International Journal of Information & Computation Technology.
ISSN 0974-2239 Volume 4, Number 10 (2014), pp. 947-958

http://www. irphouse.com

Vulnerabilities of Biometric Authentication "Threats and Countermeasures"

Abdulmonam Omar Alaswad
Faculty of Information Technology University of Tripoli
Tripoli – Libya

Ahlal H. Montaser
Faculty of Information Technology University of Tripoli
Tripoli – Libya

Fawzia Elhashmi Mohamad
Tripoli Faculty of Education University of Tripoli
Tripoli – Libya

Abstract

Biometric systems have a powerful potential to provide security for a variety of applications, systems are nowadays being introduced in many applications and have already been deployed to protect personal computers, Banking machines, credit cards, electronic transactions, airports, high security institutions like nuclear facilities, Military Bases and other applications like borders control, access control, sensitive data protection and on-line tracking systems. While biometrics may improve security in different environments and serve many purposes, biometric systems, like any other security system, have vulnerabilities and are susceptible to threats. they are susceptible to external vulnerabilities of biometric systems so that their weaknesses can be found and useful countermeasures against foreseeable attacks can be developed The increasingly high profile use of biometrics for security purposes has provoked new interest in researching and exploring methods of attacking biometric systems.
Keywords: Biometrics, Biometric Systems, Authentication, Verification, Vulnerabilities, attacks, Threats.

1. Introduction

Biometrics technologies have been around for quite some time and many have been deployed for different applications all around the world, ranging from small companies' time and attendance systems to access control systems for nuclear

facilities. Biometrics offer a reliable solution for the establishment of the distinctiveness of identity based on "who an individual is", rather than what he or she knows or carries. Biometric Systems automatically verify a person's identity based on his anatomical and behavioral characteristics. Biometric traits represent a strong and undeviating link between a person and his identity, these traits cannot be easily lost or forgotten or faked, since biometric systems require the user to be present at the time of authentication. Some biometric systems are more reliable than others, yet they are neither secure nor accurate, all biometrics have their strengths and weaknesses. Although some of these systems have shown reliability and solidarity, work still has to be done to improve the quality of service they provide. In this work we present available standing biometric systems showing their strengths and weaknesses and also presenting emerging technologies in which may have great benefits for security applications in the near future.

Different biometric technologies are available in the market today that can be used for security. Biometric technologies vary in their capabilities, performance and complexity. They can be used to verify or establish a person’s identity and they all share several elements.

Biometric identification systems are essentially pattern recognition systems. They use acquisition scanning devices and cameras to capture images, or measurements of an individual’s characteristics, and computer hardware and software to extract, encode, store, and compare these characteristics. Usually this process is fully automated, which makes decision-making very fast, in most cases, taking only a few seconds.

Depending on the application, biometric systems can be used in one of two modes: verification or identification. Verification or also known as authentication is used to verify a person’s identity “to authenticate that people are who they claim to be”. Identification is used to establish people’s identity “to determine who the people are”.

Although biometric technologies measure different characteristics in different ways, all biometric systems begin with an enrollment process followed by a matching process which uses either verification or identification. It is essential to keep in mind that the efficiency of security systems cannot be accomplished by relying on technology alone. Technology and people must work together as part of an overall security process. Weaknesses in any of these areas weaken the effectiveness of the security process. Leading biometric technologies include facial recognition, fingerprint recognition, hand geometry, iris recognition, Retina recognition, and Signature recognition.

2. Attacks on Biometric

In this section of the paper we discuss biometric devices and systems vulnerabilities. We can group attacks on biometric devices and systems into four categories:

2.1 Processing and Transmission Level Attacks

Though input-level attacks are an obvious illustration of biometric system

vulnerability, attacks at the processing and transmission level also deserve close attention.

As many biometric systems transmit sample data to local or remote workstations for processing, it is also imperative that this transmission be secure, lest the transmission be intercepted, read, or altered. Most biometric systems encrypt data in transit, but not all applications and devices lend themselves to encryption. Security techniques such as encryption are often seen as deployer-specific aspects of system design.

Deployers need to assess the degree to which sample data might be exposed in transit or during storage, and they need to define applicable system security techniques and best practices. Taken as a whole; anti-spoofing measures, encryption of data in transmission, and applying appropriate fallback techniques are all critical aspects of biometric system security. These techniques can be further enhanced through the introduction of multi-factor authentication and randomization.

Multi-factor authentication can take two primary forms: the use of multiple biometrics or the use of biometrics in conjunction with smart cards and PINs. Both methods reduce the likelihood of an imposter being authenticated. Spoofing also becomes more time consuming and challenging when multiple body physiological or behavioral characteristics need to be copied and imitated. Impostors for whom a biometric matches an enrolled user are unlikely also to match with respect to a secondary biometric. Adding randomization to the equation also adds security. Verification data, for example, could be randomized, such as asking for three fingerprints one day and a different combination of two fingerprints the next day. Additionally, where time provides, designers of biometric technologies and systems should explore random or cued challenges. That is, even if a person correctly authenticates once, the system might still challenge the user to re-authenticate to help increase its confidence that the biometric data submitted is genuine.

Cued challenges could also be paired with certain behaviors causing alarm – such as an uncommon stillness, lack of movement, or change during the acquisition of biometric data. Technologies can still bear further development and enhancement for monitoring and sensing micro-movement. Or perhaps aggressive challenges could be utilized in conjunction with measurements of intelligent response time. For example, voice verification biometric systems could measure the time it takes for a prospective entrant to read back a randomly generated pass phrase in order to try to fight playback attacks pieced together from various recordings. If the response time exceeds a minimum threshold or varies significantly from an average time captured over a series of sample submissions at enrollment, the biometric system could issue a challenge and require recitation of a new pass phrase.

Finally, in conjunction with multi-factor authentication and randomization, vendors and researchers should explore taking advantage of internal or subcutaneous characteristics. By focusing on biometric aspects that are difficult to observe, capture, and duplicate covertly, security can thus be enhanced.

However, regardless of how well one tries to secure a biometric system, failures will inevitably occur. It is therefore critical that attention not only be paid to preventing breaches, but also to handling breaches that have occurred. A recently-publicized

technique to mitigate the impact of certain system breaches is the concept of cancelable biometrics. Cancelable biometrics solution uses algorithms to distort an image proffered and records the distortion into its generated templates. The original image is never stored anywhere. The idea is that if a thief steals the template with the distortion on it, that particular distortion can be eliminated from the list of access-approved users, and the legitimate user can resubmit their original biometric data to generate a new distorted template. As long as the algorithms that generate the distortions are carefully protected and ideally varied from company to company or even system to system, this solution may be highly conducive to containment and resolution of a breach. The solution, however, is not foolproof. If the original image is captured, it could theoretically be re-enrolled to generate a new, distorted template.

2.2 Input Level Attacks

The primary input-level attacks, vulnerabilities at the point of sample acquisition and initial processing, are spoofing and bypassing. While spoofing is the most frequently-cited input-level vulnerability, other input-level vulnerabilities may be just as problematic, such as "overloading." "Overloading" is an attempt to defeat or circumvent a system by damaging the input device or overwhelming it in the attempt to generate errors. This is also sometimes called a buffer overflow attack for other security mechanisms. An example of this type of attack for a biometric system would be the rapid flashing of bright lights against optical fingerprint sensors or facial recognition capture devices can disrupt their proper functioning. Silicon sensors can be easily damaged by short circuiting them or dousing them with water.

Because many biometric systems rely on sensitive equipment that can be overloaded relatively easily, users may have opportunities to induce device or system failure. Systems must be designed such that, if overwhelmed, basic functions must not fail. And when biometric devices can no longer serve their intended function, fallback processes must be defined and enforced. A person who causes a biometric system to fail may be doing so knowing that, as a consequence, an unguarded door may be used as a temporary alternative means of entry. Security systems must account for the potential functional failure of biometric systems and devices by means of adequate backup measures.

2.3 Back-end Attacks

The previous two sections have described input level and transmission level attacks. Ensuring integrity and protecting back-end subsystems is important in distributed biometric systems. Assuming that the back-end consists of a matching subsystem, or a decision subsystem, or a combination of both attacks on the back-end will mainly be targeted at modifying the matching or decision subsystem or compromising integrity of stored templates.

Attacking the template storage database is the most apparent type of back-end attack. The threat of unauthorized modification or replacement of stored templates can result in false accepts or false rejects depending on the motives of the attacker. If an attacker can find a way of injecting templates directly into the storage database then the

attacker could introduce him/her into the system without following the appropriate enrollment procedures. The attacker could also hijack the identity of an authorized individual by replacing the original template with their own template, thereby still preserving privileges linked to the authorized individual. If a template is compromised, it could be reused in a replay attack. Although circumventing replay attacks addressed is addressed in the previous section, compromise of stored templates is one of the most important threats that should be considered when designing a distributed biometric system.

These kinds of attacks can be prevented by using encryption and data integrity (hashing) methodologies. Applying common database security methodologies can also increase the level of difficulty for the attacker.

An attacker could modify or replace the matching subsystem or the decisions subsystem so that it gives an output as desired by the attacker. This is a serious threat in a networked environment. The integrity of the sample is not relevant in such an attack, and the authentication process can be compromised without attacking the input subsystem or transmission process. This kind of an attack can be circumvented by applying security methodologies like checking code integrity, and principles of building trusted systems.

A denial of service (DOS) attack targeted at the back-end subsystems is also a very realistic threat. Overloading the processing units of the back-end subsystem with excess traffic could lead to unavailability of services. DOS attacks have received a lot of attention in media over the last few years and it should be considered a very real threat to biometric authentication systems also. Traffic analysis and traffic monitoring are commonly used methods to thwart DOS attacks.

Along with technical threats, there are also policy related challenges that should be considered. Collusion between a malicious attacker and enrollment center could allow the attacker to enroll in the system using a stolen or a false identity. Although this threat is not focused only on the back-end subsystems, a properly formulated policy involving the front-end and back-end subsystems should make such attacks harder to perpetrate.

2.4 Enrollment Attacks

The practical use of biometrics for E-Authentication is binding to one's identity. Although the concept of an Identity Management System lies outside the scope of this document, from a biometric enrollment standpoint because of the essential binding requirement, the identity proofing process is a critical related function. Trust in this process of vetting a person's claimed identity, confidence in the validity of associated documents, and reliability in the authenticity of issued electronic credentials taken together provide the very underpinning of biometric based E- Authentication. Examples of threats to identity proofing include:

1. Use of forged documents to verify a claimed identity.
2. Collusion with corrupt personnel having system access and.
3. Electronic attacks to impersonate legitimate system users and thereby

gain electronic access to the ID application, proofing process and issuance system.

The following Countermeasures can be taken against these Identity Proofing threats:

1. Enforced separation of roles and duties of those involved in the processing, approval
2. and credential issuance process.
3. Close inspection of documents for forgery or tampering and use of third party
4. substantiation; for example, use of written inquiries.
5. Electronic system security protection – strong access controls, data encryption,
6. firewalls etc.
7. Strong issuance controls which confirm the user at time of credential issuance and
8. which preclude manual modifications to personalization data.

Vulnerabilities during enrollment of a person's biometrics such as fingerprints, iris and facial features include:

1. Enrollment of a person's valid biometric(s) with a created or substituted identity. In this scenario, a person uses/enrolls their own biometrics under a false or assumed identity which subsequently allows that person to gain unauthorized access to and conduct eCommerce transactions and other logical and/or physical assets such as computers, networks, databases, applications and facilities.
2. Enrollment of substituted or swapped biometrics (not their own) along with a valid identity which subsequently can be used by a third party to masquerade and gain access to eCommerce systems and/or other logical or physical assets.
3. Enrollment of substituted or false biometrics (e.g. a "gummy bear fingerprint") with a false or assumed identity which can later be used to gain access to eCommerce systems and/or other logical or physical assets.
4. Enrollee collusion with the enrollment operator. In this scenario, any of the above can be facilitated, as well as, unauthorized entry of or modifications to system data records or input thereto.
5. External based attacks against the Enrollment Station and/or other system components it communicates with. Examples include spoofing, sniffed transmissions, Man-in-the- Middle, and Replay.

The following Countermeasures can be taken against these threats during Enrollment of Biometrics:

1. Observed enrollment of biometrics instead of un-observed self enrollment.
2. Identity check/confirmation of the applicant enrollee at time of enrollment.

3. Remote system and enrollment station network protection and access controls, secure point-to-point encrypted communications channel(s).
4. Enrollment Station device level firewall, and detection systems of unauthorized
5. modifications to all relevant data records and electronic file systems.

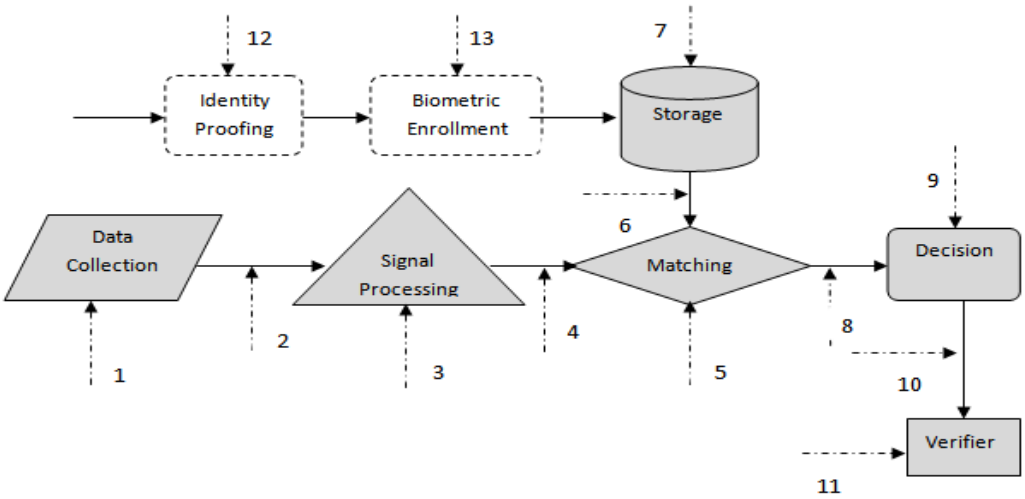

Figure 1: Attack points on a biometric system

3. Vulnerable points of biometric systems, Threats and Countermeasures.

Points of possible attacks are identified and shown in Figure 1, they fall into 4 categories as we have discussed earlier, countermeasures are described below according to the specified categories

- Attacks during processing/interaction [Attack points 1, 3, 5, 9, 11],

Location	Threats	Countermeasures
1 Data Collection	Spoofing	• Liveness detection • Challenge/response
	Use of un-trusted device (Device substitution)	• Mutually authenticate/use symmetric key or asymmetric key
	Overloading/Flooding (Denial of Service)	• Rugged devices
3 Signal Processing	Insertion of imposter data	• Use strong tested algorithms

	Component replacement	• Signed components
5 Matching	Insertion of imposter data	• Use strong tested biometric algorithms
	Component replacement	• Signed components
	"Guessing" (FAR attack)	• Use strong tested biometric algorithms • 1:1 matching • Multi-biometric/multi-factor
	Manipulation of match scores	• Debugger hostile environment
	Hill-climbing	• Coarse scoring • Trusted sensor (Mutual authentication) • Secure channel
9 Decision	Hill climbing attack	• Coarse scores • Mutual Authentication • Secure channel
	Manipulation of threshold setting	• Protected function (access control) • Data protection
	Manipulation of match decision	• Debugger hostile environment
	Component replacement ("yes machine")	• Sign components
11 Application (verifier)	Malicious code	• Conform to standards (BioAPI, CBEFF) • Code signing

- Attacks on the biometric data when it is at rest (in memory or in storage) [Attack points 1, 3, 5, 9, 11 "above" + 7 "below"].

7 Storage	Database compromise (reading template, replacing template(s), changing bindings)	• Hardened server • DB access controls • Sign templates, Store encrypted templates • Store template on smart cards or other device.

- Attacks between stages (when the biometric data is in transmission) [Attack points 2, 4, 6, 8, 10].

Location	Threats	Countermeasures
2 Raw data transmission	Eavesdropping attack	• Transmit data over encrypted path/secure channel
	Replay attack	• Mutually authenticate/use symmetric key or Asymmetric key • Digitally sign data • Utilize Timestamp/Time to Live (TTL) tag
	Man in the middle attack	• Bind biometric to PKI certificate • Transmit data over encrypted path/secure channel
	Brute force attack	• Time out/lock out policies
4 Processed data transmission	Eavesdropping attack	• Transmit data over encrypted path/secure channel
	Replay attack	• Mutually authenticate/use symmetric key or asymmetric key • Digitally sign data • Utilize Timestamp/Time to Live (TTL) tag
	Man in the middle attack	• Bind biometric to PKI certificate • Transmit data over encrypted path/secure channel
	Brute force attack	• Time out/lock out policies
6 Template retrieval	Eavesdropping attack	• Transmit data over encrypted path/secure channel
	Replay attack	• Mutually authenticate/use symmetric key or asymmetric key • Digitally sign data • Utilize Timestamp/Time to Live (TTL) tag
	Man in the middle attack	• Bind biometric to PKI certificate • Transmit data over encrypted path/secure channel
8 Matching score transmission	Hill climbing attack	• Coarse scores • Trusted sensor (Mutual authentication) • Secure channel

	Manipulation of match score	• Secure channel • Mutual authentication between matcher and decision components
	Component replacement ("yes machine")	• Sign components
10 Communication to application	Eavesdropping attack	• Transmit data over encrypted path/secure channel
	Manipulation of match decision	• Transmit data over encrypted path/secure channel

4. Conclusions

Biometrics offers a valuable approach to extending current security technologies that make it far harder for fraud to take place by preventing ready impersonation of the authorized user.

In using biometrics we must be aware of the fact that they are not measuring perfectly, and that many operational factors may cause them to fail. In such cases administrative procedures to resolve operational failures may need to be put in place to prevent adverse customer reaction, bad publicity and failures in public acceptability. Whilst these failures may not represent a significant proportion of transactions they will have a 'publicity' effect that is far more damaging to all the success gained by the service.

References

[1] K. Jain, K. Nandakumar, and A. Nagar, "Biometric template security," EUR-ASIP, vol. 8, no. 2, pp. 1–17, 2008.

[2] Jain, A.K., Ross, A., Pankanti, S.: Biometrics: a tool for information security. IEEE Trans. on Information Forensics and Security 1, 125–143 (2006)

[3] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, Handbook of Fingerprint Recognition. Springer-Verlag, 2003.

[4] U. Uludag and A. K. Jain, "Attacks on biometric systems: a case study in finger-prints," in Proc. SPIE, Security, Seganography and Watermarking of Multimedia Contents VI, vol. 5306, pp. 622–633, (San Jose, CA),January 2004.

[5] Hao, F., R. Anderson, and J. Daugman, Combining cryptography with biometrics effectively.

[6] IBG, Vulnerabilities of Biometric Technologies - Transcript of September Teleconference. 2005.

[7] Clarkson University Engineer Outwits High-Tech Fingerprint Fraud. 2005 [cited;Available from: http://www.yubanet.com/cgi-bin/artman/exec/view.cgi/8/2878.
[8] Electronic Fingerprint Transmission Specification. 2005, Federal Bureau of Investigation.
[9] Maltoni D , Maio D , Jain A K, et al. Handbook of Fingerprint Recognition[M]. NY: Springer, 2003.
[10] Prabhakar S, Pankanti S, Jain A K. , Biometric recognition: security and privacy concerns[J] IEEE Security and Privacy Magazine, 2003, 1(2): 33-42.
[11] Introduction to biometrics[EB/OL]. http://www.biometrics.org/html/introduction.html.
[12] Biometric technology: an assessment of practical application[EB/OL]. 2002, http://www.rcmp-grc.gc.ca/tsb/pubs/it_sec/r2-001_e.pdf
[13] Liu Simon, Mark Silverman. A practical guide to biometric security technology[J]. IT Professional, 2001, 3(1):27-3