Chapter XXVIII
Enterprise Access Control Policy Engineering Framework

Arjmand Samuel
Purdue University, USA

Ammar Masood
Purdue University, USA

Arif Ghafoor
Purdue University, USA

Aditya Mathur
Purdue University, USA

ABSTRACT

This chapter outlines the overall access control policy engineering framework in general and discusses the subject of validation of access control mechanisms in particular. Requirements of an access control policy language are introduced and their underlying organizational philosophy is discussed. Next, a number of access control models are discussed and a brief outline of various policy verification approaches is presented. A methodology for validation of access control implementations is presented along with two approaches for test suite generation, that is, complete FSM based and heuristics based. This chapter is aimed at providing an overview of the access control policy engineering activity and in-depth view of one approach to devise test cases for an access control implementation mechanism.

INTRODUCTION

With the increase in information and data accessibility, the concern for security and privacy of data is also increasing, accentuating the need to protect system resources from vulnerabilities introduced as a result of security system design. Engineering access control mechanisms for an enterprise entail a number of closely related activities which include selection of an appropriate security model, creation of access control policy, verification of policy for inconsistencies, and validation of access control implementations.

The wide scale application of access control policies in an enterprise make it imperative that the underlying access control software (system) is correct in that it faithfully implements a policy it is intended to; hence testing of access control system becomes critical. The challenge is in devising such testing techniques that
are scalable and effective in detecting those faults that can occur in an access control system.

In this chapter we introduce the overall policy engineering activities with stress on issue of test generation for access control systems using automata theoretic approaches to provide cost effective solutions for conformance and functional testing of an access control mechanism.

**BACKGROUND**

Security requirements of information systems include protection against unauthorized access to or modification of information, and against denial of service to authorized users. Access control is the key security service providing the foundation for information and system security. An access control implementation is responsible for granting or denying authorizations after the identity of a requesting user has been validated through an appropriate authentication mechanism. Operating systems, database systems, and other applications employ policies to constrain access to application functionality, file systems, and data. Often these policies are implemented in software that serve as front end guard to protected resources, or is interwoven within the application. Examples of application of such controls in securing system resources abound in commercial and research domains (Bhatti, 2005; Notargiacomo, 1996; Tripathi, 2003; XACML, 2005).

A number of reported common vulnerabilities and exposures are related to design and/or coding flaws in access control modules of an application. Testing remains indispensable despite advances in the formal verification of secure systems (Ahmed, 2003; Alpern, 1989; Clarke, 2000; Hansen, 2005; Landwehr, 1986; Lupu, 1999), and in static or dynamic program-analysis based techniques (Cowan, 2003; Livshits, 2005; Martin, 2005) because verification only guarantees correctness of the design under certain assumptions. Any faults in the implementation due to, for example, coding errors, incorrect configuration, and hidden or “backdoor” functionality could jeopardize the effectiveness of corresponding (access control) specification (Thompson, 2003).

Validation of access control implementations is essential because security and privacy issues are now a significant cause for concern amongst the developers of embedded systems such as those found in healthcare, nuclear, automotive, and other industries (Gupta, 2005; Ravi, 2004). The authentication and access control mechanisms in such environments pose a significant challenge to the designer and tester. The testing of authentication and access control mechanisms, carried out to ensure correctness of the underlying implementation, is necessary for enforcing accountability. Authentication establishes the identity of a user and is a prerequisite for access control.

**REQUIREMENTS OF ENTERPRISE ACCESS CONTROL POLICY LANGUAGE**

Figure 1 depicts the relationship between security requirements of an enterprise and corresponding access management policy language. While the stated enterprise requirements address the issues of interoperability and scalability, they also drive the important language design parameters of context sensitivity and ease of administration. The enterprise requirement of attribute-based control sets the stage for highly granular and flexible control of users and resources. The autonomy requirement of domains and sub-domains in the enterprise opens opportunities for collaboration with other enterprises. Next we discuss the requirements of a policy-based access management language in detail.

**Declarative Rules**

Declarative rules in an access management policy language allow each enterprise to compose rules which are both flexible and scalable. The rules can be modified without any effect on the application code and can be composed individually by participating sub-domains by using a common vocabulary and composition rules. Once created, they can be applied across domains with similar efficacy.

Use of declarative rules enables autonomy of control within a domain as well as de-centralized administration in a cluster of domains interoperating with each other. The issues of autonomy and de-centralized administration are fundamental to the design of an access control policy language for an enterprise which seeks to be part of a collaboration or federation with other enterprises. The principle of local autonomy suggests that each sub-domain of an enterprise and indeed each collaborating enterprise in inter-enterprise coloration, retain control over its