The University of Saskatchewan
Department of Computer Science

Technical Report #2012-02

UNIVERSITY OF SASKATCHEWAN

Biometric Authentication: The Security Issues

Minhaz Fahim Zibran

Department of Computer Science
University of Saskatchewan, Canada
Email: minhaz.zibran@usask.ca

Abstract. Access control and authentication have become very common activities at this modern information age to ensure information security and authorized access to the information. Traditional authentication mechanisms require the users to remember secret words or phrase, or carry identification documents like passports, smart cards, etc. Biometric authentication relieves the users from the pain of remembering numerous secret passwords. People tend to believe that biometrics would provide better security in authentication systems, and such biometric authentication systems are being developed for use in areas like border security, airport security, banking, and so on. However, there are security issues about biometric authentication, which must be taken into consideration in developing and deploying biometric authentication systems for massive use. Based on review of existing literature in the area, this paper presents security concerns about biometric authentication and its implementations.

The security issues pointed out in this paper reveals areas of further research in biometric authentication, and also will help to develop more reliable biometric authentication systems for ubiquitous use.

1 Introduction

Today we are living in digital kingdoms having computer slaves, who make our life much easier, but not necessarily more secure. With the advancement of science and technology our daily activities have become faster and easier at the cost of having complex tools and technologies. Think about the Stone Age when valuable data were probably engraved on gigantic stone, where to steal such data or corrupt it would have taken a tremendous effort. In today's modern world information storage and transfer have been much easier with the help of technologies like database, networks, etc. It has been possible to access remote information without being physically present on site. This necessitates efficient mechanisms for access control and user authentication.

Traditional authentication systems requires the user perform the cumbersome task of memorizing numerous passwords, personal identification numbers (PIN), pass-phrase, and/or answers to secret questions like "what is your mother's maiden name?", etc. in order to access various databases and systems. More often, it becomes almost impossible to the different formats due to case sensitivity, requirement of alphanumeric text, and the necessity to change passwords or

pass-phrases periodically to prevent from accidental compromise or theft. Many users choose passwords to be part of their names, phone numbers, or something which can be guessed. Moreover, to handle the hard task of remembering so many passwords, people tend to write them in files, and conspicuous places such as desk calendars, which exposes chances of security violation [4].

Biometric authentication comes in play to deal with these difficulties with traditional password systems. Potentially, biometric systems can be employed in all applications that need authentication mechanism, and so in all applications that today use passwords, PINs, ID cards, or the like [11]. However, biometric authentication is not the silver bullet for secure authentication. Spoofing of biometric systems for misappropriation of biometric data is a realistic security threat. The consequences hereof can be very severe, because biometric characteristics in principle cannot be changed, unless biometric are used in a revocable way [10]. Based on literature review, this paper identifies security issues of biometric authentication systems and possible security attacks on biometric systems.

The remaining of the paper is organized as follows. Section 2 discusses about user authentication, and introduces biometric authentication with a historical overview of it. In section 3 the security concerns of biometric authentication is discussed, and finally section 4 concludes the paper with some remarks about recent advances towards the goal of achieving better biometric security, and also discussion about the usability issues, which hinder end users' acceptance of the technology.

2 Authentication and Biometrics

In general the term *authentication* is given by Bishop [3] as:

> "Authentication is the binding of an identity to a subject."

A wider definition from the the domain of telecommunications do not bind authentication to subjects [1]:

> "[Any] security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information."

The definitions imply that any authentication process operates on information of two categories. Firstly, an identification string logically and uniquely assigned to a subject, and secondly, some sort of information related to the subject allowing a decision on authenticity, i.e., is the person the one he/she claims to be [14]. Typically, authentication is done based on information about one or more of the following [3, 13, 15]:

i. Knowledge of the subject, such as password or secret information.
ii. Possession of the user, such as smart card, passport, driver's license, etc.
iii. Biometric traits of the client, such as fingerprint, voice, iris, etc.

2.1 Biometric

This paper concentrates on the security issues to authentication scheme based on the third category of information as stated above, namely biometric authentication. A biometric system is essentially a pattern recognition system that operates by acquiring physiological and/or behavioral characteristics from individual (such as fingerprint, iris scan, retina scan, hand geometry, etc.), extracting a set of features from the acquired data, and comparing this feature set against the set of templates pre-stored in the database [8, 9].

Fingerprint is probably the most used for biometric authentication. It is also likely to be the oldest biometric in use. There is archeological evidence that fingerprints as a form of identification have been used at least since 7000 to 6000 BC by the ancient Assyrians and Chinese. Clay pottery from this age sometimes contain fingerprint impressions placed to mark the potter. Chinese documents bore a clay seal marked by the thumbprint of the originator. Till date, beside improvements of fingerprint recognition, many other biometrics have been revealed namely, face recognition, voice recognition, hand geometry, iris recognition, retinal pattern recognition, etc. The basis of every biometric based authentication system is the fact that the biometric characteristic used to identify and/or verify users is unique for each user. There are also other factors such as universality, permanence, etc., which relate to security concerns of biometric authentication.

Biometrics	Universality	Uniqueness	Permanence	Collectability	Performance	Acceptability	Circumvention
Face	high	low	medium	high	low	high	low
Fingerprint	medium	high	high	medium	high	medium	high
Hand Geometry	medium	medium	medium	high	medium	medium	medium
Iris	high	high	high	medium	high	low	high
Retinal Scan	high	high	medium	low	high	low	high
Signature	low	low	low	high	low	high	low
Voice Print	medium	low	low	medium	low	high	low
F.Thermogram	high	high	low	high	medium	high	high

Fig. 1. Comparison of biometric technologies [8]

Fugure 1 presents comparison on aspects of different biometric technologies. Security issues are discussed in detail below in section 3.

3 Security Issues

The security concerns related to biometric authentication can be organized into two categories: concern about the theoretical basis of biometrics and vulnerability of biometric authentication system.

3.1 Concerns about the Theoretical Basis of Biometrics

An obvious class of biometric authentication vulnerabilities are those faced by the system user, which impact user's privacy, and may lead to identity theft or system compromise [12]:

Biometrics are not secret. Technology is readily available to image faces. fingerprints, irises, and make recording of voice or signature - without subjects' consent or awareness. From this perspective, biometrics are not secret. On the other hand, from a cryptography or privacy perspective, biometric data are often considered to be private or secret.

Biometrics cannot be revoked. A biometric feature is permanently associated with an individual, and a compromised biometric sample will compromise all applications that use that biometric. But the user cannot change her fingerprint, or retinal patterns.

Biometrics have secondary uses. If an individual uses the same biometric feature in multiple applications, then the user can be tracked if the organization share biometric data. Because of the amount and/or type of information that are also collected along with the bio record, many end users perceive biometric authentication as an intrusive process, and express concerns about how the information will be used beyond the original purpose [4].

How reliably unique the biometrics are? Many people like to think of biometrics as 'unique', but they are not, at least not with the level of data we can measure [5].

How universal are the biometrics are? Now all biometric traits are truly universal. The National Institute of Standards and Technology (NIST) reported that it is not possible to obtain a good quality fingerprint from approximately two percent of population (due to disabilities, cuts, bruises, etc.) [9].

Biometric traits are not always invariant. The biometric data acquired from a user during verification will not be identical to the data used for generating the user's template during enrollment [9]. Even under same equipment and environmental condition biometric data collected from the same user are likely not to be identical. Biometric traits like may vary due to fatigue, sickness, etc., for example, a persons voice may change if she catches cold, children's face, gait change as they grow up.

3.2 Vulnerability of Biometric Authentication System

The security of biometric authentication depends on the vulnerability of underlying biometric system. Since biometric systems are implemented on server computers, they are vulnerable to all cryptographic, virus, and other attacks which plague modern computer systems [2].

To better understand security issues concerned with biometric authentication, it should be useful to study individual components of a typical biometric system, communication channel among the components, and their vulnerabilities. Figure 2 [2] shows major functional components of a typical biometric

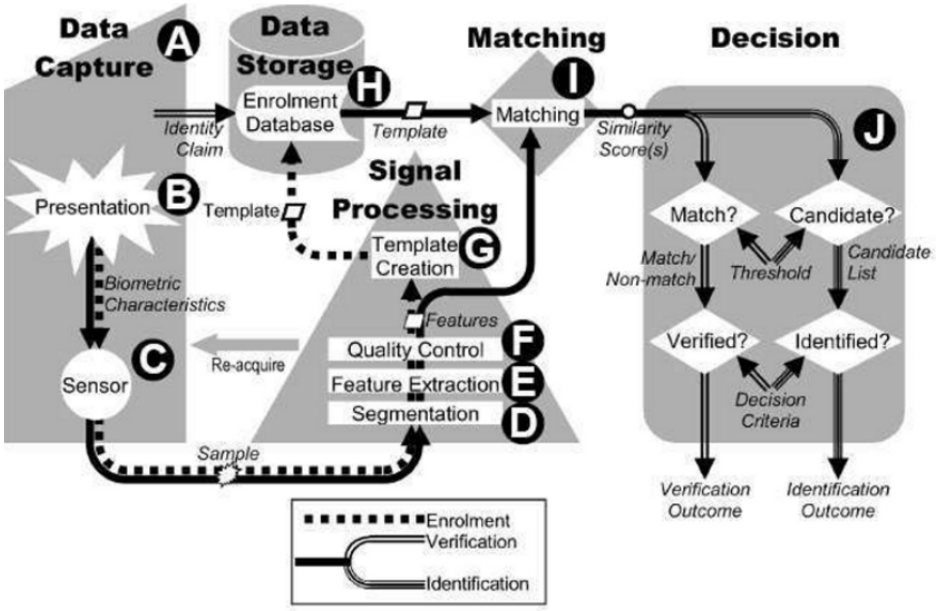

Fig. 2. Block diagram of a typical biometric authentication system [2]

system, where major steps in the process of authentication is marked as A, B, C, and so on. Typically, each presented sample (B) is acquired by a sensor (C) processed via segmentation and feature extraction (D) algorithms. If available a sample quality assessment (E) algorithm is used to indicate a need to reacquire the sample. Biometric features are encoded into template, which is stored (H) in database or any secure hardware. For biometric encryption systems, a code or token is combined with the biometric feature in the template. During enrollment, biometric samples are linked to a claimed identity (A), and during subsequent verification or identification, samples are compared with enrolled samples using matching algorithm (I), and an identity decision (J) is made either automatically, or by a human being reviewing biometric system outputs. Andy Adler [2] points out the security issues at each of these components or steps in a typical biometric authentication system, which are discussed below in short.

Sample presentation (B): The attacker may introduce false biometric sample into the system. Such attacks are mounted to avoid detection or masquerade as another person. The later attack is typically called spoofing.

Sensor (C): Noise can appear in the acquired biometric data due to environmental factors (lights, sound, humidity, etc.), as well as defective or improperly maintained sensors [9, 14]. Attacks on the biometric sensor may subvert or replace the sensor hardware. In many cases, an attack on the sensor would take the form of replay. Unlike possession or knowledge based authen-

tication, accuracy of biometric authentication is much dependent on sensor device used. For example, a computer keyboard does not reflect hardware specific characteristic in the typed text. However, keyboard characteristics used for biometric, key-stroke-based authentication significantly affects the resulting sampled signal due to physical properties like attenuation, pressure sensitivity, and others [14]. Biometric signals are exposed to distortions based on sensor characteristics. The problem of unavailability of identical sensor may be relevant for applications in large areas, as well as long term considerations, where specific hardware might no longer be available after some time.

Segmentation (D): Biometric segmentation extracts the image or signal of interest from the background, and a failure means the system does not detect the presence of appropriate biometric feature. Segmentation attacks may be used to escape surveillance or to generate denial of service (DoS).

Feature extraction and quality assessment (E): Knowledge of feature extraction or quality assessment algorithms can used in the biometric authentication system may be exploited to design special features in presented biometric samples to cause incorrect features to be calculated.

Template creation (G): One common claim is that, since template creation is a one-way function, it is impossible or infeasible to regenerate the image/signal from the templates. However, recent research has shown regeneration of biometric samples from templates to be feasible.

Data storage (H): For biometric authentication the size of reference data may become very large, and due to natural variability of biometric information, it is impossible to apply discrete mathematical techniques like cryptographic hashes to secure the reference data [14]. Vulnerabilities of template storage concern modifying the storage (adding, modifying, or removing templates), copying template data for secondary usage (identity theft), or tampering the identity to which the biometric is assigned. "The biometric dilemma is that although biometrics can initially improve security, as traditional biometric databases become widespread, compromises will ultimately destroy biometrics' value and usefulness for security" [5]

Matching (I): A biometric matcher calculates a similarity score related to the likelihood that two biometric samples are from the same individual. For multimodal or biometric fusion systems, extreme score in one biometric modality may override the influence of other modalities. Besides the concern of finding methods to increase the overall accuracy of multi-modal authentication systems, there remains open questions, for example, with respect to the degree of correlation between different modalities, question of finding a meaningful set of modalities [14]. Biometric matchers which are based on Fisher discriminant strategies calculate global thresholds based on the between class covariance, which may be modified by enrolling specifically crafted biometric samples.

Decision (J): Biometric decisions are often reviewed by human operator. Such operators are well known to be susceptible to fatigue or boredom. One of the goals of the DoS attacks is to force operators to abandon the biometric

system, or to mistrust its output (by causing it to produce sufficiently large number of errors). All biometric authentication methods are based on some statistical measurement of similarity and threshold, which make the process subject to false classification error. Biometric authentication does is based on probability of matching and so cannot give complete confirmation about certain authentication. Many biometric authentication system allows the administrator to configure a threshold level that determines false acceptance rate and false denial rate.

Figure 3 [9] summarizes the ways in which biometric authentication system may be attacked.

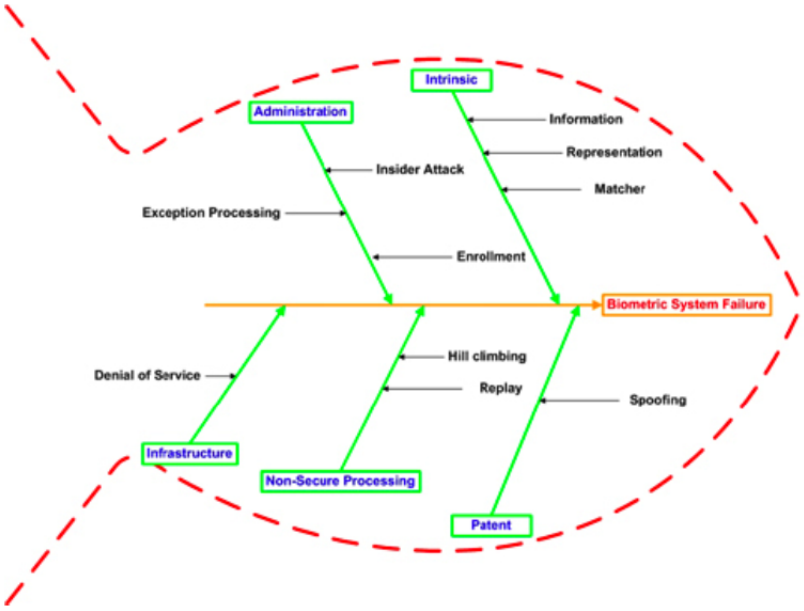

Fig. 3. Fishbone (cause-effect) illustration of biometric failure [9]

Maltoni and et al. [6] classify vulnerability of biometric authentication system as follows:

Circumvention is an attack which gains access to the protected resources by a technical measure to subvert the biometric system. Such an attack may subvert the underlying computer systems (overriding matcher decision, or replacing database templates) or may involve replay of valid data. It is possible to circumvent a biometric system using spoofed traits. For example, it is possible to construct "gummy fingers" using lifted fingerprint impressions

and utilize them to circumvent a fingerprint based authentication system [5, 9].

Covert acquisition (contamination) is use of biometric information captured from legitimate users to access a system. Examples include spoofing via capture and playback of voice password, and lifting latent fingerprints to construct a mold.

Collusion and Coercion are biometric system vulnerabilities from legitimate system users. The distinction is that, in collusion the legitimate user is will (perhaps by bribe), while the coerced user is forced (through threat or blackmail).

Denial of Service (DoS) is an attack which prevents legitimate use of the biometric system. This can take the form of slowing or stopping the system (via overload of requests) or by degrading the performance.

Repudiation is the case where the attacker denies accessing the system. A corrupt user may deny her actions by claiming that her biometric data were stolen.

4 Conclusion

Even though the area of biometric technology is flourishing so fast, biometric authentication systems have not come in use that much due to a number of reasons besides the security issues discussed above. An obvious reason is high expense to install and maintain biometric systems. Another, concern is accuracy, some biometrics technologies (such as iris, retina, fingerprint) are comparatively promising in terms of accuracy, while others (voice, gait, etc.) result high error rate. Considerably the best fingerprint systems tested by the the U.S. government in the NIST Fingerprint Vender Recognition test, only had 98% true acceptance rate, when set to reject 99.99% of false matches, and had an equal error rate of 0.2% [5].

The interface of the biometric authentication system also plays a vital role in users' acceptance [7]. For example, fingerprint based authentication is more convenient and acceptable to the subjects, compared to iris recognition or retinal pattern recognition due to the fact that eye based authentication requires the subjects to keep their eyes open for considerable duration in front of the sensor. Interoperability of the separately collected biometric data stored in different databases is another obstacle for implementation of pervasive biometric authentication systems [2, 14], whereas possession or knowledge based authentication schemes do not have such interoperability problem. To date, several standards have been proposed addressing this issue.

To increase reliability of biometric authentication, multimodal biometrics may be used at the cost of increased expenses [14]. Encoding of biometric templates would increase security of template database. Templates encryption techniques are designed to encode secret code into the template, in a way that can be decrypted only with an image of the enrolled individual. Furthermore, it may be possible to use biometrics to some extent in revokable way using distortion

scheme [2, 5], where during enrollment, the input biometric image is subjected to known distortion controlled by a set of distortion parameters. During matching the live biometric sample needs to be distorted in exactly the same way. Research in the field is still in progress aiming better security and reliability, as biometric authentication is a comparatively new area. Many people believe that biometrics will play a critical role in future computers, specially in authentication for electronic commerce [13].

References

1. American national standard for telecommunications - telecom glossary 2000, requested january 2004.
2. A. Adler. *Biometric System Security.* Springer, US, 2007.
3. M. Bishop. *Computer Security.* Addison-Wesley, Boston, USA, 2003.
4. M. Boatwright and X. Luo. What do we know about biometrics authentication? In *InfoSecCD '07: Proceedings of the 4th annual conference on Information security curriculum development*, pages 1–5, New York, NY, USA, 2007. ACM.
5. T. E. Boult and R. Woodworth. *Privacy and Security Enhancements in Biometrics.* Springer, US, 2005.
6. A. K. J. D. Maltoni, D. Miao and S. Prabhakar. *Handbook of Fingerprint Recognition.* Springer-Verlag, 2003.
7. S. J. E. Eric P. Kukula and V. G. Duffy. The effects of human interaction on biometric system performance. *V.G. Duffy (Ed.): Digital Human Modeling, HCII 2007*, LNCS 4561:904 – 914,, 2007.
8. A. Jain, L. Hong, and S. Pankanti. Biometric identification. *Commun. ACM*, 43(2):90–98, 2000.
9. A. K. Jain. *Biometric Recognition: How Do I Know Who You Are?* Springer, US, 2005.
10. E. Kindt. *Biometric applications and the data protection legislation.* Springer, US, 2007.
11. R. D. Madalina Baltatu and R. D'Amico. *Toward Ubiquitous Acceptance of Biometric Authentication: Template Protection Techniques*, volume 3087/2004. Springer Berlin / Heidelberg, 2004.
12. R. M. B. N. K. Ratha, J. H. Connel and S. Chikkerur. Cancelable biometrics: A case study in fingerprints. In *IEEE International Conference on Pattern Recognition*, volume 4, pages 370–373, Hongkong, China, 2006. IEEE.
13. N. B. Sukhai. Access control & biometrics. In *InfoSecCD '04: Proceedings of the 1st annual conference on Information security curriculum development*, pages 124–127, New York, NY, USA, 2004. ACM.
14. C. Vielhauer. *Biometric User Authentication for IT Security: from Fundamentals to Handwriting.* Springer, US, 2005.
15. J. M. Williams. Biometrics or ... biohazards? In *NSPW '02: Proceedings of the 2002 workshop on New security paradigms*, pages 97–107, New York, NY, USA, 2002. ACM.