Methodology for Developing a Mandatory Security Policy Based on Two Value Chains

Kadirov Mirhusan Mirpulatovich,Tojikhujaeva Nodirakhon Zakirovna, Kasimova Gulnora Ismoilovna, Usmanbayev Doniyorbek Shuxratovich

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

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

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

Intern teacher, Tashkent University of Information Technologies named after Muhammad al-Khwarizmi, Tashkent, Uzbekistan

ABSTRACT: This article discusses the combination of two mandatory security policies. The need to combine two mandatory security policies may arise in systems that require confidentiality and integrity of information at the same time. Confidentiality, or the impossibility of leakage of high-level information to low-level users, is guaranteed when the flow of information is prohibited from top to bottom, that is, the level of trust of the subject should dominate the level of confidentiality of the object in the value grid.

KEYWORDS: access, privacy, information leakage, user, security policy, consolidation of credential policies, value grid, security labels

I. INTRODUCTION

Integrity is guaranteed if only those accesses are allowed in which the level of the subject is not higher than the level of the object in the value grid. Thus, attempts to ensure confidentiality and integrity at the same time on the same value grid leads to conflicting rules. As a result, it is possible to transfer information only at one level and the inability to exchange data with subjects with different levels of authority [1, 4, 7].

This contradiction is usually resolved through the introduction of two value chains - one to ensure confidentiality, the other to ensure integrity. At the same time, the task of administering the system becomes very time-consuming, since each access is checked according to two independent rules. The challenge is to build a unified lattice of values, which ensures the feasibility of both security policies, so that with each access only one condition is checked [2, 9].

II. FORMULATION OF THE PROBLEM

The simplest solution to the problem is to build a single lattice of organization values as a Cartesian product of department lattices[2, 3, 5, 6, 8, 10]:

$$L_1 \times L_2$$

With this approach, each object in the system will be characterized by a pair of security labels(m_1, m_2) $(m_1 \in L_1, m_2 \in L_2)$.

Let a linear lattice of values act in the department $D_1 L_1 = a_1, a_2, a_3, a_4$ with four security levels$(a_1 < a_2 < a_3 < a_4)$.

In the second section of D_2, let a linear lattice of values act$L_1 = b_1, b_2, b_{3,}, b_{4,}$c with four security levels$(b_1 < b_2 < b_3 < b_4)$ (fig .1.1).

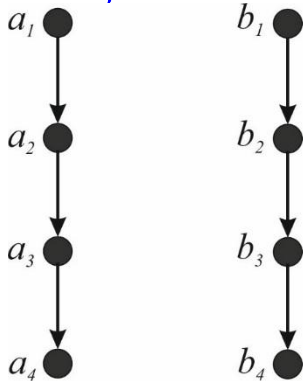

Fig. 1.1. Linear Value Grid

Figure 1.2 shows the resulting security lattice of an integrated organization that will have 16 security labels.

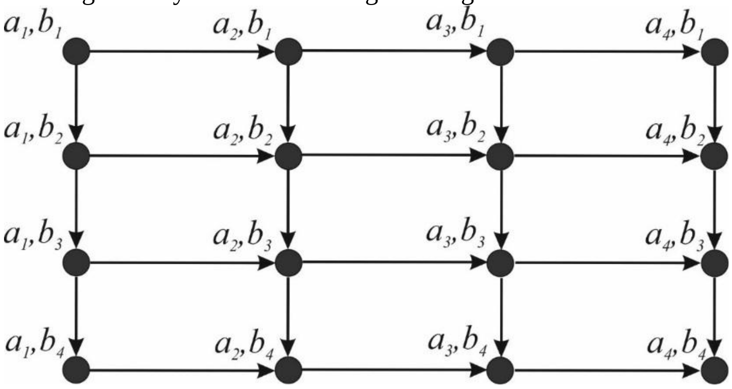

Figure 1.2. Combined Organization Security Grid

If the security label of the message from the lattice L_1 of department $D_1$is not included in the lattice D_2, then this means that no subject of the department D_2 can read such a message until they are given appropriate access, that is, a new security label from the Cartesian product of the lattices $L_1 \times L_2$.

At the same time, a situation arises where there may be a lack of exchange between some entities from different departments, which means that none of the new security labels obtained from the Cartesian product of lattices is suitable for them. Otherwise, an information leak will occur, since the lowest level a_4, b_4in the resulting new lattice assumes access to the information of each of the departments. In order to avoid this situation, it is necessary to supplement the new security lattice with additional security levels, which will be the sublattices of the new lattice and simulate the work of each of the departments before merging. For this, it is necessary to introduce an elementary transformation that will complement any lattice with an empty element, or a zero element. Returning to our example, the value grid L_1will remain linear, but the minimum element will be not $a_4, a\{0\}$. Similar considerations can be applied to the lattice L_2. As a result, we obtain the lattices $L_1 \cup \{0\} = L_1^{\emptyset} and\ L_2 \cup \{0\} = L_2^{\emptyset}$(Fig. 1.3).

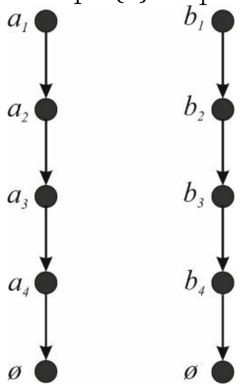

Fig.1.3. Grilles$L_1 \cup \{0\} = L_1^{\emptyset} and\ L_2 \cup \{0\} = L_2^{\emptyset}$

If the value lattice is not linear, then, by the definition of the lattice, for any two elements there is the least exact lower bound, that is, in any lattice there is the smallest element. This means that you can add an empty element, and the properties of the lattice are not violated. Figure 3.4 shows the complement of a nonlinear lattice with a zero element. The construction of a single lattice from the two we obtained by adding an empty element can also be carried out using the Cartesian product $L^{\emptyset} = L_1^{\emptyset} \times L_2^{\emptyset}$ [2].

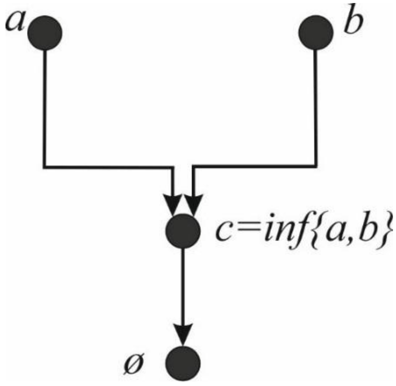

Figure 1.4. Non-linear lattice additions with a zero element

III. INTEGRATED SYSTEMS SECURITY GRID

With this approach, the resulting lattice, the diagram of which is shown in Fig. 1.5, will consist of 25 elements. Moreover, it can be noted that the 25 elements of the lattice $L^{\emptyset}$that form the sublattice are exactly the lattice, the diagram of which is shown in Fig. 1.2. We can say that the lattice $L = L_1 \times L_2$ is a tool for ensuring information exchange between departments D_1 and D_2, and this information exchange will be safe, since there is a special level of security for each type of interaction. In addition, in the lattice $L^{\emptyset}$one can also distinguish 2 more sublattices, each of which will imitate the work of departments without information exchange. The lattice diagram $L^{\emptyset}$ is shown in Fig. 1.5.

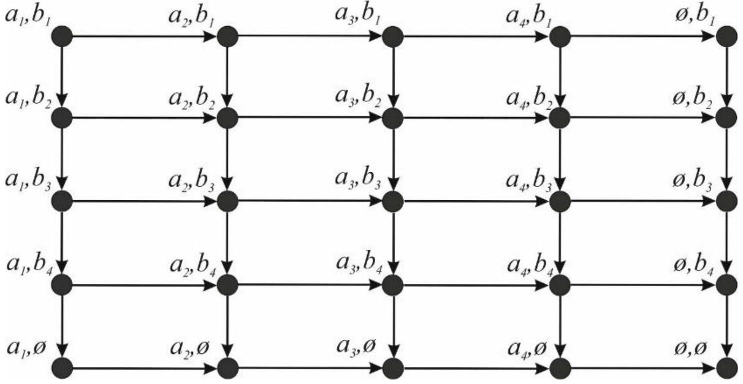

Figure 1.5. Integrated Systems Security Grid

To build a mandatory security policy of two departments or organizations on the basis of mandatory security policies of each of the departments and for the secure information exchange between them, the following steps must be performed:

1) Supplement the mandatory security policy of each of the departments with an empty element, i.e. Enter a security label that does not give any authority or privilege. In this case, the set of security labels will remain a lattice.

2) Get the Cartesian product of two lattices, i.e. iterate over all possible pairs of security labels from two departments, while each pair includes one label from each department. Since the Cartesian product of lattices is a lattice, it is possible to construct a mandatory security policy on the resulting set of pairs of vertices, while the resulting policy will perform both secure information exchange within each department (thanks to empty labels) and secure information exchange between the two departments.

3) Construct a partial order relation between label pairs according to the following rule: $\forall \mathrm{a}_1, \mathrm{a}_2 \in \mathrm{L}_1, \mathrm{b}_1, \mathrm{b}_2 \in \mathrm{L}_2$ pair $(\mathrm{a}_1, \mathrm{b}_1) \geq (\mathrm{a}_2, \mathrm{b}_2) \leftrightarrow \mathrm{a}_1 \geq \mathrm{a}_2$ and $\mathrm{b}_1 \geq \mathrm{b}_2$,, where $\mathrm{L}_1, \mathrm{L}_2$ are the sets of labels in the first and second

departments, respectively (the lattices of the departments D_1 and D_2). In this case, the partial order relation is preserved for the sublattices corresponding to the lattices L_1 and L_2.

4) Assign the necessary labels to users and resources. In this case, if the document is not involved in the information exchange between departments, one of the labels forming a pair will be empty. If the document participates in the information exchange, then the empty label will not fall into a couple of labels for this document.

IV. RESULT

The use of this method increased the efficiency of the system. Unlike the classic mandatory credential models, combining the two credential security policies is effective. Obtaining results are shown in Figure 1.6.

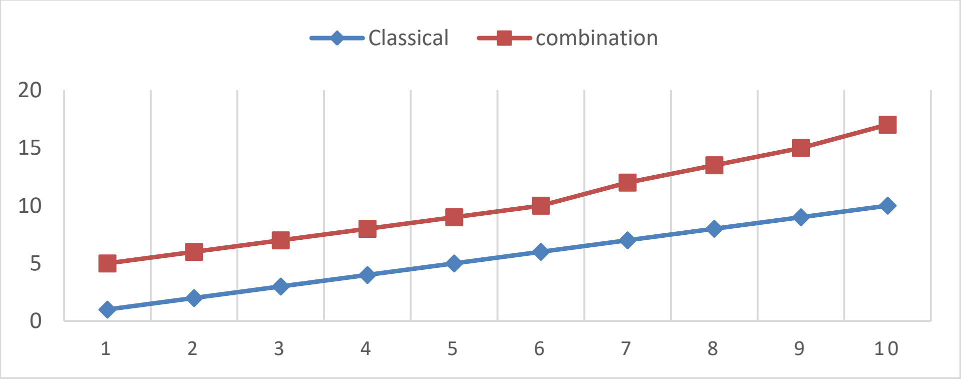

Figure 1.6.System performance when using security policies

V. CONCLUSION AND FUTURE WORK

A technique is proposed for constructing a common mandatory security policy for an organization with no information leaks, consistently including all mandatory security policies for departments, if several organizations are combined into a single corporation. The algorithm is based on the Cartesian product of lattices defining mandatory security policies of organizations.

REFERENCES

[1] Rakitskiy, Yu. S., Belim, S. V.,“Model sovmesheniyadvuxmandatnixpolitikbezopasnosti”, Bezopasnostinformatsionnixtexnologiy,Vol.18(1). pp.125-126, 2011.

[2] Belim, S. V., Rakitskiy, Yu. S.,“Ob’edineniemandatnixpolitikbezopasnosti”, Matematicheskiestrukturiimodelirovanie, Vol.21, pp. 128-132, 2010.

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

[4] Birkgof, G.,“Teoriyareshetok”,Nauka,Glavnayaredaktsiyafiziko-matematicheskoyliteraturi, pp.586, 1984.

[5] Grettser, G.,“Obshayateoriyareshetok”, Mir, pp.320, 1981.

[6] Kristofides, N.,“Teoriyagrafov”,Algoritmicheskiypodxod, Mir, pp.432, 1978.

[7] Gaydamakin, H.A.,“Razgranicheniedostupa k informatsii v kompyuternixsistemax”, IzdatelstvoUralskogoUniversiteta, pp.328, 2003.

[8] Sheglov,A.Yu.,“Zashitakompyuternoyinformatsiiotnesanktsionirovannogodostupa”, Naukaitexnika, pp. 384, 2004.

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

[10] Devyanin, P. N.,“Modelibezopasnostikompyuternixsistem. Upravleniedostupomiinformatsionnimipotokami”,Uchebnoeposobie,Goryachayaliniya-Telekom, pp.320, 2012

AUTHOR'S BIOGRAPHY

Kadirov Mirhusan Mirpulatovich. Assistant professor.
was born May 22, 1985 year in Tashkent city, Republic of Uzbekistan.
Has more than 90 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.

Tojikhujaeva Nodirakhon Zakirovna.Senior Lecturer.
was born February14, 1977 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.

Kasimova Gulnora Ismoilovna, Assistant.
was born May30, 1989 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.

Usmanbayev Doniyorbek Shuxratovich.
Currently works at the department of "Information security provision" in Tashkent University of Information Technologies named after Muhammad al-Khwarizmi.