Technical and Non-Technical Problems in Biometric Physical Access Control Systems

Ing. Mario Savastano
Institute of Biostructure and Bioimages, National Research Council of Italy
c/o DIEL, Federico II University of Napoli
Via Claudio 21
80125, Napoli
ITALY

E.mail: mario.savastano@unina.it

Dr. Luisa Riccardi
Ministero della Difesa, Segretariato Generale VI Reparto
Via Stresa 31b
00135, Roma
ITALY

E.mail: r6statistica@sgd.difesa.it

ABSTRACT

The increase in security measures due to the complex international situation is forcing the realization of physical access control systems equipped with biometric identifiers. The identification based on physical or behavioural characteristics represents one of the most sophisticated ways to protect buildings or sensible sites but, unfortunately, at the same time, requires the resolution of many different problems. While the technical difficulties may be considered "internationally transversal", and therefore reasonably "known" into the scientific community, non-technical issues may differ from country to country, thus involving often the lack of reference cases. Aspects such as labour legislation or privacy protection reflect national guidelines and may result in significant constraints on the implementation of biometrics. The present document highlights some of the constraints and problems encountered in the project of a biometric access control system for a large compound of the Italian Ministry of the Defence (MoD), attended by a reasonably high number of employees and characterized by a strong personnel degree of dishomogeneity. In addition, the present contribution intends to highlight the role played by societal and psychological issues in the implementation of a biometric project.

1.0 INTRODUCTION

Access control issues are important because improving the effectiveness and efficiency of Army operations depends on fast and accurate identification of authorized users [Woodward 2001]. Access control may be effective both at a logical (access to computer systems or identity verification for claiming social benefits) and a physical level (access to building or compounds) and, with particular reference to this application, several Italian Government Agencies intend to realize, in the near future, access control systems equipped with biometric identifiers. The biometric approach offers a significant increase in the overall security as it allows the creation of a strong association between the holder of an access card and the subject who has the legal title to own it. Furthermore, biometrics offer a convenience and efficiency that other identifiers, which must be remembered or presented, do not.

Savastano, M.; Riccardi, L. (2005) Technical and Non-Technical Problems in Biometric Physical Access Control Systems. In *Enhancing Information Systems Security through Biometrics* (pp. 2-1 – 2-6). Meeting Proceedings RTO-MP-IST-044, Paper 2. Neuilly-sur-Seine, France: RTO. Available from: http://www.rto.nato.int/abstracts.asp.

Due to all the advantages offered, since several years, the MoD, has promoted studies and research in biometrics, trying to reach the double aim of enhancing the security of physical access to sensible compounds and, at the same time, improving the time and attendance systems for employees.

The interest in biometrics has been consolidated by the decision of introducing the templates of two fingerprints into a 32k smart-card for military and civilian personnel, the so called "Carta Multiservizi della Difesa" (CMD – Multi-services Defence Card) which will be later on described and whose distribution end is foreseen within 2005.

One of the large scale biometric projects promoted by the MoD, has consisted in the realization of a new physical access control for a large compound in Rome. The completion of the project, actually in the phase of the final approval, is foreseen in the Q4 of 2005 and the present paper, focuses on some technical and non-technical problems and constraints which had to be considered by a Working Group created for the development of the project and constituted by personnel of the MoD with the collaboration of an external consultant.

As a preamble to the description of the various issues, it should be mentioned that some of the precautions taken, especially concerning social and privacy issues, reflect a national legislative framework which may differ from other international contexts. Furthermore, a particular attention was paid in order to avoid any kind of social conflict with the civilian employees. The precautions were taken because of the:

- innovative character of the project (first large scale project of MoD based on biometrics);
- numerical consistence of civilian personnel (about 40% of the overall compound's population); and
- labour legislation for civilians personnel.

With specific reference to the structure of this document, paragraph 2.0 describes the preliminary analysis which has preceded the design of the project. Paragraph 3.0 concentrates on the technical and non-technical constraints which have influenced the development of the project. Paragraph 4.0 discusses of some difficulties concerning smart-card and biometrics while, finally, paragraph 5.0 reports the conclusions.

2.0 PRELIMINARY ANALYSIS

Many experts maintain that it is important to remember the human factor when deploying and building a physical access biometric security solution [Shen 2003]. Organizations should consider the attitudes and perceptions of employees and personnel, when asking them to volunteer their personal biometric identities in exchange for access to resources and information. Unfortunately, the implementation of a biometric recognition for accessing a compound, sometimes is proposed by vendors or system integrators only as a natural extension of traditional physical access systems' capabilities. This wrongful "simplification" has often been one of the main causes of unsuccessful biometric projects.

In reality, a biometric physical access control system, especially if involves a large number of users, implies much more than solving an integration problem. Inconvenience is due not only to technical difficulties but also to aspects such as low user acceptability, privacy or trade unions requests; by now, it is widely recognized that a scarce consideration of these "non-technical" factors, generally difficult to approach, may easily lead to an unexpected and non-cooperative behaviour of the end-users which, generally, compromise the success of the biometric implementation.

Starting from these considerations, since its creation, the Working Group has attributed a strong importance to social aspects involved and has enlarged some of the meetings to representatives of the trade unions. The several meetings organized with all the parts implied in the project have contributed to clarify many technical aspects and have significantly influenced the project's specifications.

Another key factor in the achievement of a consensus among all the parts involved in the project have consisted in the involvement of representatives of personnel in some technical sessions concerning experimental tests. This approach has allowed many users to familiarize with the biometric equipments, often previously never seen or directly used, and to diffuse among the colleagues a message of transparency.

Another preliminary task of the working group has consisted in the analysis of the technical difficulties of the project and three factors have appeared to be particularly critical:

- dimension and complexity of the compound;
- number of end-users; and
- dishomogeneity of attendees' categories.

2.1 Dimension and Complexity of the Compound

The MoD project concerns a large building located in the center of Rome characterized by the typical architectural complexity of the old compounds. Since the requirements of the project were both the enhancement of security and the time and attendance control for employees, the project of the biometric access control has interested the whole location. The number of access points (about 35 barrier gates) has been determined in consequence of observations and simulations by taking into account the architectural and structural characteristics of the building.

2.2 Number of End-Users

The MoD site is attended by about 4000 people per day whose 60% is composed of military personnel, while the rest are civilians. This value has required to take in serious consideration the problem of false rejects and is influencing the selection of the biometric technique. In every case, an adequate number of special access gates manned by security personnel has been foreseen.

2.3 Dishomogeneity among Attendees

The main categories of personnel accessing the MoD compound are:

- MoD military personnel assigned to the site;
- MoD civilian personnel assigned to the site;
- MoD personnel (military and civilian) coming from other MoD sites;
- private contractors' workers (i.e. for cleaning and food services) with long time contracts;
- private contractors' occasional workers;
- MoD visitors; and
- other visitors.

The MoD project is based on the biometric authentication, at least, of the first four categories of attendees whose strong dishomogeneity as concerns labour legislations and social motivations, is evident. The Working Group has given particular relevance to the "personnel fragmentation factor" retaining that a different perception of the security issues or a hostility toward biometrics could lead to non-cooperative behaviour and to possible high rates of false rejections.

Also these considerations have played an important role, as described later on, in the choice of the biometric technique to be adopted.

3.0 OTHER TECHNICAL AND NON-TECHNICAL CONSTRAINTS

In a biometric project, involving thousands of end-users, technical and non-technical constraints often overlap. Some technical issues have anyway appeared fundamental.

3.1 Lighting Conditions

In the implementation of a biometric access control system, particular attention should be paid to the operating lighting conditions. Most biometric technologies are optically-based and, therefore, may perform poorly or not at all when used in direct sunlight [Blackburn and others 2003]. If it is not possible to shield the sensor from the direct sunlight, and/or if the lighting conditions change in a significant way during the day, some precautions must be taken in selecting the most appropriate biometric technique. Iris and face recognition, for example, are more indicated for indoor use and the MoD project is based on a high number of barrier gates located outdoor, protected from rain and direct sun exposure by only a plastic roof. These conditions have significantly reduced the selection among the biometric sensors since only fingerprints recognition and hand geometry were able to meet the environmental constraints of the application.

3.3 Trade Unions Relations

In several countries, Italy included, the trade unions may play a significant role in the realization of biometric access control system. As previously reported, trade unions have been invited to express their opinion on the project. The important issue emerged has consisted in the low acceptance of fingerprint recognition due to fear of possible misuses. Vice versa, trade unions have expressed a positive opinion on hand geometry technique, which, due to characteristics of the procedures, may operate only in "verification" mode .This issue, together with the decision of storing the template only on the smart-card (no biometric centralized database) has been considered by trade unions as fundamental elements for the acceptance of the project.

3.2 Privacy

In Italy, as in other countries, the use of biometrics has to respond, among others, to "proportionality" and "necessity" principles. If, in one hand, the "proportionality" constraint could be reasonably satisfied by the characteristics of the application (i.e. a protection of a military site), on the other hand, the "necessity" principle is not always easy to demonstrate. In other words, it should be proven that the biometric approach is the only way to reach the goal. Documentation addressing these instances is now in preparation and will be presented soon to the Personal Data Protection Commission.

3.4 User Acceptability

This aspect is often neglected, despite its primary importance to guarantee the success of a biometric application. As previously highlighted, for example, fingerprint recognition is sometimes perceived as too related to forensic investigation and some users may be not satisfied of it. In most cases user acceptability can be increased in some degree by education and information [Cherry 2003]. Unfortunately, in the MoD project, although the difference between storing the image or the template of the fingerprints was clearly explained, user acceptability for fingerprints continued to result particularly low.

3.4.1 Health and Safety

An emerging issue concerning the "user acceptability", in biometric applications, is represented by health and safety aspects. To date, there has been a generalized little consideration of the medical dimension, probably because of the lack of widespread appreciation of biometric methods among the population at

large. As applications using biometrics proliferate, more and more users could want reassurance about health and safety issues. In the MoD project, some concerns was expressed by some end-users about the possibility of infections because of contact with the sensors. A careful and patient evaluation of such concerns, together with an accurate explanation of the eventual countermeasures, has been necessary.

4.0 ACCESS CARDS AND BIOMETRICS

The selection of the card for accessing the site has represented another significant problem approached in the project. As previously mentioned, the MoD is issuing the CMD – Carta Multiservizi della Difesa (the necessity of using a card for the storage of personal and medical data of the MoD military personnel goes back to the first Italian Army peacekeeping operations). The CMD incorporates the templates of two fingerprints, intended for biometric authentications in more generic applications. Due to large number of different needs presented by diverse Departments of the MoD and to the willing of issuing one only card for the personnel, the possibility of allocating more biometric templates on the CMD is under investigation. Of course a particular attention has to be paid to biometrics using a dynamic update of the template since the process of re-writing it may be incompatible with the specifications of the card.

5.0 CONCLUSIONS

The use of biometrics for access control is the natural solution for improving the security level in physical access systems. Unfortunately, the practical implementation of biometrics give rise to a number of technical and non-technical problems which should be carefully examined before carrying out some delicate choices. The present paper has reported only a subset of the several problems encountered during the realization of the project. Independently anyway from the several technical difficulties, the aim of the paper is to highlight how important is a correct interaction with all the parts involved in a biometric project.

6.0 REFERENCES

[Shen 2003] M. Shen, “The ‘People’ Element In Biometrics And Physical Access Control” available at http://www.biometritech.com/features/shen041403.htm

[Woodward 2001] John D. Woodward, Jr., K.W. Webb, E.M. Newton, M. Bradley, D. Rubenson, “Army Biometric Applications: Identifying and Addressing Sociocultural Concerns”, available at http://www.rand.org/publications/MR/MR1237

[Blackbourne and others 2003], “2003 U.S. Government Biometrics Workshop: Overview and Summary”, available at http://www.ece.unh.edu/biometric/biomet/public_docs/workshop.pdf

[Cherry 2003] K. Cherry, “Biometrics: An In Depth Examination”, available at http://www.giac.org/practical/GSEC/Kyle_Cherry_GSEC.pdf