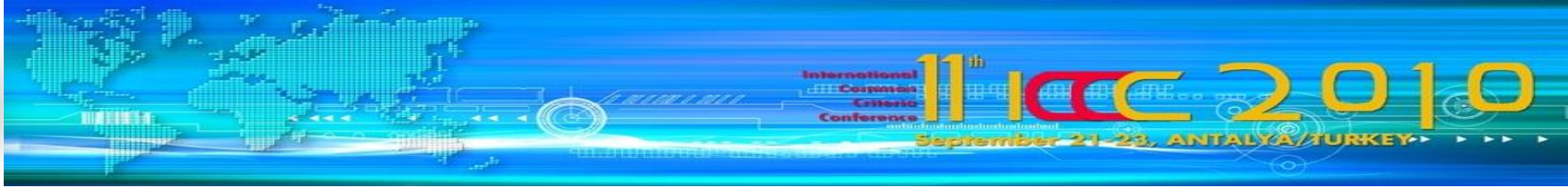

Security Evaluation of Biometric Systems in Common Criteria

Belen Fernandez-Saavedra,
R. Sanchez-Reillo, R. Alonso-Moreno, I. Tomeo-Reyes

University Carlos III of Madrid
Tlf.: +34 91 624 88 08 Fax: +34 91 624 94 30
{mbfernan,rsreillo,ramoreno,itomeo}@ing.uc3m.es

Outline

- Introduction
- Main Target
- AGD: Guidance Documents
- ATE: Tests
- Conclusions and Work Lines

Introduction (I)

- Guidelines are necessary for helping developers and evaluators to perform biometric evaluations
- Precedents:
  - BEM (Biometric Evaluation Methodology)
    - Previous version of CC
    - It refers to performance evaluation methodologies that were implemented before the development of current standards (ISO/IEC 19795)
  - PPs and STs
    - Security evaluation of biometric systems requires to meet specific error rates
      - ✓ Security policy
      - ✓ Refinement of the FIA_UAU component
    - This guidance refers to BEM and the same references that are included in it.

Introduction (II)

- It is essential for security evaluation of biometric systems to analyse the biometric system performance
- New guidelines shall be developed
  - Based on
    - BEM
    - ISO/IEC 19795 Biometric performance testing and reporting
  - Considerations
    - It will be conformant with current version of CC

Main Target

- Most relevant changes to BEM related to the following assurance requirements:
  - AGD: Guidance Documents
  - ATE: Tests
- Biometric performance evaluation that will be reproducible (ISO/IEC 19795 Parts 1 and 2)
  - Technological evaluation
    - Biometric algorithm
    - Database collection
  - Scenario evaluation
    - “End-to-end” biometric system
    - Test subjects

AGD: Guidance Documents (I)

- BEM
  - Biometric privacy
  - Environmental influences
  - Setting of thresholds
- Proposal for a new document
  - It should consider common activities for the installation and operation mode that are also relevant for performance testing
  - AGD_PRE:
    - Environmental influences considering environmental factors (as BEM) and also the operation configuration
      - ✓ Biometric system placement
      - ✓ User's interactions

AGD: Guidance Documents (II)

- Proposal for a new document
  - AGD_OPE:
    - User guides
      - ✓ Guidance for the capture process including how to present their biometric characteristic and interact with the biometric sensor
      - ✓ Feedback before, during and after the process
      - ✓ Recommendations to protect biometric data
    - Administrator guides
      - ✓ How to perform enrolment function specifying quality requirements in detail
      - ✓ How to guide and train users for enrolment and verification/identification processes

ATE: Tests (I)

- BEM
  - Performance testing: FMR and FNMR
  - Appropriate and statistically representative data
  - Take care in configuring the equipment, verifying its correct functioning and consistency in collection procedures
- Proposal for a new document
  - ATE_COV:
    - Technology evaluations: biometric systems that not include biometric capture sensor
    - Scenario evaluations: biometric systems
    - Test size, user characteristics, the number of samples and transactions shall be according to the expected results and the confidence level to achieve

ATE: Tests (II)

- Proposal for a new document
  - ATE_FUN:
    - Check that test documentation includes the mandatory parts of the ISO/IEC 19795 for planning, executing and reporting biometric evaluations
    - Check that test plan describes the scenarios for performing each test
      - ✓ Technology evaluations: conditions of the database collection
      - ✓ Scenario evaluations: user characteristic and how environmental conditions are controlled
    - Check the test application:
      - ✓ Data recording during the evaluation
      - ✓ Methods to calculate statistics
    - Check test procedures:
      - ✓ Level of effort, decision policies, visits and test crew flow

ATE: Tests (III)

- Proposal for a new document
  - ATE_IND:
    - Test subset shall include to obtain FMR and FNMR
    - Elaborate test documentation that includes the mandatory parts of the ISO/IEC 19795 for planning and executing biometric evaluations
    - Conduct testing
      - ✓ Scenario evaluations:
        - the appropriate test crew shall be recruitment according to user characteristics
        - user shall be trained and guided as it was specified in guidance documents
    - Obtain statistics: performance rates shall be calculated including the corresponding uncertainty respectively
    - Report test results considering the requirements of ISO/IEC 19795 standard

Conclusions and Future Works

- Conclusions
  - A proposal to develop new guidelines for helping developers and evaluators to perform biometric security evaluations using CC has been explained.
  - It has been based on BEM and ISO/IEC 19795 standards.
  - It shows requirements for applying AGD and ATE assurance compotents
- Future Works
  - Fulfil the proposal describing all relevant changes for the rest of assurance components
  - Implement specific methodologies for potential vulnerabilities

THANK YOU
FOR YOUR ATTENTION

Belen Fernandez-Saavedra,
R. Sanchez-Reillo, R. Alonso-Moreno, I. Tomeo-Reyes

University Carlos III of Madrid
Tlf.: +34 91 624 88 08 Fax: +34 91 624 94 30
{mbfernan,rsreillo,ramoreno,itomeo}@ing.uc3m.es