



# Development of a Protection Profile for Biometric Systems Following ISO/IEC TR 15446

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

**GUTI**

University Group for Identification Technologies  
University Carlos III of Madrid

Tlf.: +34 91 624 88 08 Fax: +34 91 624 94 30

[mbfernan,rsreillo,ramoreno}@ing.uc3m.es](mailto:{mbfernan,rsreillo,ramoreno}@ing.uc3m.es)





# Outline

- Introduction
- Main Target
- ISO/IEC TR 15446
- TOE Overview
- Security Problem Definition
- Security Objectives
- Conclusions and Work Lines





# Introduction

## Introduction

Main Target

ISO/IEC TR 15446

TOE Overview

SPD

- Informal Security Requirement
- Threats
- OSP
- Assumptions
- Rationale

Security Objectives

- Definition
- Objectives
- Rationale

Conclusions and Future Works



- Biometric systems are IT products
- They have special characteristics that make difficult the definition of a PP
  - Probabilistic functions
  - Dependent of environment, user behaviour, etc
- Current published PPs:
  - Biometric system based on verification mechanisms
  - Last versions of CC
  - Not include critical parts of a biometric system such as capture or database modules
- New guide to produce Protection Profiles and Security Targets



# Main Target

- Develop a new PP for biometric systems
  - Following ISO/IEC TR 15446 guidance
    - Defining the SPD according to the proposed methodology in this Technical Report
      - Informal security requirement
      - Rationale to link the SPD back to the informal security requirement
  - Extending the coverage of biometric products
    - Verification and identification systems
    - Capture and database modules
  - According to the new version of Common Criteria
    - CC Version 3.1 Release 3 Final

Introduction

**Main Target**

ISO/IEC TR 15446

TOE Overview

SPD

- Informal Security Requirement
- Threats
- OSP
- Assumptions
- Rationale

Security

Objectives

- Definition
- Objectives
- Rationale

Conclusions and  
Future Works





# ISO/IEC TR 15446

10th  
International  
Common  
Criteria  
Conference



Introduction

Main Target

ISO/IEC TR 15446

TOE Overview

SPD

- Informal Security Requirement
- Threats
- OSP
- Assumptions
- Rationale

Security

Objectives

- Definition
- Objectives
- Rationale

Conclusions and  
Future Works



- PP Introduction
  - PP reference
  - TOE overview
- Conformance Claims
- Security Problem Definition
  - Identify the informal security requirement
  - Identify threats
  - Document policies
  - Document assumptions
  - Check the complete SPD specification
- Security Objectives
  - Security objectives for the TOE
  - Security objectives for the environment
  - Security objectives rationale



# TOE Overview



Introduction

Main Target

ISO/IEC TR 15446

**TOE Overview**

SPD

- Informal Security Requirement
- Threats
- OSP
- Assumptions
- Rationale

Security Objectives

- Definition
- Objectives
- Rationale

Conclusions and Future Works



- Biometric systems are systems that allow automatic human recognition by means of their physiological and/or behavioural characteristics
- These systems are used in authentication or identification processes
- Security characteristics
  - Biometric characteristics:
    - Unique for human beings
    - No need to remember them
    - Cannot be lost
- Drawbacks
  - Probabilistic functions
  - Depending on environment: user, ambient conditions, etc.
  - Biometric characteristics are very sensitive information



# Informal Security Requirement

- Introduction
- Main Target
- ISO/IEC TR 15446
- TOE Overview
- SPD**
  - Informal Security Requirement**
  - Threats
  - OSP
  - Assumptions
  - Rationale
- Security Objectives
  - Definition
  - Objectives
  - Rationale
- Conclusions and Future Works

- **Required functionality**
  - Recognize authorized users using biometrics
  - Allow these users to access protected resources depending on their privileges
  - Protect sensitive information
- **Risk and threat assessment**
  - Based on:
    - Vulnerability assessment of ISO/IEC 19792
      - Impersonation
      - Disguise
      - Denial of service
    - BEM: General threats for biometric systems





# Informal Security Requirement



Introduction

Main Target

ISO/IEC TR 15446

TOE Overview

**SPD**

• Informal Security Requirement

- Threats
- OSP
- Assumptions
- Rationale

Security

Objectives

- Definition
- Objectives
- Rationale

Conclusions and Future Works



- Capture
  - Zero-effort impostor attempts (wolves & lambs, blood relationship)
  - Threaten user, user who allows an attacker to act after he has been accepted and user who modifies his own biometric characteristic
  - Attacker: artefact, modification, dead, stolen or low quality biometric characteristic
  - Hill-climbing, replay attacks
  - Signal injection, residual samples
- Database (template or feature extraction vector)
  - Modified, deleted, injected or stolen by attackers, administrators or users with administrator privileges
- Algorithm
  - Modified by virus or malware and stolen by attackers
- Communication between modules
  - Modified, injected, stolen or deleted data by attackers, virus or malware
- Configuration data, decision thresholds or quality thresholds
  - Modified by administrators, virus, malware, users with administrator privileges
- Personal data, privileges and log files
  - Modified, deleted, added or stolen by attackers, administrators or users with administrator privileges
- General biometric system
  - Hostile environment



# Informal Security Requirement



Introduction

Main Target

ISO/IEC TR 15446

TOE Overview

**SPD**

• **Informal Security Requirement**

- Threats
- OSP
- Assumptions
- Rationale

Security Objectives

- Definition
- Objectives
- Rationale

Conclusions and Future Works



- Management, presentational or evaluation policies
- Policies related to best practices for biometric products:
  - Performance rates and thresholds
  - Quality
  - Maximum number of verifications
  - Outputs and feedback
  - Communications
  - Privacy

# Informal Security Requirement (IV)



- Divide collected information in 3 areas:
  - Threats: potential attacks to counter by the TOE
  - Policies: security attributes or features that the TOE must possess
  - Assumptions: security attributes or features that the TOE not need possess

Introduction

Main Target

ISO/IEC TR 15446

TOE Overview

**SPD**

- Informal Security Requirement

- Threats
- OSP
- Assumptions
- Rationale

Security

Objectives

- Definition
- Objectives
- Rationale

Conclusions and  
Future Works





# Threats



Introduction

Main Target

ISO/IEC TR 15446

TOE Overview

**SPD**

• Informal Security Requirement

• **Threats**

• OSP

• Assumptions

• Rationale

Security

Objectives

• Definition

• Objectives

• Rationale

Conclusions and  
Future Works



- T.IMPOSTOR: An attacker may attempt to access by means of zero-effort attempt, impersonation, artefact or stolen biometric samples
- T.DISGUISE: A user may modify his biometric sample to avoid being recognized
- T.THREATEN: A user may be threaten
- T.DEAD: An attacker may use a biometric sample that belongs to a dead user to get access
- T.LOW\_QUALITY: Biometric sample may be low quality sample
- T.RESIDUAL: A residual sample may be presented to capture sensor
- T.REPLAY: An attacker may attempt to access several times
- T.HILL\_CLIMBING: An attacker may perform a hill-climbing attack
- T.ADMINISTRATOR: An administrator may allow an unauthorized user to enrol or change user privileges, configuration data or thresholds
- T.USER: A user may allow unauthorized users to access
- T.MODIFY\_PRIVILEGES, T.MODIFY\_THRESHOLDS and T.MODIFY\_CONF\_DATA: TSF data may be modified
- T.INJECTION\_SAMPLE, T.INJECTION\_TEMPLATE and T.INJECTION\_INFO: An attacker may inject TSF data
- T.DELETE\_TEMPLATE and T.DELETE\_INFO: TSF data may be deleted
- T.STEAL\_TEMPLATE, T.STEAL\_ALGORITHM and T.STEAL\_INFO: An attacker may attempt to steal TSF data
- T.FAILURE: Different hardware and software failures may produce that the TOE does not work properly
- T.ENVIRONMENT: A hostile environment may produce that the TOE does not work properly
- T.VIRUS: virus and malware may modify, delete or break data and functions of the TSF

# Organizational Security Policies



- **Mandatory security functions**
  - P.AUTHENTICATION: TOE shall authenticate user and administrator to get access to the TOE
  - P.RATES: Performance rates shall meet proper values
  - P.QUALITY: Biometric sample shall achieve specific levels of quality
- **Mandatory technologies/techniques**
  - P.BIOMETRICS: Authentication mechanisms shall use biometrics
  - P.COMMUNICATIONS: Communications will be encrypted
  - P.PRIVACY: personal data shall be separated to biometric data
- **Policies to counteract threats**
  - P.MAX\_ATTEMPTS: A maximum number of attempts will be determined for each authentication
  - P.OUTPUT: the TOE will not show similarity scores

Introduction

Main Target

ISO/IEC TR 15446

TOE Overview

**SPD**

• Informal Security Requirement

• Threats

• **OSP**

• Assumptions

• Rationale

Security

Objectives

• Definition

• Objectives

• Rationale

Conclusions and  
Future Works





# Assumptions

- Personnel, procedure and physical security
  - A.ADMINISTRATOR: administrator will be not hostile and will know how to enrol user and the usage of the TOE
  - A.USER: user will be not hostile and will know the usage of the TOE
  - A.THREATEN: User will not be threaten or there will be other methods to detect it in the IT environment such as CCTV
  - A.AUDIT\_REVIEW: Operators will review the audit information
  - A.CONNECTIONS: users will not access to connections between modules
- Technical functionality
  - A.CONFIGURATION: TSF functions will be configured following the developer instructions
  - A.ENVIRONMENT: ambient conditions will be the recommended by the developer
  - A.VIRUS: TOE will be protected against virus and malware

Introduction

Main Target

ISO/IEC TR 15446

TOE Overview

**SPD**

• Informal Security Requirement

• Threats

• OSP

• **Assumptions**

• Rationale

Security

Objectives

• Definition

• Objectives

• Rationale

Conclusions and  
Future Works





# Rationale: SPD – Informal Security Requirement



Introduction

Main Target

ISO/IEC TR 15446

TOE Overview

**SPD**

• Informal Security Requirement

• Threats

• OSP

• Assumptions

• **Rationale**

Security

Objectives

• Definition

• Objectives

• Rationale

Conclusions and  
Future Works



- Risk and threat assessment
  - Capture
    - T.IMPOSTOR, T.DISGUISE, T.THREATEN, T.DEAD, T.LOW\_QUALITY, T.RESIDUAL, T.REPLAY, T.HILL\_CLIMBING, T.ADMINISTRATOR, T.USER, T.INJECTION\_SAMPLE, P.AUTHENTICATION, P.BIOMETRICS, P.RATES, P.QUALITY, P.MAX\_ATTEMPTS, P.OUTPUT
  - Database
    - T.INJECTION\_TEMPLATE, T.DELETE\_TEMPLATE, T.STEAL\_TEMPLATE, P.PRIVACY
  - Algorithm
    - T.STEAL\_ALGORITHM, T.VIRUS
  - Communication between modules
    - T.INJECTION\_INFO, T.STEAL\_INFO, P.COMMUNICATIONS
  - Configuration data, decision thresholds or quality thresholds
    - T.INJECTION\_INFO, T.DELETE\_INFO, T.MODIFY\_THRESHOLDS, T.MODIFY\_CONF\_DATA
  - Personal data, privileges and log files
    - T.MODIFY\_PRIVILEGES, T.INJECTION\_INFO, T.STEAL\_INFO, T.DELETE\_INFO
  - General biometric system
    - T.ENVIRONMENT, T.FAILURE, T.VIRUS
- Security policies
  - Performance rates and thresholds
    - P.AUNTHENTICATION, P.BIOMETRICS, P.RATES
  - Quality
    - P.QUALITY
  - Maximum number of verification attempts
    - P.MAX\_ATTEMPTS
  - Outputs and feedback
    - P.OUTPUT
  - Communications
    - P.COMMUNICATIONS
  - Privacy
    - P.PRIVACY



# Definition



Introduction

Main Target

ISO/IEC TR 15446

TOE Overview

SPD

- Informal Security Requirement
- Threats
- OSP
- Assumptions
- Rationale

**Security Objectives**

- **Definition**
- Objectives
- Rationale

Conclusions and Future Works



- List of applicable threats, policies and assumptions from the SPD
- Some threats are discounted by risk analysis or assumptions
- Separate the rest of them:
  - TOE Functionality
  - IT Operational Environment
  - Non-IT Operational Environment



# Security Objectives



Introduction

Main Target

ISO/IEC TR 15446

TOE Overview

SPD

• Informal Security Requirement

• Threats

• OSP

• Assumptions

• Rationale

**Security Objectives**

• Definition

• **Objectives**

• Rationale

Conclusions and Future Works



- Security objectives
  - O.BIOMETRICS\_AUTHENTICATION: TOE must have biometric authentication mechanisms. It has to meet specific rates. Biometric TOE must only show a match or non-match decision. Biometric system must allow only a maximum number of attempts per user. Biometric system must have an alive detection method and a method to reject low quality samples
  - O.AUDIT: All events related to biometric authentication and TSF data modification must be audited by the TOE
  - O.CLEAR: TSF must have specific instructions to clear registers after a biometric authentication
  - O.ENCRYPT: TOE must transfer encrypted data between its modules and templates or feature extraction vectors must be saved encrypted in the database
  - O.PERSONAL\_DATA: Personal data must be saved separated to biometric data
  - O.AUTH\_ADMIN: TOE must have an alternative mechanism to authenticate the administrator
  - O.FAILURE: TOE must go to a safe state when specific failures happen
- Security objectives for the operational environment
  - OE.ADMINISTRATOR: Administrator is not hostile and knows the enrolment process and the usage of the TOE
  - OE.USER: User is not hostile and knows how to use the TOE
  - OE.THREATEN: User is not threaten or there are methods for detecting it in the IT environment
  - OE.AUDIT\_REVIEW: Operators review the audit information
  - OE.CONNECTIONS: Connections between modules of the TSF are inaccessible
  - OE.CONFIGURATION: TSF functions are configured according developer instructions



# Objectives Rationale



Introduction

Main Target

ISO/IEC TR 15446

TOE Overview

SPD

• Informal Security Requirement

• Threats

• OSP

• Assumptions

• Rationale

**Security Objectives**

• Definition

• Objectives

• **Rationale**

Conclusions and Future Works



- Security objectives

- O.BIOMETRICS\_AUTHENTICATION

- T.IMPOSTOR, T.DISGUISE, T.DEAD, T.LOW\_QUALITY, T.REPLAY, T.HILL\_CLIMBING, P.AUTHENTICATION, P.BIOMETRICS, P.RATES, P.QUALITY

- O.AUDIT

- T.REPLAY, T.MODIFY\_PRIVILEGES, T.MODIFY\_THRESHOLDS, T.MODIFY\_CONF\_DATA

- O.CLEAR

- T.RESIDUAL

- O.ENCRYPT

- T.INJECTION\_SAMPLE, T.INJECTION\_TEMPLATE, T.INJECTION\_INFO, T.STEAL\_TEMPLATE, P.COMMUNICATIONS

- O.PERSONAL\_DATA

- T.STEAL\_TEMPLATE, P.PRIVACY

- O.AUTH\_ADMIN

- T.MODIFY\_PRIVILEGES, T.MODIFY\_THRESHOLD, T.MODIFY\_CONF\_DATA

- O.FAILURE

- T.DELETE\_TEMPLATE, T.DELETE\_INFO

- Security objectives for the operational environment

- OE.ADMINISTRATOR

- A.ADMINISTRATOR, T.ADMINISTRATOR

- OE.USER

- A.USER, T.USER

- OE.THREATEN

- A.THREATEN, T.THREATEN

- OE.CONNECTIONS

- A.CONNECTIONS, T.INJECTION\_SAMPLE, T.INJECTION\_TEMPLATE, T.INJECTION\_INFO, T.DELETE\_TEMPLATE, T.DELETE\_INFO, T.STEAL\_TEMPLATE, T.STEAL\_ALGORITHM, T.STEAL\_INFO

- OE.CONFIGURATION

- A.CONFIGURATION, T.ENVIRONMENT, P.QUALITY, P.RATES

- OE.ENVIRONMENT



# Conclusions and Future Works

10th  
International  
Common  
Criteria  
Conference



Introduction

Main Target

ISO/IEC TR 15446

TOE Overview

SPD

- Informal Security Requirement
- Threats
- OSP
- Assumptions
- Rationale

Security

Objectives

- Definition
- Objectives
- Rationale

Conclusions and  
Future Works



## ● Conclusions

- A PP for biometric systems has been developed following ISO/IEC TR 15446 guidance

- Considering a generic biometric system
- Based on the last version of CC

## ● Future Works

- Implement the overall PP:

- SFRs
- SARs
- Security requirements rationale

- Check and solve inconsistencies



# THANK YOU FOR YOUR ATTENTION

---



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

**GUTI**

University Group for Identification Technologies  
University Carlos III of Madrid

Tlf.: +34 91 624 88 08 Fax: +34 91 624 94 30

[mbfernan,rsreillo,ramoreno}@ing.uc3m.es](mailto:{mbfernan,rsreillo,ramoreno}@ing.uc3m.es)