ANALYSIS OF SECURITY VULNERABILITIES IN BIOMETRIC SYSTEMS

Fargana Abdullayeva[1], Yadigar Imamverdiyev[2], Vugar Musayev[3], James Wayman[4]

[1-3]Institute of Information Technology of ANAS, Baku, Azerbaijcan
a_farqana@mail.ru, *yadigar@lan.ab.az, vuqarmusa@gmail.com*
[4]San Jose State University, San Jose, USA, *JLWayman@aol.com*

Biometrics is a rapidly developing branch of information technology. Biometric technologies are automated methods and means for identification based on biological and behavioral characteristics of an individual. There are several advantages of biometric technologies compared to traditional identification methods. To take adequate measures against increasing security risks in modern world, countries are considering these advantages and are shifting to new generation identification systems based on biometric technologies.

Biometric systems are becoming an important element (gateway) for information security systems. Therefore biometric systems themselves have to satisfy high security requirements. Unfortunately producers of biometric technologies do not always consider security precautions. In publications regarding biometric technologies, drawbacks and weaknesses of these technologies have been discussed. Since biometrics form the technology basis for large scale and very sensitive identification systems (e.g. passports, identification cards), the problem of adequate evaluation of the security of biometric technologies is a current issue.

Based on an analysis of the literature, systematic research on the analysis of the security of these technologies has emerged in last three years. This work proposes an approach for analysis of security vulnerabilities of biometric systems. The proposed approach tries the best to consider the requirements of AVA class (Assurance Vulnerability Assessment) of ISO/IEC 15408-3 and its subclasses AVA_SOF (Strength of Function) and AVA_VLA (Vulnerability Analysis). Since there are different ideas in the literature, the vulnerability analysis and vulnerability assessment concepts are defined below:

Vulnerability analysis determines the imposter usage of the vulnerabilities (those identified in the vulnerability assessment process) with the aim of breaking the security policy.

Vulnerability assessment is the systematic checking of systems in order to determine the adequacy of security measures, to determine the security weaknesses and to obtain data for forecasting effectiveness of proposed security measures. Vulnerability assessment is the sequence of the following steps:

- search for potential vulnerabilities;
- developing intrusion tests;
- making intrusion tests;
- processing of results and reporting.

The step of search for potential vulnerabilities has two phases, one of which is searching for weaknesses and the other the evaluation of potential attacks. Sources of information on potential vulnerabilities include open publications, scientific articles, conference materials, and opinions of experts.

Vulnerabilities in biometric systems stem mainly from structure of the system, biometric characteristics used (e.g. fingerprint, iris, etc.), and administration policy. Each of these areas has a set of special vulnerabilities and has to be analyzed in order to take counter measures.

A main source about vulnerabilities is information about the attacks against biometric systems [1-4]. An approach based on logical structures of biometric systems is used to describe attacks. Every biometric system is composed of four main modules [5]:

Sensor module: A sensor acquires the biometric characteristic of an individual and makes a digital description of it.

Feature extraction module: Input sample is processed and generates a compressed image called template. Template is stored in database or in a smart card.

Matching module: This module compares the presented biometric sample with the template. In verification mode only one matching is performed resulting in only one matching score and in identification mode the presented characteristic is matched with many templates and generates many matching scores.

Decision module: This module accepts or rejects the user depending on the matching score or security threshold.

Figure 1 presents such a system and possible attack points.

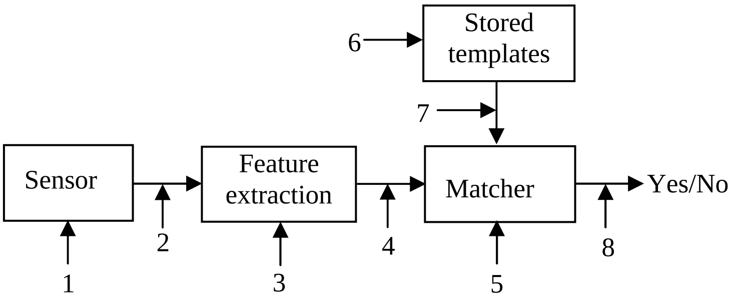

Figure 1: Attack points of a biometric system

Ratha et.al. identify eight attack points in this scheme. Let us shortly describe characteristics of these attacks denoted by numbers 1-8 [5]:

1. **Presenting a fake biometric sample to the sensor:** A fake biometric sample such as a fake finger, image of a signature, or a face mask is presented to the sensor in order to get into the system.
2. **Replay of stored digital biometric signals:** A stored signal is replayed into the system ignoring the sensor. For instance, replay of an old copy of a fingerprint image or a recorded audio signal.
3. **Denial of feature extraction:** A feature set is formed by the imposter using a Trojan horse attack.
4. **Spoofing the biometric feature:** Features extracted from input signal are replaced by a fake set of features.
5. **Attacking matching module:** Attacks on matching module result in replacement of matching scores by fake ones.
6. **Spoofing templates in database:** Database of saved templates can be local or distant. The attacker tries to fake one or more biometric templates in the database. As a result, either a fake identity is authorized or a rightful user faces a denial of service.
7. **Attacking the channel between the template database and matching module:** Stored templates are transmitted through a communication channel to the matching module. Data in the channel can be changed by attacker.
8. **Attacking the final decision process:** If the final decision can be inserted or blocked by the hacker then the authentication system function will be overridden.

Structure, architecture, production or implementation of a system may introduce a vulnerability to the biometric system. In some cases a secondary system may be integrated to the biometric system which possibly makes the biometric system vulnerable. There are five points of vulnerabilities:

- operating systems;
- database management systems (and application software);
- biometric application software;
- software for sensor;
- hardware and drivers.

Other main aspects can be categorized as follows:

- management of operations;
- management of parameters (especially FAR/FRR parameters);
- system configuration.

Wayman has studied the technical testing of biometric devices and divided it into five subsystems [6]: data collection, signal processing, transmission, data storage, decision. This makes the potential attack points more clear. [7] introduces three more components: administrative management, information technologies, and presentation of token. In total, 20 potential attack points and 22 vulnerabilities are identified. All biometric systems require administrative supervision to some extend. The level of supervision may vary for systems but it is not difficult to imagine the related vulnerabilities. Vulnerabilities in this area may devalue even the best planned system. A biometric system may or may not be related to an IT environment, but is usually part of a larger system. Interaction with an IT environment may introduce some new vulnerabilities not existing in the previous scheme. A token is required in some biometric systems which make final decisions based on presented biometric characteristic and information on the token. A token may introduce a potential attack point to the biometric system. A smart card containing biometric information is an example of a token used in this kind of system. There are several other schemes for vulnerability classification [8]. Considering them as well, a generalized list of vulnerabilities of biometric systems is suggested.

- **Administration**: Intentional or unintentional administrative mistakes.
- **User**: A legitimate user wants to upgrade his privileges to the administrative level.
- **Enrollment**: Breaking registration procedures.
- **Spoofing**: A fake biometric is used for authentication as a legitimate user.
- **Mimicry**: Attacker mimics the biometric characteristics of the legitimate user.
- **Undetect**: Attacks undetected by the system may encourage new attacks.
- **Fail secure**: Result of abnormal utilization conditions of biometric system or IT environment.
- **Power**: Power cuts.
- **Bypass:** Bypassing biometric system for access. This can be achieved by surpassing physical barriers, forcing a legitimate user to present his biometric to the sensor, or by cooperation of legitimate user.
- **Corrupt attack** – Weakening the system by making changes in the IT environment or biometric system. Modification or replacement of system parameters is an example.
- **Degrade**: Certain software in the IT environment decreases the system's security level.
- **Tamper**: Counterfeiting the hardware of the system.
- **Residual**: Latent fingerprints may be used to make artificial fingerprints or accepted directly by the sensor.
- **Cryptological attack**: Encryption can be broken in data transmission and this biometric data can be used for another type of attack (e.g. replay attack).
- **Brute force attack**: Attacker presents the biometric characteristic to the system repeatedly in order to be authenticated. This type of attack depends on FAR parameter.
- **Evil twin attacks**: Biometric characteristic of imposter is very similar to the enrolled user's biometric.
- **Replay**: Similar to the second point of attack described in the Ratha scheme.
- **Fake template:** Introducing fake biometric template into the database or onto smart cards.
- **Noise:** Access can be gained by the attacker when noise is applied to the system.
- **Poor image**: Quality supervision may be utilized. If low quality images are accepted for registration then attacker may hope to deceive the system as in the case of noisy images.
- **Weak ID:** Similar to "poor image" weakness, and tries to fake the system by weak templates.
- **FAR/FRR:** Attacker considers FAR and FRR values to fake the system.
- **Denial-of-service:** Denial of service attack aims to prevent a user from obtaining a legitimate service.

Consequently, there are many attack points and vulnerabilities in biometric systems. Using the given list of them, vulnerabilities for specific systems can be identified. A biometric system may not have all of the vulnerabilities or attack points. The list is general enough and can be applied to any system easily. For a specific system, it is essential to consider the properties of the system in order to identify the vulnerabilities. .

The aim of vulnerability analysis is to determine the possibility of utilization of weaknesses of biometric systems in an application environment. Penetration tests are carried out to determine the vulnerability in the application environment of an imposter with a certain potential of attack. Level of potential attack can be low, medium or high. In standard 15408-3, penetration tests are considered to determine the system's resistance level (low (AVA_VLA.2), medium (AVA_VLA.3), high (AVA_VLA.4)) against the penetration attacks by imposters with low, medium or high attack potentials.

There are three categories of threat agents for biometric systems [4]:

Impostor: An individual pretending authorized intentionally or unintentionally. An imposter may be authorized or not.

Attacker: Any individual or any system trying to compromise the function of the biometric system. The motive could be unauthorized access or denial of service.

Authorized users: Authorized users of biometric system unintentionally compromising the biometric device or the system. This category corresponds to unintentional human mistakes, e.g. mistakes of administrator when configuring the system.

Threat agents usually have a certain level of technical capabilities. At the lowest level of risk scale, threat agents may lack specific system information and financial resources. Capable, well informed and well financed threat agents can be more dangerous.

It is important to develop and carry out penetration tests for each attack using certain vulnerability. Therefore there is a problem of appropriate testing methodology for determination of the resistance of biometric systems by considering counter measures for certain attacks.

Acknowledgements

The work was supported by research grant Bilateral Grants Program (BGP II) – AZM1-3112-BA-08 from the U.S. Civilian Research & Development Foundation (CRDF), and Azerbaijan National Science Foundation (ANSF), the Azerbaijan National Academy of Sciences (ANAS).

Literature

1. Matsumoto T., Matsumoto H., Yamada K., Hoshino S., Impact of artificial "gummy" fingers on fingerprint systems, in Optical Security and Counterfeit Deterrence Techniques IV, vol. 4677 of Proceedings of SPIE, pp. 275–289, San Jose, Calif, USA, January 2002.
2. Jain A. K., Uludag U., Attacks on biometric systems: a case study in fingerprints, Proc. SPIE-EI 2004, Security, Seganography and Watermarking of Multimedia Contents VI, San Jose, CA, pp. 622–633, 2004.
3. Jain A. K., Ross A., Uludag U., Biometric template security: challenges and solutions, in Proceedings of the European Signal Processing Conference (EUSIPCO '05), Antalya, Turkey, September 2005.
4. Roberts C., Biometric attack vectors and defenses, Computers and Security, vol. 26, no. 1, pp. 14–25, 2007.
5. Ratha N.K., Connell J.H., Bolle R.M., An Analysis of Minutiae Matching Strength, Proc. 3rd AVBPA, Halmstad, Sweden, June 2001, pp. 223-228.
6. Wayman J.L., Technical Testing and Evaluation of Biometric Devices, in A. Jain, et. al, Biometrics – Personal Identification in a Networked Society, Kluwer Academic Publisher, 1999.
7. Cukic B., Bartlow N. The Vulnerabilities of Biometric Systems – An Integrated Look at Old and New Ideas, Technical Report, West Virginia University, 2005.
8. Dimitriadis C., Polemi D., Application of multi-criteria analysis for the creation of a risk assessment knowledgebase for biometric systems. Lecture Notes in Computer Science, Vol. 3072, Springer-Verlag, ICBA, Hong Kong, China (2004), pp.724-730.