www.ijemr.net ISSN (ONLINE): 2250-0758, ISSN (PRINT): 2394-6962

Vandana Publications
IJEMR

Volume-7, Issue-3, May-June 2017
International Journal of Engineering and Management Research
Page Number: 308-311

Biometric Security and Threats in Unique Identification Systems

Anand
Assistant Professor, Keshav Mahavidyalya, University of Delhi, INDIA

ABSTRACT

This paper discusses the various security threats to the biometric template based Unique Identification systems which are used for user identification and authentication. The biometric systems which use various physical and behavioral characteristics of the users for identity verification are prone to various security attacks that decreases their security considerably. In this paper I have presented a discussion on the threats to physical biometric traits (fingerprint, iris and face recognition) based systems. The paper discusses these possible attacks that may hamper the normal functioning of the biometric authentication system.

***Keywords*---** Biometric, Physical Traits, Security threats, Attacks, Unique Identification.

I. INTRODUCTION

The ability of a system to protect the data and resources to safeguard its integrity and confidentiality is considered to be the 'security' of the system. The Biometric systems differ in their approach from the traditional systems and like all other systems the likelihood of attacks in inherent. However, the kind of data with which biometric systems engage make them highly vulnerable to attacks and exploitations. The biometric systems use the behavioral and biological (physical) characteristics of the persons to identify and store their identity. The attacks over any biometric system may deal with the initial identification process, by forging the identities by the attackers. The vulnerability of the system is studied in terms of FAR (false acceptance rate) and the FRR (false rejection rate). Also, attackers can target the processing within any biometric system. This paper identifies the above attacks that can compromise the security, confidentiality and integrity of the biometric systems.

II. RELATED WORK: BIOMETRIC SYSTEMS AND ATTACKS

A) Biometric System: A biometric system uses biological and physical features of the person for identification. These include face, iris, fingerprint, palm print, hand geometry and DNA. Also the behavioral characteristics such as signature, voice and typing rhythm. These are used as a measure to control access and individual identification in many computers based systems. There are several factors which contribute to making the system suitable. Uniqueness of the trait being studied and the universality of the trait (being present among all the members of the population) are very important. Also the permanence of the trait and its relative rate of change over time and the easy measurability of the trait is crucial for it to be used in biometric systems. The circumvention of the trait, that is the possibility that it can be imitated and substituted make it a suitable parameter for judging its security efficiency in the attempted biometric system. The biometric system should reject the natural and environmental changes in the traits in order to focus only on the specific features which differentiate the persons.

FAR (False Acceptance Rate): The false acceptance rate is also called false match rate (FMR). The system incorrectly matches with the input provided thus the system accepts a wrong input which is above the acceptance threshold.

FRR (False Reject rate): The FRR also called as false non-match rate does not recognize or match a valid input. Thus, the correct inputs are rejected on account of invalid matching.

Detection error trade-off (DET): The threshold of the system which decides the confidence level or the acceptance level of the input is based on a normal deviation on the both axes (FMR and FRR). If the threshold of the biometric system is kept too low, then the acceptance level (FAR) will be too high. By contrast if the threshold is kept too high, then the rejection level will be too high. To avoid this DET is set at a trade off level which balance both the acceptance/ rejection rates. However, the system is vulnerable to both the kinds of situations and also to the possible exploitative threats.

B) *The Security Threats:* Based on the many studies the following have been documented as the possible threats and attacks on the biometric systems[1] [3]. We will discuss these attacks in this section and later we will classify them in various modules that can help us

in understanding the security of biometric systems more systematically.

The internal vulnerabilities of the biometric system:

i. Circumvention: This kind of attack involves gaining access to the protected resources and using technical measures. The attack targets to subvert the system and may involve replacing the database templates and intervening in the matching decisions.

ii. Covert Acquisition: It means to capture the biometric information from the valid users to access the system. This involves spoofing of voice recognition passwords, using rubber molds to imitate the fingerprints and regeneration of biometric images (using the database templates of face/fingerprint).The cross application of the biometric data can cause serious problems such as fingerprint regeneration from an attendance module can be used to access bank account).

iii. Coercion or Collusion: These attacks are based on the legitimate biometric information of the valid users when attackers use collusion techniques such as bribery to obtain their information. Sometime the legitimate users are coerced (by force) such as fear, threat or blackmail. In all these cases the attacks are difficult to be identified yet an unusual activity pattern detection may help in mounting them.

iv. Denial of Service: This attack stops or interferes in the normal functioning of the legitimate biometric system. This can happen by slowing the system or stopping it down through overload of network requests or by degrading its performance. An example could be the enrollment of many samples which have unclear fingerprints. The lowering of the system threshold to identify the users, will increase the FAR. Hence the systems integrity is compromised. The target is to fall back on another system such an operator override for easy circumvention.

v. Repudiation: In this case the legitimate and valid user may deny that he/she accessed the system. Thus making a claim that the biometric details were stolen by some false attacker.

The system vulnerabilities from outside: These attacks are another class of vulnerabilities which make the system prone to threats of compromising user's identities such as by theft or system compromise.

i. Non-secretive biometric: It is known that there are a variety of technologies available which can create images of face, iris, fingerprint, palm etc. hence the data is non-secretive and can be captured or made available. This can be done with the consent of the subject with or without his/her knowledge in this regard. The biometric data are considered as private and secret and therefore the biometric system whose technological robustness (such as cryptographic protocol) is not strong is considered worrisome.

ii. The acceptability of the system: The biometric data is unique for a person and once the data is compromised (theft or coerced) then it compromises the security of current and future applications that uses the biometric data of the same person. In case of a security compromise the person may not be willing to enroll for any biometric based system.

iii. The secondary uses of biometrics: The risks of using the biometric data by a person may be increased in an environment in which the user may use the unique biometrics across various applications. The biometric data if shared by the organizations then the user's identity may be tracked or profiled putting the future actions at risk. If biometrics are designed with low security concerns, then their future applications may be highly at risk in diverse threat environments.

Therefore, the risks and vulnerabilities of the biometric systems should be understood keeping in mind their utilization in larger systems such as unique identification systems which are applied to the entire population for varied applications such as government subsidy schemes, public distribution systems, educational and employment benefits, social security benefits etc.

III. STUDY OF POSSIBLE VULNERABILITIES IN UNIQUE IDENTIFICATION SYSTEMS

The *unique identification systems* based on the biometric are designed to capture and measure the biometric traits of a large or entire population. The systems are used to issue IDs and documents to individuals who can access various applications and services using unique ID (and similar documents). The possible vulnerabilities to such systems are studied and described below.

1. The claims of identity: The claim to identities are very integral part of the unique identification systems. The claims enable the individuals to enforce their identities. The various documents issued by the governments such as unique ID cards, high security documents such as passports and visas, are based on the feeder documents such as birth certificate, school registration certificates, certification by local authorities etc. serve as basic links to these claims. The claims to identity which form the basis of the enrolment in a system may result in different kinds of frauds related to these feeder documents.

2. False samples: The biometric system can be attacked with a false biometric data to obtain a false validation or identification. The attacker may either avoid the 'detection' (being a false negative sample) or enforce an'impersonation' (accepted as a false positive). In either case the sample of the biometric is changed to

confuse the feature extraction module. The facial features may be changed using make-up, accessories such as glasses etc. and hairstyles. Another example could be changing the head rotation for confusing the iris algorithms. The knowledge of the algorithms used in the biometric systems can be used to implement the false identification data thus making the attack easier on the unique identification systems.

3. Attacks on the sensor: The attacks on the sensor hardware, to either subvert it or replace it are used by employing various techniques. By subverting the sensor hardware, it is possible to completely bypass the biometric system such as if the sensor module includes the entire biometric system. Secondly, the attack on sensor may involve a replay to allow the entry of arbitrary inputs by altering the connection between the sensor and the biometric system. Eavesdropping and recording the signals from a sensor under the attacker's control are possible vulnerabilities to unique identification system.

4. Non-detection of features: The extraction of an image or the signal from the background data is called biometric segmentation. The failure to detect this information (image or signal) implies that the biometric system does not recognize the appropriate biometric feature in the data. This is done to avoid surveillance of the data or to implicate a denial of service. For example, the basic biometric features may be damaged or altered for non-detection of the person by the actual algorithm of the system.

5. Detectionof features: The attacks can be made on the unique identification system in two. One can be to extract the wrong features (the detection) creating impostors or to escape the detection. The feature extraction module and the knowledge of its algorithm (by knowing the characteristics of the feature detection) can be used to create those features which can make the incorrect features (false sample) to be calculated in the biometric detection. In this connection the biometric software which are largely proprietary can be compromised based on the available scientific literature. Also if the unauthorized copies of the biometric system can be obtained the attackers can use them for practice and experimentation. An interesting study by Doddington et al. [2] describing the taxonomy of the user classified on the basis of their identification of the features. The classes used are sheep (easily identified and performs well on biometric data), goats (difficult identification, reduces the performance of the system), lambs (easily imitable), and wolves (high on similarity with other persons). The identification of lambs and wolves can support attackers to misuse the unique identification systems in multiple ways (for defeating the system as well as to copy the persons for misuse of their data).

6. Quality of the biometric sample: The quality of the biometric sample in the unique identification systems can be an important vulnerable point of attack. The quality if the enrolled feature is very crucial in its future detection. The quality control is dependent on the specific algorithms used by the biometric systems. These algorithms look for the disturbing features in the captured biometric image (such as high noise levels, picture clarity, clear distribution of lines). The attacks may either be targeted to detect a 'good image' as 'poor'. This may lower the threshold of acceptance (resulting in high FAR wither for the particular image or for the global application of the biometric system). Secondly, the attack may be targeted as

7. Data Storage vulnerability: The biometric data is enrolled and stored in the form of a template in the system for future verification and identification. The major vulnerabilities of the stored biometric data in a unique identification system can involve by modifying the storage the data, copying the needed data for secondary use, modifying the identity to which the biometric is assigned. Storage may include many forms such as in database (local or distributed), ID documents such as barcodes and smartcards. The template may be encrypted, plaintext or have a digital signature. But the computer infrastructure based vulnerabilities in reference to the stored data templates also makes the unique identification number prone to risks of theft. The risks involved in the transmission of the templates is equally dangerous, even the encrypted messages can de discovered by knowledge of the key.

8. Matching and Decision making vulnerability: The matching of the templates for final identification may be attacked by specifically crafting and enrolling the biometric identities. The cases of image regeneration have also been reported in many researches [1]. Similarly, the final decision of the identification is a human operation. The DoS attack by increasing the number of errors in the output may force these operators to abandon the unique identification system.

IV. CONCLUSION

The complex and large systems based on biometric identification such as unique identification number systems, which are being adopted by the various countries for large populations, are vulnerable to possibilities of multiple type of exploitations. In this context as we have discussed above there are high level of risks involved such as theft of data, extractions of data for future use, making the system inefficient by increasing FAR, and interfering with the stored data. Although the severity of these attacks may vary and can differ as per the requirements of the attackers the countermeasures may also be equally costly and differ in maturity. The countermeasures for ensuring security is not dealt within the purview of this article but they may include steps such as high supervision of enrolment and verification, detection of the live storage, anonymity of the template, cryptography for storage and transmission, use of distributed systems of storage as opposed to centralized servers, enhancing security measures on computer infrastructure and network security. Thus the unique identification systems must be supervised for the inherent threats that can undermine their integrity,

security and uniqueness. The acceptability of the biometric systems by the larger population in future will depend on safeguarding the interests of the people related to their unique and private biometric information.

REFERENCES

[1] Adler, A. (2005).*Vulnerabilities in biometric encryption systems*. Conference paper. Doi: 10.1007/11527923_114.

[2] Doddington, G., Liggett, W., Martin, A., Przybocki, N. Reynolds, D. (1998),*Sheep, Goats, Lambs and Wolves: An Analysis of Individual Differences in Speaker Recognition Performance*. Slides of coordinated NIST presentation for the ICSLP 1998n Conference. Accessed on 8 June 2017 from https://pdfs.semanticscholar.org/8d35/c69bb93bca9dfcc8ec82ab0547c0f5ad60f3.pdf.

[3] Latha, U. and Rameshkumar, K. (2013). A study on attacks and security against fingerprint template and database. International Journal of Emerging Trends and Technology in Computer Science. Volume 2 Issue 5. 13-17.