Biometric Security Concerns

V1.0 September 2003

This document has been produce by the UK Government Biometrics Working Group (BWG). The BWG is operated by CESG, the UK Government Information Assurance Technical Authority

It is one of a series of documents addressing topics in biometrics aimed at providing informed advice to Government.

This document has been derived from work on biometric security by BWG members as part of the European Commission BIOVISION project. BIOVISION has developed a Roadmap to provide guidance to the Commission on future issues and research on biometrics in Europe to 2010.

Readers should note that the advice here carries no formal CESG endorsement and users should observe their departmental standards and practices regarding the implementation of biometric devices and systems.

Further information can be obtained by visiting the CESG: web site: www.cesg.gov.uk and clicking on the biometrics link.

Contents

Biometric Security Concerns

Overview

Many of the questions raised about the use of biometrics, particularly in connection with authentication, relate to the trust that can be placed in the biometric authentication process itself, or to the protection of the biometric data that is used by the system and which is private and personal to the users. It is this latter concern that marks out biometric systems as different from the traditional password, PIN and token based authentication technologies.

The aim of this document is to explore these issues in more detail, highlighting a number of commonly expressed security concerns, discussing the possible threats that they pose, and what can be done to eliminate or at least mitigate them.

Note that this document does not address the details of biometric technical security features and countermeasures.

Importance

The success that biometric technology and systems have in meeting the tough security challenges they face will be crucial in determining their suitability for use by government. Many government applications will demand high levels of trust in the authentication process and, in the era of “UK online” with widespread interaction with citizens, the privacy and data protection issues will assume major significance. For example, a user providing a fingerprint for the purpose of authenticating an e-vote will want to be assured that an impostor cannot masquerade as him/her, and that the data is not being supplied to a 3rd party (e.g. the police) for checking against a criminal database.

A Caveat

There is often a tendency to focus on a few specific issues when security is discussed. The subject of biometrics is particularly prone to this - the question: “what about spoofing?” usually surfaces quickly. This approach however runs the risk of overlooking the far more complex interplay of factors that determine effective security in real world applications.

System implementers and managers need a thorough understanding of all the security issues surrounding the application in order to determine the risk factors and levels.

They need to ensure that the technical, procedural and environmental measures work together to provide the appropriate level of security.

The following paragraphs highlight some of the main security concerns surrounding the use of biometric technology

1 Performance limitations

Biometrics do not provide perfect (unique) identification. The matching process is probabilistic and is subject to statistical error. A mistaken identification or verification where the wrong person is matched against an enrolled user is termed a *False Acceptance* and the rate at which these occur is the *False Acceptance Rate (FAR)*. Conversely, an error that occurs where a legitimate user fails to be recognised is termed a *False Rejection* and the corresponding rate is the *False Rejection Rate (FRR).* These errors are dependent not only on the technology but also on the application and the environment of use.

Note that FAR and FRR errors are influenced by numerous factors including:

- Uniqueness of biometric features
- Capture device
- Algorithm
- Environmental interference (lighting, noise etc.)
- User population (demographics, employment, etc.)
- User behaviour (attitude, cooperation etc.)

Both FAR and FRR errors may have security implications, the relevance of which will depend on the application.

Positive Verification Applications e.g. access control

False Accept errors represent a direct security threat that is roughly analogous with chance attacks against password/PIN systems. Suggested interpretation of security strength in terms of FAR are:

FAR	Strength
1 in 100	Basic
1 in 10000	Medium
1 in 1000000	High

False Reject errors are not a direct security threat though they may cause the system to be unusable if they are excessive.

Negative Identification Applications e.g. benefit system, citizen card

An important requirement for these types of applications is to guard against individuals enrolling more than once to establish multiple identities. At enrolment time, the biometric will need to be checked against previously enrolled biometrics to ensure that it is unique to the application. False Rejections may then become a security issue if, as a result of errors, individuals may establish multiple identities.

During normal use, False Accept errors may be a security issue as for positive identification/verification systems previously.

How do we Measure Biometric FAR and FRR?

- See “Best Practice” Biometric Testing (MS 11)

2 Enrolment integrity

Ensuring enrolment integrity is a vital underlying requirement for all authentication systems whether or not biometrics are used. If the enrolment integrity is compromised, all bets are off regarding security. System implementers will need to determine what credentials are necessary and sufficient to validate users prior to enrolment, and then to ensure that the enrolment process itself is secure – in most cases this will mean supervision by trusted trained staff.

[See UK Govt. Authentication Framework (NB v1 Dec. 2000 only)]

- Validation - is this a valid identity?
- Verification - is the registrant who they claim to be?
- Authorisation - is the registrant entitled to register?

3 Enrolment quality

The performance of biometric systems is dependent on the quality of the enrolled biometric. Enrolment quality can be affected by accidental or deliberate events and environmental conditions, and the result of low enrolment quality is almost inevitably poor system performance. If the performance is poor the security will be compromised, and there may be excessive dependence on the fallback system.

In the case of negative ID systems, poor enrolment quality will make it more likely that attempts to establish multiple identities will be successful, because biometrics that should match and trigger an alarm may in practice not do so. This is a direct security concern as it may undermine the principal intended functionality of the system. In the

case of positive ID systems, the false rejection rate will be adversely affected which may not be an immediate security concern. However, if this leads to an adjustment of the threshold to make the system work acceptably, the false acceptance rate will, in consequence, also be affected.

Countermeasures include - good enrolment procedures and trained administrators. Biometric systems should be able to check enrolment quality and reject poor quality enrolments.

4 Spoofing (physiological biometrics)

Spoofing through the use of artefacts is generally a concern for physiological biometric technologies such as fingerprint, hand, iris etc. Several studies dating from around 1998 have demonstrated the potential for successfully mounting a spoofing attack under carefully controlled conditions.

If spoofing attacks can be successful, the fundamental tenet of biometrics – the "something you are" – is undermined. Spoofing involves 2 stages: a) - the capture of a biometric "image" belonging to an enrolled user, and b) - transferring the biometric image onto an artefact.

Some features will be more difficult to observe and capture than others, and the skill needed to create a successful artefact will be dependent on both the biometric feature and how resistant the system is to artefacts. Faces are easily captured by photography. Fingerprint patterns may be captured through the lifting of latent or residual images left on smooth surfaces. Voices may be captured on tape or other audio recorder. Some biometric images will be difficult to capture, e.g. retinal patterns, without the use of sophisticated and conspicuous equipment. Of course, given cooperation by the legitimate user, the capturing of biometric features is likely to be much easier.

Constructing an artefact containing the biometric features is also subject to varying difficulty depending on the feature involved and the sophistication required of the artefact, which in turn depends on the countermeasures in place.

Spoofing attacks may be countered by technical and procedural countermeasures.

Technical solutions

Technically, the biometric system must be able to detect and reject the use of a copy of a biometric instead of the live biometric. This functionality is usually termed *liveness detection*, which refers to the ability of the system to distinguish between a sample feature provided by a live human being and a copy of a feature provided by an artefact. *Liveness detection* may be implemented by a combination of physical measures at the capture device where it interfaces with the human subject, and software

implemented as part of the image acquisition process. Note that there are 2 complementary approaches. One is the specific detection of known spoofs (e.g. silicon and gelatine fingerprint spoofs, photograph of face etc.). The other is to look for explicit signs of liveness in the presented biometric feature (e.g. temperature, humidity, pulse etc.). The principle of "simultaneity" will need to be observed. This is to ensure that the capture of the biometric and the measurement of liveness occur at the same point in space and time. Otherwise a live person might present live features to satisfy the liveness checks but also supply a fake biometric to spoof the verification process. It is unlikely that *liveness detection* will guarantee protection against sophisticated artefacts constructed to closely model human characteristics. The efficacy of the protection will need to be determined through a vulnerability assessment programme.

The barrier can be raised higher through the use of multi-mode biometrics (e.g. face and voice), through multi-factor authentication such as biometric and PIN, and through challenge/response mechanisms which utilise behavioural characteristics.

Procedural solutions

The sole procedural protection likely to be effective in combating the use of artefacts is supervision. It will be difficult for an impostor to use most artefacts if the enrolment and operational use of the system is supervised. However the use of some artefacts may be difficult to detect even with supervision, e.g. an artificial fingerprint pattern moulded on a thin laminate and attached over the top of a real fingerprint.

5 Mimicry (behavioural biometrics)

Mimicry is to behavioural biometrics what artefacts are to physiological biometrics. Through mimicry, an impostor attempts to "copy" the relevant biometric features of an enrolled user in order to fool the biometric authentication process. Because behavioural biometrics are applicable to the recognition of acquired, rather than inherited features, the features can also be acquired by an impostor.

The consequences of successful use of mimicry are likely to be the same as for spoofing previously) for given applications. Impostors are unlikely to attempt mimicry attacks against biometric systems that completely or predominately utilise physiological features (e.g. fingerprint, iris). Because mimicry may be perceived to be a low technology form of attack requiring a lower level of expertise, biometric systems employing behavioural biometrics may be subject to a higher incidence of attacks from a wider range of attackers.

As mimicry does not involve the use of an artefact*, liveness detection* is not generally applicable. Counter-measures should focus on the ability to distinguish between a genuine person and a mimicker. This could include improved technical performance (FAR/FRR), supervised operation and challenge/response features.

6 Latent/Residual images

Latency or residual images are a possible security concern that could occur in 2 forms:

- Physical residual biometric image, and
- Latency in internal memory. This could occur through a combination of failure to clear memory, and failure to detect and correctly action a "failure to acquire" (resulting in previous biometric image or template being passed to subsequent processing stage in error

[Note that we are not including latent images captured outside the system itself e.g. fingerprints lifted from a surface]

Latency or residual image problems can be addressed by correct system software design, and system maintenance (cleaning). This would form one subject for a security evaluation process.

7 Template integrity/confidentiality

Template integrity and confidentiality are distinctly different issues related to template data though similar solutions may be employed to deal with both problems. Template integrity is concerned with threats to the authentication process caused by planted or modified templates, whereas template confidentiality relates to the legal and privacy issues around the template data and the way in which the data could be misused.

Integrity

The integrity of the authentication process depends, among other factors, on the integrity of the template. If either the reference template or the "live" biometric sample is untrustworthy, the resulting authentication will be untrustworthy. Untrustworthy templates could occur for one or more of several different reasons:

- Accidental corruption due to a malfunction of the system hardware or software;
- Intentional modification of a bona-fide template by an attacker;
- The insertion of a biometric template corresponding to the attacker to substitute for the reference template of an authorised enrolee.
- The addition of a biometric template corresponding to the attacker to create a bogus "enrolment" on the system.
- The substitution of a biometric sample corresponding to that of an authorised enrolee in place of the live sample of the attacker.

Confidentiality

Biometric templates contain data that can be used to identify living persons. This means that their processing and storage on a biometric system are subject to legal constraints imposed by the European Data Protection Directive and its enactment in national legislation (the 1998 Data Protection Act in the UK). Other regulatory

mechanisms (e.g. Human Rights Act and Health and Safety legislation) may also be relevant. The primary concern is the privacy and protection of personal data and biometric applications will need to include adequate protection to comply with the legal requirements.

[It should also be noted that other stored or processed biometric data is also subject to legal constraint, e.g. biometric images]

Solutions

Biometric systems must employ appropriate template integrity and confidentiality protection. This could be through access control, to prevent unauthorised access to the templates, or through the use of cryptographic techniques. Note that digital signing of template data may be sufficient to protect the integrity, but not to protect confidentiality. Cryptographic protection may need to be combined with other techniques (such as time stamping) to protect against the reuse of stolen templates. Reference templates could also be marked (before signing or encryption) to distinguish them from live samples which may be converted to the same format as the reference template for matching purposes, in order to prevent the substitution of reference templates for live samples.

Technical solutions are available to problems of template integrity and confidentiality. However these solutions are not always implemented in products and systems, and security evaluation is needed to check for the existence, effectiveness and correct implementation of technical security features.

8 Capture/replay attacks

Capture/replay is the name given to attacks where the biometric signals from an enrolled user are captured at one place and time and replayed later (usually at the same place) in an attempt to fool the system that the enrolled used is present. Although this can arguably occur at many points in the biometric system, the terminology usually applies to electrical signals captured between the capture device and the rest of the system. It may be a particular problem where there is a large and unsupervised path between the 2 components such as a network connection.

Solutions

A number of technical and procedural solutions are available including:

- Physical security (tamper resistance and detection, guards, inspections etc)
- Data encryption with unique session keys/time stamping for communications paths
- Access control to stored reference templates
- Reference templates marked and signed

Again, security evaluation is needed to provide assurance of effective, correctly implemented solutions.

9 Biometrics do not provide absolute identification

There is sometimes a misapprehension that biometrics can provide absolute identification (e.g. of terrorists, criminals etc) as though the implementation of biometric systems will somehow solve the problem of a major terrorist attack.
Of course biometric systems can, at best, only identify/verify individuals who have been previously enrolled. Applications can use this functionality in various ways, for example to provide an alert when a stranger is detected (i.e. biometric features captured that do not correspond to an enrolled user). The feasibility and effectiveness of the application will depend on the technology, environment and other details of the implementation.

Biometric authentication only addresses part of the overall authentication framework. Non-biometric elements (pre-enrolment) are needed to establish absolute identity with the assurance standards needed for the application using acceptable credentials (e.g. birth certificate, peer endorsement etc)

10 Biometrics are not secret

Valuable assets are traditionally protected by secrecy, typically secret passwords. Biometric features are often readily observed and do not possess equivalent secrecy. They may also be captured with varying degrees of difficulty.

This is a variation on the spoofing concern. It is certainly true that the source biometric features are not secret, but the argument as expressed is based on an incorrect premise. In fact, biometric security does not depend on the secrecy of the basic biometric features (people readily rely on biometric identification in its human form in day-to-day use). Rather, it depends on the integrity of the authentication mechanism which, in the context of issue raised here, translates into the difficulty of capturing the biometric features of a target and then constructing an artefact that will spoof the system. This can be contrasted with a password which, once disclosed, is trivial to exploit.

11 Biometrics are not random enough

People are rather alike, and lack the true randomness that passwords can have. Lack of randomness means that it is harder to separate individuals by their characteristics and is easier to confuse them.

This is a concern that is hard to refute by theoretical analysis. In fact template sizes are usually much larger than password lengths, though this hardly constitutes a valid argument. Current knowledge of biometric algorithm behaviour and human feature randomness and variation does not permit theoretical analysis of biometric system performance.

The pragmatic approach is to use performance testing to explore the interaction of the human and system parameters and thence to determine the discrimination capability of the biometric system. The results are typically expressed in terms of statistical error rates such as FAR and FRR (see *Performance Limitations* previously). Managers planning to use biometric systems need to assess their error rate requirements and determine whether a biometric system can meet them. The mode of use and the number of users will also have to be considered. For systems involving identification (1 to many comparisons), error rates that may be acceptable with a small number of users rapidly become intolerable as the number of enrolled users rises. This is likely to be a particular problem for large public applications which may have many millions of enrolees.

12 Biometric algorithms are proprietary and not validated

Many encryption algorithms are publicly available to allow cryptographers to analyse and verify the strength of the encryption. Biometric algorithms are not readily available for review and are thus an unknown factor.

Biometric algorithms do not generally fulfil the same purpose as cryptographic algorithms. Rather, they represent the encoding rules for the biometric feature set to derive a template in order to provide a means of distinguishing between the features of enrolled users of the system. The purpose of the biometric algorithm is functional rather than security related, though there may be security connotations

If an analyst (or an attacker) wishes to understand the working of the algorithm, then the task is likely to be easier if the algorithm is publicly available. An impostor might wish to examine the algorithm to determine how the biometric ? template mapping works, and what elements are more and less important to the authentication process. This knowledge could aid the construction of an artefact intended to spoof the system, particularly if the approach was to be that of an artificially constructed image rather than a copy of a known legitimate image. An undisclosed algorithm would make this process more difficult (security through obscurity) but is unlikely to resist a determined attack that might involve reverse engineering of the algorithm. Conversely, a publicly available algorithm may help to highlight potential weaknesses and thereby assist in their eradication (i.e. as for the case of password algorithms)

Solutions

Security Evaluation can be used to determine the efficacy of the biometric algorithm to separate and identify/verify individuals, and any weaknesses that might be exploitable by an attacker.

13 Biometrics cannot be changed when compromised

It is true that the basic biometric features cannot be changed, though in some cases, alternatives may be available (e.g. different fingers). However the simplicity of the headline argument conceals some more complex and subtle issues. We need to understand what can be compromised, examine a number of scenarios where compromise might occur and identify what measures may be taken to counter them.

Compromise through use of an artefact

Here we are referring to the exploitation of the source biometric feature (which is generally not secret anyway) through the capture of the feature and the construction of an artefact with similar characteristics. The 2 issues are:

- How easy is it to capture the features?
- How easy is it to construct an artefact that can spoof the biometric system?

If successful; then, at a minimum, that user on that system is compromised. But the situation is actually worse than that, because once the system has been shown to be vulnerable to spoofing, every enrolled user is at risk of compromise in the same way. Re-enrolling the compromised user (using an alternate feature if available) will not resolve the fundamental problem. Other biometric systems using the same technology may also be vulnerable, which further increases the scope of the potential problem.

Compromise through capture/replay

If undetected, this attack may be used repeatedly and will compromise that user on that system. However, once in place, other users on the compromised connection may also be captured and the compromised set of users is liable to grow. Once discovered, the attack may be disabled for all compromised users, provided that the capture devices can be protected in future from similar attacks.

Various countermeasures are possible including physical hardware protection, variable signal encryption and challenge/response operation.

Compromise of template integrity

A template compromise may involve the replacement or modification of the stored biometric template of an enrolled user to substitute the template of an unauthorised user, or the addition of the template of an unauthorised user. In the former case, the impostor would assume the identity of an authorised user and be able to perform any

actions permitted to that user. However the authorised user would thereafter be unable to access the system and this may lead to the discovery of the compromise.

Adding a new template would effectively illegally enrol the impostor on the system. Existing users would be unaffected, which may lessen the chance of detection. In order for this form of attack to be successful the integrity of the template database would have to be seriously undermined.

Solutions

Solutions to the spoofing compromise include supervised operation and liveness detection built into the biometric system

Countermeasures to template integrity compromise include access control measures to templates and cryptographic protection of templates, either through check-summing (integrity) or data encryption (integrity and confidentiality).

Cancellable biometrics have been proposed, where the biometric image is distorted in a repeatable but non-reversible manner before template generation, If the biometric is compromised, the distortion characteristics are changed, and the updated image is mapped to a new template which is used subsequently.

Security evaluation will be necessary to determine the assurance that the measures employed provide against these forms of compromise.

14 Biometrics should only be stored on smart-cards

This is a sometimes heard expression of concern about the potential misuse of biometric data stored on central databases. It refers to the threat to privacy that such centralised collections of personal data could pose if compromised.

Biometric data are regarded as personal data and hence subject to the controls appropriate to personal data. There is a perceived fear that biometric data may be shared between applications, perhaps without the knowledge or consent of the subjects. This concern may be amplified if biometric images are stored, rather than the coded template data only, particularly for large-scale public applications where there may be perceived Orwellian overtones. This area is addressed in the UK by the Data Protection Act -1998 (DPA), which applies to biometric data just as much as to other personal data. Codes of conduct may be needed to provide specific interpretation of the DPA for biometric applications.

Biometric data are not usually held in isolation. They are typically associated with other personal data that may form part of the identification and authentication process itself, or subsequently for access control permissions. Associated data is normally not

unique to biometric authentication systems, and is commonly stored centrally on non-biometrics applications, not apparently eliciting equivalent concern.

Solutions

A potential solution is seen in the storing of personal data on secure tokens or smart cards that are held by the users themselves. The assumption is that this will obviate the need for a central database of biometric data, and therefore negate any privacy concerns. This is attractive because it promotes the idea of anonymous authentication. However, anonymous authentication has its limits and may not be tenable in many circumstances. For example in government applications, it will typically not be sufficient to know that the person applying for the benefit payment/passport/driving licence is who they claim to be. It will also be necessary to check that they are entitled to the service or payment requested and not enrolled multiple times under different identities. To do this a central database of claimants will almost certainly be needed, even if a token or smart card is used as part of the authentication process. In these cases, the privacy protection advantage ascribed to user-held tokens or smart cards will be largely illusory.

To mitigate the risk of functional creep, the biometric data can be bound to the application through the use of cryptographic signature techniques.

15 Biometrics do not offer non-repudiation

The question of the repudiation of biometrically authenticated transactions has been the subject of widespread discussion. Such discussion is not limited to biometric authentication though; other more traditional forms are also open to debate. Generally, signatures have been accepted as legally binding indicators but they are certainly open to challenge in the courts and such challenges are not unknown.

Non-repudiation of authentication typically rests on 2 considerations:

- Strength of binding of the authenticator to the individual in question
- Informed consent of the individual at the time the authentication was given.

Most authenticators are open to challenge on either or both of these grounds. The former is a technical issue, signifying the non-forgeability (or otherwise) of the authenticator. Normal signatures are known to be readily forgeable, so do not offer strong binding. Various other authentication tokens have been proposed and used which themselves offer much stronger binding, for example cryptographic signatures. However, cryptography does not address the crucial issue of binding the authentication to an individual. This final step has to be provided by a supplementary mechanism usually involving a PIN or password, a token, a biometric, singly or in combination. These generally have much lower strengths than the cryptography and set a limit to the true strength of the individual binding and hence the non-repudiation.

The relative strength of binding provided by biometrics compared to passwords or tokens is not straightforward to define and there is currently no generally agreed basis for the comparison. It is known that each mechanism has strengths and weaknesses in different areas, and relating these areas of difference and mapping them into a single equivalent "strength" figure has so far proved intractable.

Biometric specialists normally agree that the biometric error rates such as FAR and FRR are the equivalent of the password space in PIN/Password based authentication. The exact relation is more elusive however, because the biometric mechanism cannot be compromised by a simple exhaustion attack in the same way as that for a PIN/Password. A 4 digit pin has 10,000 distinct values, so a single chosen value has a 1 in 10,000 chance of success (assuming that the "true" value has been chosen randomly). A biometric system with a FAR of 1 in 10,000 (0.01%) might be deemed to be equivalent, as a single trial has the same chance of success. However, different values of PIN can be tried in succession, lowering the actual strength of the PIN mechanism in a way that the biometric is not subject to. Thus it could be reasonably argued that the biometric is stronger than the PIN in this case; but how much stronger? Also, the biometric may be subject to a spoofing attack which has no equivalence for the PIN, so how much (loss of) strength is this worth? However the biometric cannot be lost or disclosed in the way that a PIN can be (and often is!), so how much strength is this worth? These arguments have been extensively reviewed, and a recent consensus view relating biometric performance figures to strength of function is given in the section entitled "Performance Limitations" earlier. This can be regarded as a current UK government view, but is subject to change in the light of further analysis or practical experience.

The second factor is that of informed consent. The "informed" is important, because there are situations where an individual could give consent based on false or inadequate information. This factor also runs up against the issue of functional creep. If the declared use of the system does not correspond to its actual use, the consent is not informed and therefore not valid.

No authentication system can offer an unconditional guarantee of unique identification, because the guarantee also depends on the assumption that the mechanism has not been compromised in any way (e.g. procedural failure).

Solutions

Repudiation requirements must be determined and the authentication mechanism matched to the requirement. A proper procedural framework will need to be put in place, which may involve legal accreditation (e.g. as for digital signature legislation). The availability of such a legally accepted and enforceable framework will effectively determine the repudiation status of an application. Note that if non-repudiation is not achieved, the risk of "bad" transactions is transferred to the service provider and away from the service user.

Repudiation is likely to be an issue for applications where there are legal ramifications for identification/verification, e.g. financial transactions. This is a potential future problem, when a substantial number of financial and other contractual transactions are endorsed by biometric authentication.

16 How do we know when the system is becoming less secure?

Biometric systems may be initially adequately secure, but become less so with passing time. This could be because critical security parameters such as threshold settings become maladjusted, or sloppy enrolment procedures lead to poor enrolment quality. Some biometric systems are self-adaptive which means that the templates are updated each time a user accesses the system. This feature is intended to maintain the system performance (essentially to stop the false rejection rate increasing) if the users' biometric characteristics change over time. Such updating may result in the reference templates becoming weaker (easier for an impostor to attack) without supervisors being aware of anything untoward. The problem may be exacerbated if coupled with sloppy user behaviour which results in poor quality images that translate into weaker templates.

An impostor, working in collusion with an enrolee, could gradually "train" the system away from the enrolee's template onto the impostor's template.

Solutions

The risks can be countered through system audit and testing. If security relevant events are logged, then changes in security parameters can be audited. Suspicious events such as persistent authentication failures can also be checked. If the system is capable of checking its own performance, then it could monitor the template separation of enrolled users and flag conditions where the separation becomes inadequate. Clearly, these measures are likely to be more difficult to apply in large distributed systems where logs and templates may also be distributed.

17 Does publicising countermeasures make the systems less secure?

If details of countermeasures employed in biometric systems are publicised, it may help attackers to avoid or defeat them. Similarly, if attackers know what countermeasures are not employed, this will help them identify potential weaknesses in the system, and direct attacks towards those weak areas.

The counter-argument is that public exposure of countermeasures and vulnerabilities will lead to a more mature and responsible attitude from the biometrics community and promote the development of more secure systems in the future. Generally, achieving security through obscurity is not seen as a viable policy as it depends on the assumed difficulty of analysis which is a hostage to fortune. For example the design of a "secure"

mechanism may fall into the hands of an attacker and, if the underlying security is not adequate, compromise will result. Certainly in the traditional area of cryptography, the philosophy that is normally adopted is to assume that an opponent will have knowledge of the design of the cryptographic algorithm, but that knowledge should not compromise the cryptographic security.

That is not to say that obscurity cannot provide any protection, rather that the protection is invariably unpredictable and may be short-lived. If we wish to make biometric devices and applications secure it is necessary to understand the threats and put in place effective countermeasures, technical and procedural. A parallel may be drawn with the field of IT vulnerabilities where the world has had time to come to terms with the idea and not seek to suppress knowledge. Rather, the approach is to report problems to the developers so that they can be fixed and patches issued. The balance between (excessive) publicity and suppression has been struck, founded on pragmatic principles based on experience. If and when biometrics are widely deployed, a similar approach can be expected to be adopted.

Whatever the merits of the arguments, they are likely to be overtaken by events. Suppression by governments or companies will not inhibit individual researchers and consumer magazines from investigating the subject. Already in the biometrics area, a number of ad-hoc security evaluations have been conducted and the results published. The following table lists some of them.

Some Ad-Hoc Biometric Security Evaluations

Six biometric devices point their finger at security
- Network computing – Jun 1998
  - Fingerprint

Biometrics security
- PC magazine – Feb 1999
  - Fingerprint / face / voice

Fingerprint recognition–don't get your fingers burned
- Van der Putte, Keuning, Jan 2000

Impact of artificial "gummy" fingers
- Matsumoto, Jan 2002

Biometric access devices & programs put to the test
- c't magazine, may 2002
  - Fingerprint / face / iris

18 Could I accidentally give my biometric 'signature'?

Users may be concerned that their biometric features could be captured without their consent or even knowledge and that they might thereby unintentionally unlock a door, or authorise a payment. If true, this could have serious financial or safety consequences, however it is rather unlikely because, in any real application, the issue would be addressed if applicable. Such considerations could limit the type of technology used in an application or impose requirements for clear explicit consent where the biometric alone is not deemed sufficient to provide consent.

Non-biometric systems generally require an explicit user action. However, there are exceptions such as the use of contact-less (vicinity or proximity) smart cards or RFID tokens, which may be read as a user walks past a sensor. Such cards cannot be used as a method for giving authorisation.

For authorisation applications, the process should involve an explicit action implying consent, for example the insertion of card or typing in a Personal Identification Number. There may be a complementary application security issue, exemplified by registered traveller schemes. Here the application owner wants to ensure that it is impossible to make an accidental impostor attempt. Note however that biometrics can offer an advantage/safeguard in that biometric backed authorisation indicates that the authorisation has been given by the correct person, unlike (say) the presentation of a card.

19 Can my biometric be collected covertly?

Users may have concerns about being identified or tracked by covert applications (both legal and illegal). Users may feel they have a right to know when their biometrics are being collected and have a right to opt-out of biometric data collection. If biometrics can be collected covertly, they have no way to know whether such rights are being upheld. Examples are surveillance applications which are checking against a "watch list", looking for known terrorists or criminals, or something more innocuous like a commercial application looking for – say – favoured customers in a shop.

Some biometrics can be easily used 'covertly'. For example face recognition, speaker verification, and gait recognition can work from a distance. There is no obvious way of knowing whether a CCTV camera is biometrically enabled. Even close-up and contact biometrics could be used covertly – e.g. recognition of latent fingerprints, covert fingerprint sensor in doorknob, or iris recognition through a 1-way mirror

Non biometric identifiers cannot be so easily covertly collected in most cases (but note the example of the contact-less or RFID cards). However cards can be copied and passwords divulged, unknown to the authorised user, with similar consequences.

Solutions

There are no technical countermeasures to the threat of covert collection. The current technology most likely to be involved in covert collection is facial recognition, whose (current) poor performance in this mode imposes a self-limitation on its effectiveness. The potential for the covert use of biometrics must however be recognised and biometric applications subject to appropriate legal and procedural constraints. In many applications, prior consultation with citizens and the prominent display of information notices may serve to allay many fears. Where people can perceive some benefit to themselves (e.g. reduction in crime) they may support the implementation of biometric surveillance systems, providing that adequate safeguards to protect privacy and personal data are in place. Conversely, there are examples of biometric surveillance systems that have been introduced without adequate openness and consultation, and have resulted in substantial public disquiet and opposition.

20 Can my biometric be stolen?

Can the biometric template or biometric feature vector be stolen, and if so what are the consequences?

If biometric template data are stolen, either:

- Directly, from the stored reference templates, or
- By capturing the data in transit within the system, or
- On a communication path between the biometric capture device and the rest of the system,

then the template data could be reused by an impostor to recreate the identity of an authorised user without the user being present. This would undermine the authentication integrity and grant the impostor illegal access to the assets protected by the biometric authentication.

If the stolen template includes associated data, then the associated data could be used separately and independently of the biometric data. Any user credentials or alternative authentication data (e.g. password) might be used to compromise the system or the user without exploiting the biometric data. The degree of compromise would depend on the data and the protective measures in place to prevent exploitation of captured data.

If successful, this would be an example of identity theft (see separate concern), and all the ramifications for identity theft would follow.

An additional threat may result if a captured biometric template can be reverse-engineered. The biometric “image” thus produced might be used to construct an artefact or to discover (chance) zero-effort false matches in the criminal fraternity. This

threat could be exploited more easily if the system stores biometric images which can be recovered to generate a ready supply of targets for such attacks.

Solutions

The solutions depend on the nature of the biometric data stolen. Stored images or templates can be protected by encryption. Data intercepted between the capture device and the rest of the system could also be protected by cryptography, but here unique session keys would be necessary (e.g. through time-stamping) to prevent the data being replayed successfully.

If the stolen image data is used to construct an artefact, then liveness testing could be used to ensure that the biometric is actually being submitted from a person.

Stolen templates and template data can be rendered innocuous through the use of cryptographically based integrity checking or encryption. Alternatively, template transformation techniques have been mooted to circumvent the compromise of a template by the legitimate substitution of a transformed version of the template for matching against a similarly transformed feature vector.

See also Spoofing, Template Integrity/Confidentiality.

21 Will I know when and how my biometric has been used?

This is related to the covert use of biometrics (see “Can my biometric be collected covertly?” previously), and to functional creep in applications. It is important to realise that authentication does not necessarily imply consent, and it is consent which is the issue of concern here. Any application could be affected though the concern will grow with wider deployment of biometric systems and the opportunities and motivation for sharing biometric data increase.

It is unlikely that biometric applications using different technologies could share biometric data between them which will act as one limiting factor. Depending on future template and image standards, applications using similar technologies from different vendors may or may not be able to share data. The desire for integration and interoperability of biometric systems is likely to grow and will act as a driver for standardisation.

Functional creep and data sharing are not concerns that are limited to biometric systems. They are common experiences in the modern world with interconnection of systems, and address and lifestyle information is routinely traded as marketing commodities. Biometric data may therefore be seen as just one more example, but its intrinsically personal nature coupled with its role in defining and authenticating identity may render it peculiarly sensitive.

This is likely to become an increasing problem with the growth in use of biometrics for authentication. With the widespread use of networked applications, the opportunities for sharing data will increase and controls will be harder to enforce.

Solutions

Legal and procedural constraints are the first line of defence against functional creep and covert capture. The Data Protection Act requires that applications storing and processing personal data adhere to the principles and that the purpose and operation of the system is declared, not only to the Information Commissioner, but also to the users. Changes in functionality are not allowed unless approved by the resubmission and registration of the system.

Audit trails can provide users with evidence of proper implementation of the system privacy policy and any violations that may have occurred.

Technology can provide solutions by cryptographic binding of templates to specific applications, but successful employment will also depend on strict procedural enforcement. It should be noted that, typically, biometric data will exist (transiently) in clear form within the biometric system to allow the matching process to take place.

22 Does using biometrics increase likelihood of capture, coercion or injury?

Users may be concerned that the use of biometric authentication will increase the danger that they will find themselves targeted by ruthless criminals who are intent on gaining entry to the assets protected by the biometric. With non-biometric authentication, cards, keys, and passwords could be stolen and used by criminals without the presence of the user. If biometrics are employed so that the physical presence of the user is required, this may place the user at more risk.

It is hard to produce a definitive analysis of the situation, in the absence of any long term experience with widely deployed biometric systems. One is left to a speculative consideration on likely scenarios and outcomes. Nowadays, even low grade crimes are frequently accompanied with physical assault (e.g. muggings) for small gains such as cash, mobile phones or credit cards. If biometrics were used to provide authentication for (say) credit card transactions and mobile phone calls, would this increase or decrease the likelihood or degree of violence employed? It could reasonably be argued that petty criminals usually go for “hit and run” attacks and don’t want to hang around forcing victims to go to ATM machines and withdraw cash etc. For this type of crime, it seems likely that biometric authentication would act as a deterrent.

For serious, organised crime, violence is endemic and may be used directly against victims or their families and friends. Again, it is not clear that the use of biometrics would make a significant difference to the frequency or degree of coercion and violence used.

Solutions

Contrary to the concern expressed, the use of biometrics may actually serve to reduce the likelihood of coercion, because in many cases it would be likely to increase the risk of arrest for the perpetrator.

Effective liveness checks would act as a countermeasure to the successful use of cadavers or severed limbs etc. and hence to the motivation for such attempts.

The use of biometrics (and other electronic authentication) provides an opportunity for the use of duress codes to allow a transaction to take place but alert the authorities that it is involuntary.

23 ID fraud becomes worse if there is a single strong identifier

If a biometric identifier became the sole means of identification, identification errors could have dire consequences. In existing scenarios, identification tends to rely on an amalgam of several elements where there is less dependence on a single factor and the consequences of errors are likely to be less drastic.

Dependence on biometric identification may reduce or remove the safeguard of the human element, replacing human judgement with automated decision making. Note however that this is applicable to any automated identification processes - it is not confined to biometrics. If high reliance is to be placed in any single identification process it follows that a corresponding level of trust is required for all stages of the process. This starts with the enrolment integrity, which includes the validation of the enrolees' credentials prior to enrolment, and the quality of the biometric enrolment itself that limits the performance and reliability of the subsequent identification or verification attempts.

Operating and administrative staff will need to be aware of the importance of enrolment, and receive adequate training to ensure that adequate enrolment quality is maintained. All threats that could undermine the system integrity will need to be addressed, including technical issues such as performance, spoofing and threats to system data integrity, and procedural threats such as insecure configuration or operation, and collusion between users or between users and staff.

24 Could a biometric system with identification help a stalker?

Could, for example, an operator use a biometric system to track, identify then stalk an individual? It might be feasible in an environment where there is widespread deployment of linked technology e.g. a network of biometrically enabled CCTV cameras covering the town centre, car parks etc. if these could be subverted by an operator to track the movements of an individual.

It might be possible, offline, to analyse the output recordings from multiple unconnected CCTV cameras to provide a tracking capability, after the event. Whether this would constitute “tracking” or “stalking” in the sense implied in the heading is open to debate.

This is really an applications dependent concern. To permit online tracking, an application would have to have this capability as part of its normal function and this function would have to be misused by the errant operator. It is rather a far-fetched hypothesis which is probably not technically possible with any current system, but might conceivably be in the future.

Solutions

Technically, the removal of any capability to coordinate tracking ability across distributed biometric systems would provide effective limitation. Of course, if the coordinated tracking was a required part of the legitimate functionality of the system, this would not be a feasible solution.

Aside from technology, solutions would depend on procedural security measures (secure operating procedures, staff training etc.) backed up by proper auditing of the system use.

25 Can the enrolment database be used to search for criminal suspects?

With more biometrics around, the possibility of a chance match of a fingerprint with one found at the scene of crime will increase. Typically in such cases there may be an assumption of guilt unless the individual can either explain how their fingerprint came to be at the scene of crime, or show a good alibi.

The result of such searches could be that innocent people might be accused of crimes. Biometrics in general and fingerprints specifically would lose credibility as an authentication mechanism and there would likely be a hostile reaction to biometric systems

Current criminal fingerprint databases contain image data which could only be matched directly against equivalent images from biometric systems. However, for a

specific biometric fingerprint system with a known proprietary template format, it would be possible to map the criminal image database into corresponding templates and then to compare the templates looking for matches against samples provided by the biometric system. Furthermore, with the moves now afoot to standardise biometric image and template formats, this process would be further facilitated if the many proprietary formats give way to a single or few common formats.

Note that this concern is currently limited to fingerprint biometrics but if criminal databases of other biometric characteristics are built which correspond to current or future biometric characteristics used for biometric authentication (e.g. DNA), then the concern could grow.

Solutions

Solutions lie largely in the area of legal constraint on the use and sharing of biometric data. Technology solutions can support privacy through the encryption of biometric data. Applications where there is no central repository, i.e. where users' biometrics are held solely on a smart-card under their control, would not be susceptible.

This is likely to be a subject of increasing importance with the growth of biometric databases of features common to forensic databases. There are likely to be conflicting arguments and motivations to share/not share the data.

26 Administrator or operator misuse

An administrator could misuse their privileges by looking-up the biometric database to see whom they, or their accomplices, match. In this way, an administrator could target enrolees on systems that he/she administers, and who are also enrolled in other systems that use the same biometric. Those applications with large numbers of enrolled users employing a central database are open to exploitation. The exploitation is not technology dependent, except that for technologies with a high discriminatory capability, there is less chance that a fortuitous match with an administrator will occur.

While there are few biometric systems in use, the concern is more theoretical than real, and there is little incentive (other than curiosity) for an unscrupulous system administrator. As biometric systems become more ubiquitous, and as databases become larger, the problem is likely to grow. With a national id database, the administrator is likely to find a matching person.

Solutions

This issue is not really addressed by current systems, but will need to be for national scale applications. Partial solutions may include:

- Careful screening of administrators/operators to increase trust;
- Separation of roles, so that no single person could engineer such a look-up;

- Audit of administrator/operator access to biometric database (image or template);
- No central storage of the biometric data;
- Use multi-mode biometrics (greatly reduces chances of fortuitous match with administrator);
- Encryption of the database. Note: this may not help for single mode identification (1 to many) systems.

27 Function creep

How can it be ensured that a biometric collected for one purpose is not used for another? Sharing of biometric (personal) data would require explicit consent by users to avoid transgressing the legal requirements of the Data Protection Act. Use of non consensual biometric data would undermine the integrity of transactions and undermine any non-repudiation claims. It effectively means that the biometrics are being used covertly.

"Sharing" includes the sharing of biometric data between multiple functions of a single closed system and the sharing of biometric data between different systems. In the latter case, this assumes that the technologies are the same or sufficiently similar that the same biometric data is usable on the different systems.

This is a live issue. It is likely to be a growing problem with the wider deployment of biometric systems and increasing reliance on biometric authentication.

Solutions

Technology solutions include the binding of biometric templates to applications using cryptography. However, it would be necessary to place control of the binding in the hands of the user (or possibly a trusted 3rd party). A PKI infrastructure may offer a technical solution, but arguably, not a practicable one. Further work is required.

28 Revealing personal information

A question that can be raised is: what other information could my biometric reveal? The answer would depend on the biometric features captured and might include: gender, ethnicity, medical dispositions, medical conditions or medication.

The concern will also depend on the nature of the biometric data stored – for example images or templates. Generally, image data is more rich in features and likely to be more revealing of external factors and conditions than template data, although in all systems the image data will exist at least transitorily. For facial biometrics, images would contain obvious gender and ethnic data.

Information may be gleaned even probabilistically, for example certain fingerprint characteristics may be more likely in males than females, or in Afro-Caribbeans than Europeans. However, there is little authoritative information on the subject. Some investigation has been done using police fingerprint databases, which failed to show any clear correlations.

The sensitivity of any possible information that may be revealed needs also to be considered. For example most authentication processes record name information, which directly reveals gender. This is not normally considered to be a major issue, so arguably it should not be any more so when using biometrics. However if data contains implicit medical information it would likely class as sensitive (within the Data Protection Act meaning), and more stringent protective measures to prevent disclosure or non-permissible use would be necessary.

Additional personal information may also be revealed by an examination of the system audit log, though it is not clear that this situation is any different for non-biometric authentication.

Solutions

There is currently little indication of positive steps to deal with these issues or to assess how much of a real issue it will be in practice. Suffice it to say that there is now some awareness and it is fuelling further study.

Where to go for further information and assistance

The UK Biometric Working Group, managed by CESG, supports the UK government and provides advice and information about the implementation and use of biometric authentication systems.

For further details, see http://www.cesg.gov.uk or telephone +44 (0)1242 221491 extension 34124

.