Chapter 2
Security Evaluation of Behavioral Biometric Systems

Olaf Henniger
Fraunhofer Institute for Secure Information Technology, Germany

ABSTRACT

For establishing trust in the security of IT products, security evaluations by independent third-party testing laboratories are the first choice. In some fields of application of biometric methods (e.g., for protecting private keys for qualified electronic signatures), a security evaluation is even required by legislation. The common criteria for IT security evaluation form the basis for security evaluations for which wide international recognition is desired. Within the common criteria, predefined security assurance requirements describe actions to be carried out by the developers of the product and by the evaluators. The assurance components that require clarification in the context of biometric systems are related to vulnerability assessment. This chapter reviews the state of the art and gives a gentle introduction to the methodology for evaluating the security of biometric systems, in particular of behavioral biometric verification systems.

INTRODUCTION

Behavioral biometric characteristics, like the voice or handwritten signatures, are generally used for verification, i.e. for confirming a claimed identity through comparisons of biometric features, but rarely for identification, i.e. for finding identifiers attributable to a person through search among biometric features in a database, (see, e.g., ISO 19092, 2008). Therefore, we concentrate in this chapter on biometric verification systems.

Biometric verification systems are often embedded in larger systems as security mechanisms for user authentication purposes. Since the biometric characteristics of a person are bound to that person and cannot easily be presented by others, biometric methods can increase the binding of authentication processes to persons. It is, of course, a precondition that the biometric security mechanisms themselves are sufficiently secure (Prabhakar, Pankanti, & Jain, 2003).

DOI: 10.4018/978-1-60566-725-6.ch002

There are long-established standards and best practices for ensuring IT security, including such for preventing and mitigating such threats as the unwarranted or unwanted dissemination, alteration, or loss of information. These apply also to biometric systems. The means to achieve security are largely cryptographic, but there are also other security mechanisms, like tamper-proof enclosures, log files, locked doors, guardians, or the separation of responsibilities. In addition to the general IT security issues, there are security issues specific to biometric systems: their recognition accuracy and fraud resistance. These are the subject of this chapter.

As most users lack the resources and expertise to evaluate the security of IT products on their own and are unwilling to rely solely on claims put forth by the developers, security evaluations by independent third-party testing laboratories are the first choice for building confidence in the security of IT products. In some fields of application of biometric technologies, a security evaluation based on officially recognized criteria like the Common Criteria for IT security evaluation (ISO/IEC 15408), also known simply as the Common Criteria, is even required by legislation (see section "Specific requirements" below).

This chapter is structured as follows: The next section provides a general introduction to the Common Criteria security assurance requirements. Section "Vulnerability analysis" clarifies the evaluation methodology that is specific to biometric systems. The final section briefly summarizes the main conclusions.

SECURITY ASSURANCE REQUIREMENTS

General

To achieve comparability of the results of security evaluations, evaluation criteria have been standardized by several national and international standardization bodies. The Common Criteria for IT security evaluation (ISO/IEC 15408) arose as a basis for a wide international recognition of evaluation results. They comprise two large catalogues:

- Security functional requirements for describing the security functionality of an IT product (ISO/IEC 15408-2), and
- Security assurance requirements for describing the level of assurance provided by a security evaluation (ISO/IEC 15408-3).

The security assurance requirements define actions required from developers and evaluators. General guidance on how to perform these actions is provided in the Common Evaluation Methodology (ISO/IEC 18045). In addition to this, there are more specific guidance documents for specific purposes. A Biometric Evaluation Methodology was developed to supplement the Common Evaluation Methodology with respect to the evaluation of biometric systems (Common Criteria Biometric Evaluation Methodology Working Group, 2002). ISO/IEC 19792 (2008) specifies basic guidance on security evaluations of biometric systems independently of the Common Criteria or any other specific evaluation and certification schemes.

The security requirements are grouped into components, families and classes. A component is the smallest unit selectable for an evaluation. A family is a grouping of components that share security objectives, but differ in emphasis or rigor. A class is a grouping of families with a common focus.

The security assurance components are furthermore grouped into seven predefined Evaluation Assurance Levels (EALs). These levels, EAL1–EAL7, correspond to increasing degrees of confidence in the security of the Target of Evaluation (TOE) to be gained by increasing efforts for testing and design verification. Table 1 lists for each EAL the required security assurance com-