



Section Two

Biometrics, Cybersecurity and Enabling Standards

Biometrics can provide a key element of identity management, both in terms of biometric user authentication and identity assurance systems. In the area of cybersecurity, it is important to know both who is attempting to access a system and that biometric identity data is itself protected. Biometrics has emerged as an important tool in supporting effective identity management by strongly binding a physical person to their identity. ISO has developed several standards that support the use of biometrics in a cybersecurity environment.

“Catherine Tilton
VP, Standards and Technology, Daon”

1 INTRODUCTION

The recent spate of cyber attacks on the US and other countries, such as Estonia and South Korea, have brought the topic of cybersecurity once again to the fore [1]. Although the press have focused primarily on website and denial of service attacks, the widespread use of open computer networks creates opportunities for other, perhaps more serious, attacks as well. Underscoring this interest, early in his administration President Obama directed that a comprehensive 60-day review of US policies and structures for cybersecurity be conducted, with the final report of that review published in late May 2009 [2].

A number of different types of cyber attacks are possible and, likewise, a range of different methods and technologies exist to counter these attacks. A question then arises regarding the role of biometrics in cybersecurity.

2 BACKGROUND

Biometrics is the “automated recognition of individuals based on their behavioural and biological characteristics” [3]. Biometric technology has numerous applications involving the identification of persons or verification of the identity of a person. These range from large government systems such as national ID and border management, to fraud prevention, to time and attendance, to physical access control, to automobile locks/ignitions. Biometrics can also be used for “logical access control”, that is, the use of biometric user authentication as part of a computer, network, or software application logon process.

There are two major areas of interest regarding biometrics and cybersecurity. The first is the use of biometrics as a security mechanism itself (i.e., biometric authentication). The second is the protection of biometric (and other identity) data within a system or application that uses biometrics for some other purpose (e.g., border security).

This is in turn related to the area of "identity management". Identity management is an overloaded term that means different things to different people. In a narrow, IT-centric sense, it relates to the management of identities for the purpose of access control - mostly logical, but sometimes physical as well. In this context, definitions like "a discipline which encompasses all of the tasks required to create, manage, and delete user identities in a computing environment" and which relate to "user accounts" are typical [4]. Many organisations and companies are addressing this type of identity management. This is where biometric user authentication applies.

In a larger context, identity management relates to the use of identity information for a purpose beyond that of IT user accounts. In this case, the definition adopted by the US National Science and Technology Council (NSTC) may apply: "the combination of technical systems, rules, and procedures that define the ownership, utilisation, and safeguarding of personal identity information. The primary goal of the IdM process is to assign attributes to a digital identity and to connect that identity to an individual." [5]. Usually, this relates to the concept of "identity assurance".

Biometrics and cybersecurity apply to both of these contexts and so each are addressed herein.

3 BIOMETRIC AUTHENTICATION

Within the larger area of information security, a key element is user identification and authentication. Confidence in the identity of the user is required before authorisation (access privilege) decisions are implemented. Although important in closed networks, it becomes even more important in open networks where the user's physical location is not controlled [6].

Traditional authentication protocols are "secrets-based" and depend on proof of knowledge or possession or both. Biometric authentication, on the other hand, is based on physical or behavioural traits of a (human) individual and depends on the ability of the claimant to present a biometric characteristic from the same source as that which was previously registered. Since biometrics are not secrets per se, the integrity and authenticity of the biometric sample are generally more critical than its secrecy [7].

The primary strengths of biometric authentication, when compared with traditional methods, are its tight binding to the individual user (providing stronger non-repudiation) [8] and its general ease of use (since there is nothing to remember or carry around). Arguably, the difficulty of mounting an attack can also be greater (i.e., greater knowledge and resources may be required). By comparison, its "procedural strength" is high compared to traditional methods where a password may be shared or written down because it is too hard to remember [9]. However, its technical strength can be lower due to lower entropy and ability to be "spoofed" when unattended and where no liveness detection is provided. Figure 1 compares the relative strengths of different authentication methods [9].

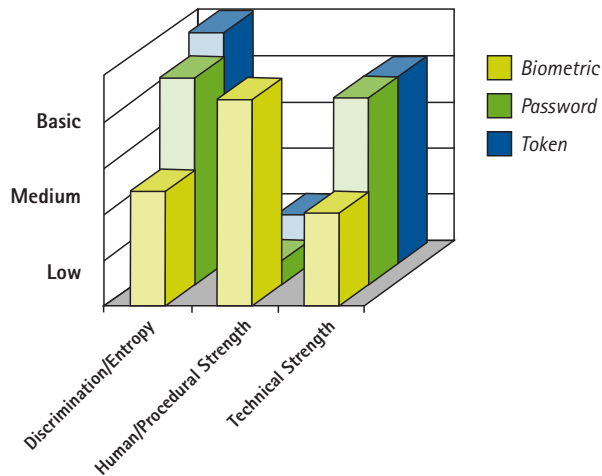


Figure 1: Comparative Strengths of Authentication Methods

Biometrics can also be used as an additional factor when used with other authentication technologies (such as a PIN/password, smartcard, and/or cryptographic token) in a multifactor authentication environment. As an example, the NIST E-Authentication Guidelines identify the use of biometrics as the means of authentication to release a cryptographic secret within a hard or soft certificate that is then used within a traditional authentication protocol [10]. Multifactor authentication is often required at higher security levels, where a higher confidence in the validity of the asserted identity is required.

When biometrics are used as part of the user authentication process, the biometric data must be protected when in transit and at rest. In addition, key biometric components used in the process should be trusted. Figure 2 illustrates the biometric process and identifies potential vulnerability points (as adapted from Ratha's original work [11]).

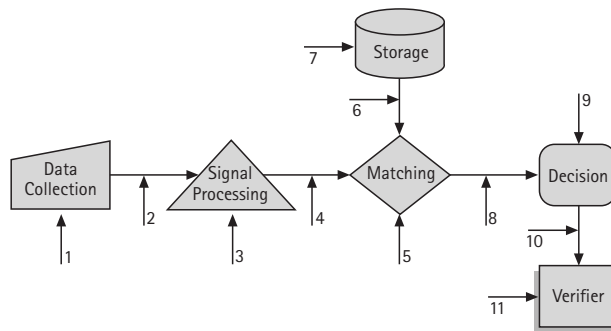


Figure 2: Biometric Threat Mode

At each point, threats and countermeasures are identified. It is noted that these threats vary depending on the biometric architecture used (e.g., where the storage and matching are located and where physical boundaries exist) [7]. As an example, the sensor spoofing threat (use of an artificial characteristic such as a latex finger) occurs at Point 1, Data Collection, and may be countered by liveness detection, challenge-response, or multi-modal implementation). Replay attacks may occur at points 2, 4, and 6 and may be countered through mutual authentication, digital signatures, timestamps and nonces.

In addition to security considerations, the privacy of biometric information must also be protected. Frequently, the same mechanisms may be applied.

For biometric authentication to be performed in either a physical or logical access control system, the biometric must be provisioned into the system. This involves an enrolment process - where the biometric information is captured from the individual and securely stored for future comparison. It may also involve the production and issuance of a credential, such as a smartcard that contains the biometric data. (In this case, the smartcard may be the only place the biometric data is retained.) The integrity of the enrolment process is also critical. Enrolment should include an "identity proofing" step to ensure that only known, eligible persons are enrolled. Also, the binding of the biometric data to the identity must be trustworthy.

4 BIOMETRIC SYSTEM SECURITY

Biometric identity systems also contain and use biometric information to accomplish other purposes than user authentication. For example, it is important to know the identity of persons crossing a border into a country. Such systems may store this information in a database in order to ensure that:

- A single identity is associated with each individual and is fixed in time.
- Individuals are not on a list of known criminals or terrorists.
- Individuals have not been previously excluded (e.g., are ineligible for services, have been deported, etc.).
- The claimed identity may be verified (i.e., at a point of service).

In such systems, the biometric (and other identity) data must be secured – protected from disclosure or manipulation – for both security and privacy reasons. This is important in single systems, but becomes even more important in a data sharing environment. The need for different systems (i.e., between agencies or even countries) to exchange information is becoming more common. For example, a border management system may need to perform a biometric search of law enforcement or national security systems to ensure that the traveller is not wanted. Similarly, in the EU a need exists for visa applicants in one country to be searched against a central system to ensure that they have not already been denied a visa by another EU member.

System security concerns for this type of system are very similar to those described above for biometric authentication systems from a general IT security perspective, and similar system design and countermeasures would apply. For instance, identity information within the database should be signed and encrypted and access controls implemented. Key components should be authenticated and transmissions protected at the application and transmission channel levels. Audit logs should be generated and protected. Robust key management and distribution is needed.

One area where the system security may differ is in the area of sensor spoofing. In IT systems, the goal of spoofing is to trick the system into believing that a falsely claimed identity is true by making the system accept an artefact that results in a successful match, thus granting access. However, in systems that perform negative identification (i.e., ensuring that to gain access/benefit/privilege the subject is NOT in the database) the subject is trying to trick the system into a non-match. This is sometimes referred to as "obfuscation" and may be attempted to avoid detection during uniqueness or watchlist checks. In this case, the subject may try to use an artefact or to hide or mutilate their biometric enough to cause it not to match. In addition to the techniques previously identified, use of image processing techniques to detect suspicious samples may be employed. Multi-biometric techniques, including fusion, can also serve to counter such attacks.

Securing biometric systems requires a layered "defense in depth" strategy, addressing both technology and systemic weaknesses. Security must be end-to-end and by design rather than spotty and "bolted on" after the fact. It should address both the insider and outsider threat and should assume a hostile network/environment.

It should be noted that although government systems have mostly been used as examples, the considerations discussed apply equally to commercial biometric systems.

5 SUPPORTING STANDARDS

Where biometrics intersect with security, the work of several ISO committees/subcommittees applies. Though not necessarily comprehensive, the following standards can help address many of the considerations identified above.

a) ISO/IEC JTC 1 SC 37

Subcommittee 37, Biometrics, develops generic biometric standards in the areas of vocabulary (WG 1), technical interfaces (WG 2), data interchange formats (WG 3), application profiles (WG 4), performance testing and reporting (WG 5), and cross-jurisdictional and societal aspects (WG 6) of biometrics. Some of these have developed standards

that are used in biometric authentication and identity systems. For example, biometric data representations are specified in the ISO/IEC 19794 (Biometric Data Interchange Format) series of standards and data structures are defined in ISO/IEC 19785 (Common Biometric Exchange Formats Framework).

Both CBEFF and BioAPI (ISO/IEC 19794) provide a biometric data structure (called a biometric information record, or BIR) that provides for the confidentiality and integrity of the biometric data through header elements and an optional security block (which could contain, for example, a digital signature or encryption parameters). In addition, other elements of the biometric header can also contribute to the protection of the data. These include payload and challenge–response elements as well as a “purpose” field. When signed, this can prevent enrolment data from being replayed as a captured biometric verification sample. BioAPI is currently being extended to support the exchange of certificates and security assertions.

The work of WG 5 in the 19795 (Biometric performance testing and reporting) series specifies the methodology for quantifying the performance of biometric systems and algorithms. This allows implementers to have more confidence in the error rates associated with biometric components used in their systems, taking these into consideration in their design.

b) ISO/IEC JTC 1 SC 27

Subcommittee 27, IT Security Techniques, in addition to general IT security and cryptographic standards that would apply to biometric system security and data protection, has several standards and projects that relate directly to the area of biometric security or identity management. These include:

- **ISO/IEC 24761:2009, Information technology – Security techniques – Authentication context for biometrics (ACBio)**
ACBio specifies a technique for securing remote biometric authentication over an open network. It includes methods for message integrity, component authentication, and an associated cryptographic syntax.
- **ISO/IEC 19792:2009, Information technology – Security techniques – Security evaluation of biometrics**
This standard addresses the basis of trust in the security of applied biometrics in the context of common criteria testing.
- **ISO/IEC 24745 – Information technology – Security techniques – Biometric template protection (Committee Draft)**
This standard addresses methods for protecting biometric data, including the confidentiality, integrity, and availability thereof. It also addresses template binding techniques and biometric cryptosystems.

- **ISO/IEC 24760, Information technology – Security techniques – A Framework for Identity Management (Committee Draft)**

This project provides an ontology and structure to facilitate common representations for the many diverse conceptualisations and implementations of Identity Management. In its draft form, it seeks to [12]:

- Define identity and the concepts of managing identity information, including identity management capabilities;
- Provide principles for frameworks that may serve the management of identities and the respective applicable requirements (e.g., policy, law); and
- Provides rules for the secure and reliable processes of managing identity information, including the control of the lifecycle of identities and identity information as they are established, activated, suspended, terminated or archived.

c) ISO TC 68

TC 68, Financial Services, has developed a standard focused on the security of biometric systems – ISO 19092 – 1:2006, Financial Services – Biometrics – Part 1: Security Framework. This standard addresses core security requirements related to the use and management of biometric data in financial systems and transactions, to include integrity, authenticity, and confidentiality. It also describes the architectures for implementation, specifies the minimum security requirements for effective management, and provides control objectives and recommendations suitable for use by a professional practitioner [13]. Though targeted at this environment, the requirements are actually very horizontal in nature and equally applicable in other environments as well.

6 CONCLUSION


Biometrics can play a key role in cybersecurity, offering the ability to both improve security and offer greater degrees of convenience as well as supplementing existing authentication mechanisms such as tokens and passwords. Their use in user authentication and identity assurance is predicated on the underlying security of the biometric data, components, and processes involved. Standards exist and are emerging that address these needs; however, system implementations must incorporate strong security layered throughout the design. A biometric identity lifecycle and chain of trust model should be part of this.

7 ACKNOWLEDGEMENTS

My appreciation to Conor White for his thought leadership in this area and to the members of the INCITS M1 Ad Hoc Group on Biometrics in E-Authentication who have contributed to the discourse on these subjects.

8 REFERENCES

- [1] Baldor, Lolita C. "Federal Web sites knocked out by cyber attack". Associated Press, 8 July 2009.
- http://news.yahoo.com/s/ap/20090708/ap_on_go_ot/us_cyber_attack
- [2] "Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure", 29 May 2009.
- http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf
- [3] "Harmonized Biometric Vocabulary". ISO/IEC JTC 1 SC 37 Standing Document 2 (SD2).
- <http://isotc.iso.org/livelink/livelink/fetch/2000/2122/327993/2262372/customview.html?func=ll&objId=2262372&objAction=browse&sort=name>
- [4] <http://www.tech-faq.com/identity-management.shtml>
- [5] National Science and Technology Council Subcommittee on Biometrics and Identity Management. "Identity Management Task Force Report 2008".
- <http://www.biometrics.gov/>
- [6] Burr, William. "Biometrics and Electronic Authentication" Biometric Consortium Conference, Arlington, VA., 20 September 2005.
- http://www.biometrics.org/bc2005/Presentations/Conference/2%20Tuesday%20September%2020/Tue_%20Ballroom%20E/BurrBiomConf05.pdf
- [7] International Council on Information Technology Standards, Technical Committee M1 (Biometrics), "Study Report on Biometrics in E-Authentication", 30 March 2007.
- http://www.incits.org/tc_home/m1htm/m1070185rev.pdf
- [8] O'Gorman, Lawrence. "Comparing Passwords, Tokens, and Biometrics for User Authentication" Proceedings of the IEEE, Vol. 91, No. 12, Dec. 2003, pp. 2019-2040.
- [9] Statham, Philip. "Threat Analysis, How Can We Compare Different Authentication Methods?" Biometric Consortium Conference, Arlington, VA., 2005.
- http://www.biometrics.org/bc2005/Presentations/Conference/Wednesday%20September%2021/Wed_Ballroom%20B/Statham%20-%20Comparing%20Auth%20Mechanisms.pdf
- [10] NIST SP800-63, Electronic Authentication Guideline (v 1.0.2), April 2006.
- http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf

- 
- [11] Ratha, N.K., Connell, J.H., and Bolle, R.M. "Enhancing security and privacy in biometrics-based authentication systems" IBM Systems Journal, 2001. 40(3).
- [12] ISO/IEC 6th Working Draft 24760 - Information technology - Security techniques - A framework for identity management (not yet published).
- [13] ISO 19092-1:2006, Financial Services - Biometrics - Part 1: Security Framework.

BIOGRAPHY OF AUTHOR



Catherine Tilton

VP, Standards and Technology
Daon

Mrs Catherine Tilton is the VP for Standards & Emerging Technologies at Daon. Cathy has over 25 years of engineering and management experience, including over 15 years in the biometrics industry. She has lead or been involved in the design, development, and deployment of numerous biometric systems in both the commercial and government domains. These include the US-VISIT program, the Transportation Worker Identification Credential (TWIC), US Registered Traveler and in a previous life, IAFIS. Past work also included several contracts prototyping the use of biometrics with the DoD CAC card and a number of international projects. Mrs Tilton is very active in the development of national and international biometric standards, currently serving as the US head of delegation to ISO/IEC JTC 1 SC 37 subcommittee on biometrics. She also chairs the BioAPI Consortium, is an officer of the International Committee on Information Technology Standards (INCITS) M1 technical committee on biometrics, and chairs the Biometric Identity Assurance Services (BIAS) Integration technical committee at OASIS. She has a BS in nuclear engineering from Mississippi State and an MS in systems engineering from Virginia Tech.