Designing a biometric access control concept

A A Troshkov, S V Bogdanova, A N Ermakova, V E Rachkov

Stavropol State Agrarian University, Stavropol, Zootechticheskiy ln., 12, 355000, Russia

E-mail troshkov1954@mail.ru

Abstract. The current legislative and regulatory database of biometric characteristics for the security of information technologies is not informative and has an imperfect system. The main disadvantages include: the lack of system and methodology for building biometric identification / authentication for managing access to protected information resources; insufficient knowledge of all possible biometric characteristics of a person; an imperfect model of the biometric system; a static approach to assessing access control. Therefore, there is a need to develop a biometric identification/authentication system to restrict access to information resources in various areas. Accordingly, we propose to systematize the biometric system for protecting and managing access to information.

Keywords: Encoding, encryption, access control, biometrics.

1. Introduction

Digitalization of society leads to changing the functioning of systems for storing, processing, receiving and transmitting useful information.

However, the increase of the information flow, storage resources require security of information that is regulated by normative-legal act of the security policy (SP).

The security policy is controlled by the governing bodies of enterprises of all ownership forms. An example of information security form and information protection is:

- order (algorithm) of access to resources;
- monitoring access to resources;
- vesting (expanding) the involvement and authority of management;
- segments distribution of information resources.

2. Model of security access control

Implementation of the system information security policy is the establishment of regulatory requirements for the composition and execution of various security mechanisms. This can be achieved by setting high requirements for software, encoding systems (encryption), and organizational and technical measures. Requirements for the functioning dynamics of the information resources describe various rules for identifying and authenticating users and registering events that occur in this area. The highest part of information security mechanisms is the access control and localization system for various types of illegal access. Currently, the information security policy in the field of user access is implemented by security personnel – access control specialists (Figure 1).

Personalized, account information, configuration parameters and encryption codes belong to the highest levels of trusted objects. The objects must also have the required security. Trusted interfaces and a certain number of officials are used for studying, reading, applying, changing and input / output.
Figure 1. Managing subjects access to information resources

Figure 2 shows the designed access control model for certain special security services.

Figure 2. Access control model

The algorithm of model functioning (Figure 2) is based on the rules of access control located in the security policy plan. Since the information resource is decomposed into segments, the segment required for access is set (or personalized) for the users.

For the design of the access matrix, individual or group placement is applied (Figure 3).
For the formalized algorithm, access control lists approved by the manager are used. Each ACL element contains rules for accessing a segment of an information resource.

However, access decisions in various scientific sources show a lack of resistance to illegal access. To solve this scientific and technical problem, we propose to involve the introduction of biometric characteristics (BC) of the user into the procedure of functioning of the identification system. In particular, to improve the access matrix by adding BC to individual and group permissions (Figure 4).

3. Functioning of group biometrics system

Figure 4 demonstrates conceptual proposals which are made for the use of the following methods for managing access to information resources in a group BC:

1. $\Sigma$ BC "Manager-user"
2. $\Sigma$ BC "Security-user"
3. $\Sigma$ BC "User-user"

Analysis of work in the field of security mechanisms and services indicates that such proposals were not previously available. Preliminary calculations show that the characteristics of RAR and RAF have a dynamic improvement when using an improved user matrix.
BC grouping for user access allows to create an attribute $\Sigma BC$ with high distinctiveness of identification by rules:
- user group – with individual BC with assigned priorities;
- creation of groups – with a dedicated list where the personal data of group members are listed, including other groups;
- all groups are part of the administrative information cloud.

Segments of information resources are defined according to the user's mandate. To accommodate collisions, a BC or BC group are allocated, which describe the priority in the cloud (Figure 5).

Figure 5. Location of collision and allocation of priorities

Figure 5 highlights the presence of rules: if they contradict each other, priority is given to the decisive rule (according to the user's mandate), which determines more specific access in accordance with the permission to access certain segments of information. For more convincing, the user can provide the subject authentication protocol (if necessary). Using such proposals and models, it is possible to organize work with information of various levels of secrecy, which eliminates the mixing of information of different labels and categories, which was previously known as a lack of access control system operation.

For example, a generalizing algorithm for the representation of group BC in Figure 6 is given. From this figure we form a biometric system:

- $S\cdot u$ (Supervisor - user)
- $S\cdot u$ (Security -user)
- $U\cdot u$ (User-user)

From the system, we design the following algorithm (Figure 6)
Summation $\oplus$ of BC allows you to increase the stability of coding, improve the quality of identification, despite its complexity.

4. Conclusion
The presented biometric concept makes it possible to form a dynamic algorithm for the functioning of access to information resources, to carry out the distribution of powers in the biometric system. In accordance with the code, the distribution of segments of information resources is proposed. The application of the presented concept allows you to form an access matrix in the information security policy of an enterprise of various forms of ownership, correctly distribute the user's mandate for access control.

References
1. Wasserman F 1992 Neurocomputer technology: Theory and practice. Per. s Engl. M.: Mir
2. S Burnet, S Payne 2002 Cryptography. Official guide to RSA Security Binom-Press p 384
3. Khoreyev P 2009 Methods and means of information protection in computer systems: a textbook Academy p 256
4. Alferov, A, Zubov A, Kuzmin A, Cheremushkin A 2009 Fundamentals of cryptography: a textbook Moscow: Helios ARV p 245
5. Troshkov M, Troshkov A, Shuvaev A 2016 Protection of business information in the field of agro-industrial complex management Scientific and practical journal "Bulletin of the Stavropol agro-industrial complex. 2 22/1 pp 135-139

6. Troshkov A, Zhuk A, Rachkov V 2016 Modern threats and methods of information protection in information systems. Collection of scientific papers on the materials of the all-Russian NPC: "Institutional transformations of national economic systems" Stavropol, Stgau, pp 78-85.

7. Troshkov A, Troshkov M 2017 Synthesis of a biometric key for the formation of a cryptographic code that controls access to information resources Collection of scientific articles based on the materials of the International scientific and practical conference pp 224-228

8. Norman T L 2017 Foundational Security and Access Control Concepts Electronic Access Control pp 21-42

9. Poniszewska-Maranda A 2012 Role Approach in Access Control Development with the Usage Control Concept Proceedings of the 11th IFIP TC 8 international conference on Computer Information Systems and Industrial Management

10. Bhalla A 2020 The latest evolution of biometrics Biometric Technology Today 8 pp 5-8