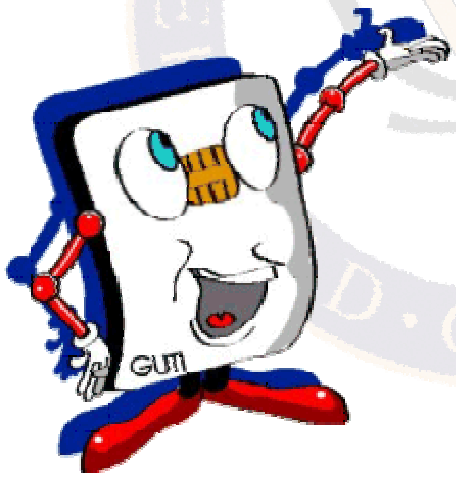
Evaluation Methodology Based on CEM for Testing Environmental Influence in Biometric Devices



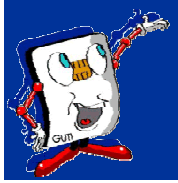
Belen Fernandez-Saavedra,
R. Sanchez-Reillo, R. Alonso-Moreno

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

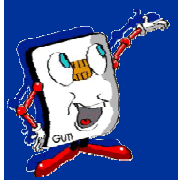
Outline

- Introduction
- Main Target
- Biometric System as TOE
- Evaluation Methodology
- Test Plans: relevant scenarios, equipment, subjects, results
- Test Procedure
- Conclusions



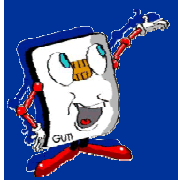
Introduction

- Biometrics is becoming important as a technique to provide security
- As IT products, biometric devices can be evaluated by Common Criteria
- Biometric products have special characteristics:
  - Biometric is based on probabilistic functions
  - It is very dependent on several factors: environmental conditions, users and their attitude, sample quality, etc
- Environmental conditions can influence on system performance and they might affect the security level achieved significantly
- Nowadays, these conditions are not evaluated



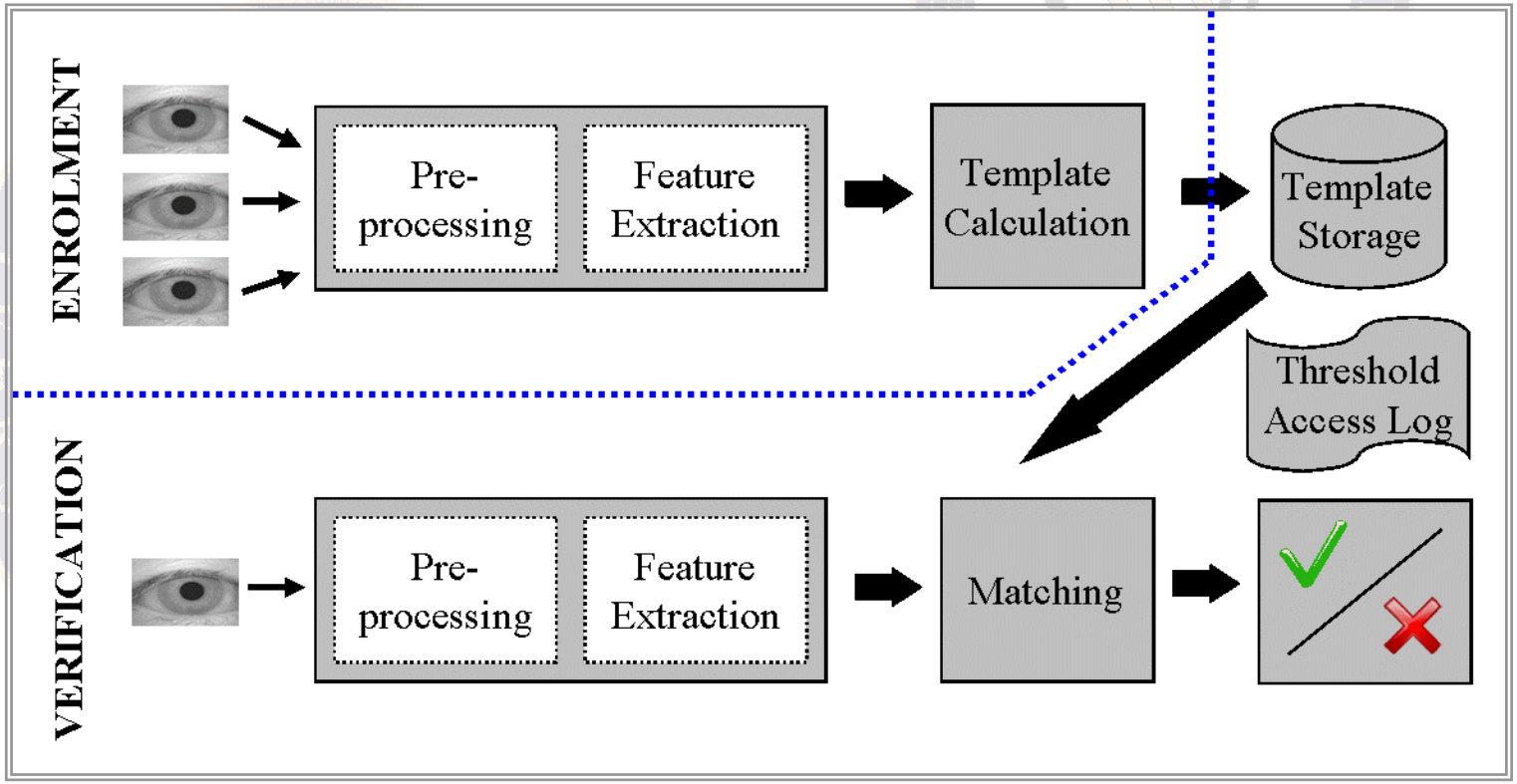
Main Target

- To create a Methodology to test biometric products under different ambient conditions
- Based on CEM Methodology
  - For independent testing in its typical operational range: ATE_IND
  - For vulnerability analysis under extreme conditions: AVA_VAN
- Example: Biometric system used for access control in a company with typical indoor conditions



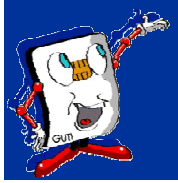
TOE Overview

- Generic biometric system used for personal identification



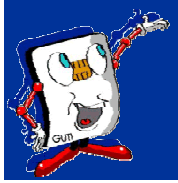
Security Problem Definition (I)

- Threats
  - T.ENVIRONMENT: Environmental conditional could be modified to get access to biometric system
  - T.IMPOSTOR: Impostors and attackers could try to access to the biometric system
- Organisational Security Policies
  - OP.FMRFNMR: Biometric system must meet a recognised national or international standard for false acceptance and false rejection rates
- Assumptions
  - A.VERIFICATION: Type of comparison mode of biometric system will be verification
  - A.SENSOR: Although performance rates are calculated within the whole biometric system, only capture sensor will be subjected to different ambient conditions
  - A.AMBIENT: Only some environmental factors will be considered. These are temperature, humidity and illumination



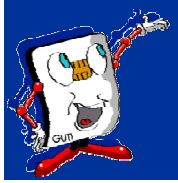
Security Problem Definition (II)

- More assumptions:
  - A.TYP_CONDITIONS: Typical ambient conditions for the complete evaluation will be the next conditions:
    - Temperature between 22 to 25ºC
    - Relative Humidity between 40 to 60% RH
    - Illumination: Visible light (400 to 750 nm) with an intensity of 1,000–2,500 and Near-Infrared light (750 to 900 nm) in the range 0–1,000
  - A.USER: Reference will be kept at typical ambient conditions
  - A.GUIDE: Users will be guided during all evaluation process
  - A.ENROL: Enrolment will be done indoors at typical conditions



Security Objectives (I)

- TOE Security objectives
  - O.FMRFNMR: Biometric system shall meet specified error rates
  - O.SENSOR: Biometric sensor has to perform correctly in its operational range
  - O.VERIFICATION: Biometric system must provide a biometric verification mechanism to authenticate users

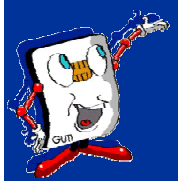


Security Objectives (II)

- Operational Environment Security Objectives
  - OE.TEMP: Operational range is between Tmin and Tmax (Example: Tmin=0ºC and Tmax=50ºC)
  - OE.HUM : Operational range is between RHmin and RHmax (Example: RHmin=0% and RHmax=50ºC)
  - OE.LIGHT: Operational for visible is between IVmin and IVmax and for near-infrared is between INIRmin and INIRmax (Example: IVmin=1,500, IVmax=3,000, INIRmin=0 and INIRmax=1,000)
  - OE.SYSTEM: Biometric system without capture sensor works in typical ambient conditions
  - OE.USER: Users are in typical ambient conditions
  - OE.GUIDE: There is an administrator to control enrolment and to guide users all the time
  - OE.ENROL: Users'enrolment is carried out in typical ambient conditions

Security Requirements

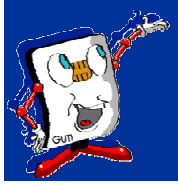
- SFRs: mainly components of identification and authentication class (FIA) with refinements for biometric systems
- SARs: their components should include specific refinement taken from BEM related to performance testing, statistically representative data and environment conditions
  - ATE_IND for addressing performance testing *into operational range*
  - AVA_VAN for addressing performance testing *outside operational range*



TOE Summary Specification

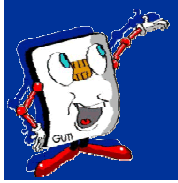
9th ICCC
9th International Common Criteria Conference

- TOE Security Functions
  - F.ENROL: it allows that users can gather into the biometric system. Biometric system generates a template and stores it into its database
  - F.VERIFY: this function provides the ability to authenticate a user. It compares user sample with the corresponding template and shows the decision of such comparison



Evaluation Methodology

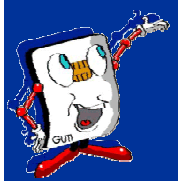
- Based on ATE_IND and AVA_VAN work unit detailed at CEM
  - Devise a test subset: evaluate F.VERIFY at different environmental conditions into its operational range
  - Devise penetration test: evaluate F.VERIFY under extreme conditions
  - Produce test documentation: procedure and requirements are similar for both test with the exception of relevant scenarios to consider



Relevant Scenarios (I)

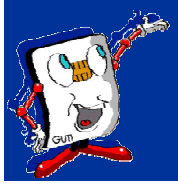
9th ICCC 9th International Common Criteria Conference

	SCENARIO	T (ºC)	RH(%)	ILLUMINATION
STD	Typical A.TYP_CONDITIONS	22-25	40-60	Visible ⇒ 1,000 to 2,500 NIR ⇒ 0 to 1,000
T	Cool	Tmin (e.g. =0)	40-60	Visible ⇒ 1,000 to 2,500 NIR ⇒ 0 to 1,000
	High	Tmax (e.g. =50)		
	Temp. Range Variability	T_1 (e.g. = 23)		
		T_2 (e.g.= 36)		
HUM.	Low humidity	22-25	RHmin (e.g. =20)	Visible ⇒ 1,000 to 2,500 NIR ⇒ 0 to 1,000
	High humidity		RHmax (e.g. =80)	
	RH. Range Variable		RH_1 (e.g.=40)	
			RH_2 (e.g.=60)	
LIGHT	Low light	22-25	40-60	Visible ⇒ IVmin (e.g.1,500 to 3,600) NIR ⇒ INIRmin (e.g. 0 to 100)
	High light			Visible ⇒ IVmax (e.g.3,400 to 3,500) NIR ⇒ INIRmax (e.g. 900 to 1000)
	Light Range Variable			Visible ⇒ IV_1 (e.g.1,600 to 2,500) NIR ⇒ $INIR_1$ (e.g. 100 to 500)
				Visible ⇒ IV_2 (e.g.2,500 to 3,400) NIR ⇒ $INIR_2$ (e.g. 500 to 900)



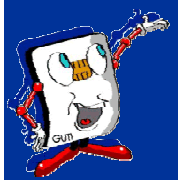
Relevant Scenarios (II)

	SCENARIO	T (ºC)	RH (%)	ILLUMINATION
T	Cold	–10- –5	40-60	Visible ⇒ 1,000 - 2,500 NIR ⇒ 0 - 1,000
	Very cold	–20- –10		
	Very high	50-60		
HUM.	Very low humidity	22-25	0-10	Visible ⇒ 1,000 - 2,500 NIR ⇒ 0 - 1,000
	Very high humidity		90-100	
LIGHT	Infrared	22-25	40-60	Visible ⇒ 1,000 - 2,500 NIR ⇒ 0 - 3,000
	Outdoor			Visible ⇒ 1,000 - 35,000 NIR ⇒ 0 - 10,000
	Darkness			Visible ⇒ 0 - 100 NIR ⇒ 0 - 100



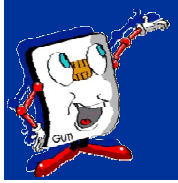
Test Equipment

- Scenario conditions
  - Temperature and humidity: climatic chamber
  - Illumination controlled area: certain space or room where different bulbs and fluorescent have to be allocated
- Measuring instruments
  - Temperature and humidity: climatic chamber with an uncertainity above 0.5 degrees for temperature and 0.5% for humidity
  - Illumination: Spectometer
- Register instruments
  - Automatic system for recording significant data



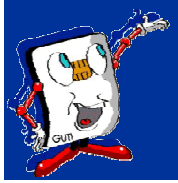
Test Subjects

- A wide set of users shall be chosen to participate in it
- Following Best Practise people have to be of different gender, age, ethnic, origin and occupation
- The number of users must be significant regarding the target user population
- Users should be information about visit schedule, legal issues and how to use the biometric system and test instruments



Test Results

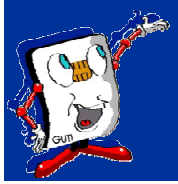
- Evaluators must check generated data to know whether methods are properly applied and test equipments work correctly. All these data have to be saved
- Later, evaluators have to calculate performance statistics and these will be reported together with non-biometric data
- At least the following information shall be recorded:
  - Performance metrics
    - Error rates: FTA, FNMR, FMR, etc
    - Throughput rates
  - Data available
    - Personal data of users: gender, age, ethnic, etc
    - Number of scenario users
    - Environmental data: atmosphere conditions for each scenario. (E.g. the average, maximun and minimun temperature and relative humidity, a graphic of the spectrum of light with the intensity for each wavelength)



Test Procedure (I)

Common steps for all scenarios

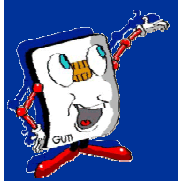
1. Explain users how to use the biometric sensor under test
2. From the complete set of users choose how many of them will behave as genuine users, and how many will be impostors
3. Begin with the enrolment process only for all genuine users selected
   a) Start function for a new enrolment
   b) Check whether the environmental conditions comply to those stated for the Office scenario
   c) User must present his/her biometric reference to sensor when biometric application requests it. During enrolment, each user will be identified by means of name or number. Evaluator must make sure that it is unique for each user
   d) Wait whereas biometric system generates the corresponding template and saves it
   e) If FTE error is returned, a new enrolment may be carried out. If not, this user has to be removed from the list for the remaining evaluation. Evaluator shall choose the best options according to the number of available users and the size o samples needed for test



Test Procedure (II)

Steps for each scenario

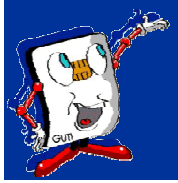
4. Introduce biometric capture sensor into the modeled scenario
5. Generate the environmental conditions and wait till scenario conditions are reached
6. Check if the environmental parameters are stable and within the ranges stated for the scenario
7. Run the biometric application and check if it is working properly
8. Begin with verification process for genuine users and impostors:
   a) Start function for authentication
   b) Introduce the identifier of the corresponding user. If it is an impostors choose randomly the identifier of a genuine user
   c) Present his/her biometric reference to the sensor
   d) Wait while biometric system matches the sample with the corresponding template
   e) Record verification results, ambient factors of scenario and any other result that may be relevant to carry out the complete analysis
   f) Wait until scenario conditions are recovered after the user interaction
9. Obtain performance rates and all statistics specified in the evaluation



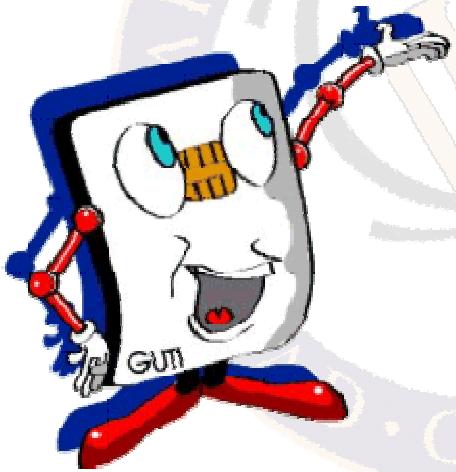
Conclusions

- This methodology has been tested with different sensors of several modalities
  - Unfortunately results are confidential
- Results obtained have proved its viability for carrying on independent, traceable and repeatable test

- A general methodology to perform independent tests of biometric systems has been defined. These tests analyse the influence of environmental conditions into the security level achieved
- Such methodology has been specified based on CC and its Common Evaluation Methodology (CEM)
- The overall test plan have been detailed following ATE_IND work units for performance testing into the operational range of the TOE
- How to analyze vulnerabilities related to extreme ambient conditions and how to carry out penetration tests have been explained



THANK YOU
FOR YOUR ATTENTION



Belen Fernandez-Saavedra,
R. Sanchez-Reillo, R. Alonso-Moreno

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