Biometrics in Common Criteria
The big picture

TÜV Informationstechnik GmbH

The Trust Provider

- TÜViT -

Content

- Biometrics Today: status of technology (short version)
- Biometrics in CC today
- ISO/IEC 19792: A model for Common Criteria?
  - The concept
  - Testing
  - Vulnerability Assessment
  - Privacy
- Other areas for biometrics in Common Criteria
  - ADV
  - AGD
  - AVA
- Other relevant activities that may support the evaluation of biometric technology
- Outlook

Biometrics Today

- The biometric technology became (more) mature over the last few years
- Biometric technology is used in sensitive areas today like
  - Electronic Passports
  - Border Security
- Some biometric evaluations have been performed but only on basic assurance levels
- Biometric technology has not reached the same standard with respect to evaluations as other technologies in such sensitive areas

Biometrics in CC Today

- A bunch of evaluations for biometric systems have been performed
- However, compared to classical technologies that are used in border security or homeland security biometrics are still way behind (with respect to evaluations)
- Potential reasons include:
  - Specific aspects of the technology
  - Frequent updates of systems
  - A missing methodology and the uncertainty that comes along with it
- So how are we currently handling biometric systems in CC and what can be used to solve at least the issue around the methodology in the near future?

BEM

- The **B**iometric **E**valuation **M**ethodology is a paper that provides basic interpretation of the criteria for biometric technologies
- It provides interpretations for several assurances classes and describes important aspects around testing and vulnerability assessment
- The BEM is the only available interpretation for biometric evaluations in Common Criteria
- Unfortunately the BEM is outdated
- There was no update to consider the latest development
  - In the area of biometrics
  - In the area of Common Criteria (the BEM is available for CC 2.1)
- ISO/IEC 19792 is currently under development in ISO/IEC SC 27 and aims to provide an update for parts of this issue

ISO/IEC 19792

- This standard aims to define the special needs of biometric technology in the context of security evaluations
- It is independent of a concrete evaluation methodology
- However, evaluations according to Common Criteria are one important field for ISO/IEC 19792
- ISO/IEC 19792 could serve as the basis for a comprehensive evaluation methodology for biometric systems in Common Criteria
- It includes
  - Terms and definitions
  - Concept for security evaluations of biometric technology
  - Error Rates
  - Vulnerability Assessment
  - Privacy
- The following slides will introduce the standard in more detail

ISO/IEC 19792: The concept

- The basic concept of this standard is that biometric systems should be treated as any other technology in IT security when under evaluation
- However, there are certain aspects of this technology that require special care:
  - Testing of error rates
  - Vulnerability assessment
  - Aspects of privacy
- Those areas are handled in separate chapters
- Further a universal design for a biometric system is introduced

ISO/IEC 19792: Testing

- The standard introduces a three step concept for testing that should also be compliant to CC requirements:
  - The developer has to provide a claim for the security relevant error rates
  - The developer has to test the biometric system and provide evidence that it meets the claim
  - The claim and the test will be verified (and repeated) by an independent party

ISO/IEC 19792: Testing II

- The standard defines requirements that have to be met by the tests regarding:
  - The assumptions the test scenario bases on
  - The test crew
  - The test environment
  - The error rates that shall be tested
  - The settings of the system under test
  - Criteria for the comparability of tests

ISO/IEC 19792: Vulnerability Assessment

- The standard introduces a basic threat model for biometric systems based on the threats of
  - Impersonation
  - Disguise
  - Denial of Service
- Further it introduces common vulnerabilities for biometric systems
- It focuses on biometric specific vulnerabilities and only touches “classical” vulnerabilities in some areas
- The list of generic vulnerabilities shall be used as the basis for each vulnerability assessment
- However, the standard acknowledges that such a list of generic vulnerabilities cannot be considered being a complete list

ISO/IEC 19792: Common Vulnerabilities

- Performance limitations
- Use of an artefact
- Conversion of biometric characteristics
- Difficulty of concealing biometric characteristics
- Similarity due to blood relationship
- Special biometric characteristics
- Synthesized abnormal biometric samples
- Hostile Environment
- Procedural Vulnerabilities
- Leakage and alteration of biometric data

ISO/IEC 19792: Privacy

- Currently ISO/IEC 19792 defines basic requirements around privacy aspects for biometric systems
- These aspects focus on:
  - Adequate Data Protection
  - Application Binding for biometric data
  - Account Deactivation
  - De-Enrolment
- However, privacy is only a side aspect for ISO/IEC 19792
- In future aspects of privacy will be handled in a separate Working Group within ISO/IEC SC 27

Other relevant areas/issues

- Beside the aspects that are currently addressed in ISO/IEC 19792 evaluations of biometric devices according to Common Criteria need additional consideration in other assurance aspects e.g.

- ADV
  - Specific attention has to be paid in order to provide the evaluator with the necessary information about the biometric algorithms
- AGD
  - Biometric systems often allow a tuning of parameters that need special consideration in the Guidance Documents
- AVA
  - Information about specific vulnerabilities and the related effort is moving fast (comparable to the smart card world)
  - This information cannot be part of a static interpretation but will need to be maintained in a different form

Other relevant standards (to be complete)

- ISO/IEC SC 37 (Biometrics)
  - ISO/IEC 19795-x: Performance evaluations of biometric systems
  - New work item proposal: Guidance on specifying performance requirements to meet security and usability needs
- ISO/IEC SC 27 WG 5
  - This Working Group has only been established recently
  - It standardizes
    - Privacy,
    - Some biometric topics (e.g. template protection) and
    - Identity Management

Outlook

- There is a need for clear requirements around the evaluation and certification of biometric systems in sensitive areas
- Without such clear requirements the assurance that can be gained on biometric technology will not rise
- There is still a need for a comprehensive interpretation of the Common Criteria for biometric systems
- ISO/IEC 19792 is a first step towards such an interpretation
- However, the standard will need to be adopted to the special requirements around Common Criteria
- Other standards that are currently under evaluation can provide additional information for certain areas.

Thanks for your attention!

TÜV Informationstechnik GmbH

Member of TÜV NORD Group

Nils Tekampe
Consultant Information Security

Langemarckstr. 20
D-45141 Essen

Phone: +49 201 8999 – 622
Fax: +49 201 8999 – 666
E-Mail: n.tekampe@tuvit.de
URL: www.tuvit.net