Anshula Garg, Prof. Pradeep Mishra / International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com
Vol. 2, Issue 5, September- October 2012, pp.342-345

# Methodologies for Access Control and their Interactions

**Anshula GARG*, Prof. Pradeep Mishra**
Department of Computer Science & Engineering, Shri Shankaracharya Institute of Professional Management & Technology,
&
Shri Shankaracharya College of Engineering & Technology, Bhilai

**Abstract:**

**We propose the use of process-based access-control methods in the construction of privacy systems in the present paper. Segregation of duties and least privilege are two key business principles that protect an organization's valuable data and resources from deliberate or accidental information leak, or data corruption by staff. As a substantial amount of this information is stored on computer systems then control over computer access represents a major security component through its implementation of the key business principles.**

**Access control systems have been the subject of considerable academic research. Some of these systems represent complex solutions, theoretically grounded in logic and mathematics, while others have addressed ease of use from a management or programming perspective. To facilitate this process, certain business principles are applied as structurally fundamental to the access control paradigm.**

**Keywords:**

Business Process, Access Control, Mandatory Access Control, Role-Based Access Control.

## I. Introduction

Authorization or access control within computer systems of organizations is a major component of the application of regulatory constraints. Access control is required to replicate the complex regulatory requirements within a heterogeneous mix of hardware and software by ensuring that users are properly assigned the resources to ensure the fulfillment of their responsibilities and resources are not accessible to those agents who lack the required levels of authorization.

Process control systems, which are a special type of access systems, currently suffer from the complexity of privacy models, leading to difficulty of verification, since enforcement in privacy is increasingly dependent on business function and human behavior, where business context (process) has to be considered in issuing access rights. Access rights may depend not only on the role of the person in the organization, but also on the process in which the person is involved at the time of access. Prerequisite for such a policy system is an enterprise control framework that takes into consideration an operational control model. This paper addresses various types of access control policies for organization.

Formal models for process control systems are essential for verification of system properties and detection of interactions [1]. Verifying properties is an important requirement. It is particularly relevant in the privacy domain, as companies need to prove their privacy commitments to their consumers, i.e. a corporation needs to show that its practices are compliant with their published privacy policy. The possibility of specifying and verifying systems formally will lead to much tighter and reliable privacy systems than can be considered now. Verifying a system policy can be equivalent to proving the impossibility of some situations.

Thurner suggested, reducing complexity requires the reduction of included artifacts and focusing on a single system view [2]. Decoupling of entities and attributes is a common technique. Role Based Access Control (RBAC) is an example for separation between users and access-rights by introducing roles [3].

## II. Access Control Models

Access control models are generally concerned with whether subjects, any entity that can manipulate information (i.e. user, user process, system process), can access objects, entities through which information flows through the actions of a subject (i.e. directory, file, screen, keyboard, memory, storage, printer), and how this access can occur. Access control models are usually seen as frameworks for implementing and ensuring the integrity of security policies that mandate how information can be accessed and shared on a system. The most common, oldest, and most well-known access control models are Mandatory Access Control and Discretionary Access Control but limitations inherent to each has stimulated further research into alternatives including Role Based Access Control, Dynamic Typed Access Control, and Domain Type Enforcement.

### 1.1. Mandatory Access Control (MAC)

MAC was an authorization method devised for the US military based upon the US classification system and the assignment of access rights according to clearance. A system-wide policy

decrees who is allowed to have access; individual user cannot alter that access. It relies on the system to control access. Specifically, the MAC model is somewhat inflexible and unsuited to situations where practical constraints such as staff sickness and holidays require a softening of the strict security requirements. For instance, flexibility may be required to facilitate delegation of responsibilities and the selective elevation of access rights and privileges. Traditional MAC mechanisms have been tightly coupled to a few security models. Recently, systems supporting flexible security models start to appear (e.g., SELinux, Trusted Solaris, TrustedBSD, etc.).

MAC is relatively straightforward and is considered a good model for commercial systems that operate in hostile environments (web servers and financial institutions) where the risk of attack is very high, confidentiality is a primary access control concern, or the objects being protected are valuable.

The assignment and enforcement of security levels by the system under the MAC model places restrictions on user actions that, while adhering to security policies, prevents dynamic alteration of the underlying policies, and requires large parts of the operating system and associated utilities to be "trusted" and placed outside of the access control frame- work.

#### *2.1.1. Biba Integrity Model*

Bell-LaPadulas model describes methods for assuring confidentiality of information flows; Biba developed a similar method aimed at information integrity. Integrity is maintained through adherence to reading writing principles that can be thought of as a reverse of the Bell-LaPadula principles.

In the Biba model, integrity levels are low to high with objects labeled high having high integrity. A subject can read objects at a higher level but can only write to objects of lower levels. This is known as the low water mark principle and assigns created objects the lowest integrity level that contributed to the creation of the object. Because the MAC method is primary developed for purposes where confidentiality is far more important than integrity, Bibas influence was minor on further development of MAC models.

### 2.2. Discretionary Access Control (DAC)

The Discretionary Access control (DAC) model provides flexibility of assignment of access rights to the owner of resources, hence the title. The DAC model subsequently evolved into Access Control Lists and the attributes-based system of access control that is familiar to users of modern operating systems. Although DAC provides greater flexibility than MAC, it does so through the dilution of the security model. DAC incurs scalability and management problems as the numbers of users and resources increases, particularly in respect of the ACM implementation of the model.

Additionally, users do not necessarily understand their assigned rights and responsibilities and system security can be seriously undermined by the inappropriate use of root or administrator access capabilities. In DAC an individual user can set an access control mechanism to allow or deny access to an object.

Discretionary Access Control (DAC) works both as a centralized security model and a distributed model. A centralized security model is when an administrator or team of administrators distributes access to data, applications and network devices. All requests for access changes need to be completed by this single department. In a large organization this can be very time consuming, especially if the administrators are off site or outsourced.

A distributed model allows responsible and knowledgeable personnel to distribute access to data and applications. In large companies this may be a manager, supervisor, or team lead. In small organizations it may simply be the most computer savvy team member. The benefit of a distributed model is that delays can be avoided since the administration of accounts is dispersed.

Allowing users to control object access permissions has a side-effect of opening the system up to Trojan horse susceptibility. The lack of constraints on copying info from one file to another makes it difficult to maintain safety policies and verify that safety policies have are not compromised while opening potential exploits for Trojan horses.

### 2.3. Role-Based Access Control

Whilst MAC was the generally accepted authorization model within the military and DAC evolved into the access control system applied to the major operating systems, the academic world was shifting its attention elsewhere within the field of authorization. Research was directed towards the formal analysis of access control systems and to the development of scalable models of access control that were more appropriate to complex heterogeneous computer systems, such as Role-Based Access Control (RBAC) [4, 5].

David Ferraiolo and Richard Kuhn outlined their basic RBAC model as a more appropriate system of control in civilian government or commercial organizations than either the multilayer security of MAC or the user-centered security model of DAC [4]. Matunda Nyanchama and Sylvia Osborn concentrated on the development of a hierarchical role graph model for role-based access control based upon organizational hierarchies. Ravi Sandhu et al

developed a family of RBAC models to provide a reference point for further RBAC development [5].

The principle of the RBAC model is the abstraction of resources from users via a set of roles. Consequently, the set of users are mapped many-to-many to the set of roles; a given user can occupy a number of roles and a number of users can occupy a given role. The set of roles is mapped many-to-many to the set of resources.

RBAC marks a great advance in access control; the administrative issues of large systems still exist, albeit in a markedly more manageable form. In large systems, memberships, role inheritance, and the need for finer-grained customized privileges make administration potentially unwieldy. RBAC supports data abstraction through transactions; it cannot be used to ensure permissions on sequences of operations need to be controlled. To do this, a less general and more sophisticated access control model must be used. RBAC assumes that all permissions needed to perform a job function can be neatly encapsulated. In fact, role engineering has turned out to be a difficult task. The challenge of RBAC is the contention between strong security and easier administration. For stronger security, it is better for each role to be more granular, thus having multiple roles per user. For easier administration, it is better to have fewer roles to manage. Organizations need to comply with privacy and other regulatory mandates and to improve enforcement of security policies while lowering overall risk and administrative costs.

Meanwhile, Web-based and other types of new applications are proliferating, and the Web services application model promises to add to the complexity by weaving separate components together over the Internet to deliver application services. Moreover, the allocation of files and servers (therefore, access control) may be incompatible with organization structure (therefore, process) that requires users to focus on practical matters such as opening accounts and paying bills. RBAC products have sometimes proved challenging to implement and will, for some organizations, need to be combined with rule-based and other more time-tested access control methods to achieve the most practical value.

### 2.4. Domain Type Enforcemet (DTE) Model

Domain Type Enforcement (DTE) is an extension of Type Enforcement (TE) and is itself extended into Dynamic Typed Access Control (DTAC). The principle of type enforcement is more that flexible policy expressions are possible when objects are assigned to types and thus columns in the access control matrix are replaced by types. The DTE extension to this is to assign subjects to domains and complete the matrix transformation so the access control matrix is now a domain definition table (DDT) with rows of domains and columns of types. DTAC expanded upon this to include RBAC type administrative controls. [7] It is claimed that DTE models can implement the Bell-LaPadula confidentiality model as well as some of the more robust integrity features in DAC and RBAC.

### 2.5. Business Process Access Control (BPAC) Model

BPAC provides a formal underlying structure and analysis model to ensure that the business principles are properly implemented and maintained. It is a workflow based system of access control that properly addresses the key business principles. This model concentrates on the mappings of users to roles and roles to tasks, the mapping of roles to resources in RBAC and the mapping of tasks to resources in workflow-based access control is also a significant part of the security model that requires careful consideration.

## III. Results and Discussion

As we have discussed, a number of access control models for workflows [2], web services, and role based access control on the web [5], possibly coupled by sophisticated policy, combination algorithms. However, they have mostly remained within the classical framework. Even more liberal models such as those for DRM based on usage [6] have assumed that servers know their clients pretty well: they might not know their names but they know everything about what, when, and how can be used by these clients.

## IV. Conclusions

Access Control models have come quite a ways since the initial implementations of MAC and DAC in the early 70's. Researchers have learned volumes about the complexities of maintaining security policies through model applications and with RBAC, BPAC have come very close to seamlessly integrating integrity and confidentiality.

Future work in the area of models for access control is likely to be focused on the proliferation of Business Process Access Control models and case study analysis of their relative effectiveness. Oracle has incorporated BPAC as part of their database management access controls as has the SQL: 2004 standard, PostgreSQL, and SAP. Solaris, Windows Active Directory, and SELinux all also provide support for the use of Business Process Access Control.

## References

[1] G. Karjoth and M. Schunter, A Privacy Policy Model for Enterprises, 5th IEEE Computer Security Foundations Workshop, 271-281, 2002.

[2] V. Thurner, A formally founded description technique for business processes, Technical

Report, Technical University of Munich, Germany, 1997.

[3] D. Ferraiolo, D. Kuhn, R. Chandramouli, Role-Based Access Control, Artech House, 2003.

[4] Ferraiolo, D. F., and Kuhn, D. R. Role based access control. In Proceedings of 15th National Computer Security Conference (1992).

[5] Sandhu, R. S., Coyne, E. J., Feinstein, H. L., and Youman, C. E. Rolebased access control models. IEEE Computer 29, 2 (1996), 38–47.

[6] Roscheisen, M., and Winograd, T. A communication agreement framework for access/action control. In Proc. of the SS&P (1996), IEEE Press, pp. 154-163.

[7] J. A. Solworth and R. H. Sload. Security property based administrative controls. 2005.