r1.html, accessed 29 January 2006

[3] Impact of Artificial "Gummy" Fingers on Fingerprint Systems, Tsutomu Matsumoto *et al*, January 2002, http://cryptome.org/gummy.htm, accessed 29 September 2005

[4] Body Check, Lisa Thalheim, Jan Krissler, Peter-Michael Ziegler, c't magazine, http://www.heise.de/ct/english/02/11/114/, accessed 05 February 2006

[5] Hackers Claim New Fingerprint Biometric Attack, Ann Harrison, SecurityFocus, 13 August 2003, http://www.securityfocus.com/print/news/6717, accessed 13 August 2006

[6] Clarkson University Engineer Outwits High-Tech Fingerprint Fraud, Clarkson University, 10 December 2005, http://www.yubanet.com/artman/publish/printer_28878.shtml, accessed 19 December 2005

[7] Enhancing security and privacy in biometrics-based authentication systems N. K. Ratha, J. H. Connell, R. M. Bolle, IBM Systems Journal, Vol 40, No 3, 2001, http://domino.research.ibm.com/tchjr/journalindex.nsf/a3807c5b4823c53f85256561006324be/dd12e71773f23bcb85256bfa00685d76?OpenDocument, accessed 1 September 2006

[8] Biometrics: A Grand Challenge, Jain *et al,* Michigan State University, http://biometrics.cse.msu.edu/icprareareviewtalk.pdf, accessed 05 February 2006

[9] J.L. Wayman, "Technical Testing and Evaluation of Biometric Devices", in A. Jain, *et al*, Biometrics - Personal Identification in Networked Society, Kluwer Academic Publisher, 1999, Michigan State University, http://www.cse.msu.edu/~cse891/Sect601/textbook/17.pdf#search=%22wayman%20%2B%20%22technical%20testing%22%22

[10] The Vulnerabilities of Biometric Systems - An Integrated Look and Old and New Ideas, Bartlow & Cukic, Technical report, West Virginia University, 2005

[11] Biomentric System Threats and Countermeasures: A Risk-Based Approach, Bartlow & Cukic, Biometric Consortium Conference, September 2005, http://www.biometrics.org/bc2005/Presentations/Conference/2%20Tuesday%20September%2020/Tue_Ballroom%20B/Cukic_Threats%20and%20countermeasures.pdf

[12] Biometric Device Protection Profile, UK Government Biometrics Working Group, Draft Issue 0.82 - 5 September 2001, http://www.cesg.gov.uk/site/ast/biometrics/media/bdpp082.pdf, accessed 13 August 2006

[13] 2005 Computer Crime and Security Survey, University of Otago, http://eprints.otago.ac.nz/342/01/2005NZComputerCrimeAndSecuritySurveyResults.pdf, accessed 8 September 2006

[14] CSI/FBI Annual Surveys, Computer Security Institute, 1996 to 2006, http://www.gocsi.com

[15] Biometric Device Protection Profile, UK Government Biometrics Working Group, Draft Issue 0.82 - 5 September 2001, http://www.cesg.gov.uk/site/ast/biometrics/media/bdpp082.pdf, accessed 13 August 2006

[16] Study Report on Biometrics in E-Authentication Ver 0.2, InterNational Committee for Information Technology Standards, February 2006, http://www.incits.org/tc_home/m1htm/2006docs/m1060112.pdf#search=%22%22Study%20Report%20on%20Biometrics%22%20%2B%20%22INCITS%20M1%2F06-0112%22%22, accessed 8 September 2006

[17] Biometric Template Security: Challenges And Solutions, Jain *et al,* Proceedings of the 13th European Signal Processing Conference 9EU-SIPCO), Antalya, Turkey, 2005, http://biometrics.cse.msu.edu/Publications/SecureBiometrics/JainRossUludag_TemplateSecurity_EUSIPCO05.pdf, accessed 3 September 2006

[18] Hill-Climbing and Brute-Force Attacks on Biometric Systems: A Case Study in Match-on-Card Fingerprint Verification, Martinez-Diaz *et al*, Universidad Autonoma de Madrid, http://fierrez.ii.uam.es/docs/2006_ICCST_HillClimbingAttackMoC_Martinez.pdf#search=%22%22hill-climbing%22%20%2B%20martinez%22, accessed 3 September 2006

[19] Biometrics Security Technical Implementation Guide Version 1, Release 2, Defense Information Systems Agency for the US Department of Defense, 23 August 2004, http://csrc.nist.gov/pcig/STIGs/biometrics-stig-v1r2.pdf, accessed 13 September 2005

[20] AS/NZS 4360:2004 Risk Management, Standards New Zealand, http://www.standards.co.nz, accessed 1 September 2006

[21] *Integrated Risk Management Framework* (IRMF), the Treasury Board of Canada Secretariat (TBS), April 2001, http://www.tbs-sct.gc.ca/pubs_pol/dcgpubs/RiskManagement/dwnld/rmf-cgr_e.pdf, accessed 1 September 2006

[22] Risk Management Guide for Information Technology Systems; Special Publication 800-30, National Institute of Standards and Technology, http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf, accessed 1 September 2006

[23] Study Report on Biometrics in E-Authentication Ver 0.2, InterNational Committee for Information Technology Standards, February 2006, http://www.incits.org/tc_home/m1htm/2006docs/m1060112.pdf#search=%22%22Study%20Report%20on%20Biometrics%22%20%2B%20%22INCITS%20M1%2F06-0112%22%22, accessed 8 September 2006

[24] Liveness Detection in Biometric Systems, Biometrics Information Resource, http://www.biometricsinfo.org/whitepaper1.htm, accessed 05 February 2006

[25] Biometrics Security Technical Implementation Guide Version 1, Release 2, Defense Information Systems Agency for the US Department of Defense, 23 August 2004, http://csrc.nist.gov/pcig/STIGs/biometrics-stig-v1r2.pdf, accessed 13 September 2005

[26] Biometric Device Protection Profile, UK Government Biometrics Working Group, Draft Issue 0.82 - 5 September 2001, http://www.cesg.gov.uk/site/ast/biometrics/media/bdpp082.pdf, accessed 13 August 2006

[27] Audio-Video Biometric Systems with Liveness Checks, Chetty and Wagner, University of Canberra, http://pixel.otago.ac.nz/ipapers/24.pdf#search=%22%22Audio-Video%22%20%2B%20Chetty%22, accessed 3 September 2006

[28] Hiding Biometric Data, Jain and Uludag, IEEE Short Papers, IEEE Transactions On Pattern Analysis And Machine Intelligence, Vol. 25, No. 11, November 2003, http://biometrics.cse.msu.edu/Publications/SecureBiometrics/JainUludag_HidingBiometrics_PAMI03.pdf#search=%22%22hiding%20biometric%20data%22%20%2B%20jain%22, accessed 8 September 2006

[29] Verification Watermarks on Fingerprint Recognition and Retrieval, Yeung and Pankanti, http://www.research.ibm.com/ecvg/pubs/sharat-water.pdf#search=%22%22verification%20watermarks%20on%20fingerprint%22%20%2B%20yeung%22, accessed 8 September 2006

[30] On the reconstruction of biometric raw data from template data, Manfred Bromba, Bromba GmbH , July 2003, http://www.bromba.com/, accessed 14 August 2006

[31] Biometric Systems Security, Colin Soutar, Bioscrypt Inc, , http://www.silicon-trust.com/pdf/secure_5/46_techno_4.pdf#search=%22%22Biometric%20System%20Security%22%20%2B%20%22Colin%20Soutar%22%22, accessed 3 September 2006

[32] Reconstruction of source images from quantized biometric match score data, Andy Adler, University of Ottawa, http://www.wvu.edu/~bknc/2004%20Abstracts/Reconstruction%20source%20images%20from%20quantized.pdf, accessed 25 November 2005

[33] Enhancing security and privacy in biometrics-based authentication systems N. K. Ratha, J. H. Connell, R. M. Bolle, IBM Systems Journal, Vol 40, No 3, 2001, http://domino.research.ibm.com/tchjr/journalindex.nsf/a3807c5b4823c53f85256561006324be/dd12e71773f23bcb85256bfa00685d76?OpenDocument

[34] Enhancing security and privacy in biometrics-based authentication systems N. K. Ratha, J. H. Connell, R. M. Bolle, IBM Systems Journal, Vol 40, No 3, 2001, http://domino.research.ibm.com/tchjr/journalindex.nsf/a3807c5b4823c53f85256561006324be/dd12e71773f23bcb85256bfa00685d76?OpenDocument, accessed 1 September 2006

[35] IT Infrastructure Library, Hompage, http://www.itil.co.uk/, accessed 10 February 2006

[36] ISO/IEC 27001:2005, Information technology -- Security techniques -- Information security management systems – Requirements, http://www.iso.org, accessed 10 February 2006

[37] COBIT®, Information Systems Audit and Control Association®, http://www.isaca.org/, accessed 10 February 2006

[38] Cybersecurity Operations Handbook, 1st Edition, Rittinghouse and Hancock, Elsevier Digital Press, 2003, ISBN 1-55558-306-7

[39] Information security management systems, International Organization for Standardization, http://www.iso.org, accessed 10 September 2006

[40] Information Security Standard, BSI Management Systems, http://emea.bsi-global.com/InformationSecurity/Overview/index.xalter, accessed 10 September 2006

[41] Evaluation criteria for IT security -- Parts 1, 2 & 3, International Organization for Standardization, http://www.iso.org, accessed 10 September 2006

[42] Computer Security Resource Center, National Institute of Standards and Technology, http://csrc.nist.gov/, accessed 10 September 2006

[43] COBIT®, Information Systems Audit and Control Association®, http://www.isaca.org/, accessed 10 September 2006

[44] Site Security Handbook, RFC 2196, Internet Engineering Task Force, http://tools.ietf.org/html/rfc2196, accessed 10 September 2006

[45] Nessus Vulnerability Scanner, Tenable Network Security, http://www.nessus.org/index.php, accessed 10 September 2006