ISSN: 2350-0328
International Journal of AdvancedResearch in Science, Engineering and Technology
Vol. 6, Issue 2, February 2019

Comparative Analysis of Information Security Models in Computer Networks

KadirovMirhusanMirpulatovich, TashmatovaShaxnozaSabirovna*, GaniyevaToxiraIrkinovna*, KurbonovaKabiraErkinovna*

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

ABSTRACT: The article is devoted to the problems of security of info-communication systems. The main ways to protect information during access control are considered. The features of the use of existing models of access control are considered. Both classical models of access control, and models intended for use in dynamic systems are considered. A comparative analysis of the disadvantages and advantages of access control models is made.

KEYWORDS: information security, access models, access control models, object, subject, HRU, RBAC, TBAC.

I. INTRODUCTION

In the context of the widespread use of computer technology for the organization of business documents, storage and transmission of confidential information, the problem of computer security comes to the fore. The statistics of unauthorized access facts (unauthorized access to information) shows that most modern information systems are quite vulnerable from a security point of view.

The solution of the problem of protecting information from unauthorized access in any information system is based on the implementation of control and delimitation of access rights of subjects to protected resources, first of all, to file objects, since they are intended to store the processed data. In this case, the subjects of access in the demarcation policy are the users identified by the accounts. The rules of access of subjects to objects are set, as a rule, in the form of an access matrix (a matrix representation is expedient from the point of view of the possibility of matrix transposition, which allows us to present two ways of defining a demarcation policy - subjects to objects or, conversely, to subjects objects). The primary purpose of defining access control in known methods of access control is an object, for example, a file object. Various objects (files), identified by their names in the file system, are assigned by the administrator to store various kinds of information processed by users, including information from different privacy categories.

To date, many models of access control have been developed, based on different paradigms (access matrix, roles, tasks, events, etc.), which is explained by the extensive nature of modern systems.

Below are some of the existing models of access control.

II. HARRISON-RUZZO-ULMAN ACCESS MATRIX MODEL

Harrison-Ruzzo-Ulman (HRW) [1, 2] is used to analyze security systems that implement a discretionary access control policy.

The model HRU uses the following notation:

O - many objects of the system;

S - many subjects of the system $(S \subseteq O)$;

R - a set of types of subjects' access rights to objects, for example, rights to read $(read)$, to write $(write)$, possession (own).

M - access matrix.

ISSN: 2350-0328
International Journal of AdvancedResearch in Science, Engineering and Technology
Vol. 6, Issue 2, February 2019

The functioning of the system is considered only in terms of changes in the access matrix. Possible changes are determined by six types of primitive operators, presented in Table. 1.2.

Tabl.1.2. Primitive HRU model operators

Primitive operator	The initial state $q=(S,O,M)$	Resultant state $q'=(S',O',M')$
"Make" right r to $M[s,o]$	$s\in S,$ $o\in O,$ $r\in R$	$S'=S,O'=O,M'[s,o]=M[s,o]\cup\{r\}$, for $(s',o')\neq(s,o)$ equality is fulfilled $M'[s',o']=M[s',o']$
"Delete" right r of $M[s,o]$	$s\in S,$ $o\in O,$ $r\in R$	$S'=S,O'=O,M'[s,o]=M[s,o]\setminus\{r\}$, for $(s',o')\neq(s,o)$ equality is fulfilled $M'[s',o']=M[s',o']$
"Create" a subject s'	$s'\notin O$	$S'=S\cup\{s'\},O'=O\cup\{s'\}$, for $(s,o)\in S\times O$ equality is fulfilled $M'[s,o]=M[s,o]$, for $o\in O'$ equality is fulfilled $M'[s',o]=\varnothing$, for $s\in S'$ equality is fulfilled $M'[s,s']=\varnothing$
"Create" a subject o'	$o'\notin O$	$S'=S,O'=O\cup\{o'\}$, for $(s,o)\in S\times O$ equality is fulfilled $M'[s,o]=M[s,o]$, for $s\notin S'$ equality is fulfilled $M'[s,o']=\varnothing$,
"Delete" the subject s'	$s'\notin S$	$S'=S\setminus\{s'\},O'=O\setminus\{s'\}$, for $(s,o)\in S'\times O'$ equality is fulfilled $M'[s,o]=M[s,o]$
"Delete" the subject o'	$o'\notin O,$ $o'\notin S$	$S'=S,O'=O\setminus\{o'\}$, for $(s,o)\in S'\times O'$ equality is fulfilled $M'[s,o]=M[s,o]$

As a result of the primitive operator α transition from state $q=(S,O,M)$ in the resultant state $q'=(S',O',M')$. This transition is denoted by $q\mapsto_{\alpha} q'$.

Primitive operators make up a finite number of commands of the HRW system. Each team includes two parts: 1) the conditions under which the command is executed; 2) a sequence of primitive operators.

Thus, the command entry is as follows:

$command\quad c(x_1,...,x_k)$

$if\,(r_1\in M[x_{s1},x_{o1}])and..and(r_m\in M[x_{sm},x_{om}])\quad then$

$\alpha_1;$

...

$\alpha_n;$

$endif$

$end,$

ISSN: 2350-0328
International Journal of AdvancedResearch in Science, Engineering and Technology
Vol. 6, Issue 2, February 2019

Where $r_1,..., r_m \in R$ - access rights; $\alpha_1,..., \alpha_n$ - a sequence of primitive operators whose parameters and conditions parameters are command parameters $x_1,..., x_\kappa$. It should be noted that the presence of a condition in the body of the team is not required.

III. BELL LAPADULA MODEL

In the classical model of Bella LaPadula, conditions are considered under which the occurrence of information flows from objects with a higher level of confidentiality to objects with a lower level of confidentiality is impossible in computer systems [3]. The main elements of the classic Bella LaPadula model are:

S - many subjects;

O - many objects;

R - many types of access and types of access rights;

$B = \{b \subseteq S \times O \times R\}$ - The set of possible sets of current accesses in the system.

$(L, \leq)$ - grid of privacy levels for example $L = \{U(unclussifed),\ C(confidental),\ S(\sec ret),\ TS(top\ \sec ret)\}$ where $U < C < S < TS$;

$M = \{m_{|S|\times|O|}\}$ - the set of possible access matrices, where $m_{|S|\times|O|}$ access matrix, $m[S,O] \subseteq R$ - access rights of the subject to the object S to the object O;

$(f_s, f_o, f_c) \in F = L^s \times L^o \times L^s$ three functions (f_s, f_o, f_c), assignments respectively: $f_s : S \to L$ - the level of access of subjects; $f_o : O \to L$ - object privacy level; $f_c : S \to L$ - current access level of subjects, for any $s \in S$ inequality holds $f_c(s) \leq f_s(s)$;

$V = B \times M \times F$ - multiple system states;

Q - many requests to the system;

D - multiple answers for requests, for example $D = \{yes, no, error\}$;

$W \subseteq Q \times D \times V \times V$ - set of system actions, where the four $(q, d, v^*, v) \in W$ means system on request q with the answer d passed from state v in state v^*;

$N_0 = \{0,1,2,...\}$ - set of time values;

X - set of time values; $x : N_0 \to Q$ specifying all possible sequences of requests to the system;

Y - many functions $y : N_0 \to D$, specifying all possible sequences of system responses for queries;

Z - many functions $z : N_0 \to V$, specifying all possible sequences of system states;

Definition. $\sum(Q, D, W, z_0) \subseteq X \times Y \times Z$ called a system when for each $(x, y, z) \in \sum(Q, D, W, z_0)$ condition: for $t \in N_0, (x_t, y_t, z_{t+1}, z_t) \in W$, where z_0 – initial state of the system. In addition, each set $(x, y, z) \in \sum(Q, D, W, z_0)$ called the system implementation, and $(x_t, y_t, z_{t+1}, z_t) \in W$ system action at time $t \in N_0$.

IV. RBACMODEL

The RBAC (Role-based Access Control) [4] model controls the access of subjects of the system to objects in accordance with a set of actions and responsibilities associated with a specific activity of the subjects. Such powers are semantic constructs called subject roles that underlie the access control model. Roles allow individuals to access objects to the extent they need to perform their duties.

The main elements of the basic RBAC model are:

ISSN: 2350-0328
International Journal of AdvancedResearch in Science, Engineering and Technology
Vol. 6, Issue 2, February 2019

U - many users;
R - many roles;
P - multiple access rights to computer system objects;
S - multiple user sessions;
$PA: R \to 2^P$ - a function that specifies a set of access rights for each role; in addition, for each access right $p \in P$ there is a role $r \in R$ such that $p \in PA(r)$;
$UA: U \to 2^R$ - a function that sets for each user a set of roles for which he can be authorized;
$user: S \to U$ - a function that sets for each user session, on behalf of which it is activated;
$roles: S \to 2^R$ - a function that sets the user a set of roles for which he is authorized in this session, at the same time for each session $s \in S$ condition is met $roles(s) \subseteq UA(user(s))$.

The RBAC model can be applied in systems with equal-valued objects, if for each role access rights are determined based on all possible combinations of using equivalent objects [5]. Thus, the roles will be formed in such a way that each of them provides access only to one of the equivalent objects of the group.For example, the subject s_2 may have the following access rights:

$$PA(r_1) = \{o_2, \ o_4\} \times use$$

$$PA(r_2) = \{o_2, \ o_7\} \times use$$

$$PA(r_3) = \{o_5, \ o_4\} \times use$$

$$PA(r_4) = \{o_5, \ o_7\} \times use,$$

where $\{r_1, r_2, r_3, r_4\}$ many roles that a user can log in to s_2.

The RBAC model makes it possible to distinguish between access of subjects in the system relative to the tasks they perform separately, and at the same time provides tools for differentiating access to equivalent objects. Moreover, user access rights in the system are not permanent and may vary depending on which role the user has authorized. Note the following disadvantages of using RBAC:

- the decision on which of the roles available to the user will be authorized is taken by the user himself.

- the number of defined roles increases significantly compared with the actual number of functional responsibilities of the user in the system. For example, user s_2 performs only one function in the system - problem solving. However, in order to minimize his rights, four roles are defined for him. If denoted by $G_t = \{g_{t_i}^1, g_{t_i}^2, ..., g_{t_i}^m\} \subseteq G$ a set of groups of equivalent objects to which the system user must have access to solve the problem t_i, then the total number of roles to be defined can be written as

$$\sum_{i=1}^{|T|} \prod_{j=1}^{|G_{t_i}|} \left| g_{t_i}^j \right| \qquad (1.1)$$

- the procedures for administering the security system are complicated, both at the stage of its formation and when making changes. This disadvantage is a consequence of the previous one. It is obvious that in real systems with a large number of tasks the number of defined roles will be quite large. In turn, this can lead to errors, an increase in the number of vulnerabilities, etc., which adversely affects the security system.

V. TBAC MODEL

At the heart of the Task-based Authorization Controls (TBAC) model [6] is the notion of "task". User access rights are changed taking into account the specifics of the task being performed for which it is currently authorized, which provides dynamic access control. Thus, the access rights of subjects in the system are provided depending on the

ISSN: 2350-0328
International Journal of AdvancedResearch in Science, Engineering and Technology
Vol. 6, Issue 2, February 2019

context of the task are not permanent. Permissions are granted and revoked for each task separately. TBAC defines access rights as $P \subseteq S \times O \times A \times U \times AS$.

Let us apply the TBAC model in systems with equal-valued objects. We have the following items:

$S = \{s_1, s_2, s_3\}$ - many subjects;

$O = \{o_1, o_2, ..., o_7\}$ - many objects;

$A = \{use\}$ - many types of subjects' access rights to objects;

$AS = \{as_1, as_2, ..., as_{16}\}$ - multiple authorization steps.

M - access matrix, the rows of which correspond to the authorization steps, and the columns correspond to the objects. $M[as, o] \subseteq A$ access rights of the subject that passed the authorization stage as, to the object o.

$SAS : S \to 2^{AS}$ a function that sets for each subject a subset of the authorization steps that he can pass.

In TBAC, each access right is given to subjects for a period of time. We assume that for any access right this value is constant, so it will not be taken into account in the further presentation.

Then the state of the system in TBAC with regard to auxiliary elements can be written as $P \subseteq S \times O \times M \times AS \times SAS$ [5].

We define the function values as follows.:

$SAS(s_1) = \{as_1, as_2, ..., as_6\}$

$SAS(s_2) = \{as_7, as_8, as_9, as_{10}\}$

$SAS(s_3) = \{as_{11}, as_{12}, ..., as_{16}\}$

Set the Access Control Matrix M :

	o_1	o_2	o_3	o_4	o_5	o_6	o_7
as_1	use			use			
as_2	use						use
as_3			use	use			
as_4			use				use
as_5				use		use	
as_6						use	use
as_7		use		use			
as_8		use					use
as_9				use	use		
as_{10}					use		use
as_{11}	use	use					
as_{12}	use				use		
as_{13}		use	use				
as_{14}			use		use		
as_{15}		use				use	
as_{16}					use	use	

In this case, each task from T is divided into several tasks in the system, each of which corresponds to its own authorization stage. In this case, the subject S_1 can be authenticated to the six stages defined by the SAS function, each of which represents a task $task_1$. For each stage of authorization access matrix$M$defined access rights in the system for

ISSN: 2350-0328
International Journal of AdvancedResearch in Science, Engineering and Technology
Vol. 6, Issue 2, February 2019

the subject who passed it. In this case, access rights in *M*are set so that the subject has access to only one object from the group.

VI. RESULT

On the basis of the comparative analysis carried out, general weaknesses and advantages of security models are highlighted. The result of the comparison of access control models is given in Table 1.1.

Tab. 1.1. Comparative analysis of the disadvantages and advantages of access control models

Model	Benefits	Disadvantage
Harrison-Ruzzo-Ulman model	- Prostate and visibility, since this model does not require complex algorithms. - Efficiency in management, as it is possible to manage user rights with an accuracy of the operation. - Strongsafetycriteria.	- There is no security check algorithm for an arbitrary system. - Vulnerability to attack using a Trojan horse, since in this model there is no control over the flow of information between subjects. - Subject is granted insufficient access rights. - The set of access rights of the subject is static. Regardless of what task the subject performs in the system, the set of his access rights remains constant.
Bell LaPadula model	- Ease of administration. - The access entity can only access objects from which the level of secrecy is not lower than the level of secrecy of the subject. - The subject does not have the right to write information into an object with a level of secrecy lower than the level of the subject.	- Problem in distributed systems - remote reading. - The problem of trusted subjects. - declassification of the object. - Hard classification systems for security levels.
RBAC model	- Widely used to manage user privileges within a single system or application. - The formation of roles is designed to define clear and understandable for users of the computer system access control rules. - Allows you to implement flexible, changing dynamically in the process of functioning of the computer systemaccess control rules.	- The decision on which of the roles available to the user will be authorized is taken by the user himself. - Significantly increases the number of defined roles, compared with the actual number of functional responsibilities of the user in the system. - Complicated security administration procedures, both at the stage of its formation, and when making changes.
TBAC model	- In accordance with the definitions of the model, the access rights of the subjects of the system are differentiated in accordance with the tasks that they perform separately. - The rights of subjects in the system are not permanent and are granted only for the time they perform the assigned task. - The model allows you to implement access control to equivalent objects of the system by adding several authorization steps for tasks.	- Administering security policies with this approach is difficult. - The need to include contextual parameters in security considerations. - It is limited to contexts related to actions, tasks and implemented by tracking the use and validity of permissions. - Permissions are activated and deactivated on time.

VII. CONCLUSION AND FUTURE WORK

The possibilities of enhancing security were studied. Based on the analysis and research of information security models against unauthorized access, it was revealed that it is necessary to develop new methods, modified access control models that ensure high system security.

ISSN: 2350-0328

International Journal of AdvancedResearch in Science, Engineering and Technology

Vol. 6, Issue 2, February 2019

REFERENCES

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

[2] Harrison M., Ruzzo W., Ullman J. Protection in Operating Systems // Commun. ACM. _New York, 1976. _ V. 19, №8.

[3] Bell D., LaPadula L. Secure Computer Systems: Uni_ed Exposition and Multics Interpretation // Bedford, Mass. MITRE Corp. 1976. MTR 2997. Rev. 1.

[4] D.F.Ferraiolo, D.Kuhn, and R.Chandramouli. Role-Based Access Control. ArtechHouse, 2ndedition, 2010.

[5] Лапин С. А. Сравнительный анализ использования существующих моделей разграничения доступа в системах, обладающих равнозначными объектами //Известия Алтайского государственного университета. – 2016. – №. 1 (89).

[6] S.Oh, S.Park. Task–role-based access control model. Information Systems 28 (2013) pp.533-562, 2013.

ISSN: 2350-0328

International Journal of AdvancedResearch in Science, Engineering and Technology

Vol. 6, Issue 2, February 2019

KadirovMirhusanMirpulatovich. Assistant professor.
was born May 22, 1985 year in Tashkent city, Republic of Uzbekistan.
Has more than 80 published scientific works in the form of articles, journals, theses and tutorials. Currently works at the department of "Information technologies" in Tashkent State Technical University.

TashmatovaShaxnozaSabirovna.Senior Lecturer.
was born july06, 1957 year in Tashkent city, Republic of Uzbekistan. Has more than 20 published scientific works in the form of articles, journals, theses and tutorials. Currently works at the department of "Information technologies" in Tashkent State Technical University.

GaniyevaToxiraIrkinovna.Senior Lecturer.
was born july21, 1962 year in Tashkent city, Republic of Uzbekistan. Has more than 10 published scientific works in the form of articles, journals, theses and tutorials. Currently works at the department of "Information technologies" in Tashkent State Technical University.

KurbonovaKabiraErkinovna.Senior Lecturer.
was born july21, 1962 year in Tashkent city, Republic of Uzbekistan. Has more than 10 published scientific works in the form of articles, journals, theses and tutorials. Currently works at the department of "Information technologies" in Tashkent State Technical University.