ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 8, Issue 6 , June 2021

Automatic Marking Engine, Algorithm and Software Module for Automatic Marking

Kadirov Mir-Khusan Mirpulatovich, Karimova Dilbar, Tojikhujaeva Nodirakhon Zakirovna, Tulyaganov Zoxidjon Yakubdjanovich

Assistant professor, Department of Information Technologies, Tashkent State Technical University, Tashkent, Uzbekistan.
Assistant professor, Department of Information Technologies, Tashkent State Technical University, Tashkent, Uzbekistan.
Senior Lecturer, Department of Information Technologies, Tashkent State Technical University, Tashkent, Uzbekistan.
Senior Lecturer, Department of Information Technologies, Tashkent State Technical University, Tashkent, Uzbekistan.

ABSTRACT: The solution to the problem of protecting information from unauthorized access in any information system is based on the implementation of control and differentiation of access rights of subjects to protected resources, primarily to file objects, since they are intended to store the processed data.

KEYWORDS: access, privacy, information leakage, user, security policy, automatic marking, security labels

I. INTRODUCTION

The solution to the problem of protecting information from unauthorized access in any information system is based on the implementation of control and differentiation of access rights of subjects to protected resources, primarily to file objects, since they are intended to store the processed data. In this case, the subjects of access in the delimiting policy are users identified by their accounts [1].

II. FORMULATION OF THE PROBLEM

An automatic control system is designed to control the progress of a process. Such a system includes sensor B, amplifier A, which receives the signal from the sensor and transmits it after amplification to a special element P. which implements the final operation of automatic control - the presentation of the controlled value in a form convenient for observation or registration.

In a particular case, signal lamps or sound signaling devices can serve as an actuating element P. A system with such elements is called an alarm system.

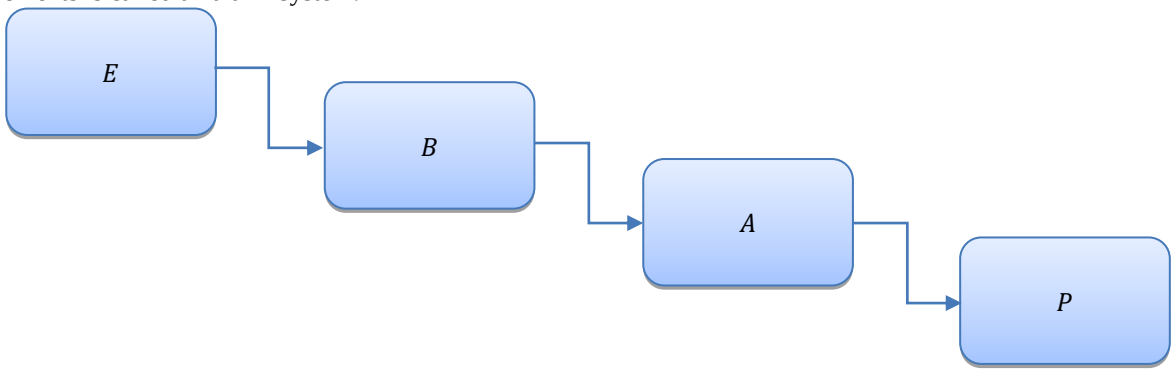

Fig. 1. Automatic control system.

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 8, Issue 6 , June 2021

Regardless of the number of elements, automatic control systems are open-loop and the signal passes through them only in one direction - from the controlled object. E to actuator P.

The automatic control system is designed for partial or complete (without human participation) control of an object or a technological process.

A fundamental question in the formation of requirements for the implementation of access control to protected resources, including file objects, is the answer to the following question: how and in what form are the rules for subjects 'access to objects (or to subjects' objects) stored? It is the way access rules are stored that greatly influences the access control functionality, since it determines how the access object is identified in the delimiting policy [2, 3].

Alternative ways of storing access rules is to store them either as attributes associated with access objects, or as a separate access table (matrix), stored, for example, in a separate file. Access attributes for defining a delimiting policy are used, for example, in the access control scheme, including to file objects, in modern operating systems.

One of the key tasks of information protection, formulated on the assumption that it is the process that carries the dominant threat of unauthorized access to information for the reasons discussed in, is solved today by the so-called intrusion detection (detection and prevention) systems, the basis of which (for level systems host) compiles an analysis of the behavior of processes (applications) by periodically analyzing the OS and application logs. This protection technology has many drawbacks, the key of which is the practical impossibility, in the general case, of preventing a process from attacking the protected resource in real time, even in the event of an intrusion [4].

As access objects in the created delimiting policies, including the creation of new file objects, file objects can be used, including those on external drives, that are present at the time of setting access rules by the administrator, including system file objects.

III. ALGORITHM AND SOFTWARE MODULE FOR AUTOMATIC MARKING

As computing progressed, there were more and more files on systems. For the convenience of working with them, they, like other data, began to be organized into structures (at the same time symbolic names appeared). In the beginning it was a simple array, "tied" to a specific information carrier. Currently, the most common is a tree-like organization with the ability to mount and insert additional links (that is, links). Accordingly, the file name has acquired the character of a file path: a listing of the nodes in the file system tree that must be traversed to get to it.

The operating system provides applications with a set of functions and structures for working with files. The capabilities of the operating system impose additional restrictions on the limitations of the file system. From the point of view of the API, a file is an object in relation to which the functions of this API can be applied. At the API level, it is no longer important whether the file exists as a file system object or is, for example, an I / O device.

Depending on the file system, a file can have a different set of properties.

Most file systems use the filename to indicate which file is being accessed. In different file systems, file name restrictions are very different: in FAT16 and FAT12, the file name size is limited to 8.3 characters (8 for the name and 3 for the extension); on other systems, the file name is usually limited to 255 bytes; in NTFS, the name is limited in some OS to 255 Unicode characters (according to the specification - 32,768 characters).

In addition to the limitations of the file system, the operating system interfaces additionally restrict the character set that is allowed when working with files.

The file name extension (often a file extension or extension) as an independent file attribute exists in the FAT16, FAT32, NTFS file systems used by MS-DOS, DR-DOS, PC DOS, MS Windows operating systems and is used to determine the file type. It allows the system to determine which application should open a given file. By default, in the Windows operating system, the extension is hidden from the user.

Local and network-shared file objects can act as file access objects in the delimiting policy (when delimiting access rights to network-shared objects, the access object is specified in the delimiting access policy as follows: "// machine name is the name of the file object", while masks and environment variables are also used [5].

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 8, Issue 6 , June 2021

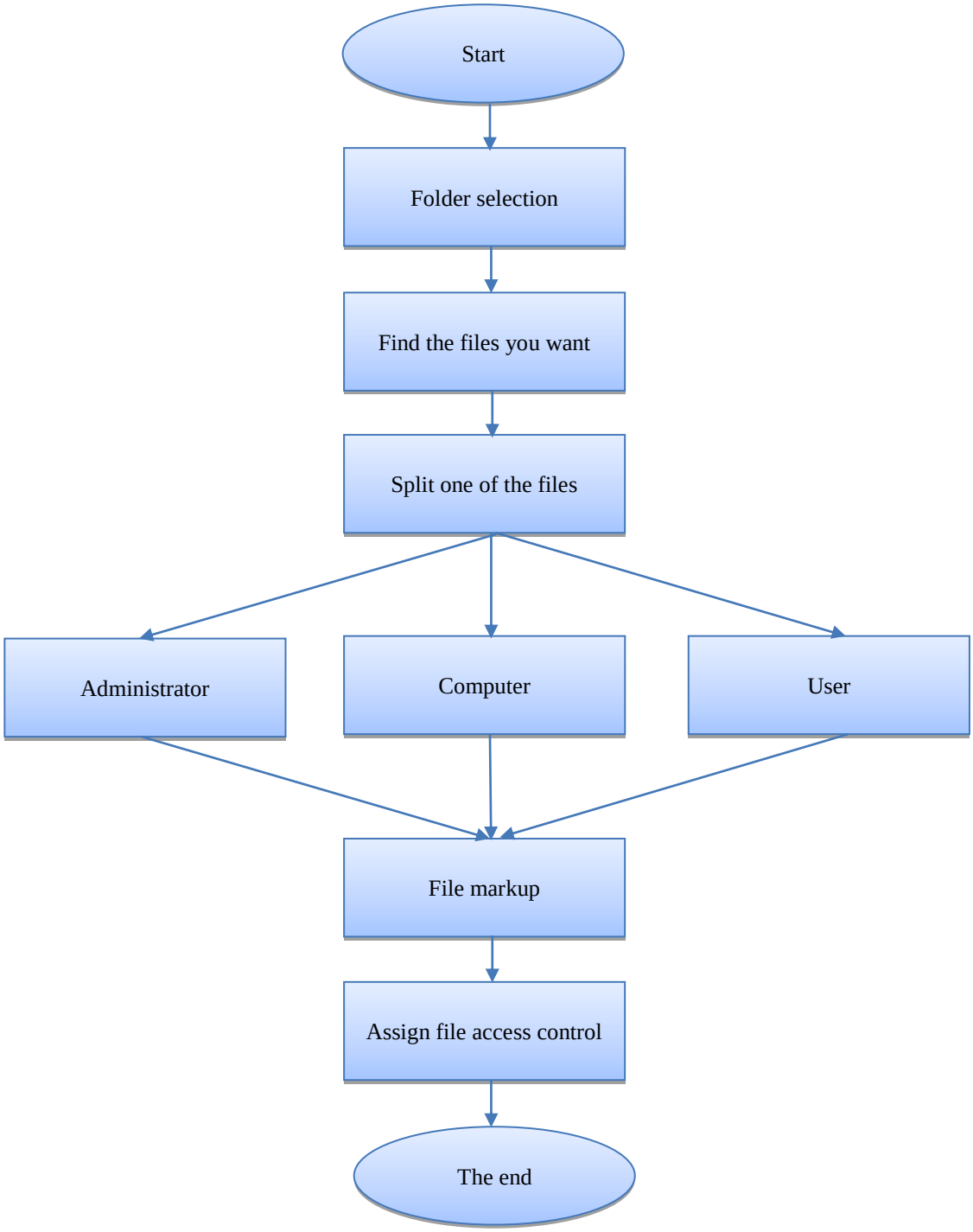

Fig. 2. Algorithm of the program module.

The object type (file, file mask, directory, directory mask, mask) is set automatically when it is created in the system, but when a specific delimiting policy is implemented, the administrator is given the opportunity to change the file object type (assignment manually) when it is created. The user may need to set the object type manually.

Consider the use of masks when specifying subjects and access objects in a delimiting policy.

Access subjects are identified in the delimiting access policy by three entities, created from the menu shown in Fig. 3.

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 8, Issue 6 , June 2021

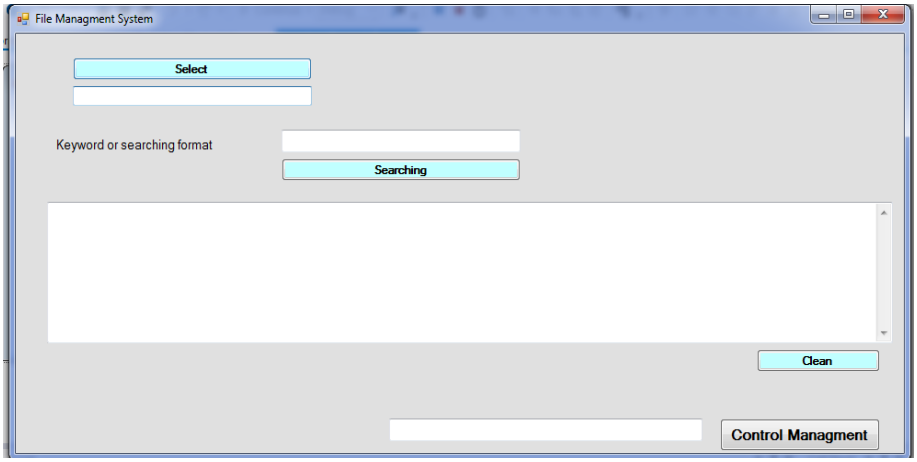

Fig. 3. Access Principal Creation

The created subjects are automatically ranked (according to the specified rules) and we select the folder according to the descriptor accuracy and are displayed in the interface in the appropriate order (either from top to bottom or from bottom to top), see (Fig. 4).

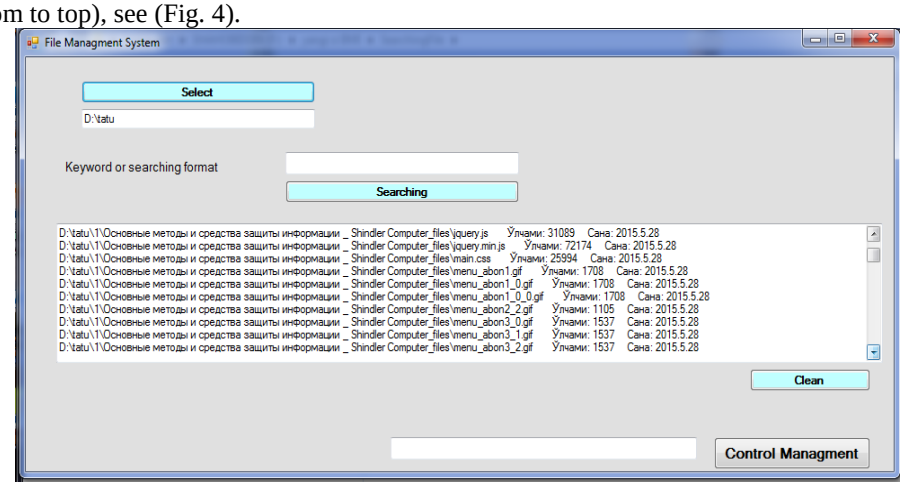

Fig. 4. Program module interface

When specifying access objects, masks and environment variables can be used. Taking into account the possibility of using masks, several created objects at the same time can correspond to a real object, determined by its full path name, to which access is requested. To select an access rule, the following priority is implemented for the accuracy of describing objects in the delimiting policy, based on their type: file, file mask, directory, directory mask, mask. The objects specified in the delimiting policy are compared with the real object and the access request in order to determine the most accurate descriptor, in the specified processing order - a file, if not suitable, then the file mask, respectively, directory, directory mask, mask.

In the line "Object name", as a result of using the device overview, the device identifier appears. In this line, you can manually complete the name of a file object on the device, including using masks, or by copying the name of a directory or file located on the device from the “Object name” line obtained by browsing directories or files on this device.

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 8, Issue 6 , June 2021

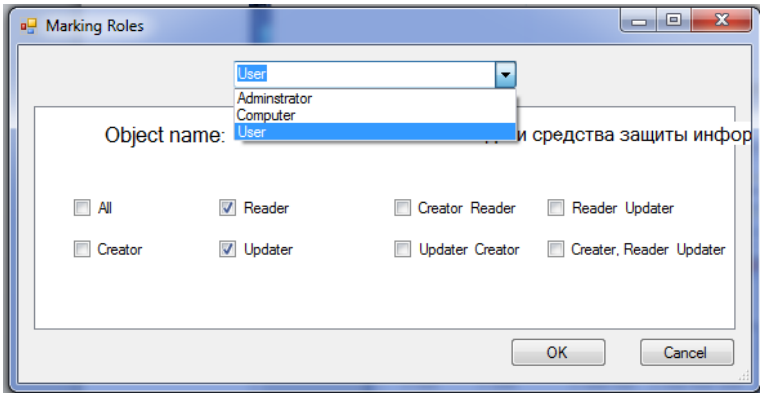

Fig. 5. Role-based access control selection

Profiles are used as access subjects in the delimiting policy, which, among other things, makes it possible to implement a role-based access control model in the event that profiles are created for certain roles.

IV. RESULT

The use of this method increased the efficiency of the system. Obtaining results are shown in Figure 6.

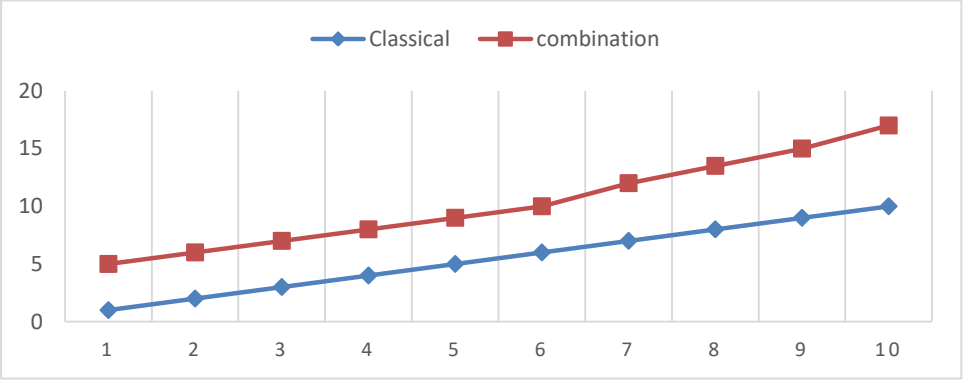

Figure 6.System performance when using security policies

REFERENCES

[1] Devyanin P.N. Modelibezopasnostikompyuternyxsistem. Upravleniedostupomiinformacionnymipotokami: ucheb. Posobiedlyavuzov. – 2-e izd., ispr. idop. – M.: Goryachayaliniya-Telekom, 2013.

[2]]Mirpulatovich K. M., Zakirovna T. N., Ismoilovna K. G. Classification of Modern Security Monitoring Systems in Computer Systems and Networks, International Journal of Advanced Research in Science, Engineering and Technology, Vol. 5, Issue 9, India 2018, p. 6764–6769.

[3] Belim,S. V., Belim, S. Yu., "Problemipostroeniyapolitikibezopasnostipriobedineniiinformatsionnixsystem", Matematicheskiestrukturiimodelirovanie, Vol. 3(47), pp.126-131, 2018

[4] Sheglov,A.Yu.,"Zashitakompyuternoyinformatsiiotnesanktsionirovannogodostupa", Naukaitexnika, pp. 384, 2004.

[5] Rog, O. A.,"Mnogokriterialnaya model reshetkisennosteydlyarealizatsiimandatnixpolitikbezopasnosti v sistemaxrazgranicheniyadostupa", Informatsionnoeprotivodeystvieugrozamterrorizma, Vol.20, pp. 116-121, 2013.