Biometric access control for athletic events

Christos K. Dimitriadis, Despina Polemi
University of Piraeus, 80 A. Dimitriou, 18534 Piraeus, Greece
{cricodc, dpolemi} @unipi.gr

Abstract. The confidence level of citizens, as far as the ability of the organizers to provide security is concerned, is a factor directly impacting their attendance in athletic events. This paper, proposes a system called BioAthletics that implements strong access control, enhancing the safety feeling of event spectators. BioAthletics integrates intelligent biometric access control systems and smart cards for authenticating participants. A pilot version of BioAthletics was deployed and tested in terms of acceptability, information security and performance.

1 Introduction

Modern biometric technologies provide enhanced security levels by introducing a new dimension in the authentication process called "proof by property". However, the design and deployment of a security architecture incorporating biometric technologies hides many pitfalls, which when underestimated can lead to major security weaknesses [1]. Although biometrics have been deployed in pilot systems for protecting access to athletic events in the past, no integrated solution has been proposed taking into account the related security standards and no complete studies ever proven the benefits of such deployments.

This paper, proposes a system called BioAthletics that implements strong access control, enhancing the safety feeling of event spectators. The system integrates intelligent biometric access control systems and smart cards. A pilot version of BioAthletics was deployed and tested in terms of acceptability, information security and performance, within the framework of a research project of the Greek Secretariat of Research and Technology. The authors would like to thank GSRT for funding part of this work.

2 Access control systems in stadiums

During the Athens 2004 Olympic Games, almost 70,000 security personnel was overseeing the event, with the help of technology. More than 1,100 poles topped with video cameras, speakers and microphones created a distributed net of surveillance posts aimed at locating disturbances quickly [2]. Barcode scanners and ID cards allowed athletes and trainers into the Olympic Village. In Sydney 2000 Olympic Games, a security system integrated with intelligent camera functions was deployed, in order to provide security, surveillance and access control [3]. The systems consisted of the combination of security, CCTV Switcher, Smart Card

Access Control and Photo Identification Systems and provided a total solution to monitor and report on all activities. Furthermore, in the Commonwealth 2002 Games in Manchester, a security system protected almost 6,000 athletes and officials representing 72 countries and territories [4]. The system involved the installation of a sophisticated CCTV system that included 79 cameras in the athletics stadium, which enabled Greater Manchester Police to zoom in on every single person in attendance. There were also installed an access control system with intruder alarms, fire alarms and an emergency telephone network in the main stadium. The Millennium Stadium also completed a £2.8 million project, to supply and install systems for crisis management such as fire detection, security and CCTV and PAVA (Public Address Voice Alarm), as well as a system for the distribution of radio, television, data and telephone signals [5].

Biometrics and smart card technology is widely used during athletic events of known stadiums inside the UK. Manchester City Football Stadium, Crystal Palace, England Rugby Supporters, Chelsea and Bolton Wanderers have come up with a high-tech way to profile their sport fans and accredited persons in an attempt to drive revenue, improve the game environment and provide the greater security in order to better control the flow of crowds from possible crisis situations around and in the stadiums. This was a centralized authentication solution, using personalized smart cards –in some cases the cards configured to include biometric data such as fingerprint- to provide secure and better service. Similar systems have been adopted by the Belgian Football and PSV Eindhoven Stadiums. In the Cricket World Cup (South Africa, 2003) bar coded tickets were deployed, using a two-dimensional barcode, which cannot be duplicated or forged [6]. The system handled 825.000 ticket sales. The bar code allowed for scanning and verification through a sophisticated venue access control system, which in turn generated a customer database holding valuable information on all ticket purchasers. In addition, all stadiums were monitored with CCTV, (eight cameras per event) and had full digital recording facilities.

The various systems that were implemented proved that technology consists of an integral part in the athletic events. Such systems fulfill the requirements of the organizers, but there are not always effective and efficient in large-scale athletic events, mainly because there is not an integrated system for addressing completely a crisis situation. In 2002 World cup in South Korea, all stadiums were monitored with CCTV cameras. A problem occurred with the metal detector checkpoints causing delays and many fans were unable to enter in time. It was recognized that such incidents wouldn't have occurred if an effective coordination centre was developed [7]. Athletic related crimes require more mature and tested systems for implementing secure access control.

3 Biometrics and smart cards

The biometric technology has been recognized as a key technology for improving security and trust in different fields of modern society [8]. Biometrics is defined as *the automatic use of human physiological or behavioral characteristics to determine*

or verify an identity [9]. The system conducts a measurement of the features of the user, encodes the data creating a *template* and compares it against a physical measurement from the user each time accessing the system is attempted. The most widespread biometric technology in today's markets is fingerprint recognition [10]. The sensor's size is conveniently small (area of a few square centimetres, thickness of a few millimetres), enabling easy incorporation into any fixed or mobile terminal and the weight of the sensor is negligible. Reusability on a wide scale is possible through the use of different encodings and undergoes continuous improvement as standardisation is gradually taking effect. Fingerprint recognition systems fit quite well as an integral part of any fixed or mobile terminal. For all the above reasons, fingerprint technologies have achieved the dominant position in the year 2005 in terms of total revenue, achieving approximately 48% of the total biometric market [10]. The biometric component of the system takes into account all relevant aspects including technological, societal and legal issues. More specifically security, performance, privacy, standardization, scalability, responsibility, interoperability, usability, acceptability and liability issues, were studied, targeting to the development of a biometric component that meets all necessary state-of-the-art specifications. This was accomplished by the exploitation of results of research projects, such as FP6-001766 (BIOSEC) "Biometrics and Security".

The smart cards that use contacts are in line with the guidelines determined in the Standard of ISO 7816 Part 1. The reliability of these smart cards has been improved constantly during the previous years, because of the increasing experience in the manufacturing of such cards. On the other hand, the contacts remain one of the more frequent sources of problems in electromagnetic systems. For example, some problems can result from the attrition of contact. Since the contacts, placed in the surface of card are connected immediately with the inputs of the integrated circuit that is incorporated in the card, there is a danger of damage or even destruction of the integrated circuit from the electromagnetic discharges - load of enough thousands of volts is not infrequent. These technical problems are overcome with the contactless (wireless, RFID) smart cards. Apart from its technical advantages, the wireless technology offers also to the issuer and the holder of the card some interesting new applications [11]. For example, the contactless cards do not need to be imported essentially in a card reader, since there are RFID reading systems that function in a distance of up to one meter. This is a big advantage in access control systems where a door or a circular gate should be opened, since the granting of access of an individual can be checked without the requirement of the card to be removed from the wallet or the pocket and to be inserted into the reader. An extensive range of applications for this technology is the public transportation systems, in which a big number of passengers should be identified in a very short time interval. In addition, the wireless technology is suitable in systems that require the deliberate import of the card into a reader, since it is not important how the contactless card will be inserted into the reader. This is in contrast to case of the magnetic or smart cards with contacts, that function only if they are inserted in a consistent way. This freedom of the orientation restrictions simplifies the operation and increases the user acceptance [12]. Apart from the simplicity of use, this solution is attractive because it considerably decreases the danger of vandalism (for example, with the placement of chewing gum or glue in the slot of the reader). Up to now, the wireless cards have

been mainly used for the public transportation systems, acting as electronic tickets. These systems currently employ single-use cards that are cheap to develop. Nevertheless, there is an increasing demand for the incorporation of additional features into the electronic ticket. For this reason, the employment multi-use RFID cards with incorporated microprocessors will be increased in the near future.

4 Architecture Description

The architecture of the proposed system is depicted in the following figure.

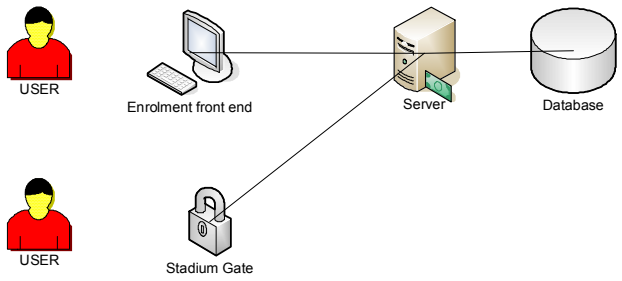

Fig. 1: System architecture

The system comprises of an enrolment front-end, an application server, a database (DB) and the equipment in the stadium gate, used for user verification. The following steps describe the user enrolment procedure.

1. The sports fan visits the stadium's desk with the ID documents, which are checked for duplicate registration.
2. Once his identity is verified, a smart card is issued to him and the card gets personalized.
3. The user enrolls in the biometric system and a biometric template is created.
4. The template is encrypted using a key known only to the proposed system. The template is stored encrypted in a tamper-resistant memory module of the smart card
5. The template is erased from any intermediate storage mediums.
6. A file of the user is created in the DB, including his ID number, name, smart card serial number etc (not the template).
7. The user receives his smart card and the PIN of the smart card.

For gaining access to the stadium, the user follows the procedure described below:

1. The sports fan visits the gate of the stadium.
2. The smart card is accessed by an RFID smartcard reader.
3. The user puts his finger on the sensor for the biometric measurement.
4. A template is generated by the measurement and compared to the pre-stored template (decrypted by the stadium's gate equipment)
5. If the comparison is positive, a request based on the serial number of the smart card is submitted to the DB server for downloading the privileges of the user.

6. If the decision is positive and the privileges permit entrance to the stadium, the user passes the gate after showing his ticket.

At this point we present a procedure for understanding the complete operation of the system, which is independent of the final decision of which approach (centralized or not) will be used.

1. The sports fan who causes trouble in the stadium must be arrested by the authorities.
2. His/her name and ID number are registered by the authorities
3. The authorities inform the organization responsible for the system to update the database and change a flag in the file of the user for not permitting entrance in future events (perhaps for a certain period of time).

5 Testing environment

A pilot version of BioAthletics was implemented in a stadium hosting athletic events, including basketball games, athletics and gymnastics. The main target of evaluation was system security, performance and acceptance.

6 Acceptance testing

For testing the acceptance and usability of the BioAthletics pilot system, an extended version of the Davis' Technology Acceptance Model was deployed [13]. TAM contains two dimensions: usefulness (divided into accomplishment and efficiency) and ease of use (divided into learnability, control and mental effort). The extension to the TAM was provided by Amberg et al. [14]. They introduced a Dynamic Acceptance Model for the Reevaluation of Technologies (DART) including dimensions of perceived ease of use, perceived usefulness, perceived network effects and perceived costs.

Based on DART, a survey regarding acceptance and usability of BioAthletics was conducted, focusing on the biometric access control system, taking into account possible privacy consideration of the users. A total of 110 participants, 45% female and 55% male filled the questionnaire, during a 2-month period. Their age varied between 18-65 years. Most participants were familiar with the use of automated systems. The aims of the study were to investigate participants' acceptance and general attitudes towards biometrics and more generally BioAthletics. The questionnaire was answered in three phases: before informing the user regarding the operation of BioAthletics, after informing the user and finally after the user was enrolled and tested the system in practice, during an athletic event.

During the first phase, the acceptance of biometrics was relatively high amongst the participants. The overall mean of the attitude was 3,24 measured in a five-point scale (1=negative, 2=quite negative, 3=neutral, 4=quite positive, 5=positive). Similarly, the acceptance of BioAthletics in total was high, with an overall mean of 4,01 measured in the same scale as above. During the second phase, the acceptance of biometrics was even higher amongst the participants. The overall mean of the

attitude was 4,14. Similarly, the acceptance of BioAthletics in total was high, with an overall mean of 4,68 measured in the same scale as above. The main reason for this increase in user acceptance, was that the users' privacy concerns, especially regarding the collection and use of biometric data were minimized, after being informed of the operation of the system and especially regarding the fact that the users carry within their smartcards their own biometric data in encoded and encrypted forms, while no storage takes place in any central database. During the last phase, the acceptance and usability of biometrics had an overall mean of 4,43, while the acceptance and usability of BioAthletics has a mean of 4,77 measured in the same scale as above. The participants recognized the benefits of the system and reported that it would increase their level of security while attending an athletic event, without compromising issues, such as usability and privacy.

7 Information Security and Privacy Assessment

Risk analysis was conducted, during the implementation of BioAthletics, for evaluating its security level, focusing on the use of biometrics and RFID smart cards, in relation to the users personal, biometric and medical data. For this purpose a specialized methodology and knowledgebase of vulnerabilities, risk and countermeasures for security and privacy was deployed [15]. The vulnerabilities addressed by BioAthletics are described below.

The utilization of the template in two or more applications with different security levels (i.e. convenience applications and security applications) tends to equalize these security levels, by decreasing the higher security level to the lower one - if a template is compromised in one application, it can be used for gaining access to the other. The biometric algorithm of BioAthletics is custom, producing unique biometric templates hence this vulnerability was addressed.

Capturing the power consumption of a chip can reveal the software code running on the chip, even the actual command. The application of Simple Power Analysis and Differential Power Analysis techniques is possible to break the matching mechanism of the biometric system or reveal the biometric template, or even medical data stored in smart card. Timing attacks are similar and measure the processing time instead of the power consumption. The RFID smart card had countermeasures implemented against these types of attacks, including low power consumption chips, noise generators and time-neutral code design.

Poor biometric implementations are vulnerable to spoofing and mimicry attacks. An artificial finger made of commercially available silicon or gelatine, can deceive a fingerprint biometric sensor. This vulnerability is addressed, since vitality detection features were implemented in the fingerprint sensor and the environment was controlled.

Poor enrolment, system administration and system use procedures, expose the biometric system. During the enrolment phase, raw biometric data and biometric templates can be compromised and databases can be altered or filled with imprecise user data. Poor system administration procedures, in addition to the above, might lead to altered system configuration files, with decreased False Acceptance Rates,

making false acceptance easier, thus security weaker. Similarly, a user might exceed his/her authority, threatening the system. This vulnerability was addressed, since enrolment, administration and system use was implemented according to international standards and best practices.

Server based architectures, where the biometric templates and medical records are stored centrally inherit the vulnerabilities of such systems. A possible attack can be realized when the impostor inserts his template in the system under someone else's name, or attacks the central database in order to breach the confidentiality or integrity of medical data. This vulnerability was addressed, since the template was stored in the protected memory of the smart card.

Data could be captured from a communication channel, between the various components of a biometric system, in order to be replayed at another time for gaining access. This vulnerability was addressed, since the biometric component was limited in a hardware security module, with physical security countermeasure implemented and the environment was controlled by the personnel of the stadium.

Off-limit power fluctuation or flooding of a biometric sensor with noise data - for example flashing light on an optical sensor, changing the temperature or humidity of the fingerprint sensor, spraying materials on the surface of a sensor or vibrating the sensor outside its limits - might cause the biometric device to fail. Since the corresponding part of the security policy implementation ensured a controlled environment for the biometric devices.

The residual biometric characteristic of a user on the sensor may be sufficient to allow access to an impostor (e.g. a fingerprint the sensor). The attack is realized on a fingerprint sensor with a residual fingerprint from the previous measurement, by pressing a thin plastic bag of warm water on the sensor, by breathing on the sensor or by using dust with graphite, attaching a tape to the dust and pressing the sensor. This vulnerability was addressed, since the sensor deployed was capacital and not applicable to these types of attacks. Furthermore the environment is controlled by personnel, not permitting such attacks.

A user having a similar template or a similar characteristic with a legitimate one, might deceive the system, especially in identification applications, where one to many template comparisons are conducted. This vulnerability was addressed, since the algorithm performance had adequate performance references, according to international best practices for performance testing.

The impostor is attempting continuously to enter the system, by sending incrementally increased matching data to the matching function until a successful score is accomplished. Biometrics however are more resistant to this attack, than traditional systems, since the impostor has to find a way to insert the trial data to the system, thus combine this vulnerability with one of those described above. This vulnerability was addressed, since the environment is controlled by personnel, not permitting such attacks.

Regarding the remainder of the infrastructure, a security study was conducted, including a vulnerability assessment for the network elements, the database, the operating systems, the applications and the servers. All necessary network security controls were deployed, including firewalling and intrusion detection systems, as well as network device hardening and the deployment of secure network protocols. The database security controls were deployed according to best practices, for

realizing confidentiality, integrity and availability especially for the user data. Operating system hardening and application level countermeasures were also deployed, implementing a standard security policy. The security policy also covered security organization issues and personnel procedures, being compatible with ISO/IEC 17799:2005: Information technology - Security techniques - Code of practice for information security management.

8 Performance evaluation

During the pilot operation, we examined a number of performance factors, including: delay time. Compared to the manual user access, the mean time of user access was almost equal, since the biometric template comparison was one-to-one – comparison of the on-spot generated template by the biometric measurement, with the pre-stored template on the smartcard. In that sense, access control through RDID smartcards, facilitates user entrance, as also proven in similar access control systems described in the state of the art section of this paper. User access was acceptable according to the response of the users during the evaluation assessment. Regarding the performance of the biometric device, the point of equalization of the false acceptance and false rejection rates (called equal error rate) was 0,001, according to evaluation tests that were conducted by following international best practices on biometric performance testing [16]. One-to-many biometric template comparison in identification applications may have increased the delay time and user false acceptance or false rejection. The overall system performance was found compatible with the specifications.

9 Conclusions

Bioathletics was evaluated in terms of acceptability, security and performance. Acceptability was a very important factor, since the deployment of biometrics usually have a negative impact to the public due to the consideration of privacy issues. The acceptance assessment however, revealed that especially after informing the users regarding the system operation, biometrics were not only accepted by the users but also recognized as a mean to increase security and relief users from the anxiety of incidents during an athletic event. System security was mainly focused on the biometric component of the pilot implementation. A specialized methodology was deployed for assessing the risk of the biometric component of Bioathletics and all necessary countermeasures were developed within the system in order to address all known vulnerabilities. The performance of Bioathletics finally revealed that biometrics can be deployed without causing significant delays in user entrance, while the total operation of the system was found more than useful to the administrators of the stadium. Future work, involves a full deployment of the system and the system testing in total in athletic events of different types.

References

1. C. Dimitriadis and D. Polemi, Biometrics – Risks and Controls, *Information Systems Control Journal (ISACA)* **4**, 41-43 (2004).

2. SAIC. Helping Greece Secure the 2004 Olympic Games Security, *SAIC Magazine*, **Summer**, 10-11 (2004) http://www.saic.com/news/saicmag/2003-summer/olympics.html

3. INFRA, Sydney 2000 Olympic, INFRA (INFRA Success Stories, Sidney, 2000) http://www.infra.com.au/SuccessStories/Sydney2000.asp

4. BBC Sports, Security tight for games, *BBC Sports* (23 July 2002), http://news.bbc.co.uk/sport3/commonwealthgames2002/hi/front_page/newsid_2146000/2146550.stm.

5. Sportsvenue-technology.com. Millenium Stadium, Cardiff, United Kingdom, *Sportsvenue-technology.com* (2004), http://www.sportsvenue-technology.com/projects/cardiff/.

6. Sportsvenue-technology.com. 2003 World Cricket Cup, South Africa, *Sportsvenue-technology.com* (2003), http://www.sportsvenue-technology.com/projects/cricket.

7. BBC News. "Keeping the peace at the World Cup", *BBC News World Edition* (31 May 2002) http://news.bbc.co.uk/2/hi/asia-pacific/2018292.stm.

8. R. Bolle et al., *Guide to Biometrics* (Springer Professional Computing, Dordrecht, 2004).

9. S.A. Shaikh and C.K. Dimitriadis, Modelling a Biometric Authentication Protocol for 3G Mobile Systems using CSP, in**:** *Communication, Network, and Information Security (CNIS 2005)* (Acta Press, Calgary Canada, 2005).

10. International Biometric Group, *Biometrics Market and Industry Report 2004-2008* (International Biometric Group, New York, 2004).

11. D. Paret, *RFID and Contactless Smart Card Applications* (John Wiley & Sons, Chichester, England, 2005).

12. K. Finkenzellen, RFID *Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification* (John Wiley & Sons, Chichester, England, 2003).

13. F. D. Davis, User acceptance of information technology: System Characteristics, User Perceptions and Behavioral Impacts, *International Journal of Man-Machine Studies* **38** (3), 475-487 (1993).

14. M. Amberg, M. Hirchmeier and D. Schobert, DART – Ein Ansatz zur Analyse und Evaluierung der Benutzerakzeptanz, *Wirtschaftsinformatik* **1**, 573-592 (2003).

15. C. Dimitriadis and D. Polemi, Application of multi-criteria analysis for the creation of a risk assessment knowledgebase for biometric systems, in: *Lecture Notes in Computer Science, Volume 3072: Biometric Authentication ICBA 2004, Hong Kong China* (Springer-Verlag, Berlin, Heidelberg, 2004), pp. 724-730.

16. J. Wayman, A. K. Jain, D. Maltoni and D. Maio, *Biometric Systems - Technology, Design and Performance Evaluation* (Springer, London, 2005)