The Second International Conference "Problems of Cybernetics and Informatics" September 10-12, 2008, Baku, Azerbaijan. Section #1 "Information and Communication Technologies" www.pci2008.science.az/1/18.pdf

ANALYSIS OF THE BIOMETRIC SYSTEMS SECURITY EVALUATION METHODOLOGIES

Ramiz Shikhaliyev[1], Yadigar Imamverdiyev[2], Vugar Musayev[3], James Wayman[4]

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

A biometric identification system is an important part of the national identification infrastructure. Application of biometric identification technologies provides higher level of security for passports, visas and other identification documents, a better supervision opportunity against fraud in identification documents, an improvement of protection mechanisms for strategic and other locations, accuracy in identification processes, and a complex handling of personal information saved in several information resources. "State Program 2007-2012 on Biometric Identification System" approved by the order 1963 issued on 13. 02. 2007 by the President of Azerbaijan Republic has introduced scientific-theoretical and practical problems for academic society besides legislative, organizational, technical and economic problems regarding the national biometric identification scheme.

One of the problems is the certification of biometric systems on the basis of international standards issued for various biometric technologies. Considering the problem, this work analyzes the methodological basis for certification of biometric systems.

Biometric systems have been used in security systems for last 5-10 years. It is clear that, since biometric systems are new emerging technologies and there is not enough experience in the field, consumers should consider the problem of adequate evaluation of biometric systems and used technologies. In general, there are two directions in the evaluation of biometric technologies:

- performance evaluation of biometric technologies;
- security evaluation of biometric technologies.

Performance evaluation not only measures the speed characteristics but also covers the evaluations of accuracy measures such as FAR (False Acceptance Rate), FRR (False Rejection Rate), ROC (Receiver Operating Characteristics), EER (Equal Error Rate), and FTE (Failure to Enroll) [1]. Standardization of performance evaluations (e.g. ISO/IEC 19795) are mainly undertaken by NIST and ISO.

Standardization of security evaluation of biometric technologies has several directions in international and national standardization organizations. ISO/IEC 2nd CD 19792 and ANSI X9.84-2003 standards by ISO/IEC JTC 1/SC27 are examples.

In the ISO/IEC CD 19792 international standard [2], the proposed methodology for security evaluation of biometric technologies cover the biometric components are determined and described in detail. In addition, biometric aspects used in evaluation process of biometric systems are determined as well as vulnerabilities of biometric technologies. As a result of the analysis of the proposed evaluation methodology it can be noted that performance evaluation of biometric technologies is based on this technology and the evaluation is performed in the security context.

The second direction of the standardization activities of security evaluation of biometric systems is the application of common criteria in biometric technologies and development of evaluation methodologies as well as protection profiles.

It is known that the main methodological base for security evaluation of information technologies (IT) is common criteria (CC). Common criteria suggests general requirements for evaluation of IT systems and devices. They are the functional and assurance requirements. Functional requirements are considered for security functions and mechanisms realizing them. Assurance requirements are considered for IT processes as well as its use and development.

Main aim of the common criteria based evaluation is helping consumers in determination of security level of using IT products.

Evaluation of specific technologies such as biometric ones requires more detailed methods. Evaluation of biometric systems is not at a desired level in common criteria. Successful use of biometric systems depends on both application type and application environment. Security functions and assurance requirements for a complete evaluation of biometric systems are not determined in common criteria. Activation quality of any biometric system depends on application type. Thus displacement, environmental factors, user demography and other factors affecting the test should be thoroughly evaluated and reported. Testing methodology of Common Evaluation Methodology considered in Common Criteria should determine the biometric problems and requirements. Therefore certain security functions and assurance requirements for security evaluation of biometric systems should be modified or reestablished and an evaluation methodology must be determined.

Protection profiles determine information security requirements in specific information technology area (e.g. operating system, database, inter-networks screen, smart-card and etc.). Protection profile forms families of technologies and it is neutral in terms of organization and policy among families and within the families. Three protection profiles of every protection family form the basic, extended and advanced levels of the protection.

Working Group on evaluation of biometric systems has suggested a methodology for evaluation of biometric systems based on CC [3]. In the methodology certain assurance requirements of CC are suggested to apply for evaluation of biometric systems. Additional explanations and guidelines are given. In addition, guidelines for Security Target evaluation (e.g. choosing appropriate security functions, determining vulnerabilities and threats, testing statistical and security characteristics) are proposed. It is also suggested that the characteristics complicating the evaluation of biometric systems should be considered. As a result of the analysis of the suggested methodology it can be noted that, biometric systems can also be evaluated by IT evaluation methods based on CC. Target of evaluation can be system or apparatus, biometric software or hardware. All the functional requirements of CC for IT can be used in Security Targets of biometric evaluation. Although CC does not consider the evaluation of biometric systems, biometric systems can be evaluated based on the additional explanations suggested in the methodology. Evaluation Assurance Levels in CC, with a little modification, could be used for biometric evaluations. For instance, EAL1 is supported by adding the Strength of Function.

A biometric evaluation methodology based on CC is suggested in [4]. Methodology proposes a modification of appropriate security functions and assurance requirements for evaluations of biometric technologies. For the purposes of the study, fingerprint technology is used as a basis. However, the methodology may be applied for the other biometric technologies as well. This study differentiates between performance- and security-oriented testing. The followings may be noted as some results of the analysis of the methodology:

- Security evaluations of biometric targets of evaluation (TOEs) are not the same as performance evaluations.
- Models representing biometric functions can assist in the identification of applicable functional and assurance requirements.
- The environment has a significant impact in the evaluation of a biometric TOE.
- Most of the security functions require additional explanation and guidelines in their application to biometric TOEs
- Assurance requirements are generally applicable to biometric TOEs. However, AGD– Guidance, ATE-Tests, AVA - Vulnerability Assessment, and ALC - Life Cycle Support require significant explanation and guidelines in their application to biometric TOEs.
- The assurance requirements assigned by EAL1- EAL4 are applicable to biometric evaluations with the caution that the recommended guidelines and recommendations be considered.

- The potential strength of function (SOF) of a biometric technology can be determined qualitatively.
- FM and FNM rates can be used as means of determining SOF.
- FM and FNM rate claims must be supported by appropriate testing.

A Protection Profile (PP) for biometric TOE can be defined on the basis of methodology proposed in [5] for evaluation of biometric systems. PP is described on the basis of information defining security requirements and application area according to biometric TOE type. In addition, it is suggested to define TOE security and environment security as well as target of security for both. In order to realize biometric TOE and target of security of environment, functional and assurance requirements of CC are used. As a result of the methodology it can be noted that, in order to define PP it is essential to determine TOE security and targets of environment security as well as to choose corresponding functional and assurance requirements.

Biometric evaluation methodology of biometric TOE suggested in [6] defines PP for biometric verification. Explanations, format and conditions comply with CC. Firstly, biometric TOE is described. For this, biometric processes, biometric TOE (using CC), configuration of the environment, and general model of biometric system are described. The security targets defining security targets of biometric TOE and environment are determined.

[7], [8] proposes a verification method of biometric PP for environments having basic and extended assurance levels. A description defining TOE and the context of TOE based on the generalized security requirements is presented. The security environment of TOE is described and threats against security activity of TOE are determined. Security targets ensuring the security of TOE and the security of application environment of TOE are determined. Security targets should comply with the threats and the security policy.

U.S. Government Biometric Verification Mode Protection Profile for Basic Robustness Environments determines the minimum functional and assurance requirements for biometric products of verification purposes in order to provide authentication that allows supervision for physical and logical access to information systems and devices in the main robustness environment. The choice of robustness levels for security environment of TOE depends on the cost of resources, authorization of subjects for these resources, and the probability of attacks tried.

Requirement part of this PP determines the necessity of biometric template protection to assure the confidentiality and integrity in the transmission. Biometric packet (identification of the user and associated templates) can be stored in a device out of the supervision of TOE, so biometric packet may be encrypted before transmission in order to make the modification detectable. A vendor should choose the best method to protect the data because this PP operates in the basic robustness environment.

TOE complying with this PP satisfies the determined functional requirements as well as the basic robustness assurance requirements. TOE security assurance requirements bases on the Evaluated Assurance Level (EAL) 2 in terms of source. In order to reach the necessary assurance level of basic robustness environments FLC_FLR.2 (Flaw Reporting Procedures) and AVA_MSU.1 (Examination of Guidance.) should be added.

The PP defined in U.S. Government Biometric Verification Mode Protection Profile for Medium Robustness Environments is different from a PP in basic robustness environment at some points:

- roles and distant administration (FMT_SMR);
- hardware is included in TOE;
- requirements to be included in TOE (FTA requirements);
- potential violation analysis (FAU_SAA requirements);
- assurance requirements base on EAL 4 in terms of source.

For the medium robustness environment, in order to obtain the necessary level of assurance, some clear requirements for several families of ADV class are formed. As a result, the duality in ADV classes could be removed and more than EAL4 assurance could be gained.

As a conclusion, it should be noted that regardless of the standardization attempts of general biometric methodologies in biometric technology security, the proposed methods are quite general and covers more general technologies. There is a need for making CC requirements more clear and specific.

Acknowledgement

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. Mansfield T. , Wayman J. , Best Practices in Testing and Reporting Performance of Biometric Devices, UK Biometrics Working Group, NPL Report CMSC 1402, Version 2, August 2002.
2. ISO/IEC CD 19792 "Information technology – Security techniques – Security evaluation of biometrics" 2006-07-14.
3. Common Methodology for Information Technology Security Evaluation – "Biometric Evaluation Methodology Supplement [BEM]". v1.0.
4. Biometric Technology Security Evaluation under the Common Criteria, Version 1.2, (CSE, Canada).
5. UK Government Biometrics Working Group, "Biometric Device Protection Profile (BDPP)", Draft Issue 0.82, 2001.
6. BSI, Common Criteria Protection Profile: Biometric Verification Mechanisms, BSI-PP-0016, v1.04. 2005.
7. US Information Assurance Directorate, "Biometric Verification Mode Protection Profile for Basic Robustness Environments", v1.1, 2007.
8. US Information Assurance Directorate, "Biometric Verification Mode Protection Profile for Medium Robustness Environments", v1.1, 2007.