Application-Oriented Confidentiality and Integrity Dynamic Union Security Model Based on MLS Policy*

Mingfu XUE††, Aiqun HU†, Nonmembers, and Chunlong HE†††, Student Member

SUMMARY We propose a new security model based on MLS Policy to achieve a better security performance on confidentiality, integrity and availability. First, it realizes a combination of BLP model and Biba model through a two-dimensional independent adjustment of integrity and confidentiality. And, the subject’s access range is adjusted dynamically according to the security label of related objects and the subject’s access history. Second, the security level of the trusted subject is extended to writing and reading privilege range respectively, following the principle of least privilege. Third, it adjusts the objects’ security levels after adding confidential information to prevent the information disclosure. Fourth, it uses application-oriented logic to protect specific applications to avoid the degradation of security levels. Thus, it can ensure certain applications operate smoothly. Lastly, examples are presented to show the effectiveness and usability of the proposed model.

key words: Multi-Level Security policy, security model, confidentiality and integrity, least privilege, application-oriented logic

1. Introduction

Research on security models is an important part of the development of secure system. Confidentiality, integrity, and availability are three important characteristics which must be considered in designing a high-level security system. Bell-LaPadula model [1] (BLP model) is a classical model of MLS confidentiality policies. In the past 40 years, it has been widely used and has a variety of improvements. In order to achieve the “least privilege” control, Bell first proposed the idea of using a range of sensitive level to limit the trusted subject’s authority [2]. Subsequently, multi-level subject has been proposed similarly, and the famous TMach project, Fluke project, SELinux project and later studies followed this idea. In BLP model, sensitivity labels of subjects and objects are fixed. This stable principle limits its flexibility for wide application. To solve this, new rules are introduced to make the current security levels of subjects can adjust dynamically [3].

The integrity security which is missing in BLP model is also not involved in the above models. Biba model is an other important access control policy which is designed to ensure data integrity [4]. In order to achieve a combination of confidentiality and integrity, many researches were carried out. In the ASOS system [5], a confidentiality marker \( \lambda \) and an integrity mark \( w \) together constitute the access label, while the BLP model and the Biba model are applied to \( \lambda \) and \( w \) respectively. However, this simple combination of such rules may cause that legal requirements of resource access are denied. Yihe Liu gives an integrated scheme of BLP and Biba model using the formula \( C = \alpha T(N) - \beta I(N) \) to calculate the security levels [6]. In which, \( \alpha, \beta \) indicates the user’s degree of concern on confidentiality and integrity respectively. In fact, the confidentiality and integrity are two different security features with different connotations and grades, and they can’t be simply marked by a function. Cai Yi et al proposed a planar attributes model. In their model, confidentiality label and reliability label constitute the access label of an object [7]. Shen Ying proposed an lattice based BLP extended model, in which, the linear order trust level is used as integrity component [8]. But these models lack of appropriate description on how trust subject improves the credibility of an object and how to grant access rights. Zhang Jun et al proposed a dynamic unified model of confidentiality and integrity through dynamically adjusting subjects’ security labels [9]. However, the security labels are not recoverable once they are adjusted.

In general, the confidentiality level and integrity level of subjects or objects are consistent. Since the information flows of BLP model and BIBA model are opposite, a simple combination of them, will lead to poor availability of the system. Furthermore, all of the above models do not consider the adjustment of the objects’ security levels. So there may be a risk of information disclosure when confidential information is added to an object. What’s more, the above models are not transparent to applications. There may be an “authority shrink” phenomenon after dynamical adjustments. In other words, the range of the read and write authority of a subject is shrinking. And finally the subject can only read and write objects with specific security levels, thus certain applications will be affected. Based on the above analysis, this paper proposes an application-oriented confidentiality and integrity dynamic union model (ADUM) based on Multi-Level Security (MLS) Policy.

Our main contributions are as follows. First, the two independent dimensions of this model are confidentiality and integrity. And the subject’s access range is adjusted dynamically according to the security labels of related objects and...
the subject’s access history. Through this method, we can provide confidentiality and integrity to the system simultaneously. Thus, a combination of BLP model and Biba model is realized. Second, the security level of the trusted subject is extended to writing and reading privilege range respectively, so as to control the trusted subject’s authority. Third, in order to avoid the information disclosure after adding confidentiality information to an object, we adjust the object’s security level according to the added information’s confidentiality. Fourth, the degradation of security levels may occur after dynamic adjustments of security identities, which prevents some applications from operating successfully. To solve this problem, we propose an application-oriented logic configuration arbitration rule. And it also improves security by eliminating the risks of several covert channels effectively.

2. ADUM Model

2.1 Model Elements

We give the following definitions referring to the literature [1], [3], [4], [9], [10].

**Definition 1**: S denotes the set of subjects, ST denotes the set of trusted subjects. S’ denotes the non-trusted subjects, while S’ = S − ST. O denotes the set of objects.

**Definition 2**: A denotes the set of access methods. A = {r, a, w, e}. r: observation with no alteration. a: alteration with no observation. w: both observation and alteration. e: neither observation nor alteration.

**Definition 3**: The subset of (S × O × A) is denoted B, which is called current access set. Mij records the modes in which subject Sj is permitted to access object Oj. M = (Mij) is the access matrix. H denotes the set of objects’ hierarchy.

**Definition 4**: rq(Si, Oj, A) denotes Sj’s x-operation access request on the object Oj. The model notation for a state is V = {(b, m, f, h)|b ∈ B, m ∈ M, f ∈ F, h ∈ H}.

**Definition 5**: LC = {(c, k)|c ∈ C, k ∈ KC} denotes the set of confidentiality marks. In which, C denotes the set of confidentiality level classification, and KC denotes the set of confidentiality category. Ll = {(i, k)|i ∈ I, k ∈ KI} denotes the set of integrity marks. In which, I denotes the set of integrity level classification, and KI denotes the set of integrity category.

**Definition 6**: The set of security marks function is denoted F. F = {fs, fcs, fco, fis, fio}. In which, fs denotes the maximum confidentiality function of a subject. Similarly, fcs and fis denote the current confidentiality function of a subject and the current integrity function of a subject. fco and fio denote the current confidentiality function and the current integrity function of an object.

**Definition 7**: The security identity of a model consists of confidentiality identity and integrity identity. The set of security identity is denoted SL. SL = {(lci, li)|lci ∈ LC, li ∈ LI}.

**Definition 8**: There are four referenced variables in the life cycle of a subject: CRH ∈ LC, CWL ∈ LC, IRL ∈ LI, IWH ∈ LI. CRH: the highest confidentiality identity of objects a subject has read. CWL: the lowest confidentiality identity of objects a subject has written. IRL: the lowest integrity identity of objects a subject has read. IWH: the highest integrity identity of objects a subject has written.

**Definition 9**: The scope of a subject’s confidentiality marks is denoted ranTC = [CRH, CWL], while the scope of a subject’s integrity marks is denoted ranTI = [IRL, IWH].

2.2 The Model Rules and State Transitions

Table 1 shows the requirements of BLP model and Biba model on the sensitivity label function. Partially referring the description of [1], [3], [4], [9], [10], we give the decisions of access authorization and dynamic adjustment rules of sensitive labels.

**Rule 1**: ("Read Rule"): In (b, m, f, h) state, r ∈ Mij, the treatment to rq(s, o, r) is as follows:

| Operation | BLP model’s requirements | Biba model’s requirements |
|-----------|--------------------------|---------------------------|
| r         | fcs ≥ fco                | fis ≤ fio                |
| a         | fcs ≤ fco                | fis ≥ fio                |
| w         | fcs = fco                | fis = fio                |

Table 1: The requirements of BLP model and Biba model on sensitivity label function.

In “Read rule”, if the sensitivity labels of subjects and objects meet the requirements of BLP and Biba model simultaneously, the direct authorization to operations and adjustment of the access historical labels will be performed. Otherwise, we can appropriately adjust the subjects’ current security labels to meet the access requirements on the premise of certain conditions. fcs(s) is adjusted to the least upper bound of fcs(s) and fco(o), while fis(s) is adjusted to the greatest lower bound of fis(s) and fio(o). And after reading operations, the CRH(s) is adjusted to the least upper bound of CRH(s) and fco(o), while the IRL(s) is adjusted to the greatest lower bound of fio(o) and IRL(s). These adjustments can ensure that after reading an object, the subject can’t write objects with lower integrity level. Thus, this rule can ensure the confidentiality of a system by preventing the high-level confidentiality information flow to low confidentiality level objects (If it is a writing operation, we adjust CWL and IWH after operations to ensure integrity). The “Write rule” and the “Read-Write rule” are similar.
Rule 2: (“Write Rule”): In \((b,m,f,h)\) state, \(a \in M_{ij}\), the treatment to \(rq(s,o,a)\) is as follows:
If \(f_{CO}(o) \geq f_{CS}(s)\&\& f_{IS}(s) \geq f_{IO}(o)\), Then
(1) Structure \(F^*\), so \(F^* = F\);
(2) \(C_{RH}(s) = f_{CO}(o)\), \(C_{WL}(s) = MIN(f_{CO}(o), f_{WL}(s)), \)
\(I_{WL}(s) = I_{WL}(s), I_{WH}(s) = MAX(f_{IO}(o), I_{WH}(s));\)
(3) Authorize to \(rq(s,o,a)\). Structure \(b^*\), so \(b^* = b \cup (s,o,a)\).
Get into the state of \((b^*, m, f^*, h)\).
Else If \((f_3(s) \geq f_{CO}(o))\&\& f_{CO}(o) \geq C_{RH}(s)\&\& I_{WL}(s) \geq f_{IO}(o)\), Then
(1) Structure \(F^*\), so \(f_3(s) = f_{CO}(o), f_{CS}(s) = MIN(f_{CS}(s), f_{CO}(o)), f_{IO}(o) = MAX(f_{IO}(s), f_{IO}(o)), f_{IO}(o) = f_{IO}(o)\);
(2) The same as (2),(3) above.
Else Refuse \(rq(s,o,a)\).

Rule 3: (“Read-Write Rule”): In \((b,m,f,h)\) state, \(w \in M_{ij}\), the treatment to \(rq(s,o,w)\) is as follows:
If \(f_{CO}(o) = f_{CS}(s)\&\& f_{IS}(s) = f_{IO}(o)\), Then
(1) Structure \(F^*\), so \(F^* = F\);
(2) \(C_{RH}(s) = MAX(C_{RH}(s), f_{CO}(o)), C_{WL}(s) = MIN(f_{CO}(o), C_{WL}(s)), I_{WL}(s) = MIN(I_{WL}(s), f_{IO}(o)), I_{WH}(s) = MAX(f_{IO}(s), I_{WH}(s));\)
(3) Authorize to \(rq(s,o,w)\). Structure \(b^*\), so \(b^* = b \cup (s,o,w)\).
Get into the state of \((b^*, m, f^*, h)\).
Else If \((f_3(s) \geq f_{CO}(o))\&\& f_{CO}(o) \geq C_{RH}(s)\&\& C_{WL}(s) \geq f_{CO}(o) \&\& I_{WL}(s) \geq f_{IO}(o))\), Then
(1) Structure \(F^*\), so \(f_3(s) = f_{CO}(o), f_{CS}(s) = f_{CO}(o), f_{IO}(o) = f_{IO}(o), f_{IO}(o) = f_{IO}(o)\);
(2) The same as (2),(3) above.
Else Refuse \(rq(s,o,w)\).

From the above three rules, we can see the flow of information depends on the dominance relations between a subject’s seven marks and an object’s two marks. The dynamic changes of a subject's marks depend on its access history and the adjustment of permissions.

The rights restriction and conversion rules of the trusted subject are as follows.

Rule 4: (“The trusted subject rule”): \(\forall s \in S_T\), the treatment to \(rq(s,o,x)\) is as follows:
\(x = r, e \in M_{ij} \Rightarrow f_{CO}(o) \in ran_C(s) \&\& f_3(s) \geq f_{CO}(o); (1)\)
\(x = w, a \in M_{ij} \Rightarrow f_{CO}(o) \in ran_I(s) \&\& f_3(s) \geq f_{IO}(o); (2)\)

Formula 1 means a low confidentiality level trusted subject can’t steal high confidentiality level information and irrelevant information. But it has the ability to read low integrity level information, and it is guaranteed not to undermine its integrity. Formula 2 means a low integrity level trusted subject can’t destroy the integrity of high integrity level objects. But it has the ability to write objects with low confidentiality level, and it is able to ensure that high confidentiality level information will not be leaked to low confidentiality level objects.

The above four rules have achieved a dynamic adjusted two-dimensional unified models. But the adjustment of objects’ security levels are not considered. We argue that in some cases, after an operation, if we do not adjust the object’s level accordingly, an confidential information disclosure risk may exist and a new covert channel may form. For example, a high confidentiality level subject writes high confidentiality contents to a lower confidentiality level object. However, if the objects’ levels are adjusted after each operation, some applications may not operate, because the security levels of necessary objects are raised.

So in this paper, we introduce an adjustment rule to objects under the intervention of the security manager and the credible arbiter. When a writing operation from a high confidentiality level subject to a low confidentiality level object causes high confidentiality level information added to the object, the security manager and the trusted arbiter will adjust the object’s security level based on the additive contents. Typically, the object’s level is adjusted to the subject’s level.

Definition 10: \(C_C\) identifies the confidential contents. \(C_C = 1\), high confidentiality; \(C_C = 0\), common.

Rule 5: (“Adjustment rule of objects’ level”): \(x = a, w \in M_{ij}\). If \(C_C = 1\). Then \(f_{CO} = f_{CS}\). Else \(f_{CO} = f_{CO}\)

What’s more, the subject’s marks are not recoverable once adjusted. This may cause a degradation of security levels. In other words, there may be an “authority shrinking” phenomenon after adjusting the authorities. And finally the subject can only read or write objects with specific security levels. Thus, certain applications will be affected. Currently, the research of high level security systems mostly concentrates in production information systems, such as government networks, military networks, classified networks, etc. Most of these systems have clear application process, exact security requirements, and a lot of prior knowledge. The requirements and configuration of applications are often already known. For such applications, we can introduce configuration parameters \((f_{CS}, f_{IS})\) to prevent the authority shrinking.

Rule 6: (“The application-oriented logic configuration arbitration rule”): After an adjustment by rules 1-4, the treatment to the subject is as follows:
If \(f_3(s) \leq f_{CS}\), Then \(f_3(s) = f_{CS}\), Else if \(f_3(s) \leq f_{IS}\), Then \(f_3(s) = f_{IS}\), Else nop

3. Case Studies

The proposed ADUM model has been developed in the implementation of our micro-information system. Here we use three examples to illustrate the process of the dynamic adjustment of two-dimensional labels in ADUM model. Here, \(C_{RH}\) and \(I_{WH}\) are initialized to the minimum confidentiality label \(MIN_C\) and the minimum integrity label \(MIN_I\). \(C_{WL}\) and \(I_{RL}\) are initialized to the maximum confidentiality label \(MAX_C\) and the maximum integrity label \(MAX_I\). The operations are shown in Fig. 1.

**Example 1**: Step 1: A subject \(S_1\) (eg. a process) requests to read an object \(O_1\) (eg. a file).
Step 2: \(S_1\) requests to write the object \(O_2\).
The changes of subject $S_1$’s security marks in step 1 and step 2.

| Label | Initial Value | Step1: $r(O_1)$ | Step2: $a(O_2)$ |
|-------|---------------|----------------|----------------|
| $f_S$ | 4             | 4              | 4              |
| $(l_c, l_t)$ | (4,4) | (4,3) | (4,3) |
| $C_{RH}$ | MINC | 3 | 3 |
| $C_{WL}$ | MAXC | MAXC | MAXC |
| $I_{WH}$ | MINI | MINI | MINI |
| $I_{GL}$ | MAXI | 3 | 3 |

The changes of subject $S_1$’s security marks in step 3 and step 4.

| Label | Initial Value | Step3: $w(O_1)$ | Step4: $r(O_2)$ |
|-------|---------------|----------------|----------------|
| $f_S$ | 4             | 4              | 4              |
| $(l_c, l_t)$ | (4,4) | (3,3) | (3,3) |
| $C_{RH}$ | MINC | 3 | 3 |
| $C_{WL}$ | MAXC | MAXC | 3 |
| $I_{WH}$ | MINI | 3 | 3 |
| $I_{GL}$ | MAXI | 3 | 3 |

For step 1, there exists $f_{CS}(S_1) \geq f_{CO}(O_1)$, and $f_{IS}(S_1) \geq f_{IO}(O_1)$, which meet the authorized condition of rule 1. So $rq(S_1, O_1, r)$ is authorized, and the adjustments of labels are as shown in Table 2. Then $S_1$ requests to write $O_2$, we know that there exists $f_{CS}(S_1) \geq f_{CO}(O_2)$, and $f_{CO}(O_2) \geq C_{RH}(S_1)$, which don’t meet the authorized condition of rule 2. So $rq(S_1, O_2, a)$ is refused. This example indicates that, after reading an object, the subject can’t write objects with lower confidentiality level than the former object. Thus, it can ensure the confidentiality of a system.

**Example 3**: Step 5: $S_2$ requests to write $O_3$.

At this time, the information $S_2$ writes to $O_3$ is confidential information ($C_C = 1$). According to rule 5, the object’s level is adjusted to (4, 2). However, $S_2$ and $O_3$ are the specific subject and object of application 1. In order to ensure the smooth operation of application 1, the configuration parameter is set to $O_4$’s level. This means, $C{f_{CS}}$ is 4, and $C{f_{JS}}$ is 3. After the above adjustment, $S_2$’s level is adjusted to (3, 2). The degradation of security levels makes it unable to complete application 1. Then, Rule 6 is triggered, and $S_2$’s marks is re-adjusted to (4, 3). These changes in step 5 are shown in Table 4. This step indicates that, after adding confidential information to an object, the object’s level is adjusted correspondingly to avoid the disclosure of confidential information. What’s more, it also indicates that in a production information system, the application-oriented configuration rules can avoid the degradation of security levels after dynamical adjustments. Thus it can ensure the smooth operation of specific applications.

### 4. Conclusions

Compared with related works, the main contributions of our work involve three aspects: the combination of confidentiality and integrity with better availability, eliminating several covert channels, the application-oriented logic configuration to ensure applications operate smoothly. These ideas will help to complete the security model of information systems.

### References

[1] D.E. Bell and L.J. Lapadula, “Secure computer systems: Unified exposition and MULTICS interpretation,” MTR-2997 Rev.1, The MITRE Corporation, Bedford, MA 01730, March 1976.

[2] D.E. Bell, “Security policy modeling for the next-generation packet switch,” Proc. IEEE Symp. on Security and Privacy 1988, pp.212–216, April 1988.

[3] W.C. Shi, H.L. Liang, and Y.F. Sun, “On scheme for dynamic determination of subjects current sensitivity label,” Acta Electronica Sinica, vol.29, no.8, pp.1046−1049, Aug. 2001.

[4] K.J. Biba, “Integrity considerations for the secure computer systems,” Bedford: ESD-TR-76-732, April 1977.

[5] B.L. Di Vitol, P.H. Palmquist, E.R. Anderson, and M.L. Johnston, “Specification and verification of the ASOS kernel,” Proc. 1990 IEEE Computer Society Symposium on Research in Security and Privacy, pp.61–74, May 1990.

[6] Y.H. Liu and X.S. Chen, “A new information security model on BLP model and Biba model,” ICSP’04 Proc., pp.2643–2646, Sept. 2004.

[7] Y. Cai, Z.R. Zheng, and C.X. Shen, “Design and implementation MAC in security operating system,” Proc. IEEE TENCOW02, pp.216–219, Oct. 2002.

[8] Y. Shen and L.R. Xiong, “Lattice based BLP extended model,” 2009 Second International Conference on Future Information Technology and Management Engineering, pp.309−312, Dec. 2009.

[9] J. Zhang, L.J. Yun, and Z. Zhou, “Research of BLP and Biba dynamic union model based on check domain,” Proc. Seventh International Conference on Machine Learning and Cybernetics, pp.3679–3683, July 2008.

[10] Y. Huang, X.P. Chen, W.Z. Chen, L. Jiang, and X.Z. Pan, “Dynamically modified union model combining confidentiality and integrity,” J. Zhejiang University, vol.43, no.8, pp.1377−1382, Aug. 2009.