IN CONFIDENCE TO PROJECT PARTNERS

BIOVISION
User and Application Security Issues for Biometric Systems
Interim version

Project Number	IST-2001-38236
Project Title	BIOVISION Roadmap to Successful Deployments from the User and System Integrator Perspective
Deliverable Type	Document

Deliverable Number	**D4.1.1 Draft 3**
Contractual date of delivery to Commission	
Actual date of delivery to Commission	
Title of the Deliverable	User and Application Security Issues for Biometric Systems
Workpackage contributing to the Deliverable	WP 4
Authors	Dr Tony Mansfield and Philip Statham

Abstract
This is a first draft of a report to provide an inventory of user and application security concerns for biometric authentication systems; to detail how such issues are currently being addressed by the biometrics industry; and to identify which serious concerns remain, and require further work.

About this document

This deliverable D4.1.1 is an interim version for deliverable D4.2.1 – Application and User Security Concerns for Biometric Systems (due at the end of the Biovision project). A second interim version D4.1.2 will be released in early 2003.

This version outlines:

- Current initiatives in biometric system security
- Application and user security concerns
- Current technical and procedural solutions to these concerns.

Future versions will:

- Expand upon description of activities, concerns and solutions
- Organise the security concerns to determine which are the fundamental issues (currently there is much overlap between the concerns).
- Document the main security requirements
- Determine how well current initiatives meet the security issues, and note any gaps.
- Provide integration with WP3 (User perceptions), WP4 (Medical Perspectives), and WP7 (Regulatory)

Document history

Issue - Date	Date	Author	Comments	Reviewed
411 Draft 3 = Issue 1?	6/12/02	AJM	Minor updates	
411 Draft 2	29/11/02	AJM PS	Further application concerns described Further references added	
411 Draft 1	4/10/02	AJM PS	List of concerns added References to existing work on biometric system security	
411 Draft 0	2/9/02	AJM	Outline	Described at BVN meeting 6/9/02

Contents

1 Introduction

This report is concerned with the security of biometric authentication systems.

Previous work on security assessment of biometric systems has concentrated mainly on application security, rather than user concerns that their data is confidential, their biometric is secure against “identity theft”, and that they are protected against “function creep” with their identity eventually being monitored for more intrusive applications. Furthermore, many aspects of biometric system security are poorly understood, and there are conflicting opinions on the best way to use them in conjunction with other security system components such as smart cards, PKI etc.

This report provides an inventory of security concerns for biometric systems from both the user and application perspective. It gives details of how these issues are being addressed by the biometric technology, by standards, by application procedures, and looks at the adequacy of such solutions for future applications.

Security problems: Can biometric systems be fooled? How easy might this be? What are the consequences for trust and confidence? (For example does it matter that a person cannot change their biometric in the same way they might change a password?) Are these issues fundamentally different from PIN/password/token based approaches? We look at the consequences of an attack, (rather than developing methods for spoofing biometric systems), and separate myths, problems that are easily resolved, and those security issues that require further work.

Technical solutions: Are all the security problems being addressed by the technical solutions being developed by biometric system suppliers and application developers, the standards for security assessment, and legislation? Are these solutions adequate for future scenarios in which biometrics may be deployed. What further initiatives are necessary?

2 Work on user and application security for biometrics

In this section we document activities on biometric system security.

2.1 Standards

2.1.1 ANSI X9.84 – Biometric information management & security

The standard X9.84 [ANSI, 2001] specifies minimum security requirements for effective management of biometric data.

- Security for the collection, distribution, and processing, of biometric data, encompassing data integrity.
- Management of biometric data across its life cycle: enrolment, transmission, storage, verification, identification, and termination processes.
- Usage of biometric technology, including one-to-one and one-to-many matching, for the identification and authentication of customers and employees, for both logical and physical access control.
- Security of the physical hardware used throughout the biometric data life cycle.

Items considered out of scope of the standard are:

- Application specific requirements and limitations for employing biometric technology.
- The individual's privacy and ownership of biometric data. For example the standard does not require encryption of the biometric data for the purposes of confidentiality. Moreover, the standard assumes that identification of an individual is on a voluntary basis whereby the individual is recognized as part of the transaction process and is not intended for surreptitious activity

2.1.2 CBEFF – Biometric information management & security

This proposed standard [Podio et al, 2001] includes provisions for data encryption and digital signatures to provide template privacy and template integrity, respectively.

2.2 Common Criteria security evaluation

2.2.1 Biometric Evaluation Methodology supplement for Common Criteria

[Common Criteria Biometric Evaluation Working Group, 2002]

2.2.2 Biometric Device Protection Profiles

[BMO, 2002] DoD Biometrics Management Office Biometric System Protection Profile for Medium Robustness Environments

[BWG, 2001] CESG Biometrics Working Group Biometric Device Protection Profile, Issue 0.82

2.2.3 Common Criteria biometric evaluations

So far only one biometric product has been evaluated under the common criteria

Product Name	Manufacturer	Conformance Claim	Valid. Date	CC Scheme
Bioscrypt Enterprise for NT Logon, V2.1.3	Bioscrypt, Inc.	EAL 2	Jun 01	🇨🇦

Iridian SecureID and KnowWho server with Iris Recognition Authenticam also undergoing an EAL2 evaluation in Australia. (Precursor to EAL 4 evaluation).

2.3 Biometric interoperability, performance and assurance working group

Template protection [Soutar, 2002]

Security perceptions [not yet ready for release]

2.4 Ad hoc security evaluations

Network computing [Willis & Lee, 1998]

PC Magazine [Gunnerson, 1999]

Spoofing of fingerprint systems [Matsumoto et al, 2002; Tekey, 2001; van der Putte & Keuning, 2000]

C’t magazine [Thalheim et al, 2002]

2.5 Initiatives improving biometric product security

2.5.1 Liveness testing

Catalogue of potential methods [Valencia, 2002]

Fingerprint sweat pores [Derakhshani & Schuckers, 2003]

2.5.2 Investigation of other potential attacks

Hill climbing attack [Griffin, 1999]

Image reconstruction from fingerprint template [Hill, 2001]

2.5.3 Other investigations

We are aware of several biometric system suppliers, system integrators, and companies enabling biometric applications that are conducting their own in-house investigations of the security of their biometric products.

3 Inventory of security concerns

3.1 Application security concerns

3.1.1 Performance limitations

Biometrics do not provide perfect (unique) identification. There are performance limitations due to errors & throughput: Operational errors classed as FAR, FRR ▪ Enrolment error FTE ▪ FTA will cause FTE (enrolment) or FRR (operational) These errors are influenced by: ▪ uniqueness of biometric features ▪ capture device ▪ algorithm ▪ environmental interference (lighting, noise etc.) ▪ user behaviour	
Ramifications	Errors affect security ▪ “zero effort” successes ▪ Invoke backup system ▪ Denial of service attack ▪ Ease of spoofing, mimicry attack The variability of error rates can make it difficult to know how secure the system really is. Throughput limits usability/applicability
Applications affected	Major impact on applications requiring: ▪ Security ▪ High throughput ▪ User friendliness/acceptance
Biometrics affected	All types are affected. Some technologies have lower error rates than others in (current) practice There is no significant correlation between throughput and technology type
Differences to non-biometric authentication	Passwords and tokens have no probabilistic errors Passwords and biometrics have similar throughput rates. Tokens can be faster for large-scale applications (eg swipe-cards, contact-less smart-cards), but if PIN is also required, this will limit throughput.
How is the issue dealt with?	Technology Development Performance Testing (Best Practice Testing [Mansfield & Wayman, 2002])
Is the issue resolved?	Problem now, and likely to persist into the future. Further technology development required

3.1.2 Enrolment integrity

<table>
<tr><td colspan="2">Dependence on establishing correct identity prior to enrolment [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? (I have added this; not in Govt. Authentication framework doc. - but I think that it is missing in error there)</td></tr>
<tr><td><b>Ramifications</b></td><td>All bets off if no enrolment integrity. Pre-enrolment authentication credentials should match risk and consequences of failure</td></tr>
<tr><td><b>Applications affected</b></td><td>All where it is required to identify/verify individuals</td></tr>
<tr><td><b>Biometrics affected</b></td><td>All; not technology dependent</td></tr>
<tr><td><b>Differences to non-biometric authentication</b></td><td>No direct difference. However, if automatic authentication through biometric (or other) technology replaces manual authentication, it may result in a single point of failure which did not exist previously. This will then place more onus on enrolment integrity.</td></tr>
<tr><td><b>How is the issue dealt with?</b></td><td>Determine adequate enrolment criteria/credentials
Ensure that procedural measures are properly implemented
Audit system enrolments</td></tr>
<tr><td><b>Is the issue resolved?</b></td><td>Current, but likely increased concern in future with the wider deployment of biometric systems in the public domain and, probably, multiple distributed enrolment locations. Procedural issue; solutions are available</td></tr>
</table>

3.1.3 Enrolment Quality

Performance of biometric systems dependent on enrolment quality. Enrolment quality can be affected by accidental or deliberate events	
Ramifications	Poor system performance. Compromised security or excessive dependence on fallback system. Major effect is likely to be on the FNMR. In the case of negative ID systems, this is the false acceptance rate, and is a direct security concern. In the case of Negative ID systems, it is the false rejection rate that is affected, though this may lead to a consequential adjustment of the threshold thus affecting FAR.
Applications affected	All. Likely for large-scale systems, particularly where enrolment centres distributed.
Biometrics affected	All
Differences to non-biometric authentication	Analogue might be weak password Probably no equivalent for token (except weak PIN if applicable)
How is the issue dealt with?	Good enrolment procedures Administrator training Technology able to check enrolment quality and reject poor quality enrolments Technology able to display enrolment quality to allow user/administrator to check and maintain quality Make sure measures to improve enrolment quality don't compromise security
Is the issue resolved?	Current issue, and increasing with future large scale systems with distributed enrolment centres, which may suffer variable quality enrolments across system. Many current systems do not address issue. More awareness needed

3.1.4 Spoofing (using artefacts)

Several recent studies [Gunnerson, 1999; Matsumoto et al, 2002; Tekey, 2001; Thalheim et al, 2002; van der Putte & Keuning, 2000; Willis & Lee, 1998] have shown it is possible to spoof biometrics by using artificial fingers, photographs, and recordings.	
Ramifications	Biometric no longer based on what you are, but what you possess (artificial finger etc) or what you know (template).
Applications affected	Any
Biometrics affected	Physiological biometrics. 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, eg retinal patterns, without the use of sophisticated and conspicuous equipment. This will offer some security protection against copying
Differences to non-biometric authentication	Identification systems that are similar to biometric identification, but lack the "automatic" element, may be vulnerable to spoofing attacks. For example, a person may disguise his/her face in order to fool a security guard. The closest analogue for password authentication is probably acquiring and using an authorised user's password, and for a token based system, copying a genuine token
How is the issue dealt with?	*Technical counter-measures* The basic premise of technical counter-measures in biometric systems is to design and implement the system such that its security does not depend on the secrecy of the biometric features. To protect the authentication process, the biometric system must be able to detect and reject the use of a copy of a biometric instead of the live biometric. The biometric verification/identification process is concerned with the technical exercise of capturing data, mapping to a template form and comparing sample and reference templates. This process typically has no inherent ability to detect artefacts, except as an accidental side-effect of the process. The detection and rejection of artefacts must generally be added as a specific capability to the biometric verification/identification function. This additional 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. 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 (eg face and voice) or through multi-factor authentication such as biometric

	and PIN. *Procedural counter-measures* 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, eg an artificial fingerprint pattern moulded on a thin laminate and attached over the top of a real fingerprint.
Is the issue resolved?	There is much evidence of current awareness on the spoofing issue, both among the user community and the biometric developers. There is also evidence that developers are beginning to address spoofing concerns through the inclusion of liveness detection. There are however, no extant standards that specify a methodical approach to identifying biometric vulnerabilities, and for assessing and categorising their exploitability with regard to individual products and systems. The lack of such standards is an inhibiting factor to developers, security evaluators and users, and ultimately to the wider deployment of biometric systems. This issue is likely to be a major and long-running one for biometric identification.

3.1.5 Mimicry (behavioural biometrics)

<table>
<tr><td colspan="2">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 concerned with the recognition of acquired, rather than inherited features, the features can also be acquired by an impostor.</td></tr>
<tr><td><b>Ramifications</b></td><td>The consequences of successful use of mimicry are likely to be the same as for an artefact (see spoofing previously) for given applications. Impostors are unlikely to attempt mimicry attacks against biometric systems that completely or predominately utilise physiological features (eg 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</td></tr>
<tr><td><b>Applications affected</b></td><td>Mimicry is a threat that depends on the biometric technology used rather than the application. However, where there is a correlation between types of application and biometric technologies used, there may be an indirect connection. It may be that certain types of application will favour particular biometric technologies; for example, a surveillance system may utilise facial recognition biometrics.</td></tr>
<tr><td><b>Biometrics affected</b></td><td>Mimicry affects behavioural biometric technologies, such as signature or voice. However, in reality, most biometric systems include both physiological and behavioural elements. For example, voice patterns are often a combination of the physiological characteristics of the vocal tract, and acquired characteristics such as accent and pronunciation.
Also with some biometrics, the boundary between artefact and mimicry is blurred. In face recognition, an impostor might alter his/her hairstyle or wear a hat or spectacles to achieve a closer resemblance to an enrolled user.</td></tr>
<tr><td><b>Differences to non-biometric authentication</b></td><td>Non-biometric systems are not generally susceptible to mimicry. The nearest equivalent is probably a human engineering attack. For example, an impostor disguises him/herself as an authorised and succeeds in fooling a security guard. Or an impostor persuades an administrator that he/she is an authorised user and thereby obtains a password.</td></tr>
<tr><td><b>How is the issue dealt with?</b></td><td>Since mimicry does not involve the use of an artefact, liveness detection will not be an effective countermeasure. Counter-measures will 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.</td></tr>
<tr><td><b>Is the issue resolved?</b></td><td>Although mimicry has not so far attracted the same level of general interest as spoofing, it shares many of the characteristics and consequences of spoofing., It will be an issue of both current and future importance for biometric systems that depend principally on behavioural features.
As for the case of spoofing previously, mimicry will need to be included in the assessment process for biometric vulnerabilities and standards and methodology will need to address mimicry alongside spoofing.</td></tr>
</table>

3.1.6 Latent/Residual Images

<table>
<tr><td colspan="2">Two causes: (We shall ignore images captured outside scope of system eg fingerprints lifted from a surface).
▪ Physical residual biometric image, and
▪ Latency in internal memory. This could occur with 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). See eg [Thalheim et al, 2002] for examples.</td></tr>
<tr><td><b>Ramifications</b></td><td>Could allow impostor to gain access with identity of previous user</td></tr>
<tr><td><b>Applications affected</b></td><td>Any</td></tr>
<tr><td><b>Biometrics affected</b></td><td>Physical residual not an issue for non-contact capture devices (probably limited to contact fingerprint readers for current technologies)
Residual fingerprint image could be left on contact fingerprint reader and registered as genuine image of subsequent user (possibly in association with other exploitation such as use of stray light illumination or dummy finger)
Memory latency could affect any technology</td></tr>
<tr><td><b>Differences to non-biometric authentication</b></td><td>Physical residual not applicable to password/token systems
Memory latency effect could be present on non-biometric systems but less likely because failure to acquire is not likely to be an issue for non-biometric authentication</td></tr>
<tr><td><b>How is the issue dealt with?</b></td><td>Correct system software design
System maintenance (cleaning)
Security evaluation</td></tr>
<tr><td><b>Is the issue resolved?</b></td><td>Current and future problem. But solvable with more awareness.</td></tr>
</table>

3.1.7 Template integrity/confidentiality

Integrity

Biometric data occurs in 2 basic forms; images of the biometric features (which includes non-graphical images in the case of voice etc), and biometric templates which contain encoded versions of biometric features that are used in the comparison process which forms the basis of biometric identification or verification. In addition to the encoded biometric features, the template may also contain associated data relating to the user including credentials that will be used subsequently by the underlying system to grant access to assets protected by the system.

The integrity of the authentication process is dependent on the integrity of the template (among other things). If either the reference template or the "live" template 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 insertion of the biometric template corresponding to an authorised enrolee to substitute for the live template of the attacker.

The deliberate modification or insertion of a template would typically be the action of an attacker attempting to subvert the normal biometric authentication function and thereby gain access to the protected assets.

To use a fake template to defeat the biometric authentication mechanism, the template would need to be injected into an appropriate point in the biometric system. This could be the template database or a communications path in the system. For example the impostor could claim to be an authorised user but, when requested to supply the biometric feature, would instead inject the template belonging to the authorised user in the communications path.

A fake template would need to be able to overcome any integrity checking of the biometric system. Conversely, to protect the authentication integrity, the system must be able to detect and reject such attempts at meddling. Thus template integrity is a key issue in protecting authentication integrity. Note that template confidentiality is not an essential requirement for this purpose.

Confidentiality

Biometric templates contain data that can be used to identify living persons, and their processing and storage on a biometric system are therefore 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 (eg 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.

- In addition to the legal requirements, general user concern on the capture and storage of biometric data may impact on the acceptability and use of biometric systems.

Ramifications	*Ramifications for Applications*

	For a positive identification or verification of identity system such as an access control application, successful exploitation of this attack would compromise the authentication process and allow unauthorised access to the assets protected by the biometric. If the stolen template contained associated data that included alternative authentication data, then that data might be used to gain unauthorised access without any need to use the biometric authentication mechanism. For a negative identification system where one objective is to detect and prevent attempts to create multiple identities on the system, an impostor could not use captured templates directly, because they would correspond to users already enrolled on the system and therefore defeat the object of the exercise. However, an impostor might modify a captured biometric template and substitute it for his/her own biometric feature at an appropriate stage in the proceedings. Note that, if such an attack can be successfully mounted, the templates of many, perhaps all authorised users, could be stolen thus rendering the whole system ineffective. On positive or negative authentication systems, successful exploitation of this type of attack will undermine the system accountability functions and any audit trails. If a system can be shown to be potentially vulnerable to such an attack, then prosecution of cases of fraud based on audit evidence may not be possible, even if there is no reason to believe that actual exploitation has taken place. Other systems using the same or similar biometric technology may be at risk from this type of attack. If system templates are usable across a range of applications, then templates captured on one system may be usable against users enrolled in other systems utilising the same technology. *Ramifications for Users* This forms one example of identity theft. Any form of successful identity theft has similar ramifications for users. These include: loss of assets owned by the user, and invasion of the user's privacy. Furthermore, if the user is enrolled in several systems using the same technology and biometric feature, then the user's assets may be at risk on other systems. If an impostor successfully masquerades as an authorised user, then the system accountability will be compromised and the user may be held accountable for actions that he/she did not perform.
Applications affected	*Integrity* All applications are affected by the template integrity issue. The effect of a breach of integrity will depend on the value of the assets being protected by the biometric system and possibly with the number of people with access to the system. *Confidentiality* Applications that have large numbers of users, particularly those in the public domain (eg e-government and e-commerce applications) are likely to

	be most affected. Small, self- contained systems within companies, used only by company staff may have less of a problem with confidentiality issues. However, all applications will need to conform to the DPA and other relevant legislation.
Biometrics affected	All biometric systems use templates and all will be affected by template integrity/confidentiality issues.
Differences to non-biometric authentication	Authentication integrity is a key issue for all authentication mechanisms. For passwords, the integrity hinges on the confidentiality of the password, and for tokens by a combination of the unforgeability of the token together with the integrity of the binding between the token and the authorised user.
How is the issue dealt with?	Biometric systems must employ effective template integrity protection. This could be through access control, to prevent unauthorised access to the templates, or by integrity checking, probably using cryptographic techniques. This could involve digital signatures, or template encryption. Integrity protection may need to be combined with other techniques (such as time stamping) to protect against the reuse of stolen templates. Reference templates can also be marked (before signing) to distinguish them from live templates, in order to prevent the substitution of reference templates for live ones. Note that while digitally signing a template may be adequate to protect its integrity, it will not (on its own) provide any confidentiality to the data. If confidentiality is required (for example to protect the privacy of the biometric data), access control and/or encryption may be necessary.
Is the issue resolved?	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 and correct implementation of technical security features.

3.1.8 Capture/replay attacks

Meaning usually restricted to electrical signal capture/replay. Signals may be captured at various point in the system and replayed to simulate authorised user. Main point is between capture device and rest of system. Particular problem where signals pass across network.	
Ramifications	Access by impostors
Applications affected	More likely on unsupervised systems, networked systems where there is no trusted human supervision/visibility of system components or communications paths More likely with large distributed (public) systems and where there is clear motivation (eg financial, information)
Biometrics affected	All technologies could be susceptible
Differences to non-biometric authentication	Can also happen with other authentication technologies. No obvious reason why issue should be worse for biometric authentication.
How is the issue dealt with?	▪ Physical security (guards, inspections etc) ▪ Unique session keys for communications paths ▪ Access control to stored reference templates ▪ Reference templates marked and signed ▪ Security evaluation to ensure effective, correctly implemented solutions
Is the issue resolved?	An increasing problem with future wider deployment of large networked applications. ▪ Solutions to problems known ▪ More awareness needed ▪ Products/systems need to be designed to meet requirements ▪ Products/systems need to be evaluated

3.1.9 Biometrics do not provide absolute identification

Biometric authentication only addresses part of the overall authentication framework. Non-biometric elements (pre-enrolment) need to establish absolute identity against (application) acceptable credentials (eg birth certificate, peer endorsement etc) Biometric authentication only establishes or verifies individual identity against previously enrolled individuals	
Ramifications	
Applications affected	Not application dependent
Biometrics affected	Not technology dependent
Differences to non-biometric authentication	
How is the issue dealt with?	Education
Is the issue resolved?	This issue is one of misperception. It can be dispelled through a programme of education.

3.1.10 Biometrics are not secret

<table>
<tr><td colspan="2">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.</td></tr>
<tr><td><b>Ramifications</b></td><td>If the applications depend on biometric authentication to protect the assets and the system is susceptible to exploitation by artefacts or recorded biometric features, the authentication integrity will fail.
The ramifications will depend on the ownership and the value of the assets protected by the authentication mechanism and on the purpose of the authentication process. For access control authentication, positive identification or verification of identity is required. If the authentication process fails such that an impostor is falsely identified or verified as an authorised user, the security (confidentiality, integrity and availability) of the asset will be compromised. The impostor will gain access to and control of the assets with the same capabilities as the authorised user.
If the purpose of the authentication is to prevent a person from being enrolled more than once in the application, a failure of the authentication process may allow a person multiple access to the assets under different identities. The impostor may thereby obtain multiple welfare benefits, drivers licences etc. Many such applications will use both positive and negative identification in operation, ie they will seek to check that an applicant for a service is authorised to receive the service under the claimed identity, and is not also known to the system under another identity. For the former purpose, biometric authentication operating in identification or verification mode may be used; for the latter, identification mode is required.
<i>Consequences for users</i>
If biometric authentication becomes widely used in applications, there will be an incentive for impostors to attempt to masquerade as authorised users in order to gain unauthorised access to the assets rightly available to authorised users. There are several potential ramifications:
▪ The general populace would (perhaps for the 1^{st} time) be subject to malicious attempts to capture their biometric features. This would represent a new infringement of individual privacy and human rights. Although this form of abuse might, in principle, be conducted regardless of the existence of biometric systems, the widespread use of biometric authentication would provide motivation that was previously lacking.
▪ If an impostor can successfully masquerade as an authorised user, then the user's assets may be misappropriated and the user will lose the rights to or ownership of the assets.
▪ If an impostor can successfully masquerade as an authorised user, this could result in the authorised user being held accountable for actions which he/she did not perform and thereby incur unspecified consequences.
A masquerade attack could also be mounted during the enrolment phase. This would be more likely for enrolment in negative identification systems,</td></tr>
</table>

	where the objective of the impostor might be to establish multiple enrolled identities. In this case the impostor would need to use the same artefact on subsequent occasions when he/she needed to access the system. However this form of attack would not necessarily require copying the biometric feature of a real person; an artificial construct, capable of fooling the biometric system and allowing enrolment, would be sufficient.
Applications affected	All types of application are potentially affected. The effect of compromise will generally be to allow illegal access to the protected assets. During enrolment, the effect will be to allow the creation of illegal single or multiple identities on the system database
Biometrics affected	All types of biometric are potentially affected. Some features will be more difficult to observe and capture than others. For example, faces are easily captured by photography, and hands may be similarly recorded. Fingerprint patterns may be captured through the lifting of latent or residual images left on smooth surfaces, or directly through the exploitation of residual images left on the capture device. Voices may be captured on tape or other audio recorder. Some biometric images will be difficult to capture, eg retinal patterns, without the use of sophisticated and conspicuous equipment. This will offer some security protection against copying.
Differences to non-biometric authentication	Non-biometric analogues are possible. Passwords and tokens may be stolen or copied with similar consequences for the authentication integrity. However, passwords and tokens can be easily revoked and changed, whereas a biometric characteristic cannot be changed. In some cases, an alternative feature (eg a different finger) may be used but there are, at best, only limited possibilities (see also "Biometrics cannot be changed when compromised", "Spoofing" and "Mimicry").
How is the issue dealt with?	The direct issue of biometrics not being secrets cannot be dealt with – it is a fact. However, the consequences can be mitigated by making it impractical to exploit copied biometric features, through the incorporation of appropriate safeguards in the technology, and procedural security measures implemented in the application domain.
Is the issue resolved?	This is a current issue and will continue to be relevant in the future. The resolution needs to be indirect, through removing the motivation for copying biometric features. If the technology is robust against copied features and the procedural measures adequate, then the use of copied biometrics will be impractical.

3.1.11 Biometrics are not random enough

<table>
<tr><td colspan="2">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 easier to confuse them
An unclear argument, as it depends on the interpretation of “randomness” and what is deemed to be adequate. Perhaps the intention is to compare biometrics to passwords, which may be defined in terms of the way in which the password is constructed (the randomness) and the total size of the password space (the adequacy). With this comparison, the argument is generally non provable. For a biometric system the template size will limit the maximum possible number of states. Typically, biometric template sizes exceed password spaces so, from a simple theoretical standpoint, the argument fails.
However it is well known that biometric template size is no real indicator of the ability of the system to discriminate between individuals. Biometric discrimination will depend on 2 different factors: Firstly, the degree of distinctiveness of the biometric feature among the population of likely users of the system; and secondly, the ability of the biometric system to uniquely separate these features. Additional, practical considerations also affect the results, including the acceptable rates of false rejection, and environmental conditions. It is sometimes possible to gain some theoretical view of the likely system discrimination potential, but this can currently only be validated through a programme of practical performance testing with real users. Measurement of high discrimination capability inevitably entails the use of large test populations and this in turn places a practical limitation on the achievable accuracy.</td></tr>
<tr><td><b>Ramifications</b></td><td>Characteristics that lack randomness have a reduced feature space, compared to random ones</td></tr>
<tr><td><b>Applications affected</b></td><td>Any application</td></tr>
<tr><td><b>Biometrics affected</b></td><td>Arguably, iris patterns are more random than other biometrics</td></tr>
<tr><td><b>Differences to non-biometric authentication</b></td><td>Password and tokens can be randomised</td></tr>
<tr><td><b>How is the issue dealt with?</b></td><td>Practical test programmes can provide an insight into the capability of biometric systems to discriminate between individuals. The determination of adequacy is an issue that must depend on an assessment of the value of the assets to be protected and the perceived threats.
Verification does not require uniqueness</td></tr>
<tr><td><b>Is the issue resolved?</b></td><td>Mostly future for large systems with millions of enrolees
Developing or using high-resolution biometrics (iris?)
Verification rather than identification where appropriate</td></tr>
</table>

3.1.12 Biometric algorithms are proprietary and not validated

<table>
<tr><td colspan="2">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 (see below).</td></tr>
<tr><td><b>Ramifications</b></td><td>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 (ie as for the case of password algorithms)</td></tr>
<tr><td><b>Applications affected</b></td><td>Any</td></tr>
<tr><td><b>Biometrics affected</b></td><td>Any</td></tr>
<tr><td><b>Differences to non-biometric authentication</b></td><td>Cryptographic algorithms do not serve the same purpose as biometric algorithms</td></tr>
<tr><td><b>How is the issue dealt with?</b></td><td>Security Evaluation to determine the efficacy of the biometric algorithm to separate and identify/verify individuals</td></tr>
<tr><td><b>Is the issue resolved?</b></td><td>Yes, through security evaluation</td></tr>
</table>

3.1.13 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 (eg different fingers). However the simplicity of the headline argument conceals some more complex and subtle issues. We need to examine a number of scenarios where compromise may occur and identify what measures may be taken to counter them.

The first issue is closely related to the argument that biometrics are not secrets; ie copies of biometric features may be obtained with varying degrees of difficulty. If an artefact can be constructed from the captured feature and this is accepted by a biometric system, then what is compromised? At a minimum, that user on that system (we assume here that the biometric feature is the sole means of authentication). But the situation is actually worse than that, because the system has been shown to be vulnerable to spoofing, and therefore every enrolled user is at risk of compromise in the same way. Re-enrolling the compromised user (using an alternate feature if available) does 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.

Another form of compromise is the capture and replay of the signal between the capture device and the rest of the biometric system. This signal may flow along a wire in the case of a local stand-alone system, or across a network in the case of a distributed system. 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 compromise 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.

A third form of compromise is 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, if successful, the impostor would assume the identity of an authorised user and be able to perform any actions permitted to the authorised user. However the authorised user would thereafter be unable to access the system and this may lead to the discovery of the compromise. Template addition 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.

Ramifications	Consequence of compromise may be severe because the compromise is essentially a system compromise rather than only an individual, and all systems on which the user is enrolled become compromised.
Applications affected	All
Biometrics affected	All
Differences to non-biometric authentication	Passwords, tokens can be changed if compromised
How is the issue dealt	Countermeasures to this form of spoofing attack include supervised operation and liveness detection built into the biometric system

with?	Countermeasures could include access control measures to templates and cryptographic protection of templates, either through check-summing (integrity) or data encryption. Cancellable biometrics have been proposed, where the biometric image is distorted in a known and repeatable manner before template generation, If the biometric is compromised, the distortion characteristic is changed, and the updated image is mapped to a new template which is used subsequently Security evaluation should provide assurance against this threat
Is the issue resolved?	No - Except for the assurance provided by security evaluation. The ideas of cancellable biometrics have yet to be proved

3.1.14 Biometrics should only be stored on smart-cards

<table>
<tr><td colspan="2">This probably refers to the privacy issue. Biometric data is regarded as personal data and hence subject to the controls appropriate to personal data. One perceived fear is that biometric data may be shared between applications, perhaps without the knowledge or consent of the subjects. This concern is already addressed in the UK by the Data Protection Act (1998), which is applicable to biometric as well as to other personal data.
One way to strongly enforce the provisions of the DPA and ensure privacy is seen as storing of personal data on memory or smart cards that are held by the users themselves. This is regarded as particularly relevant to biometric data, which is often perceived to be highly sensitive.
Biometric data is not usually held in isolation. It is typically associated with other data that may form part of the identification and authentication process itself, or for subsequent access control purposes. This associated data is normally not unique to biometric authentication systems, though there is no general feeling that such data should be limited to storage on a smart card</td></tr>
<tr><td><b>Ramifications</b></td><td>Lack of trust
User resistance
Application failure</td></tr>
<tr><td><b>Applications affected</b></td><td>All, particularly applications with large numbers of users, and applications depending on central databases of templates</td></tr>
<tr><td><b>Biometrics affected</b></td><td>All. May be more sensitive if image data stored</td></tr>
<tr><td><b>Differences to non-biometric authentication</b></td><td>Password, token authentication not considered personal or private data</td></tr>
<tr><td><b>How is the issue dealt with?</b></td><td>Use smartcards
Legislation
Codes of conduct
Bind biometric data to application</td></tr>
<tr><td><b>Is the issue resolved?</b></td><td>More of a problem in future with larger systems and bigger databases
Needs further work, both on privacy enhancing technology and on the legal/procedural areas.</td></tr>
</table>

3.1.15 Biometrics do not offer non-repudiation

Equivalent to the assertion that biometrics cannot uniquely discriminate between individuals	
Ramifications	Lack of non-repudiation will transfer risk to service provider and away from service user
Applications affected	Applications where there are legal ramifications for identification/verification, eg financial transactions
Biometrics affected	Biometrics with lower discriminating power may be more suspect, (eg hand) compared to higher discrimination power biometrics (eg iris)
Differences to non-biometric authentication	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 (eg procedural failure).
How is the issue dealt with?	Repudiation requirement must be determined and the authentication mechanism matched to the requirement. Procedural framework Legal accreditation (eg as for digital signature legislation) Service provider willing to accept risk
Is the issue resolved?	Mostly a problem for the future, when a substantial number of financial and other contractual transactions are endorsed by biometric authentication. Needs further development of technology and supporting legal framework

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

Biometric system may be initially adequately secure but become less secure: Security sensitive parameters become misadjusted Procedural lapses lead to poor quality enrolments System has been successfully attacked and impostors become enrolled Self-adaptive biometric system develops poor reference templates through poor user discipline	
Ramifications	Poor reference templates may allow impostor access Adaptive systems may allow impostor to train him/herself onto the system (in collusion with an enrolee)
Applications affected	Any
Biometrics affected	Any, but may be a particular problem with self-adaptive systems
Differences to non-biometric authentication	Systems using non-biometric authentication may also become less secure (eg strong passwords changed to weak ones)
How is the issue dealt with?	System detects poor discrimination between enrolled templates System records values and changes to security parameter, details of new enrolees, authentication failures. Procedural measures to check audit log
Is the issue resolved?	Current and future issue. In the future, large scale systems will make the problem worse, particularly if the security data is distributed round a network, making overall system audit difficult Needs further work to scope problem and develop better solutions

3.1.17 Does publicizing countermeasures make the systems less secure?

If countermeasures employed in biometric systems are publicised, it will help attackers to avoid or defeat them Similarly, if attackers know what countermeasures are not employed, this will help them identify likely weaknesses in the system, and direct attacks towards weak areas Complement of the argument about publicising vulnerabilities (ie countermeasure = [probable]lack of vulnerability; no-countermeasure= [potential] vulnerability) 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	
Ramifications	Can't depend on security through obscurity indefinitely. Can't put the genie back in the bottle
Applications affected	Applications employing biometrics with known vulnerabilities may be subject to attack
Biometrics affected	Any
Differences to non-biometric authentication	Compare to current situation of widespread public knowledge of IT security countermeasures and vulnerabilities
How is the issue dealt with?	Draw parallel with IT security technology, vulnerabilities and countermeasures. This is not an argument in the IT field Promote similar handling to IT industry handling of security vulnerabilities/countermeasures eg CERT Use knowledge to build in and improve security countermeasures
Is the issue resolved?	Current issue, likely to be even bigger issue in future.

3.2 User security issues

3.2.1 Could I accidentally give my biometric 'signature'?

Users may be concerned that they unintentionally unlock a door, or authorise a payment when close to a biometric application	
Ramifications	This might have serious financial or safety consequences, but is unlikely since the issue is generally addressed if applicable.
Applications affected	Applications where the biometric is used to authorise or sign a transaction.
Biometrics affected	Any that do not require an explicit consensual action
Differences to non-biometric authentication	Non-biometric systems generally require an explicit user action. An exception is the use of contactless (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.
How is the issue dealt with?	For authorisation type applications, the process should involve an explicit action implying consent, for example the insertion of card or typing in a Personal Identification Number. There is a converse 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.
Is the issue resolved?	The issue is easily addressed, and this is not likely to change.

3.2.2 Can my biometric be collected covertly?

Users may have concerns about being identified or tracked by covert applications (both legal and illegal).	
Ramifications	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.
Applications affected	Watchlist applications, biometrics on top of existing applications (for example keystroke monitoring).
Biometrics affected	Some biometrics are easily used 'covertly'. For example face recognition, speaker verification, and gait recognition can work from a distance. There is no way of knowing whether a CCTV camera is biometrically enabled. Even close-up and contact biometrics can be used covertly – eg recognition of latent fingerprints, covert fingerprint sensor in doorknob, or iris recognition through a 1-way mirror
Differences to non-biometric authentication	Non biometric identifiers cannot be collected covertly
How is the issue dealt with?	Currently storage capacities, and poor performance of face recognition systems limit its covert use.
Is the issue resolved?	Currently this is of minor concern. However as the technology develops, the performance of covert biometric identification is likely to increase. So this is potentially a major concern for the future.

3.2.3 Can my biometric be stolen?

<table>
<tr><td colspan="2">Can the biometric template or biometric feature vector be stolen, and if so what are the consequences.</td></tr>
<tr><td><b>Ramifications</b></td><td>If biometric template data are stolen, either: (i) directly, from the stored reference templates, or (ii) by capturing the data in transit within the system or (iii) on a communication path between the biometric capture device and the rest of the system; then that template data could be reused by an impostor to recreate the identity of the authorised user without the user being present, thus undermining the authentication integrity and granting 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 (eg 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.
The captured biometric might be used to discover zero-effort false matches in the criminal fraternity.</td></tr>
<tr><td><b>Applications affected</b></td><td>All</td></tr>
<tr><td><b>Biometrics affected</b></td><td>All</td></tr>
<tr><td><b>Differences to non-biometric authentication</b></td><td>PINs and Passwords can be stolen by shoulder surfing, and smart cards and tokens can be stolen. However these are replaceable whereas biometrics are not.</td></tr>
<tr><td><b>How is the issue dealt with?</b></td><td>Liveness tests would ensure that the biometric is actually being submitted from a person.
Template & feature vector time stamping and encryption can prevent re-use. Template transformation techniques can prevent compromise of the template or feature vector from compromising the entire template.</td></tr>
<tr><td><b>Is the issue resolved?</b></td><td>Further work is needed.</td></tr>
</table>

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

Can the user find out when they have been biometrically identified?	
Ramifications	
Applications affected	
Biometrics affected	
Differences to non-biometric authentication	
How is the issue dealt with?	If audit trails are kept, users might already have this right under data protection legislation.
Is the issue resolved?	

3.2.5 Does the use of biometrics increase likelihood of capture/coercion?

Ramifications	
Applications affected	
Biometrics affected	
Differences to non-biometric authentication	In non-biometric applications the token/password can be surrendered. But the criminal would not release the person until the password is known to have worked. The dependency is less on the technology and more on the value of the protected assets.
How is the issue dealt with?	Duress codes
Is the issue resolved?	

3.2.6 ID theft becomes worse if there is a single strong identifier

A biometric identifier might become the sole means of identification. Then any identification error can have dire consequences. Without biometrics people rely on a multitude of components that each provide a weaker identification. The consequences of a single failure are then less drastic.	
Ramifications	
Applications affected	
Biometrics affected	
Differences to non-biometric authentication	Without biometrics people rely on a multitude of components that each provide a weaker identification. The consequences of a single failure are then less drastic.
How is the issue dealt with?	
Is the issue resolved?	

3.2.7 Can the biometric system with identification help a stalker?

Could, for example, an operator use the biometric system to track, identify then stalk an individual?	
Ramifications	
Applications affected	
Biometrics affected	
Differences to non-biometric authentication	
How is the issue dealt with?	
Is the issue resolved?	

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

With more biometrics around the possibility of a chance match of my fingerprint with one found at the scene of crime will increase. Typically in such cases there is the assumption of guilt unless individual can either explain how their fingerprint came to be at the scene of crime, or show a good alibi.	
Ramifications	
Applications affected	
Biometrics affected	
Differences to non-biometric authentication	
How is the issue dealt with?	
Is the issue resolved?	

3.2.9 Administrator or operator misuse

An administrator can look-up the biometric database to see whom they, or their accomplices, match.	
Ramifications	An administrator on one system may be able to target his enrolees that are enrolled on another biometric system.
Applications affected	Those with a central database can be exploited in this way. Applications affected are those using the same biometric features..
Biometrics affected	Any
Differences to non-biometric authentication	In password or PIN bases systems it is recommended that different passwords are used for each system (though users often keep all their passwords to be the same!)
How is the issue dealt with?	Not really addressed by current systems, but will need to be addressed by national scale applications. Partial solutions may be: • Separation of roles, so that no single person could engineer such a look-up; • No central storage of the biometrics; • Using a different biometric for an identification check than is used for later verification; • Encryption of the database.
Is the issue resolved?	Problem exists currently, but as there are few biometric systems in use the consequences would be minor, and there is little incentive (other than curiosity) for an unscrupulous system administrator. As biometrics become more ubiquitous, and as database become larger the problems become worse. With a national id database, the administrator is likely to find a matching person. Solutions need further investigation

3.2.10 Function creep

How can one ensure that a biometric collected for one purpose is not used for another?	
Ramifications	
Applications affected	
Biometrics affected	
Differences to non-biometric authentication	
How is the issue dealt with?	Can the user bind the template to a particular application?
Is the issue resolved?	

3.2.11 Revealing personal information

What other information does my biometric reveal – either directly or probabilistically • Ethnicity • Diseases • Medication • Gender	
Ramifications	Audit log would reveal locations where the user has been present. Biometrics where there is genetic penetrance might show non-paternity if comparisons are made between family members.
Applications affected	Those with audit log, or where biometric details (eg images, templates) are revealed outside the matching engine.
Biometrics affected	Face image templates are typically compressed images. These would reveal gender and ethnicity. With speaker verification, hand image systems, gait, it should be possible to detect whether the user is probably male, or probably female.
Differences to non-biometric authentication	PINs and tokens are person independent. Non-biometric systems may still have an audit log.
How is the issue dealt with?	
Is the issue resolved?	No – refer to Biovision workpackage WP5

4 Concerns by application

Main application and user concerns by application				Application concerns											User concerns								
H = high level M = moderate L = low level	Biometric Technology	Template storage	Biometric Supervised	Performance limitations	Enrolment integrity	Enrolment quality	Spoofing (artefact/mimicry)	Residual Latent	Template integrity	Capture / replay	Biometrics not secret	Unvalidated Algorithms	Cannot change if compromised	System can become less secure	Cannot change if compromised	Template confidentiality	Biometric can be stolen	Capture / coercion	ID theft	Search against justice DB	Admin/operator misuse	Function creep	Reveals personal info
Physical access control	Hand geometry	Device	N	L	L	L	H	L	L	M	L	L	M	H	M	L	L	L	L		L		
Computer logon	Fingerprint	Central	N	L	L	L	H	H	H	H	M	L	M	M	H	M	M	L	M		M		L
Time and attendance	Hand geometry	Device	N	L	L	L	M	L	L	L	L	L	M	M	L	L	L	L	L		L		
ATM & POS	Fingerprint	Card	N	L	H	M	H	H	H	M	M	M	H	M	H	H	M	H	M	M	H	L	L
Telephone banking	Voice	Central	Y	L	H	L	H		L	H	M	L		M		M	L	L	L	L	L	L	L
Welfare, verify ID	Fingerprint	Card	Y	L	H	L	M	M	H	L	M	L	L	M	M	M	M	L	H	M	M	M	M
Welfare, unique ID	Fingerprint	Central	Y	M	H	H	L	L	L	L	M	L	L	M	L	M	M	L	J	M	M	H	M
Unique National ID	Iris	Central	Y	M	H	H	L	L	L	L	M	M	H	M	H	H	H	L	H		M	H	M
Registered traveller	Iris	Card	N	L	H	H	M		H	L	L	M	L	L	H	H	H	L	H		M	M	M
Border control	Face & hand g.	Card	Y	M	H	M	L	L	H	L	L	M	M	M	H	M	M	L	H	H	M	H	M
Watchlist	Face	Central	Y	H	L	M	M					L		L	M					M	M	M	M

5 Solutions to security problems

5.1 Device or system solutions

5.1.1 Liveness tests

For various types of liveness tests see [Valencia, 2002]	
Problems addressed	Makes it more difficult to spoof the system using artefacts
Application types	All – especially unsupervised
Biometric types	Physiological biometrics
Degree of development	Much work still required. Improvements still possible to even the systems currently best at checking liveness. No standard method for evaluating liveness claims.
Conflicts	Can increase failure to acquire rate

5.1.2 Template encryption

Problems addressed	Template integrity and confidentiality Replay attacks (if template time-stamped)
Application types	
Biometric types	
Degree of development	
Conflicts	

5.1.3 Binding template to application, Cancellable biometrics

[Cambier, 2002] – Binding template to application [Ratha et al, 2001] – Cancellable biometrics [Soutar, 2002] – Template protection	
Problems addressed	Template compromise Function creep (except with permission of application owner)
Application types	
Biometric types	
Degree of development	
Conflicts	

5.1.4 Duress codes

Entering a different PIN, or using a modified biometric (e.g. left eye instead of right) can be used as a duress signal, to raise an alarm that the user is being coerced into giving their biometric to an application.	
Problems addressed	Capture coercion
Application types	Access control, ATM,
Biometric types	
Degree of development	Standard feature for RSI HandKey
Conflicts	

5.1.5 Transaction log/audit trail

Problems addressed	Determining whether system is becoming insecure
Application types	
Biometric types	
Degree of development	
Conflicts	

5.2 Procedural solutions

5.2.1 Supervision

Problems addressed	Spoofing, Mimicry
Application types	
Biometric types	
Degree of development	
Conflicts	

5.2.2 No central database

Storing biometric on smart-card reduces problems associated with a central database. Even for applications ensuring a unique identity it is possible to have a "shadow" database that does not include any identification details, just the biometric. (The UNHCR Afghan refugee repatriation iris recognition system is an example).	
Problems addressed	Security of template storage. User concerns about misuse and function creep.
Application types	
Biometric types	
Degree of development	
Conflicts	

5.2.3 Security audit

Problems addressed	
Application types	
Biometric types	
Degree of development	
Conflicts	

5.2.4 User audit

Problems addressed	User can find out how his biometric is being used, in particular if someone else is trying to impersonate him/her.
Application types	
Biometric types	
Degree of development	
Conflicts	

5.2.5 Security evaluation/vulnerability assessment

Problems addressed	
Application types	
Biometric types	
Degree of development	So far only one biometric system has completed a common criteria evaluation.
Conflicts	

5.3 Legislation

5.3.1 Data protection act

Problems addressed	
Application types	
Biometric types	
Degree of development	
Conflicts	

6 Defining user and application security requirements

To be added in a future draft

7 References

ANSI. (2001). X9.84 Biometric Information Management and Security.

BMO. (2002). *Biometric System Protection Profile for Medium Robustness Environments.*: DoD Biometrics Management Office.

BWG. (2001). *Biometric Device Protection Profile, Issue 0.82.*: CESG Biometrics Working Group.

Cambier, J. (2002, February 2002). *Application Specific Biometric Templates.* Paper presented at the Biometrics Consortium Conference, Crystal City, VA.

Common Criteria Biometric Evaluation Working Group. (2002). *Biometrics Evaluation Methodology Supplement, Version 1.0.*: CESG.

Derakhshani, R & Schuckers, SAC. (2003). Determination of Vitality from a Non-Invasive Biomedical Measurement for Use in Fingerprint Scanners. *Pattern Recognition*.

Griffin, P. (1999). *Face Recognition and the Hill Climbing Attack.* Paper presented at the Biometric Consortium Fall '99 Conference, Crystal City.

Gunnerson, G. (1999). Are You Ready for Biometrics? *PC Magazine*(February 8).

Hill, CJ. (2001). *Risk of Masquerade Arising from the Storage of Biometrics.*, Australian National University.

Mansfield, AJ & Wayman, JL. (2002). *Best Practices in Testing and Reporting Performance of Biometric Devices. Issue 2.*: Biometrics Working Group.

Matsumoto, T, Matsumoto, H, Yamada, K & Hoshino, S. (2002). *Impact of Artificial Gummy Fingers on Fingerprint Systems.* Paper presented at the SPIE, Optical Security and Counterfeit Detection Techniques IV.

Podio, FL, Dunn, JS, Reinert, L, Tilton, CJ, O'Gorman, L, Collier, PM, Jerde, M & Wirtz, B. (2001). *CBEFF - Common Biometric Exchange File Format* (NISTIR 6529).

Ratha, NK, Connell, JH & Bolle, RM. (2001). Enhancing Security and Privacy in Biometrics-Based Authentication Systems. *IBM Systems Journal, 40*(3), 614-634.

Soutar, C. (2002). *Biometric Template Protection & Usage.* Paper presented at the Biometrics Consortium Conference, Crystal City, VA.

Tekey. (2001). How to Trick a Bright Field Optical Fingerprint Capture Sensor.

Thalheim, L, Krissler, J & Ziegler, P-M. (2002). Body Check: Biometric Access Protection Devices and Their Programs Put to the Test. *c't magazine, 11/2002*, 114.

Valencia, V. (2002). *Biometric Liveness Testing.* Paper presented at the CTST, New Orleans.

van der Putte, T & Keuning, J. (2000). *Biometrical Fingerprint Recognition Don't Get Your Fingers Burned.* Paper presented at the IFIP TC8/WG8.8 Fourth Working Conference on Smart Card Research and Advanced Applications.

Willis, D & Lee, M. (1998). Six Biometric Devices Point the Finger at Security. *Network Computing, June 1.*