OPERATIONAL AND SECURITY EVALUATION OF AUTHENTICATION SYSTEMS IN CRITICAL INFRASTRUCTURES

Belen Fernandez-Saavedra, Inmaculada Tomeo-Reyes, Francisco J. Diez-Jimeno*, **Raul Sanchez-Reillo***

IDTestingLab
Carlos III University of Madrid
Avda. Gregorio Peces Barba, 1; 28918, Leganes
(Madrid), Spain
e-mail: {mbfernan, itomeo}@ing.uc3m.es

*University Group for ID Technologies
Carlos III University of Madrid
Avda. de la Universidad, 30; 28911, Leganes
(Madrid), Spain
e-mail: {fjdiez, rsreillo}@ing.uc3m.es

Keywords: Access Control, Crisis Scenarios, Environmental conditions, Robustness and Security Evaluation

Abstract. *Security of Critical Infrastructures is of paramount importance given the potential consequences of a crisis situation on them. Among all security aspects, access control to certain CI facilities is essential. One of the potential technologies to be used for guaranteeing access restrictions to these facilities are biometric-based solutions. Biometrics avoids the problem of passwords, cards or tokens, which can be easily copied, exchanged or stolen. In the case of biometrics, the identification/authentication process is based on probabilistic functions, and both the environment and user can influence the system performance. Being this the situation, the need of identifying the specific CI access requirements and evaluating the systems performance under critical situations, as those provoked by direct attacks or any other trial to breach the CI security, is clear. It has been demonstrated that recognition systems performance diminishes when identifying/authenticating users in non-controlled environments (e.g. scenarios under non-controlled adverse conditions after an attack), increasing the risk of two unacceptable situations: granting access to CI facilities to non-authorized users or impostors, or denying access to authorized users. In both cases, the security of both the infrastructures and/or the systems they support is compromised. Avoiding this kind of situations is fundamental to mitigate further consequences in case a critical situation that affects a CI occurs. There is a need to develop an appropriate methodology to evaluate the degree of vulnerability of Critical Infrastructures and assessment of potential pre-emptive solutions for threats mitigation. Focusing these needs in access control, this work analyses the CI scenarios in which an authentication system is needed and describes the environmental factors that can affect the authentication system performance in a crisis situation, considering the previous scenarios and different biometric modalities. Besides, a methodology to evaluate the influence of such factors on authentication systems performance is established specifying testing requirements, protocols and procedures.*

1 INTRODUCTION

Since human societies live in modern cities, several and very diverse infrastructures have become essential, as they provide basic services as electricity, water, gas, oil, telecommunication, transportation, public health, etc. These infrastructures are the so-called critical infrastructures (CI). Due to the nature of these infrastructures, it is necessary to protect them against any damage in order to avoid the disruption of their operation. Such damage can be deliberate (e.g. sabotage or terrorist attacks) or fortuitous (e.g. a natural catastrophe). All CI have specific buildings, stations, control rooms or other kind of installations where key systems to warranty a proper service of the corresponding infrastructure are located. Such places shall be provided with strict security measures to assure that non-authorized personnel cannot gain access to them.

Biometrics is a security technology used to automatically recognize individuals. Biometric systems can successfully identify people by means of physical or behavioural characteristics which are unique and intrinsic to human beings. This property has several advantages in comparison to other technologies based on elements that can be forgotten, lost, exchanged or stolen such as passwords, cards or ID tokens. Considering these properties, biometric-based authentication systems are an appropriate solution for controlling the access of individuals to CI restricted areas. However, biometrics has also a disadvantage that cannot be overlooked. The nature of the recognition process is probabilistic and it has been demonstrated that several contour conditions such as environmental conditions[1][2], user interaction with the capture device[3][4], biometric characteristic distinctiveness[5] [6], etc., negatively influence biometric performance. In case of CI, one of the most worrying effects is the environment. For example, the effect of user interaction can be mitigated with a suitable training of users [7] and biometric characteristics distinctiveness can be reduced selecting the most proper biometric modality and adjusting the recognition algorithm and/or matching thresholds. However, the environment is a factor always present which may be very variable depending on where CI and biometric authentication systems are located. Being this the situation, biometric authentication systems shall be assessed to check not only if a specific security level is achieved, but also if this security level is kept under any environmental condition or in a crisis situation.

At this time, International Standards exist that cover evaluation methodologies for testing and reporting biometric systems performance and the environment influence on them. The former are the group of standards ISO/IEC 19795. Among them, the most important are ISO/IEC 19795 Part 1[8] and Part 2[9], which were approved in 2006 and 2007 respectively. The latter is the standard ISO/IEC 29197[10] which is currently under development, although its technical content is already defined. A proof of that are the works[11] [12] performed following this methodology to contribute to such development. It is important to mention that this methodology is generic for covering any kind of biometric system and application.

In this paper, authors describe an evaluation methodology for environmental testing of biometric systems performance, which is based on the abovementioned standards. In particular, CI scenarios are specified. This specification includes characteristic environmental conditions in which CI can be involved, especially extreme climatic conditions and other conditions provoked by critical situations such as explosions or natural disasters. In addition, particular considerations are described for requirements and testing protocols considering CI applications, and more specifically, for the defined scenarios. Finally, conclusions and future work lines are stated.

2 ENVIRONMENTAL TESTING BIOMETRIC PERFORMANCE EVALUATION

An environmental testing of biometric systems performance is a biometric performance evaluation in which authentication attempts are carried out under different environmental conditions. The objective is to obtain performance results per each group of environmental conditions in order to determine if performance has suffered significant variations. In order to do these comparisons, it is necessary to carry out evaluations according to a set of rules and procedures. These have to be based on the exiting standards as it was mentioned in the Introduction.

ISO/IEC 19795-1[8] classifies biometric performance evaluations in three types: technology, scenario and operational evaluation. However, not all of them are suitable to quantify the influence of environmental parameters. Technology evaluations are evaluations that only assess recognition algorithms using databases whereas scenario and operational evaluations assess the overall system using live subjects. The difference between them consists of the fact that scenario evaluations are performed in a modelled environment (simulating the target application in laboratories) where all variables are controlled, whereas operational evaluations are performed in a real environment where controlling most of the variables is not possible. As a consequence, the environmental methodology specified in ISO/IEC 29197[10] standard establishes requirements for scenario and operational biometric performance evaluations. Technology evaluations are out of the scope of this standard, because the effects of environmental conditions in the capture process are not examined.

When the target application is a CI, in which security is an imperative, both kinds of evaluations can be significant. Scenario evaluations are usually carried out in the first steps of the product design and implementation in order to check different solutions and select the most suitable biometric authentication system. However, operational evaluations are also important to test the final solution with the target population and to adjust or configure it. Nevertheless, biometric performance evaluations entail considerable time and cost effort so, in many cases, executing both types of evaluations is not feasible. In the same way, a CI can be allocated in many locations and it will be impossible to carry out an operational evaluation in all these places. For this reason, and because a desirable evaluation shall be traceable and reproducible, this work has been focused in scenario evaluations.

It is important to emphasize that the environmental testing of biometric systems performance analyzes biometric systems as a whole. This evaluation does not carry out an environmental testing of hardware parts because this is already covered by other standards such as MIL-STD-810[13], the series IEC 60068[14], etc.

3 ENVIRONMENTAL CONDITIONS OF CI AUTHENTICATION SCENARIOS

The most important part of an environmental testing of biometric performance is the selection of environmental conditions to assess. These conditions must be in accordance with the environment of CI places or rooms where biometric authentication systems are needed, as well as their corresponding circumstances. Each location is affected by several conditions and depending on factors such as climate, season, hour of day, etc., their value can vary considerably. This fact entails that a significant amount of scenarios have to be evaluated, but, as explained in Section 2, this is not feasible. Nevertheless, not all conditions affect biometric systems performance in the same manner. Its influence depends on the biometric modality, the type of biometric capture sensor, as well as the values of the different environmental parameters. Thus, the number of environmental conditions can be reduced to those that noticeably affect these systems. These are the following:

- Temperature and humidity. These factors affect not only the biometric sensor operation, but also the biometric characteristic. Together, they can cause that the quality of the biometric sample gets worse and the overall biometric performance decreases. It is important to note that these factors are essential for biometric systems in which modalities are based on physical characteristics[15].
- Illumination. This factor influences biometric modalities whose samples are images and the capture sensor is a camera, such as fingerprint, vascular, iris, face recognition, etc. Depending on the type of light and its intensity, it is possible that the biometric sample cannot be acquired[1][16].
- Visibility. In the same way as illumination, the quality of air is very important to obtain a good image. Due to variables such as air pollution (smoke) or high humidity (fog), such quality might be reduced. There are not previous studies about this factor as such, but it has to be considered because it is very probable in outdoor environments or when fires or explosions occur.
- Noise. This is a factor that directly affects voice recognition modality[15]. However, many biometric systems (regardless of the modality) are provided with audio instructions during the recognition process. These guides are denominated "feedback" and are very helpful to achieve better performance results[17].

This section describes the most relevant CI scenarios in which biometric authentication systems must operate, considering the abovementioned environmental parameters for standard conditions, extreme conditions and crisis situation conditions. Nevertheless, if it were necessary to analyze the biometric performance considering other scenarios or environmental parameters (i.e. atmospheric pressure, dust, vibration, etc.), evaluators only had to specify such parameters as well as their corresponding measuring points, and performed evaluations applying the same requirements, protocols and procedures determined in the next sections.

3.1 Standard conditions scenario

This scenario is the typical indoor scenario. The corresponding environmental parameter values are shown in Table 1. These values have been specified according to the standard conditions recommended in ISO/IEC 29197 Annex A[10]. In fact, such standard scenario is based on standard scenarios or values specified in other standards related to testing methodologies and/or ergonomic and comfort guidelines such as MIL-STD-810G[13], IEC 60068[14], DEF STAN 00-35 Part 3 Issue 4[18], Office Ergonomic Guidelines[19], CEN EN 12464-1[20].

Environmental Parameter	Values
Temperature	20 to 26 ºC
Humidity	40 to 60 %
Illumination	300 to 1500 lux (Fluorescent light)
Visibility	Clear air
Noise	< 60 dB

Table 1. Environmental parameter values of standard conditions scenarios.

3.2 Extreme conditions scenarios

These scenarios are usually outdoor scenarios. Table 2 shows the potential parameter values. These values have been specified considering extreme values of each environmental condition, as well as values that human beings can bear. In the case of visibility, no high extreme value has been specified because a high visibility is the ideal situation. It is important to note that certain circumstances must be considered when selecting scenarios to evaluate. Temperature and humidity are dependent and climatic chambers cannot generate all combinations of values. Besides, the perception of temperature by human beings depends on air humidity, so test subjects cannot feel comfortable under particular combinations (e.g. people feel warmer when the relative humidity is high rather than low).

Environmental Parameter	Values	
	Low	**High**
Temperature	- 20 to 0 ºC	40 to 50 ºC
Humidity	1 to 39 (% RH)	41 to 99 (% RH)
Illumination	Darkness	Sunlight. Infrared light. Incandescent light.
Visibility	Non - visibility (< 100 m) Fog (< 1 km)	-----
Noise	55 to 60 dB	60 to 120 dB

Table 2. Environmental parameter values of extreme conditions scenarios.

3.3 Crisis situation scenarios

A crisis situation must be understood as the existing conditions after an explosion, a natural catastrophe or any other crisis situation. Typically, this environment is characterized by the existence of fires, the breakage of pipelines and the interruption of power, among others. According to these circumstances, as well as human beings safety and endurance, Table 3 shows the environmental parameters values for this scenario.

Environmental Parameter	Values
Temperature	50 to 55 ºC
Humidity	> 95 %
Illumination	Sunlight (daylight) or Darkness (nigh)
Visibility	Smoke (< 5 m)
Noise	100 to 120 dB

Table 3. Environmental parameter values of crisis situation scenarios.

4 TESTING REQUIREMENTS AND PROTOCOLS

An environmental testing evaluation of biometric performance is a complex process. Firstly, it entails to perform a biometric performance evaluation. This evaluation consists of two phases: enrolment and verification. During the enrolment, test subjects are enrolled in the system, whereas during the verification, test subjects carry out authentication attempts. These attempts are of two types: genuine attempts in which the test subject's characteristic is compared with his own template, and impostor attempts in which the test subject's characteristic is compared with other user´s template. For environmental testing evaluation, the verification phase has to be repeated per each scenario selected to be analyzed. In both phases, results provided by the biometric system are recorded. After that, performance metrics must be obtained from results of different scenarios and later compared to observe any variation.

This section describes testing requirements and protocols for carrying out each and every one of the procedures to execute biometric performance evaluations in the scenarios specified in Section 3. All of them are in accordance to ISO/IEC 29197 standard as well as the CI users' characteristics. This description has been divided in three parts: requirements to select scenarios to analyze, requirements and protocols to generate and control environmental conditions and requirements and protocols to carry out a scenario evaluation of biometric performance.

4.1 Requirements to select environmental conditions

The most significant environmental conditions of CI authentication scenarios have been specified in Section 3. Nevertheless, to evaluate such conditions, they shall be defined according to ISO/IEC 29197 requirements. In general, this standard addresses to specify two types of scenarios:

- Enrolment scenario. It is the environment in which test subjects shall be enrolled. This process can be conducted in a specific facility, different from the place where authentication attempts will be executed. Thus, the environment shall be selected with similar environmental conditions to the enrolment location. If there is not any specification for these conditions, authors recommend using the values of the standard scenario.

- Verification scenarios. These are the scenarios in which test subjects shall execute their authentication attempts. ISO/IEC 29197 considers also two types of scenarios:
  - A reference scenario. This scenario shall be analyzed in order to obtain a baseline performance. This result is basic to make comparisons and quantify the effects of any environmental parameter.

    In some cases, the establishment of the baseline performance requires the evaluation of two reference scenarios: Baseline 1 and Baseline 2. This happens when the test equipments that are needed for the rest of scenarios may modify the user's behaviour during their interactions and, as a consequence, modify the biometric performance. In such case, the calculation of the baseline shall measure this possible effect. Both scenarios shall have the same environmental parameter values, but not similar scenario configuration. The layout of Baseline 1 must include only the biometric system, whereas the layout of Baseline 2 must include the biometric system in addition to any test equipment essential to generate, control and/or measure the environmental conditions.
  - Evaluation scenarios. These are the target scenarios to analyze. One evaluation scenario shall be specified per each specific environment or environmental parameter to analyze. ISO/IEC 29197 standard establishes that parts involved in the evaluation are those who have to decide them.

In relation to those scenarios, the standard refers to them as evaluation conditions. In addition, it establishes that every evaluation condition shall be defined by means of the specification of two elements:

- The environmental conditions to analyze. These are the environmental conditions of which influence is going to be studied. Such conditions will be established to a specific value denominated measuring point. Environmental conditions have to be maintained at such value during the time the corresponding process (enrolment or verification) takes. It is mandatory to specify one condition at least to conform to the standard.
- The environmental conditions to control. These conditions are environmental parameters that might influence biometric performance and which have been decided to be controlled; however, they are not the target of the trial. Nevertheless, the standard does not oblige to specify any. In case that more than one condition want to be controlled, a value or range shall be defined for each of them. ISO/IEC 29197 states that these values or ranges have to be similar to the values of the reference scenario, when the evaluation scenario does not correspond to any specific environment, or in other words, when environmental parameters want to be examined separately. In the same manner to the environmental conditions to analyse, these values must be maintained at such value or inside that range during the time the corresponding process takes.

Applying these requirements and the CI authentication scenarios specified in Section 2, the evaluation scenarios to test regarding CI are show in Table 4. For this table, authors have considered that the enrolment scenario does not have specific values, and environmental parameters are assessed separately.

Process		**Values of environmental conditions to assess**	**Values of environmental conditions to control**
Enrolment		Standard conditions scenario (Table 1)	
Verification	Reference scenario	Standard conditions scenario (Table 1)	
	Evaluation scenarios	Extreme conditions scenario (Table 2)	Standard conditions scenario (Table 1)
		Critical situation scenario (Table 3)	Standard conditions scenario (Table 1)

Table 4. CI evaluation scenarios.

Regarding the specific environmental parameters to assess and control, as well as the number of measuring points, authors recommend that their selection is commensurate with the level of assurance to achieve and with the relevance of the protected assets. Nevertheless, as minimum, such evaluation conditions should include the environmental parameters for which a possible influence on the biometric modality and/or the type of capture sensor, have been demonstrated. ISO/IEC TR 19795-3[15] Technical Report contains detailed tables in which these factors are enumerated per biometric modality. Regarding the measuring points, authors suggest to analyze, at least, those specified in Table 3 for a crisis situation.

4.2 Requirements and protocols to generate, control and measure environmental conditions

Biometric performance scenario evaluations are executed in a modelled environment, so an environment which meets the evaluation conditions to analyze in each moment, shall be established. This environment must be kept while test subjects interact with the biometric system. Moreover, it is essential to record the results of the biometric interactions together with the measurement of the environmental conditions to analyze. All these tasks require suitable equipments to generate, control and measure the environmental parameters, as well as the proper protocols to assure that these tasks are correctly developed.

ISO/IEC 29197 does not specify the use of any particular equipment. Besides, it addresses that equipments can be different or be integrated in the same device. However, it states that equipment to generate, control and measure the environmental conditions must fulfil the following requirements:

- Equipments shall be able to achieve the maximum and minimum value of the conditions to assess.
- Their resolution shall be appropriate in order to adjust the value of the different conditions.
- They have to be calibrated.

Regarding the protocols for the establishment of evaluation conditions, this standard specifies that these conditions are met when the environmental parameters have reached their measuring point values as well as when these values are stable. Evaluators have to define the criteria to determine this stable stage, because the stabilization time will depend on the environmental parameters, the area to cover and the equipments used. It is important to emphasize that the evaluation environment area shall cover enough space in order to allow the test subjects interact with the biometric system without modifying their behaviour.

Besides, evaluators have to take into account that when test subjects interact with the biometric system, the environmental conditions can be sensitively modified. Thus, the standard also addresses that in case the evaluation conditions are different from the specified value or out the specified range, evaluators shall wait until the measuring point conditions are reached and are stable again.

All these specifications do not need to define extra considerations in case of CI, but authors suggest to introduce the biometric system in the evaluation environment before the generation of the evaluation conditions. In addition, these conditions will be generated gradually, especially in the case of extreme temperature and humidity measuring points, in order to avoid causing any damage to the biometric system.

4.3 Requirements and protocols for a scenario biometric performance evaluation

Apart from the environmental specifications, the environmental testing of biometric performance entails the definition of requirements and protocols for planning, executing and reporting a biometric performance evaluation. Regarding these requirements, ISO/IEC 29197 conforms to ISO/IEC 19795 Part 1 and Part 2. Specifically, for biometric scenario evaluations, these standards address requirements for environment, test subjects characteristics and their interactions, as well as performance metrics to obtain. All of them and the specific details for CI are described below.

4.3.1 Environment

The evaluation environment includes two factors: the evaluation conditions and the physical layout. The evaluation conditions have been already described in Sections 2 and 3. The physical layout shall be similar to the target localization in the real environment. In the case of CI buildings or stations, this location could be a wall, a door handle, etc., whereas in the case of CI systems, it could be a PC.

4.3.2 Test crew

In relation to this aspect, ISO/IEC 29197 establishes that test subjects shall be representative of the target user population considering characteristics such as age, gender, ethnic origin and occupation. In addition, the number of test subjects to participate in the evaluation process shall be enough to achieve statistically significant results.

When the target application is a CI, there is not any extra consideration about the number of test subjects. This number shall be calculated to achieve a significant number of comparisons, i.e. considering factors such as the expected error rates, number of visits, number of transactions and number of attempts per transaction in a similar way to other biometric applications. However, CI users have specific characteristics. Therefore, test subjects have to satisfy the following characteristics:

- Age. CI users are typically working people, so test subjects have to be between 18 and 65 years old.
- Gender. This aspect must be well-balanced between men and women according to CI employees.

- Ethnic origin. Usually, CI users are citizens of the own country. Thus, test subjects must have similar ethnic origin than those of the country where the biometric authentication system is going to operate. If there is more than one race, test subjects shall be proportionally chosen to the number of workers of each race.
- Occupation. Regarding occupation, CI users can be people with different level of studies such as engineers, technician experts, maintenance staff or cleaning staff. Therefore, test subjects selected to participate in the evaluation must have different occupations and different level of studies.

Furthermore, the standards state the requirements for test instructions, training, guidance and feedback to provide to test subjects. Basically, these requirements address that they shall be similar to the target application. CI staff is typically people who know facilities and systems so, in case the biometric authentication systems are used to protect a CI, users also know how to interact with them. As a consequence, test subjects shall be trained and guided for the evaluation process. Besides, the feedback shall be the same as the one the biometric system usually has.

4.3.3 Level of effort and decision policies

This part of the standard defines constraints for the enrolment and verification processes. ISO/IEC 29197 states that the number of transactions, the number of attempts per transaction and the time limit per each interaction shall be commensurate with the target application. Nevertheless, if there is not any specification, authors recommend to consider the standard ISO/IEC 19795-5[21]. This standard specifies a biometric performance scenario evaluation for access control systems. For this kind of evaluation, it establishes that test subjects shall perform two visits. In the first visit, test subjects have to be enrolled and execute five genuine transactions. They have three enrolment transactions to get a successful enrolment. Both enrolment and verification transactions are composed of three attempts. In the second visit, they have to execute five genuine transactions and fifteen impostor transactions. Each transaction is also composed of three attempts. There are not any constraints for transactions time. However, the first visit shall be at least one week separated from the second visit, and no more than three months. In addition, the second visit shall be carried out between the fourth and eighth week after the first visit. Besides, all attempts must be executed with the disengagement from the device.

4.3.4 Test order and execution sequence

The evaluation process must follow a proper order, specially the evaluation scenarios testing. ISO/IEC 29197 specifies protocols for both test order and execution sequence. Those protocols do not need to be modified in the case of CI applications. Regarding the order for analysing the different evaluation conditions, the standard states that this order shall be defined considering the test subjects habituation and order effects (e.g. tiredness), as well as other aspects such as availability of test equipments, availability of test subjects, number of evaluation conditions to analyse, time to modify evaluation conditions and time to achieve the specific measuring points. Moreover, the reference evaluation conditions (Baseline 1 and Baseline 2) have to be included in the evaluation conditions sequence as the rest of evaluation conditions. On the other hand, the standard addresses the complete execution sequence. It is explained as follows.

- Pre-test activities:
    - Design the testing plan
    - Develop the visit schedule, legal forms as well as the guides and instructions for test subjects
    - Implement the evaluation software to collect the essential data
    - Instruct test operators and calibrate test equipments.
    - Recruit test subjects
- Test activities:
    - First visit:
        1. Explain test instructions and train test subjects
        2. Establish evaluation conditions for enrolment
        3. Enrol test subjects
        4. Establish the first evaluation conditions for verification
        5. Perform genuine and impostor verification transactions
        6. Change the evaluation conditions and carry out steps 4 to 6 till test subjects have been verified in all evaluation conditions
    - Second or subsequent visits:
        1. Remind test subjects the test instructions
        2. Establish the first evaluation conditions for verification
        3. Perform genuine and impostor verification transactions

4. Change the evaluation conditions and carry out steps 2 to 4 till test subjects have been verified in all evaluation conditions

- Post-test activities:
  - Analyze all data collected during the evaluation
  - Calculate performance metrics
  - Generate reports
  - Take the complete evaluation down

4.3.5 Error protocols

In this kind of evaluations, several number of errors can happen that can influence results. ISO/IEC 29197 distinguishes three types of typical errors and provides a solution for them. These are general errors, environmental anomalies and enrolment or verification errors. In general, if an error occurs, evaluators must stop the evaluation, solve the problem and check that there are not errors in the recorded data. Then, the evaluation must continue. Besides this kind of errors, authors recommend the evaluators to revise the entire evaluation process and develop an exhaustive list of errors including the precise tasks to carry out in case that some of them occurs.

4.3.6 Data to record and test results

A biometric performance evaluation mainly measures two types of performance metrics: error rates and times. Error rates quantify the probability that users cannot be enrolled (Failure to enrol), the probability that the biometric system cannot correctly acquire the biometric sample (Failure to acquire), the probability that a genuine user is rejected (Failure non-match rate) and the probability that an impostor is accepted (Failure to Match). Usually, False Non-Match Rate (FNMR) and False Match Rate (FMR) are plotted together in curves denominated Receiver Operating Characteristic curve (ROC) or Detection Error Trade-off curve (DET). Times quantify basically the time that takes to enrol users (enrolment time) and the time that takes to verify users (verification time).

ISO/IEC 29197 states that the necessary data to obtain these performance metrics have to be recorded. In addition, the performance rates per each environmental parameter and the particular measuring point shall be calculated and reported. Furthermore, a comparison between reference results (Baseline 1 and Baseline 2) and the analyzed evaluation conditions must be performed. Authors consider that the best way to report these results is by means of a ROC and/or DET graph. Each kind of evaluation conditions has to be depicted at a curve, so that differences among them can be observed.

5 CONCLUSIONS

Biometric-based authentication systems are an excellent solution for CI access control in order to protect either key facilities or systems. However, it is essential to evaluate its performance because this technology is based on probabilistic functions that can be influenced by factors such as environmental conditions. Specifically, this is the case of CI, as these structures can be located in places subjected to extreme conditions, or may have to endure crisis situations caused, for example, by explosions or natural disasters.

Bearing this problem in mind, authors have specified in this work an environmental testing evaluation methodology to analyze biometric systems performance considering CI applications and their particular environmental conditions. This evaluation has been based on standards already developed as well as in biometric performance scenario evaluations. In particular, both environmental parameters and specific values to assess have been defined. Furthermore, the evaluation requirements and protocols have been described for such environmental parameters and the specific characteristics of CI users and target applications.

Nevertheless, there are other factors that can affect the security provided by biometric systems such as usability factors or spoofing techniques. Authors will continue working in this area in order to specify similar evaluation methodologies that are able to quantify the effects of such factors and/or identify potential vulnerabilities of these systems.

REFERENCES

[1] R. Sanchez-Reillo, B. Fernandez-Saavedra, J. Liu-Jimenez and Y. B. Kwon, *Changes to vascular biometric system security & performance.* Aerospace and Electronic Systems Magazine, IEEE, 2009. 24(6): p. 4-14.

[2] E. P. Kukula, S. J. Elliott, R. Waupotitsch and B. Pesenti. *Effects of illumination changes on the performance of Geometrix FaceVision 3D FRS*. in *Security Technology, 2004. 38th Annual 2004 International Carnahan Conference on*. 2004.

[3] The National Institute of Standards and Tecnology (NIST). *Biometrics and Usability; Efficiency, Effectiveness and User Satisfaction*. 2006; Available from: http://zing.ncsl.nist.gov/biousa/.

[4] B. Fernandez-Saavedra, R. Alonso-Moreno, J. Uriarte-Antonio and R. Sanchez-Reillo, *Evaluation methodology for analyzing usability factors in biometrics.* Aerospace and Electronic Systems Magazine, IEEE, 2010. 25(8): p. 20-31.

[5] G. Doddington, W. Liggett, A. Martin, M. Pizybocki, and D. Reynolds. *Sheep, Goats, Lambs and Wolves: A Statistical Analysis of Speaker Performance in the NIST 1998 Speaker Recognition Evaluation*. in *Int'l Conf. Spoken Language Processing (ICSLP)*. 1998. Sydney.

[6] N.Yager and T. Dunstone. *Worms, chameleons, phantoms and doves: New additions to the biometric menagerie," Automatic Identification Advanced Technologies*. in *IEEE Workshop on Automatic Identification Advanced Technologies*. 2007.

[7] Elliott, Stephen J., Kukula and Eric P., *A Definitional Framework for the Human-Biometric Sensor Interaction Model*. Vol. 7667. 2010, Bellingham, WA, ETATS-UNIS: Society of Photo-Optical Instrumentation Engineers. 1 vol.

[8] International Organization for Standardization, *ISO/IEC 19795-1: - Information technology -- Biometric performance testing and reporting -- Part 1: Principles and framework.* 2006.

[9] International Organization for Standardization, *ISO/IEC 19795-2: - Information technology -- Biometric performance testing and reporting -- Part 2: Testing methodologies for technology and scenario evaluation.* 2007.

[10] International Organization for Standardization, *ISO/IEC 3WD 29197: - Information technology -- Evaluation methodology for environmental influence in biometric systems.* 2011.

[11] Belen Fernandez-Saavedra, Raul Sanchez-Reillo, Raul Alonso-Moreno and Oscar Miguel-Hurtado. *Environmental Testing Methodology in Biometrics*. in *International Biometric Performance Testing Conference (ICBP 2010)*. 2010: National Institute of Standards and Technology (NIST).

[12] B. Fernandez-Saavedra, F. J. Diez-Jimeno, R. Sanchez-Reillo and R. Lazarick. *Establishment of baseline performance for "end to end" biometric system evaluations*. in *Security Technology (ICCST), 2010 IEEE International Carnahan Conference on*. 2010.

[13] United States Military Standards, *Department of Defense: Test Method Standard for Environmental Engineering Considerations and Laboratory Test.* 2008.

[14] International Electrotechnical Commission (IEC), *IEC 60068: Environmental Testing.* . 1988.

[15] International Organization for Standardization, *ISO/IEC TR 19795-3: - Information technology -- Biometric performance testing and reporting -- Part 3: Modality-specific testing.* 2007.

[16] Ted Dunstone and Yager Neil, *Biometric Systems and Data Analysis. Design, Evaluation, and Data Mining*. 2009: Springer.

[17] Ross Micheals Mary Theofanos, Jean Scholtz, Emile Morse, Peter May, *Does Habituation Affect Fingerprint Quality?* 2006.

[18] Ministry of Defence; Defence Standard 00-35 Issue 4, *Environmental Handbook for Defence Material - Part 3: Environmental Test Methods* 2006.

[19] The University of Sydney, *General Office Environment.* 2010.

[20] CEN: European Committee for Standardization, *CEN EN 12464-1: Ligh and lighting - Lighting of work places - Part 1 : Indoor work places.* 2011.

[21] International Organization for Standardization, *ISO/IEC 19795-5: - Information technology -- Biometric performance testing and reporting -- Part 5: Access control scenario and grading scheme.* 2011.