TOWARDS A MULTI-MODEL VIEWS SECURITY FRAMEWORK

Lei Xia, Hao Huang and Shuying Yu
State Key Laboratory for Novel Software Technology, Nanjing University, 22 Hankou Road, Nanjing, China 210093

Keywords: Multiple model views, access control model, security model, security framework.

Abstract: With increasing diversity and complexity of the computing environments, various security needs in one system can no longer be met by single access control model at the same time. An operating system should be able to enforce multiple access control models. A Multi-Model Views Security Framework is proposed, which is able to enforce multiple access control model views in operating system flexibly.

1 INTRODUCTION

Various security requirements are coming up with the sharply increased diversity and complexity of the computing environments (Rushby, 1992; Saltzer, 1973). To satisfy these security requirements, a variety of security models were proposed in last twenty years. Currently widely-used security models include multilevel security model (BLP - Bell, 1975) and its variants (Biba, 1977), Dion model (Dion, 1981), Domain and Type Enforcement (DTE) (Walker, 1996; Badger, 1995), RBAC (Sandhu, 1996; Sandhu, 1997), and etc. Each of these models aims mainly at one or few security requirements, such as BLP aiming at the confidentiality assurance, Biba at integrity assurance, DTE aiming at confining the information flow channels (Rushby, 1992).

Previous operating system usually enforced only one kind of access control model, for instance, Multics (Organick, 1972) implemented only BLP model in it. However, as mentioned above, the security goals in different applications are various. These different security requirements result in different security models needed for them. How operating system to support this kind of multiple security model views needs?

As a policy neutral security model, RBAC provides a valuable level of permission abstraction. However, using RBAC to simulate MLS or DAC models (Osborn, 2000) is over complex and therefore unpractical in real-world operating system.

The Multi-Model Views Security Framework (MMVSF) is proposed. Several access control models are embodied in MMVSF, including BLP, Biba, DTE and RBAC. These classical models can be easily enforced in MMVSF to implement multiple access control model views in system.

The remainder is organized as follows. Section 2 formally describes the MMVSF. Section 3 gives the examples of enforcing multiple access control model views. And section 4 is the conclusion.

2 MMVSF

2.1 The Framework Overview

The architecture of the MMVSF is shown in figure 1. MMVSF comprises of elements, relations and mappings. A user in the framework is a system user. A role is a job function or job title within some associated authority. Subjects are active entities. Objects are resource objects. Domain is a control access attribute associated with each subject. And type is the other control attribute associated with objects. Permission is an approval of a particular mode of access to object or interaction to subject. Security label contains a confidentiality label and an integrity label.

There are several relations and mappings between elements. user-role assignment relation, user-subject relation, and subject-role mapping figure out the relations between users, roles and subjects.

*This research is supported by National Natural Science Foundation of China under grant 60473093.
Permissions in system can be authorized to roles, which are given in role-permission authorization relation. Role-domain authorization relation gives the authorized domains of each role. Each subject has only one running domain, which is given in subject-domain mapping. Besides, each role has a security label, and subject’s security label is determined by its running role. Each object has a type and security label.

The Final Permissions the subject gets are based on three kinds of permissions corresponding to that subject: MLS Permissions, Domain Permissions, Role Permissions.

2.2 Formal Definitions

Table 1: Symbols of Elements Sets in MMVSF.

<table>
<thead>
<tr>
<th>Set Name</th>
<th>Symbol</th>
<th>Set Name</th>
<th>Symbol</th>
</tr>
</thead>
<tbody>
<tr>
<td>Users</td>
<td>U</td>
<td>Subjects</td>
<td>S</td>
</tr>
<tr>
<td>Objects</td>
<td>O</td>
<td>Domains</td>
<td>D</td>
</tr>
<tr>
<td>Roles</td>
<td>R</td>
<td>Types</td>
<td>T</td>
</tr>
<tr>
<td>Confidentiality Labels</td>
<td>C</td>
<td>Integrity Labels</td>
<td>I</td>
</tr>
</tbody>
</table>

- Security Labels: \( SL \subseteq C \times I \)
- Access modes: \( M = \{ \text{read, write, execute, } \ldots \} \).
- Domain transfer operation: \( \text{transfer} \), denotes subject transfer from one domain to another domain.
- Permissions: \( CAP \subseteq O \times M \). \((o, m) \in AP \) denotes permission to access object \( o \) in mode \( m \).

Definition 2.2 \( US \subseteq U \times S \), user-subject relation. Many subjects can run on behalf of one user, but each subject can only have one running user.

- \( \text{user}: S \rightarrow U \), mapping from subject to its running user. \( \text{user}(s) = u \) if and only if \( u \in U \) \( (u, s) \in US \).

Definition 2.3 \( UA \subseteq U \times R \), user-role assignment relation. Each user can be assigned many roles and each role can be assigned to many users.

- \( \text{UR}: U \rightarrow 2^R \), mapping from user to its assigned role set: \( UR(u) = \{ r \in R \mid (u, r) \in UA \} \).
- \( \text{SR}: S \rightarrow R \), subject-role mapping, from the subject to its running role. Each subject’s running role be assigned to its running user: \( \text{SR}(s) \in UR(\text{user}(s)) \).

Definition 2.4 \( RL: R \rightarrow SL \), mapping from role to its security label.

- \( \text{SSL}: S \rightarrow SL \), mapping from subject to its security label. Subject’s security label is equal to its running role’s label: \( \text{SSL}(s) = \text{RL}(\text{SR}(s)) \).

Definition 2.5 \( RD \subseteq R \times D \), role-domain authorization relation, a many to many relation.

- \( \text{RDom}: R \rightarrow 2^D \), mapping from role to its authorized domains set. \( \text{RDom}(r) = \{ d \in D \mid (r, d) \in RD \} \).
- \( \text{SDom}: S \rightarrow D \), mapping from subject to its running domain. Subject’s running domain must have been authorized to its running role, which means: \( \text{SDom}(s) \in \text{RDom}(\text{SR}(s)) \).

Definition 2.6 object’s security attribute

- \( OT: O \rightarrow T \), mapping from an object to its type.
- \( O \rightarrow SL \), from an object to its security label.

Definition 2.7 \( RCAP \subseteq R \times CAP \), role-permission authorization relation. \( (r_1, \text{cap}) \in RCAP \) denotes role \( r_1 \) has the Role permission cap.

- \( \text{Rolecap}: R \rightarrow 2^{CAP} \), role’s authorized permissions set. \( \text{Rolecap}(r) = \{ \text{cap} \mid (r, \text{cap}) \in RCAP \} \).

Definition 2.8 Two control matrices

- \( \text{DTM}: D \times T \rightarrow 2^D \), domain-type access control matrix. \( m \in \text{DTM}(d, t) \) denotes subjects in domain \( d \) can access objects with type \( t \) in mode \( p \).
- \( \text{DDI}: D \times D \rightarrow \{ \Phi, \{ \text{transfer} \} \} \), domain interaction control matrix. \( \text{transfer} \in \text{DDI}(d_1, d_2) \) denotes subjects in domain \( d_1 \) can transfer into domain \( d_2 \).

Definition 2.9 Multilevel Security rule: \( \text{Mls rule}: SL \times SL \rightarrow 2^D \), \( a \in \text{Mls rule}(l_1, l_2) \) implies subjects with security label \( l_1 \) can access target objects or subjects with security label \( l_2 \) in mode \( a \). All of BLP and Biba security rules are implemented in this mapping. As a framework, the concrete implementing of this function is not given here.

2.3 Permissions

- \( \text{MLS Permission: } mp(s, o) = \{ (o, p) \mid p \in \text{MLS rule}(\text{SSL}(s), \text{OL}(o)) \} \).
3 ENFORCE MULTIPLE MODELS

3.1 Enforcing Multilevel Security Model

The way configuring MMVSF to enforce BLP model is described as following:

1. $D = \{\text{only}_I\}$, there is only one integrity label in system. $|R| = |S_L|$, the number of roles in the system is the same as the number of the security labels. Each role corresponds to one security label.

2. $D = \{\text{gen}_d\}$, $T = \{\text{gen}_t\}$, only one domain and type in system. $RD = \{(r, \text{gen}_d) | r \in R\}$, all roles’ authorized domain is $\text{gen}_d$. All objects’ type is $\text{gen}_t$. $OT = \{(o, \text{gen}_t) | o \in O\}$.

3. $\text{DTM} = \{(d, t, p) | d \in D, t \in T, p \in OM\}$, domain $\text{gen}_d$ have all Domain Permissions to type $\text{gen}_t$.

4. $\text{Rolecap}(r:R) = \Phi$, each role has no Role Permissions.

We can use the similar way to enforce Biba model.

3.2 Enforcing DTE

1. $R = \{\text{gen}_r\}$, one role in system. $UA = \{(u, \text{gen}_r) | u \in U\}$, $\text{gen}_r$ is assigned to every user.

2. $RD = \{(\text{gen}_r, d) | d \in D\}$, all domains in system are authorized to the role $\text{gen}_r$.

3. $SL = \{\text{only}_sl\}$, only one security label in system. $RL = \{(r, \text{only}_sl) | r \in R\}$. MLS rule (only_sl, only_sl) = $\Phi$.

4. $\text{Rolecap}(r:R) = \Phi$.

3.3 Enforcing RBAC

1. $D = \{\text{gen}_d\}$, $T = \{\text{gen}_t\}$, one domain and one type in system. $RD = \{(r, \text{gen}_d) | r \in R\}$, $\text{gen}_d$ is automated to every role and all objects’ type is $\text{gen}_t$. $OT = \{(o, \text{gen}_t) | o \in O\}$.

2. $\text{DTM}(\text{gen}_d, \text{gen}_t) = \Phi$, subjects in domain $\text{gen}_d$ have no Domain Permissions to all objects in type $\text{gen}_t$.

3. $SL = \{\text{only}_sl\}$, only one security label in system. $RL = \{(r, \text{only}_sl) | r \in R\}$. MLS rule (only_sl, only_sl) = $\Phi$.

3.4 Enforcing Multi-model Views

Assume all users in system can be divided into three groups: Grpa, Grpb and Grpc. Now we hope that the model enforced on users in Grpa is MLS, on Grpb is RBAC and on Grpc is DTE. The configuration that enforces this multi-model views in one system is given below.

1. $U = \text{Grpa}\cup\text{Grpb}\cup\text{Grpc}$, three disjointed subsets.

2. $R = \text{mls}_rs\cup\text{rbac}_rs\cup\text{dte}_r$. $\text{mls}_rs$ is the roles set corresponding to MLS model. $\text{rbac}_rs$ corresponding to RBAC and $\text{dte}_r$ to DTE.

3. $D = \{\text{mls}_d\} \cup \{\text{rbac}_d\} \cup \{\text{dte}_d\}$.

4. $(u, r) \in \text{UA}$, where $u \in \text{Grpa}$, $r \in \text{mls}_rs$, $r' \notin \text{mls}_rs$, roles in $\text{mls}_rs$ are only permitted to be assigned to users in Grpa. $(u, r) \in \text{UA}$, where $u \in \text{Grpb}$, $r \in \text{rbac}_rs$, $r' \notin \text{rbac}_rs$, roles in $\text{rbac}_rs$ can only be assigned to users in Grpb. In the same way, $(u, dte_r) \in \text{UA}$, where $u \in \text{Grpc}$, $r' \notin dte_r$.

5. $\text{mls}_rs = |S_L|$, number of roles in set $\text{mls}_rs$ is the same as number of security labels in system. Each role in $\text{mls}_rs$ corresponds to one security label. MLS rule $(S_sl, t_sl) = \Phi$, $r \in \text{rbac}_rs$, $t_sl \in SL$, roles in $\text{rbac}_rs$ have no MLS Permissions. MLS rule $(S_sl, t_sl) = M$, $t_sl \in SL$, role $\text{dte}_r$’s has all of possible MLS permissions.

6. $(r, \text{mls}_d) \in RD \in (r, d) \notin RD$, where $r \in \text{mls}_rs$, $d \neq \text{mls}_d$, roles in $\text{mls}_rs$ are only authorized domain $\text{mls}_d$. $(dte_r, d) \in RD \in (r, d) \notin RD$, $d \neq dte_r$, all domains in $\text{dte}_d$ are authorized to role $\text{dte}_r$. Similarly, $(\text{rbac}_d) \in RD \in (r, d) \notin RD$, where $r \in \text{rbac}_rs$, $d \neq \text{rbac}_d$, roles in $\text{rbac}_rs$ are only authorized domain $\text{rbac}_d$.

7. $(\text{mls}_d, t, m) \notin DTM$, $t, m \in M$. DDI $(\text{mls}_d, d) = \Phi$, $d \in D$.

8. $\text{Rolecap}(r:R) = \Phi$, $r \in \text{mls}_rs\cup\{\text{dte}_r\}$. $\text{dte}_r$ and all roles in $\text{mls}_rs$ have no Role Permissions.
4 CONCLUSION

The MMVSF security framework provides a way to easily enforce multiple access control models in an operating system to satisfy the diverse security requirements in one system.

REFERENCES


