Department of Computer Science,
University of Otago

Technical Report OUCS-2004-21

Biometric security: Concepts, Issues and Flaws

Author:
Stewart Fleming
Department of Computer Science, University of Otago

Status:
To appear in M. Pagani (ed) Encyclopedia of Multimedia & Technology.
Hershey, PA: IDEA Group Publishing.

Department of Computer Science,
University of Otago, PO Box 56, Dunedin, Otago, New Zealand

http://www.cs.otago.ac.nz/research/techreports.html

DRAFT ENCYCLOPEDIA SUBMISSION

Biometric Security
Concepts, Issues and Flaws

Stewart T. Fleming
Department of Computer Science, University of Otago,
Dunedin, New Zealand.

INTRODUCTION

Information security is concerned with the assurance of confidentiality, integrity and availability of information in all forms. There are many tools and techniques that can support the management of information security and systems based on biometrics have evolved to support some aspects of information security. Biometric systems support the facets of identification/authorization, authentication and non-repudiation in information security.

Biometric systems have grown in popularity as a way to provide personal identification. Personal identification is crucially important in many applications and the upsurge in credit-card fraud and identity theft in recent years indicates that this is an issue of major concern in wider society. Individual passwords, PIN identification, cued keyword personal questions or even token-based arrangements all have deficiencies that restrict their applicability in a widely-networked society. The advantage claimed by biometric systems is that they can establish an unbreakable one-to-one correspondence between an individual and a piece of data.

The drawback with biometric systems is their perceived invasiveness and the general risks that can emerge when biometric data is not properly handled. There are good practices which, when followed, can provide the excellent match between data and identity that biometrics promise; if not followed, can lead to enormous risks to privacy for an individual.

Biometric Security

Jain *et al.* (2000) define a biometric security system as: "...essentially a pattern-matching system which makes a personal identification by establishing the authenticity of a specific physiological or biological characteristic possessed by the user." An effective security system combines at least two of the following three elements: "something you have, something you know are something you are" (Schneier, 2000). Biometric data provides the "something you are" – data is acquired from some biological characteristic of an individual. However, biometric data is itself no guarantee of perfect security – a combination of security factors, even a combination of two or more biometric characteristics, is likely to be effective (Jain *et al.*, 1999). Other techniques are needed to combine with biometrics to offer the characteristics of a secure system – confidentiality (privacy), integrity, authentication and non-repudiation (Clarke, 1998).

Biometric data comes in several different forms that can be readily acquired, digitized, transmitted, stored and compared in some biometric authentication device. The personal and extremely sensitive nature of biometric data implies that there are significant privacy and security risks associated with capture, storage and use (Schneier, 1999).

Biometric data is only one component in wider systems of security. Typical phases of biometric security would include acquisition of data (the biological characteristic), extraction (of a template based on the data), comparison (with another biological characteristic) and storage. The exact design of biometric systems provides a degree of flexibility in how activities of enrollment, authentication, identification and long-term storage are arranged. Some systems only require storage of the data locally within a biometric device; others require a distributed database that holds many individual biometric samples.

B A C K G R O U N D

Biometric security systems can be logically divided into separate phases of operation – separating enrollment of a biometric from extraction and coding into a template form to authentication where a sample acquired from an individual at some time is compared with one enrolled at a previous time. The enrollment and comparison of biometric data is done by some biometric authentication device and a variety of biometric data can be used as the basis for the authentication. The characteristics of a number of different devices are described and then the particular risks and issues with these devices are discussed in the main part of this article.

Types of Biometric device

Several types of biometric data are commonly in use. Each of the following types of device captures data in a different form and by a different mechanism. The nature of the biometric data and the method by which it is acquired determines the invasiveness of the protocol for enrollment and authentication. The method of acquisition and any associated uncertainties in the measurement process can allow a malicious individual to attack the security of the biometric system, by interfering with the capture mechanism or by substituting biometric data.

Fingerprint scanner – acquires an image of a fingerprint, either by optical scanning or capacitance sensing. Generation of biometric templates is based on matching minutiae – characteristic features in fingerprints.

Retinal / iris scanner – both are forms of biometric data capture based on scanning different parts of the eye. In a retinal scan, a biometric template is formed by recording the patterns of capillary blood vessels at the back of the eye. Iris scanning can be performed remotely using a high-resolution camera and templates generated by a similar process to retinal scanning.

Facial scanner – facial recognition works by extracting key characteristics such as relative position of eyes, nose, mouth and ears from photographs of an individual's head or face. Authentication of facial features is quite sensitive to variations in the environment (camera position, lighting etc) to those at enrollment.

Hand geometry – scanners generate templates based on various features of an individual's hand, including finger length. Templates generated can be very compact and the method is often perceived by users to be less invasive than other types of biometric device.

Voiceprint – voiceprint recognition compares the vocal patterns of an individual with previously enrolled samples. An advantage of voiceprint techniques over other forms of biometric is the potential to detect duress or coercion through the analysis of stress patterns in the sample voiceprint.

DNA fingerprint – this method works by taking a tissue sample from an individual and then sequencing and comparing short segments of DNA. The disadvantages of the technique

are in its overall invasiveness and the speed at which samples can be processed. Due to the nature of the process itself, there is an extremely low false acceptance rate but an uncertain false rejection rate.

Deep tissue illumination – a relatively new technique (Nixon, 2003) that involves illumination of human tissue by specific lighting conditions and the detection of deep tissue patterns based on light reflection. The technique is claimed to have less susceptibility for spoofing than other forms of biometric techniques as it is harder to simulate the process of light reflection.

Keystroke pattern – technique works by detecting patterns of typing on a keyboard by an individual against patterns previously enrolled. Keystroke biometrics have been used to "harden" password entry – to provide greater assurance that a password was typed by the same individual that enrolled it, by comparing the pace at which it was typed.

Typically, the raw biometric data that is captured from the device (the measurement) is encoded into a biometric template. Extraction of features from the raw data and coding of the template are usually proprietary processes. The biometric templates are normally used as the basis for comparison during authentication. Acquisition, transmission and storage of biometric templates are important aspects of biometric security systems as these are areas where risks can arise and attacks on the integrity of the system can be made.

In considering the different aspects of a biometric system below, we focus on the emergent issues and risks concerned with the use of this kind of data. Careful consideration of these issues is important due to the overall concern with which users view biometric systems and the gaps between the current state of technological development and legislation to protect the individual. In considering these issues, we present a framework based on three important principles of privacy, awareness and control.

M A I N F O C U S

For a relatively new technology, biometric security has the potential to affect broad sectors of commerce and public society. While there are security benefits and a degree of convenience that can be offered by the use of biometric security, there are also several areas of concern. We examine here the interaction of the three main issues: privacy, awareness and consent as regards biometric security systems and show how these can contribute to risks that can emerge from these systems.

Privacy

There are several aspects to privacy with relation to biometrics. Firstly, there is the necessary invasiveness association with the acquisition of biometric data itself. Then there are the wider issues concerned with association of such personal data with the real identity of an individual. Since biometric data can never be revoked, there are concerns about the protection of biometric data and in many areas.

A biometric security system should promote the principle of authentication without identification where possible. That is, rather than identifying an individual first and then determining the level of access that they might have, authentication without identification uses the biometric data in an anonymous fashion to determine access rights. Authentication without identification protects the privacy of the user by allowing individuals to engage in activities that require authentication without revealing their identities.

Such protection can be offered by some technologies that combine biometric authentication with encryption (Bleumer, 1998, Impagliazzo & More, 2003). However, in many situations, more general protection needs to be offered through legislation rather than

from any characteristic of the technology itself. Here we find a serious gap between the state of technological and ethical or legal developments.

Legislative protections are widely variable across different jurisdictions. The United Kingdom Data Protection Act (1998), European Union Data Protection Directive (1995) and New Zealand Privacy Act (1994) afford protection to biometric data at the same level as personal data. In the United States, the Biometric Identifier Privacy Act in New Jersey has been enacted to provide similar levels of protection. The Online Personal Privacy Act that proposed similar protections for privacy of consumers on the Internet was introduced into the United States Senate (Hollings 2002, SS2201 Online Personal Privacy Act, 2002) but was not completed during the session; the bill has yet to be re-introduced.

Awareness and Consent

If an individual is unaware that biometric data has been acquired, then they can hardly have given consent for it to be collected and used. Various systems have been proposed (and installed) to capture biometric data without the expressed consent of an individual, or even without informing the individual that such data is being captured. Examples of such systems include the deployment of facial recognition systems linked to crowd-scanning cameras at the Superbowl in Tampa Bay (Wired, December 2002) or at various airports (*e.g.* Logan International Airport, reported in Boston Globe July 2002). While it would appear from the results of such trials that these forms of biometric data acquisition/matching are not yet effective, awareness that such methods could be deployed is a major concern.

Consent presupposes awareness; however, consent is not such an easy issue to resolve with biometrics. It also presupposes that either the user has some control over how their biometric data is stored and processed, or that some suitable level of protection is afforded to the user within the context of the system. The use of strong encryption to protect biometric data during storage would be a good example of such protection. It is crucial to reach some form of agreement between all parties involved in using the system – both those responsible for authenticating and the individuals being authenticated. If the user has no alternative other than to use the biometric system, can they really be said to consent to use it?

Risks

Biometric devices themselves are susceptible to a variety of attacks. (Ratha, Connell & Boyle, 2001) list eight possible forms of attack (Table 1) that can be used by a malicious individual to attempt to breach the integrity of a system in different ways.

Table 1: Types of attack on a biometric system.

Generic attacks

- Presentation of a fake biometric ("spoofing"),
- Replay attack (pre-recorded biometric data),
- Interference with biometric feature extraction,
- Interference with template generation,
- Interference with comparison algorithm,
- Data substitution of biometric in storage,
- Interception of biometric data between device and storage,
- Overriding the final decision to match the biometric data

Specific attacks

- Dummy silicone fingers, duplication with and without cooperation (van der Putte and Keuning, 2000)
- Present a fake fingerprint based on a gelatine mould (Matsumoto, 2002).
- Present fake biometrics or confuse the biometric scanners for fingerprints, facial recognition and retinal scanners (Thalheim *et al.*, 2002).

Uncertainty in the precision of acquiring and comparing biometric data raises risks of different kinds – associated with false acceptance and false rejection of biometric credentials. False acceptance has the more significant impact – if a user who has not enrolled biometric data is ever authenticated, this represents a serious breakdown in the security of the overall system. On the other hand, false rejection is more of an inconvenience for the individual – they have correctly enrolled data but the device has not authenticated them for some reason. The degree of uncertainty varies between devices for the same type of biometric data and between different types of biometric. Adjusting the degree of uncertainty of measurement allows the designer of a biometric security system to make the appropriate trade-offs between security and convenience.

"Biometrics are not secrets" (Schneier, 1999). If biometric data is ever compromised, it raises a significant problem for an individual. If that data is substituted by a malicious individual, then the future transactions involving their credentials are suspect. Biometric data can never be revoked and hence should be afforded the highest protection. Fingerprint-based biometrics for example, are relatively commonly used and yet fingerprints are easily compromised, and can even be stolen without the knowledge of the individual concerned.

The class of attacks noted as "spoofing" above exploit this uncertainty and allow the integrity of a biometric system to be undermined by allowing fake biometric data to be introduced. We examine below how this class of attack can be conducted.

Spoofing Biometric Security

"Spoofing" is a class of attack on a biometric security system where a malicious individual attempts to circumvent the correspondence between the biometric data acquired from an individual and the individual themselves. That is, they try to introduce fake biometric data into a system that does not belong to them, either at enrollment and/or authentication.

The exact techniques for spoofing vary depending on the particular type of biometric involved. Typically though, such methods involve the use of some form of prosthetic, such as a fake finger, or substitution of a high-resolution image of an iris, or a mask and so on. The degree of veracity of the prosthetic varies according to the precision of the biometric device being spoofed and the freedom that the attacker has in interacting with the device. It

is surprising how relatively simple methods can be successful at circumventing the security of commonly-available contemporary biometric devices (Thalheim et al, 2002, Matsumoto, 2002). Reducing the freedom that a potential attacker has via close supervision of interaction with the authentication device may be a solution; incorporation of different security elements into a system is another.

Two- or even three-factor (inclusion of two or three of the elements of security from Schneier's definition) security systems are harder to spoof, hence the current interest in smart-cards and embedded authentication systems where biometric authentication is integrated with a device that the individual carries with them and uses during enrollment and authentication. A wider solution is the notion of a competitive or adversarial approach to verifying manufacturer's claims and attempting to circumvent biometric security (Matsumoto, 2002). Taking the claims made by manufacturers regarding false acceptance and false rejection rates and the degree to which their products can guarantee consideration only of "live" biometric sources, is risky and can lead to a reduction in overall system integrity.

C O N C L U S I O N

While biometric security systems can offer a high degree of security, they are far from perfect solutions. Sound principles of system engineering are still required to ensure a high level of security rather than the assurance of security coming simply from the inclusion of biometrics in some form.

The risks of compromise of distributed database of biometrics used in security applications are high – particularly where the privacy of individuals and hence non-repudiation and irrevocability are concerned (see (Meeks, 2001) for a particularly nasty example). It is possible to remove the need for such distributed databases through the careful application of biometric infrastructure without compromising security.

The influence of biometric technology on society and the potential risks to privacy and threat to identity will require mediation through legislation. For much of the short history of biometrics, the technological developments have been in advance of the ethical or legal ones. Careful consideration of the importance of biometric data and how it should be legally protected is now required on a wider scale.

R E F E R E N C E S

Clarke, R. (1998). Cryptography in Plain Text. *Privacy Law and Policy Reporter, 3*(2), 24-27.

Hollings, F. (2002). *Hollings Introduces Comprehensive Online Privacy Legislation*. [online] Available: http://hollings.senate.gov/~hollings/press/2002613911.html

Jain, A., Hong, L., & Pankanti, S. (2000). Biometrics: Promising Frontiers for Emerging Identification Market. *Communications of the ACM, 43*(2), 91-98.

Jain, A. K., Prabhakar, S., & Pankanti, S. (1999). *Can multi-biometrics improve performance?* In Proceedings of AutoID '99, Summit, NJ (pp. 59-64).

Matsumoto, T. (2002). *Gummy and Conductive Silicone Rubber Fingers: Importance of Vulnerability Analysis.* In Y. Zheng (ed.) Advances in Cryptology - ASIACRYPT 2002, Queenstown, New Zealand (pp. 574-575).

Meeks, B. N. (2001). Blanking on Rebellion: where the future is "Nabster". *Communications of the ACM, 44*(11), 17.

Nixon, K. (2003). *Research & Development in Biometric Anti-Spoofing.* Paper presented at the Biometric Consortium Conference, Arlington, VA.

Putte, T. van der, & Keuning, J. (2000). *Biometrical Fingerprint Recognition: Don't Get Your Fingers Burned.* In J. Domingo-Ferrer, D. Chan & A. Watson (ed.) Fourth Working Conference on Smart Card Research and Advanced Applications, Bristol, UK (pp. 289-303).

Ratha, N. K., Cornell, J. H., & Bolle, R. M. (2001). A biometrics-based secure authentication system. *IBM Systems Journal, 40*(3).

S2201 Online Personal Privacy Act: Hearing before the Committee on Commerce, Science and Transportation, United States Senate, 107th Sess. (2002).

Schneier, B. (1999). Biometrics: Uses and abuses. *Communications of the ACM, 42*(8).

Schneier, B. (2000). *Secrets and Lies: Digital Security in a Networked World*. New York: Wiley.

Thalheim, L., Krissler, J., & Ziegler, P.-M. (2002, November). Body Check - Biometric Access Protection Devices and their Programs put to the test. *c't Magazine*, 114.

Tomko, G. (1998). *Biometrics as a Privacy-Enhancing Technology: Friend or Foe of Privacy*. Paper presented at the Privacy Laws and Business Privacy Commissioners / Data Protection Authorities Workshop, Santiago de Compostela, Spain.

Terms and Definitions

Biometric – some measurement of the biological characteristics of a human subject. A useful biometric is one that is easily acquired and digitized and where historical samples can be readily compared with contemporary ones.

Biometric encryption – a technique whereby the biometric data is used as a personal or private key to be used in some cryptographic process.

Enrolment – the initial acquisition and registration of biometric data for an individual. Dependent on the type of biometric system, this data may be registered in association with the identity of the user, or against some pseudonym that preserves anonymity.

Authentication – the process by which a contemporary biometric sample is acquired from an individual and used to compare against a historically enrolled sample. If the samples match, the user is authenticated. Depending on the type of system, the authentication may be prompted by some additional information – a key to the identity of the user, or the pseudonym against which the enrolled data was registered.

False acceptance – a case where an individual is authenticated when they were not the person that enrolled the original sample.

False rejection – a case where an individual is not authenticated, although they have previously enrolled biometric data.

Spoofing – an activity where a malicious individual aims to compromise the security of a biometric system by substituting fake biometric data in some form or another. Anti-spoofing techniques are measures designed to counteract spoofing activities.

Irrevocability – the inability of an individual to be able to somehow cancel some credential. Biometric systems run a high risk of compromising irrevocability if biometric data belonging to an individual is ever acquired and used to spoof a system.

Non-repudiation – the inability of an individual to disavow some action, or their presence at a particular location at some specific time. Biometric security systems have the potential to offer a high degree of non-repudiation due to the intimately personal nature of biometric data.