Access Control Method Based on Workstation Binding

Yurii Baryshev
dept. of Information Protection
Vinnytsia National Technical University
Vinnytsia, Ukraine
yuriy.baryshev@gmail.com

Kristina Neuimina
dept. of Information Protection
Vinnytsia National Technical University
Vinnytsia, Ukraine
kris.vladimirovna99@gmail.com

Метод Розмежування Прав Доступу з Прив'язкою до Робочої Станції

Юрій Баришев
кафедра захисту інформації
Вінницький національний технічний університет
Вінниця, Україна
yuriy.baryshev@gmail.com

Крістіна Неуйміна
кафедра захисту інформації
Вінницький національний технічний університет
Вінниця, Україна
kris.vladimirovna99@gmail.com

***Abstract*—This paper presents an analysis of access control models. The proposed method of access control based on the hashing process peculiarities allowing to limit the quantity of workstations from which users are to get remote access to information resources.**

***Анотація*—В даній роботі представлено аналіз моделей розмежування прав доступу. Запропонований метод розмежування доступу, який базуючись на особливостях процесу гешування дозволяє обмежити перелік робочих станції, з яких користувачу дозволяється отримувати віддалений доступ до інформаційних ресурсів.**

Keywords—authentication; hash; access control model; workstation parameters; authentication factors.

Ключові слова—автентифікація; гешування; модель розмежування прав доступу, параметри робочої станції; фактори автентифікації.

I. Introduction

There are a lot of information threats for one processed by computer means, that is caused by the presence of different possible threat sources within hardware and software used for the data processing. In particular the role of such sources might be performed by an enterprise personnel, intruders, malware, technical failures, backdoors etc [1-3]. The latter determines importance of tasks of information protection providing and simultaneously avoiding the substantial worsening computational processes performance quality. One of protection methods, which could be used for this task solving, is user access control. It allows to limit informational resources available to users in the computer system [2, 3]. At the same time mobile devices are spreading among users, and they also could be used to access this informational resources, but ones are quite limited of computing resources and hence information protection providing abilities. The typical workstation might provide high level of informational security and if it is situated at the enterprise, the information protection department of the enterprise could ensure that. All of these are out of reaching in the case, when valid users apply mobile devices or home personal computers for accessing critical informational resources of the enterprise.

The goal of this research is information confidentiality improvement for remotely accessed critical informational resources.

For reaching this goal it is essential to solve the set of different tasks. This work is to solve the following ones of these tasks:

- known access models analyses performing for determining ones, which could be used for reaching goal of the research;
- upgrading the access control models considering research goal;
- the method of user authentication development, that allows to implement selected access control models.

II. Access Control Models Analyses

The access control systems perform access management for subjects using information system to the objects of this system. The certain set of rules lies in the basis of access control model. The well-known models are divided into following groups: discretionary; mandatory; role-based.

During this research the following models were analysed: Harrison-Ruzzo-Ulman, Take-Grant, access matrix, Bell-LaPadula, RBAC [1, 4-6].

The Harrison-Ruzzo-Ulman model (known also as HRU) is the example of discretionary model of access control. The model allows to consider access control system as an automaton, that functions according to the certain rules of transition [1, 4, 5]. This model caused theoretical impact, because it allows research performing based on the automaton theory.

Another analyzed discretionary access control model is Take-Grant [1, 5, 6]. It provides possibility to analyse and check up the state of information system security. The Take-Grant model uses as basic elements type of user access and transformation allowed. It is based on the graph model, which allows to visualise enterprise information protection policy. The main task of the model is determination of user rights to access system as its subject relatively to certain object, which is described as some graph of allowed access types. Using this model, it is possible to study the states of information system depending of access granted to information system users [4, 6]. The access matrix hash the same approach as the latter model, but is presented in the way two-dimensional matrix.

The advantage of discretionary access control models is implementation evidence, independence from the information system type and extreme flexibility. However a key lack is necessity of the manual control over protection systems based on this model, and thus increasing of human factor impact on protection system that uses such model of access control.

The Bell-LaPadula model guarantees that a subject is able to become familiar with information only in case, when he has sufficient authority, and no subject (except the administrator authority to set up the confidentiality levels of objects) in no way will be able to carry out data transfer from an object with the higher level of confidentiality to an object with less level of confidentiality. The Bell-LaPadula model uses classifications of subjects by authority (or mandate) levels and objects by level of confidentiality [1].

If the user of the information system, that owns the high level of authority, would send some data (for instance, that have a level of secrecy, that equals his authority) to an object with less level of confidentiality, then it could become accessible to the subject with lower authority level, than it is settled by information protection policy [1, 5]. This model is also difficult for implementation and requires the considerable amount of computer system resources, thus it limits quantity of enterprises, where it can be used.

The role-based access control (RBAC) model considers additional element comparatively to the above-mentioned models. This model presents the computer system as sets sequence: the set of users, the set roles, the set of rights and privileges, the set of user sessions with the information system [1]. This access control model is appears as compromise between discretionary models manual control management complexity and its flexibility. The former is reduced by sacrificing the latter. However from the practical point of view this model seems to be most useful fro the most types of information systems [2, 3, 5].

The general lack of all these abovementioned models is that they do not provide limitations of workstations, that can be applied by the user to gain an access to informational resources of the system. And according to the previous analyses results, this is the most inappropriate for the remote access distribution systems such as file servers or cloud services providers.

For this research aim reaching the access control model, which is proposed at the article [7], was chosen to be implemented. This model allows access control rules forming depending on authentication data of the user and workstations, those are authorised to be used by him to get access to the certain information resource.

III. AUTHENTICATION METHOD ANALYSES

User gaining access process consists of three related consistently executable procedures: identification, authentication and authorization [3, 5].

There are a few methods of authentication, that differ in complexity, reliability, cost and other parameters. Each of these methods has its pros and cons. The methods of authentication conditionally can be divided into one factor (weak, from the security point of view) and multivariable (strong) [3-5], where features of the subject, who are to be authenticated, are used as factors.

The password authentication is the most widespread, simple and common method, where knowledge of the certain secret are used as an authentication factor. The role of password usually is performed by some word, but recently other types of passwords gain spreading, graphical ones, for instance [5].

The well-known methods of authentication, which are based on the unique objects usage. They could provide more reliable protection, than password authentication methods. These objects usually are divided into two groups [3, 5]:

- passive objects, that contain authentication information (for example, the randomly generated number, which could be interpreted as some kind of a password) and pass it during authentication process after the respective query from authentication module
- active objects, that has sufficient processing resources and actively participate at the authentication process (for example microprocessor-based smart cards and USB-tokens).

The authentication based on unique objects usage has the set of drawbacks concerning their application at the remote access control system [5]:

- the object can be stolen from the user;
- in most cases the special equipment is needed for working with such unique objects;

it is possible to make a copy of the object or emulate its presence.

The biometrical methods of authentication work on the basis of the usage of the equipment for measuring and comparing to the standards of the individual user's body features [5]. It could be implemented by the means of automated methods, that makes it posiible to be used at the informational systems. The authentication of people is performed on the basis of their physiology (static) and behavioural characteristics (dynamic) [5].

As physiological characteristics could be used features of finger-prints, retina and cornea of eyes, geometry of hands or face etc. As behavioural characteristics could be used the style of working tasks solution performing, for example using a keyboard or a mouse. Authentication systems based on voice recognition are also could be selected as the latter type.

Such means allow with high accuracy to recognize a user using certain biometrical characteristics, and they are difficult to being forged. The general lack of biometrical authentication means is a necessity for the addtitional equipment for biometrical characteristics estimation, that can be expensive and inconvenient in the case of remote access control systems. For workstation authentication it is suggested to use combination from a few unique parameters of this station such as [5, 7, 8]: hard drive serial number; date of creation and checksum of BIOS; hardware productivity; MAC-address and others.

In certain cases for granting iniquity to each of authentication sessions it is proposed to add cryptographic salt – a random number.

IV. Access Control Method

The implementation of selected access control model requires development of users authentication method. The method that is executed in accordance with a scheme presented on figure 1 [7]. The database of the authentication contains data presented by the set of vectors of following kind $\{h_i, h_{ij}, Access_i, ID_i, PC_j\}$, where h_i – hash value of *i*th user password; h_{ij} – hash value gotten on side of the client; $Access_i$ – the set of rights and privileges for *i*th user access; ID_i – *i*th user identifier; PC_j – *j*th workstation identifier [8].

It is seen from fig. 1, that the method using the iterative hash construction, which allows to keep at the server the hash value of user authentication factors (such as his password) without storing key used for the hashing process. Further hashing of *j*th workstation parameters guarantees coincidence of hash value yielded by user and server. For reduction of server computational resources usage it is proposed to execute the process of workstations parameters hashing after they are inserted into the database and their storing in the same way as other database content.

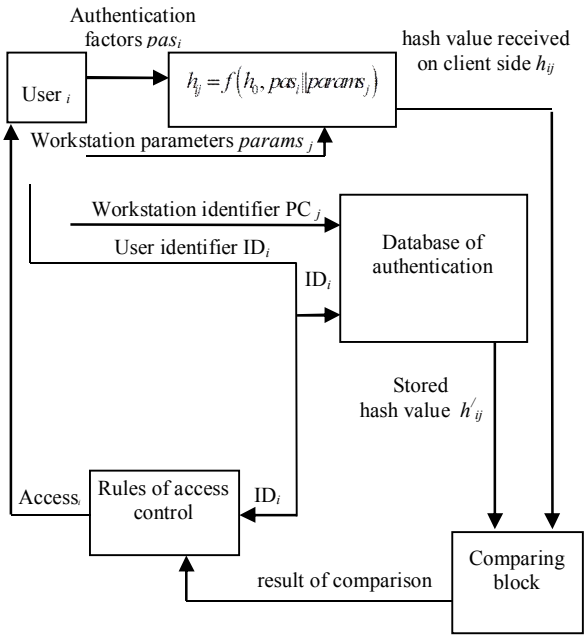

Fig. 1. Scheme of user authorisation

The method is based on the discretionary access control model. But the proposed approach of the workstations involvement into the authentication process could be applied to the all access control models, which were analysed above in this work.

In particular a discretionary model on the basis of access matrix after approach application would change in the following way: instead of two-dimensional matrix, a three-measurable matrix is to be used. Thus there are the dimension for subjects properties, the dimension – for user authentication factors and one – for workstation authentication factors.

For this user authentication method the scheme of the authentication system was developed, which implements access control model for distributed informational resources, those are stored remotely from the used workstation. An user sends his registration data to the hashing block on the client side. Then the hash value yielding is performed on the basis of user authentication factors and parameters of the workstation. The workstation identifier is sent to the server. On the server side it workstation parameters hashing is performed using the user authentication factors hash value as a key for the hashing process. If received from user hash value match the yielded one the authentication is considered to be successful and the user authentication – to be completed. Otherwise parameters of the next workstation allowed to be used be the user for accessing the informational resource are hashed.

On figure 2 the scheme of client side of the authentication system is presented.

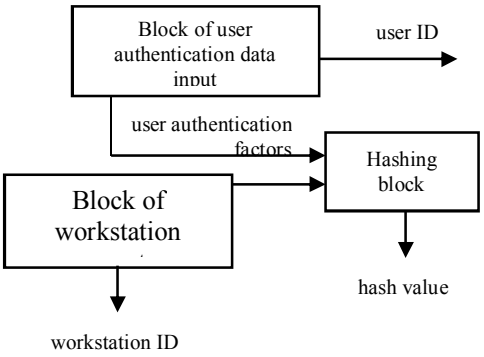

Fig. 2. The scheme of client side of the authentication system

The side of server of the system is shown on figure 3.

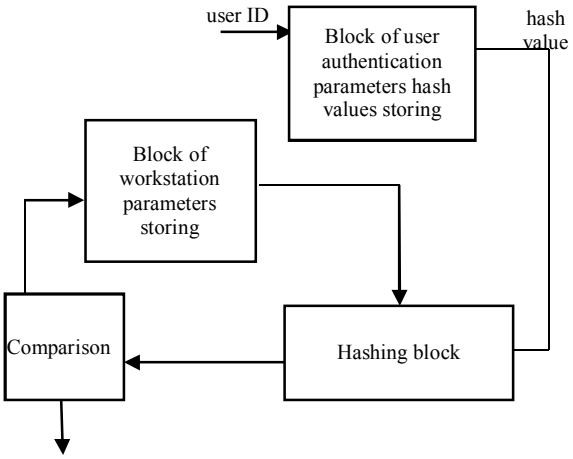

Fig. 3. The scheme of server side of the authentication system

The user authentication is performed in the following way. On side of the client user enters his identifier and authentication factors. The latter is concatenated with workstation parameters, the list of which was presented with the previous analyses results. The concatenation result is hashed using secret key known to user only. The hashing result is sent to the server as well as workstation identifier and user identifier.

The server side using received user identifier the hash value of the user authentication factors is determined by the means of the respective block. Parameters of the first workstation allowed for user to be used are yielded from the block of workstation parameters storing. Using the hashing block the server performs hashing of the parameters using the output of the clock of user authentication parameters hash values storing as a key.

The yielded hash value is compared with the received one. If they match the user is allowed to get access. Otherwise the next workstation parameters would be hashed at the next iteration. If there is no next workstation parameters stored at the respective block the access is denied for the user.

The proposed access control method could be used for other types of access control model (mandatory or role-based ones). The system is also quite flexible to the change of user authentication factors type, because if caused respective change of the user software/hardware platform without altering server. The latter is essential for the remote access granting information systems.

V. CONCLUSIONS

According to the performed analysis of access control models the number of tasks, for those it is important to limit the list of the workstations from which the user can get access to the critical information resources, were determined. As the result of access control system analyses the access control model, which allows to reach the research goal, was found. The method of remote users authentication and structure of the access control system, those due to the iterativeness of hashing process allow to execute users binding to the workstations, were performed for the implementation of the selected access control model. The method is planned to be used for the file server access control system.

REFERENCES

[1] П.Н. Девянин, Модели безопасности компьютерных систем. – М.: Издательский центр «Академия», 2005. – 144 с.

[2] Теория и практика обеспечения безопасного доступа к информационным ресурсам. Учебное пособие для вузов / А. А. Афанасьев, Л. Т. Веденьев, А. А. Воронцов и др.; Под ред. А. А. Шелупанова, С. Л. Груздева. – М.: Горячая линия – Телеком, 2009. – 552 с.

[3] В. А. Лужецький, Основи інформаційної безпеки : навчальний посібник / В. А. Лужецький, А. Д. Кожухівський, О. П. Войтович. – Вінниця: ВНТУ, 2013. – 221 с.

[4] В. В. Жора, Підхід до моделювання рольової політики безпеки *Правове нормативне та метрологічне забезпечення систем захисту інформації в Україн*.– 2003, Вип. 7 – С. 45–49

[5] Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам. Учебное пособие для вузов. / А. А. Афанасьев, Л. Т. Веденьев, А. А. Воронцов и др.; Под ред. А. А. Шелупанова, С. Л. Груздева, Ю. С. Нахаева. – М. : Горячая линия-Телеком, 2009. – 552 с.

[6] В. Г. Миронова, А. А. Шелупанов, Н. Т. Югов, Реализация модели Take-Grant как представление систем разграничения прав доступа в помещениях *Доклады ТУСУРа*. – 2011. – № 2 (24). – С. 206– 210.

[7] Ю. В. Баришев, В. А. Каплун, Метод автентифікації віддалених користувачів для мережевих сервісів. *Інформаційні технологій та комп'ютерна інженерія*. – 2014. – №2. – С. 13-17.

[8] Ю. В. Баришев, К. В. Неуйміна, Метод розмежування прав доступу з прив'язкою до робочої станції. *Науково-технічна конференція факультету інформаційних технологій та комп'ютерної інженерії,* 2017 – https://conferences.vntu.edu.ua/index.php/all-fitki/all-fitki-2017/paper/view/2937/2501