Journal of Network and Computer Applications 34 (2011) 1342–1352

Contents lists available at ScienceDirect

Journal of Network and Computer Applications

journal homepage: www.elsevier.com/locate/jnca

Applying a usage control model in an operating system kernel

Rafael Teigão, Carlos Maziero *, Altair Santin

Graduate Program in Computer Science, Pontifical Catholic University of Paraná State, Rua Imaculada Conceição 1155, 80.215-901 Curitiba, PR, Brazil

ARTICLE INFO

Article history:
Received 4 December 2009
Received in revised form
24 November 2010
Accepted 10 March 2011
Available online 16 March 2011

Keywords:
Access control
Usage control
Kernel services

ABSTRACT

Operating systems traditionally use access control mechanisms to manage access to system resources like files, network connections, and memory areas. However, classic access control models are not suitable for regulating access to the diversity of ways data is available and used today. Modern usage control models go beyond traditional access control, addressing its limitations related to attribute mutability and continuous usage permission validation. The recently proposed $UCON_{ABC}$ model establishes a predicate-based framework to satisfy the new access/usage control needs in computing systems. This paper defines a usage control model based on $UCON_{ABC}$ and describes a framework to implement it in an operating system kernel, on top of the existing DAC mechanism. A language for representing usage control entities and rules is also proposed, and some typical access/usage control scenarios are represented using it, to show its usefulness. Finally, a prototype of the proposed framework was built in an operating system kernel, to control the usage of local files. The prototype evaluation shows that the proposed model is feasible, straightforward, and may serve as a basis for more complex usage control frameworks.

1. Introduction

Classic access control models are not suitable for regulating access to the diversity of ways digital content is available and used today. For instance, *Digital Rights Management* (DRM) requires control that goes beyond the simple one-step access granting. This is also true for the manipulation of related data collected from several independent sources, such as medical information about patients in a hospital. Current electronic commerce of digital items brings with it the necessity of checking whether some requirements have been met, like accepting an end-user license agreement (EULA), or enforcing time restrictions in a commercial transaction. Although most of these controls are employed at the application level, they would be easier to deploy and harder to circumvent if more sophisticated access control mechanisms were made available by the underlying operating system.

The formal concept of *usage control* (UCON), presented by Park and Sandhu (2003), introduces the evaluation of attributes and requirements during the use of a resource (e.g., permission of a user to continue to watch a movie). It also considers the *mutability* of such attributes as a consequence of actions by users. Furthermore, the usage control concept includes the notion of dependency of the access policies on *external information*, like the time of day or the system load, which was not explicit in previous access control models. The $UCON_{ABC}$ model (Park and Sandhu, 2004) formalizes such concept.

This paper proposes a usage control model derived from the $UCON_{ABC}$ model. It considers the formal UCON specification defined in Zhang et al. (2004), adapting it to be implemented in an operating system context. From the proposed model, a language to describe usage control policies on system objects is defined, and its expressiveness is evaluated through a series of typical usage control scenarios. It also describes a prototype implementation for the proposed model, which was built in an operating system kernel to mediate operations on files. The prototype evaluation shows that the model is feasible and may serve as a basis for more complex usage control frameworks. This paper is an extended version of a previous work (Teigao et al., 2007), including a formal presentation of the usage control model, more details about its framework, the grammar specification, more usage examples, and the description/evaluation of an implementation prototype.

The paper is organized as follows. Section 2 describes the main features of usage control and the $UCON_{ABC}$ model. Section 3 explains the usage control model adopted in this paper. Section 4 presents the framework which implements the proposed model. Section 5 details the language proposed for representing usage control policies. Examples of the language representing common usage and access control scenarios are given in Section 6. Section 7 gives some details of the implemented prototype and its evaluation. Section 8 discusses related work. Finally, Section 9 gives some conclusions and presents future research directions.

* Corresponding author. Tel.: +55 41 3271 1669; fax: +55 41 3271 2121.
E-mail addresses: rafael.teigao@tjpr.jus.br (R. Teigão), maziero@ppgia.pucpr.br (C. Maziero), santin@ppgia.pucpr.br (A. Santin).

1084-8045/$ - see front matter © 2011 Elsevier Ltd. All rights reserved.
doi:10.1016/j.jnca.2011.03.019