Security Evaluation of Biometric Systems in the Context of Common Criteria

Belen Fernandez-Saavedra

Carlos III University of Madrid
Tlf.: +34 91 624 40 35  Fax: +34 91 624 40 96
mbfernan@ing.uc3m.es
Outline

● Introduction to CC

● CC & Biometric Systems
  ➢ Protection Profiles (PP)
  ➢ Security Targets (ST)

● CEM & Biometric Evaluation

● Previous works

● New guidelines

● Conclusions
Common Criteria (CC)

Product under evaluation

Target of evaluation (TOE)

Specifications

Security Target (ST)

SPD

- Threats
- OSPs
- Assumptions

Security Objectives

Security Requirements

Based or not on a Protection Profile (PP)

Evaluation Methodology

Evaluation Activities

Common Evaluation Methodology (CEM)
Protection Profiles

- **Current PPs**
  - Biometric Verification Mechanisms (2005)
  - Fingerprint Spoof Detection Protection Profile based on Organizational Security Policies (2010)

- **Former PPs**
  - Biometric Device Protection Profile (2001)
  - U.S. Government Biometric Verification Mode Protection Profile for Basic Robustness Environments (2007)
  - Fingerprint Spoof Detection Protection Profile (2010)
Security Targets

- **Current STs**
  - Voiceldent Unit 1.0 (2007)
  - Authentest Server v1.2.6 (2010)

- **Former STs**
  - Bioscrypt™ Inc. Bioscrypt™ Enterprise for NT Logon, version 2.1.3. (2001)
  - Authentication Engine of VOICE.TRUST Server Version 4.1.2.0 (2005)
  - Voiceldent Unit 2.0 (2008)
CC & Biometric Systems (I)

● **Security properties**
  - Capability of correctly identifying persons using physical or behavioural features
  - Specific security properties of these features
    ▪ Uniqueness and robustness

● **Required Functionality**
  - Recognize authorized users using their biometric characteristics

● **Security Problem Definition**
  - General threats
    ▪ Non-authorized users or impostors gain access to the protected assets
    ▪ Authorized users are not being recognized
Security objectives

- User has to be authenticated/identified before any action
- It has to meet specific performance rates (FNMR/FRR and FMR/FAR)

Security Functional Requirements (SFRs)

- FIA: Identification and authentication
  - Refinement to meet specific error rates

Security Assurance Requirements (SARs)

- ATE: Tests
- AVA: Vulnerability assessment
CEM & Biometric Systems

- It is not completely specified for covering the particular characteristics of biometric systems

  - Biometrics is based on non-deterministic processes
    - Biometric performance is obtained calculating the probability of errors
    - Calculate such errors entails:
      - Strict repeatability
      - Restrictions in the set of valid input parameters

  - Biometric performance are influenced by several contour conditions (e.g. environment, users and their interactions, application, etc)
Previous works (I)

- Biometric Technology Security Evaluation under Common Criteria (BTSE)
  - Electronic Warfare Associates-Canada Ltd in 2001

- Biometric Evaluation Methodology Supplement (BEM)
  - Biometric Evaluation Methodology Working Group in 2002

Purpose

- Help developers and evaluators to interpret CC in case of biometric products
  - Additional explanation of security requirements in case of biometric TOEs
  - Additional guidelines of CEM methodology for their application to biometric TOEs

BTSE relevant contents

- Two representations of biometric functional models
- Differences between security testing and performance testing
• BEM relevant contents
  ➢ A summary of EALs including the recommended components for biometric system evaluations
  ➢ General threats of biometric systems

• Limitations
  ➢ Outdated
    ▪ Developed for previous versions of CC (CC v.2.1 / CEM v.1.0)
    ▪ Refers to performance evaluation methodologies that were implemented before the development of currents standards (ISO/IEC19795)
  ➢ Focused on verification performance metrics
    ▪ Identification performance metrics are not mentioned
Purpose

- Specify principal requirements for conducting a security evaluation of biometric systems
  - Provide guidance for evaluations
  - Help developers to prepare the evaluations

Relevant contents

- Requirements for testing security-relevant error rates following ISO/IEC 19795 Part 1
- Potential vulnerabilities of biometric systems
  - Explanation of typical vulnerabilities
  - Considerations for assessing these vulnerabilities
- Requirements to address privacy aspects
ISO/IEC 19792 (II)

- Limitations
  - The methodology does not provide details for technology evaluations specifically
    - Technology evaluations are useful for testing:
      - TOEs do not have to include the biometric capture sensor
      - Different subsystems and modules of a biometric system
  - It does not consider ISO/IEC 19795-2 standard
  - A relation between CEM Evaluation Activities and the proposed testing requirements does not exist
  - Testing guidelines are focused on verification performance metrics
    - Identification performance metrics are not mentioned
New Guidelines (I)

- Update to current version of CC
  - CC v.3.1/CEM v3.1 Release 3
- Specify for covering technology and scenario biometric performance evaluations
  - ISO/IEC 19795 - 1: Principles and Framework
  - ISO/IEC 19795 - 2: Testing methodologies for technology and scenario evaluation
- Base on previous works
  - BEM, BTSE and ISO/IEC 19792
  - PPs and STs
New Guidelines (II)

- Specify for testing all kind of biometric systems
  - All modalities
  - Different identification mechanisms: verification and identification

- Provide a relation between biometric evaluation methodologies and CEM Evaluation Activities
  - AGD: Guidance Documents
  - ATE: Tests
  - AVA: Vulnerability Assessment
Conclusions

- CC/CEM do not cover the particular characteristics of biometric systems
- Evaluators and developers need specific guidelines to apply CC/CEM
- Some works have been developed but these works are outdated or do not conform the current biometric testing standards
- New guidelines have to be developed to define the necessary additional requirements to CEM work units for covering security evaluation of biometric products
THANK YOU FOR YOUR ATTENTION

Belen Fernandez-Saavedra

Carlos III University of Madrid
Tlf.: +34 91 624 40 35   Fax: +34 91 624 40 96
mbfernan@ing.uc3m.es