

Kernel Framework for an Immune-Based Security System: A Work-In-Progress Report

Martim d'Orey Posser de Andrade Carbone¹*, Paulo Lício de Geus¹

¹Institute of Computing – State University of Campinas (UNICAMP)
PO Box 6176 – 13083-970 Campinas, SP

{martim,paulo}@las.ic.unicamp.br

***Abstract.** This report informs on the current status of the project whose goal is to design, implement and integrate into the 2.6 version of the Linux kernel a generic framework to support a computer security system inspired in the principles of the human immune system. A brief introduction to the project is given, followed by a more in-depth discussion of the framework requirements and its overall architecture. It concludes by pointing out the future research and development stages.*

1. Introduction

Modern security threats create the demand for robust and complete models on which security systems can be built upon, such as the human immune system. This system is capable of automatically recognizing and responding to a wide variety of biological and chemical threats, as well as to learn from those threats and accelerate future responses. It successfully integrates prevention, detection, and reaction counter-measures in a fully adaptative and automatic manner, making it extremely desirable for a computer.

Fundamental steps towards the construction of such a system were made before by former lab members working at the *Imuno* project [de Paula et al. 2004, de Paula et al. 2002]. In this project, we aim to continue their work by implementing a framework that will allow the integration of that system into the Linux operating system. This framework will consist mainly of a set of hooks (alongside with its access and management infrastructure) implemented inside the Linux kernel (version 2.6) to address the low-level prevention, detection, learning and response needs of the immune modules.

The framework will be implemented as an extension of LSM (*Linux Security Modules*) [Wright et al. 2002], an established framework for granular access control support inside the Linux kernel. The main goal is to generalize LSM's access control infrastructure by creating a more sophisticated and dynamic hook management engine, so as to support other security functionalities, and also complement it with additional hook points. The CKRM (Class-based Kernel Resource Management) [Nagar et al. 2004] and Netfilter [Russell and Welte 2002] frameworks will also be used in this project.

This paper is organized as follows: it will first discuss the framework's requirements in Section 2., followed by the first model of its overall architecture, in Section 3.. Finally, Section 4. will conclude with some closing remarks and future steps.

*Supported by CNPq

