Software and hardware user authentication methods in the information and control systems based on biometrics

Z Boriev, A Nyrkov, S Sokolov and S Chernyi

Admiral Makarov State University of Maritime and Island Shipping, 5/7, Dvinskaya st., Saint-Petersburg, 198035, Russia

E-mail: za_mir_b@mail.ru

Abstract. The possibility of using biometric information technologies in management is considered in this article. A brief review of access control and time attendance is made as well. Biometric methods and systems for user identification are analyzed. Recommendations on the use of various systems depending on the specific tasks are given in the article.

1. Introduction

Nowadays the problem of using biometric identification systems is becoming more urgent. However, in fact, traditional methods of personal identification and authorization based on the use of passwords or physical media (in the form of a pass, a passport, a driving license, electronic keys and cards) do not meet modern requirements for reliability in the determination of the individual. A password can be forgotten or intercepted, a material carrier can be copied, lost or given to another person. All of the above mentioned does not allow the traditional access control systems to ensure an adequate level of reliability. As a result, companies are looking for more efficient ways of ensuring security. One way to solve this issue is to move to biometric identification systems [1].

2. Information and Control Systems

Effective management requires constant monitoring and planning of all processes in the organization. Planning activities are carried out taking into account the fact that they will be followed by the monitoring function. It is necessary for the control to have timely, accurate information that will be effective with respect to the cost to develop it. To implement these requirements it is necessary to enter information and to control the system.

Management Information System (MIS) is a set of hardware and software that allows the company management to obtain timely information which is necessary for making effective decisions.

The administration of the enterprise daily deals with the problems of payroll, time tracking, providing access to certain resources of the staff, whose number is constantly changing. The automation of management processes in the company is not a big problem itself. The real difficulties arise due to the fact that the components of any organization are constantly changing, upgraded or even can be deleted. The environment and the structure are changing; technological processes of the enterprise are being modernized. If the administration of the organization is deprived of the opportunity to react promptly to these changes, the consequences for the enterprise can take a serious nature [2].
3. Access control systems

Access control systems (ACS) is an essential component of the information management system of any business or office building. ACS is a very complicated hardware-software system that is responsible for the registration and the restriction of entry and exit of people and vehicles in a certain area through check points (gates, doors). The main objectives of the ACS are to determine the time of admission to the territory and identify the objects that are eligible for admission. In addition, the access control system can perform a range of additional features, which include:

- keeping records of working time.
- conducting employees’ payroll (integrated if possible with the accounting system).
- maintaining a database of visitors and employees.

Any ACS has an email id (key), which is used to determine the rights of the owner. The following arrangements can be used as a key in Access control systems: barcode, magnetic or smart (smart cards) Plastic cards; ‘Electronic tablets’ (Touch Memory); Wiegand cards; remote reading cards (proximity); PIN-code. Moreover, the biometric parameters of a person can be used as an identifier.

‘Electronic tablets’ (Touch Memory) are microchips arranged in a sturdy metal case. The code information is recorded in the memory of the circuit. It is necessary to attach the tablet to the reader to identify the user. The Reading Speed is 0.1 second. Some models allow one to enter some information about the user. The advantages are compactness, high resistance to mechanical damages, corrosion, temperature extremes and a low cost (comparable to the cost of magnetic stripe cards).

A card with a bar code is a plate coated with black stripes (strokes). The code information is contained in the variable width of strokes and the distance between them. The code of the card is read by the optical reader. The code information of a magnetic card is recorded on the magnetic strip. The bar code can simply be soiled with mud. A magnetic card can easily be damaged in daily use.

A perforated card is a plate (plastic or metal). The code information to a perforated card is applied as the holes arranged in a specific order. The code card is read by mechanical or optical readers.

The code information on a Wiegand card is contained on the thin metal wires arranged in a certain way and glued with special glue. An electromagnetic reader reads the information from a card.

Proximity technologies have a lot of advantages, which are much greater compared with other methods of identification: reliability and durability, lack of power (in passive cards). A proximity reader constantly sends a radio signal. When being in contact with the zone of the reader, a card takes its radiation and sends a signal containing a recorded microchip code. The distance between the reader and the card depends on the power of the reader and varies from 5 cm to several meters. The lack of the mechanical contact during operation allows producing identifiers of an arbitrary form, the identifier can be implanted into the object of the identification. The advantages of proximity technologies are the complexity of falsification, the possibility of using encryption algorithms.

A smart card (‘smart card’) is a plastic card with an integrated microcontroller and all its attributes (a processor, RAM, nonvolatile memory with a file system, input-output means, additional coprocessors). The main advantages of smart cards are a large memory capacity and high information security which protects against attempts of modifying and duplication. The drawback is the high cost. A smart card is the standard equipment of appropriate automated systems and it can be simply implemented in any arbitrary system.

PIN-code. The memory of a man is the code information carrier. A user independently types the code on the keyboard and it gives the signal to the actuating device [3].

4. Biometric identification systems. Legislative regulation

In the Russian Federation in the field of rights protection of personal data a special attention is paid to biometric data. Article 11 of the Federal Law ‘On Personal Data’ gives the following definition of biometric data - ‘data that characterize the physiological and biological characteristics of the person, according to which it is possible to establish his or her identity (biometric personal data), are used by the operator to identify the subject of personal data. It is necessary to have a written consent of a person to process the biometric personal data, except as provided by paragraph 2 of this Article’.
Part 2 of Article 11 of the Federal Law ‘On Personal Data’ states that the processing of biometric personal data can be carried out without the consent of the subject of personal data in connection with the implementation of international treaties of the Russian Federation on readmission, in connection with the administration of justice and all that is connected with it.

Besides, the law provides specific requirements for material carriers of biometric personal data and storage technologies of such data if personal data are outside of information systems.

A material carrier must provide:
• protection against unauthorized addition and re-recording of information after removing it from the information system of personal data;
• access to biometric personal data recorded on a material carrier carried out by an operator and persons authorized to work with biometric PD in accordance with the legislation of the Russian Federation;
• ability to identify the personal data information system, in which a biometric record of PD was implemented, as well as the operator, who carried out such record;
• preventing from unauthorized access to biometric personal data contained on a material carrier.

An operator of biometric data, used outside of personal data information systems, must:
• maintain the registration of the number of copies of material carriers;
• provide an appropriate material carrier with a unique identification number that allows the operator to be accurately determined.

5. Biometric identification systems. Hardware and software

Biometric identification systems are the most effective ones because they do not recognize the physical media, but the unique physical characteristics of a human. Access and data protection systems, based on such technologies, are not only the most reliable but also the most user-friendly nowadays. All biometric devices have specific requirements for hardware and software. In any identification system users must be registered first. A lot of biometric systems allow users to do it themselves.

Biometric access control systems allow organizing an efficient, reliable and cost-effective system of access control. The use of biometric technologies avoids such problems as loss, re-release and transfer of electronic passes to other persons.

Timesheet is no less important issue for the management of companies. Time tracking system supplies reporting data, corresponding to the time of staff arrival and departure at the workplace, delays at the workplace, overworking and underworking. In its turn, the information availability allows managing the distribution of wages, bonuses, penalties more flexibly, increases discipline in the enterprise and, of course, results into economic benefits. It is important that the time tracking system, constructed on the basis of biometric identification, allows eliminating instances of intentional violation of the regime related to the lack of binding - e.g., the magnetic card to a specific person, so that the card can easily be transferred from one person to another.

There are several ways to provide access to the necessary resources:
1. Verification based on biometrics and a unique identifier that identifies a particular person (e.g., ID number), that is, this method is based on a combination of identification and authentication techniques.
2. Identification based only on the biometric measurements. The measured parameters are compared to all records from the database of registered users, rather than with one of them, selected on the basis of any ID.

Generally, both methods are used equally. The selection of the authentication method is carried out directly on the basis of security requirements, as well as the funds allocated for these purposes. But the reliability of the access system depends not only on the way of authentication. An important factor in this regard is the selection of the biometric parameters based on the type of access, which is going to be implemented.
6. Biometric parameters
There are a number of biometric parameters, on which base the identification and authentication of a personality are carried out. They are the iris of the eye, the retina of the eye, a hand vein pattern, a fingerprint, a handprint, a hand geometry, a face geometry, 2D / 3D face models, a signature, a voice, a gait, a shape of ears.

Every year more and more biometric parameters, which can identify and authenticate a personality, appear. But it takes a lot of time and money to study them and find methods and algorithms of processing. Therefore, the scrutiny degree of a biometric parameter directly affects the extent of its using.

A fingerprint is the most-used parameter today. This is due to the fact that fingerprinting got its spread in the late 19th and early 20th century. Every day the cost of fingerprint scanners is more and more reduced, but the number of additional parameters, such as finger temperature, pressing force and the like ones, increases. We can say that scanner manufacturers will reach the limit of opportunities in this area in the nearest future.

The most statistically reliable and forgery resistant access parameters are the iris of the eye and a hand vein pattern. But the process of collecting and processing such parameters takes a bit longer time than the processing of a fingerprint or a face shape. The indicators of reliability are such features as a false rejection and a false access. A false denial of access for biometric data tends to 0%, and a false access does not exceed 1-2%.

Despite all the differences between the biometric parameters, it was decided to use the False Acceptance Rate (FAR) and False Rejection Rate (FRR) as the basic characteristics of biometric systems. Obviously, the smaller these ratios, the more reliable one or the other parameter. These factors help to decide whether to use a particular method of identification and authentication, depending on the task. Table 1 shows the average values for the various biometric systems[4]:

|     | Fingerprints | Face Geometry | Iris     |
|-----|--------------|---------------|----------|
| FAR | 0.001 %      | 0.1 %         | 0.00001 %|
| FRR | 0.8 %        | 7 %           | 0.10 %   |

7. Structure of biometric systems of access control
For the most part ACS and the working time control systems are network distributed systems with the user access rights, stackable if necessary, open to the integration with other manufacturers' equipment. The controllers connected to the control PC or the server via USB or LAN Ethernet are set at the points of passage [7, 8].

The user registration is performed by means of special software. A control reader, connected via the USB port of a personal computer, is applied to register fingerprints. Users can also be registered independently at the terminals of the system using specific procedures.

As we can see in Figure 1, the ACS has a modular structure. It allows the system to be scalable and more stable. In the event of failure of one of the elements, the system continues working, of course, in a limited function mode. In most cases the software consists of two modules – a ‘working time control system’ and an ‘access control system’. The time tracking system works with a staff, shifts, schedules, events, obtained automatically or listed in the manual mode. It allows making reports. The access control program is responsible for connecting and configuring devices, setting the rights of passage and time zones, synchronization of data between the database and terminals [9].
8. Comparative evaluation of biometric systems

Let us select several empirical characteristics for assessing the quality of the system:

1. Forgery resistance.
2. Environmental resistance – a characteristic estimating system stability under various environmental conditions, such as changing the lighting or the room temperature.
3. Ease of using - shows how difficult it is to use a biometric scanner, whether it is possible to identify ‘on the fly’.
4. Operation speed.
5. The cost of the system

You can see a comparative evaluation of biometric systems based on the ten-point scale.

Table 2. Comparative evaluation of biometric systems.

| Parameter     | Forgery resistance | Environmental resistance | Ease of using | Speed | Cost | Stability of characteristic over time |
|---------------|--------------------|--------------------------|---------------|-------|------|--------------------------------------|
| Iris          | 10                 | 9                        | 8             | 7     | 10   | 10                                   |
| Fingerprinting| 6                  | 10                       | 9             | 10    | 10   | 9                                    |
| 2D face       | 4                  | 6                        | 6             | 10    | 10   | 8                                    |
| 3D face       | 9                  | 8                        | 10            | 5     | 7    | 10                                   |
| Arm veins     | 10                 | 7                        | 9             | 7     | 8    | 7                                    |
| Retina        | 10                 | 10                       | 6             | 3     | 6    | 9                                    |

It can be concluded that forgery resistance of one or the other biometric parameter is inversely proportional to the speed of processing it by the system.

9. Conclusion

The choice in favour of using a certain parameter when organizing access or working hours accounting depends directly on the system requirements. The most statistically reliable and forgery resistant access systems are the admission systems based on the iris of the eye and on a hand vein pattern. The least expensive and easiest to use, but having good statistics are the fingerprints admission systems. The admission on 2D face is convenient and cheap, but it has a limited range of applications due to poor statistics.
In addition to combining the used biometric parameters, it is possible to combine the parts of the body, from which the parameters are removed. For example, for the iris of the eye we can increase the accuracy of the system almost quadratically without time-consuming. We can complicate the system by making it for two eyes. As for the fingerprint method, it is possible to do it by combining several fingers; as for the vein pattern recognition, it may be done by combining two hands, but in this case, the improvement is only possible by increasing the time of human interaction with extractors.

Thus, summarizing the results of the methods it can be said that the iris biometric access and possibly the vein pattern recognition should be used for medium and large objects as well as for the objects with maximum safety requirements. The fingerprint access control will be optimal for the objects with the number of staff to several hundred people. 2D face recognition systems are very specific. They may be required in cases when the detection requires the absence of a physical contact, but it is impossible to supply the control system on the iris of the eye. For example, if identification of a person is required without his or her participation, with a hidden camera or with an outdoor motion detection camera, which is possible only for a small number of subjects in the database and for a small stream of people shot on a camera.

References
[1] Boreysho A 2005 J. Security of Business Information 59 40–43
[2] Aleshin A 2008 Dashkov & Co. Moscow
[3] Balle R, Pankanti S, Ratha N, Senior A 2004 Springer Science+Business Media. New York
[4] Kharitonov A 2013 J. Cybernetics and programming 2 12–19
[5] Korobeynikov A, Gatchin Y 2014 World Applied Sciences Journal 30 165–169
[6] Nyrkov A P, Belousov A S, Sokolov S S 2015 Modern Applied Science 10(5) 162–176
[7] Chernyi S, Zhilenkov A, Sokolov S, Titov L 2015 Metallurg. and Mining Industry 7(3) 66–73
[8] Chernyi S 2015 Metallurgical and Mining Industry 3 60–65
[9] Nyrkov A, Sokolov S, Chernyi S, Mamunts D 2015 Metall. and Mining Industry 7(6) 521–524