Policy Mining: A Bottom-Up Approach toward a Model Based Firewall Management

Safaà Hachana\textsuperscript{1,3}, Frédéric Cuppens\textsuperscript{2}, Nora Cuppens-Boulahia\textsuperscript{1,2}, Vijay Atluri\textsuperscript{4}, and Stephane Morucci\textsuperscript{1}

\textsuperscript{1} Swid Web Performance Service, France  \\ \{safa,stephane.morucci\}@swid.fr
\textsuperscript{2} Institut Telecom-Mines/Telecom Bretagne, Dépt. LUSSI, France  \\ \{frederic.cuppens,nora.cuppens\}@telecom-bretagne.eu
\textsuperscript{3} École Nationale Supérieure de Mécanique et d’Aérotechnique, Dépt. LIAS, France
\textsuperscript{4} CIMIC, Rutgers University, USA  \\ atluri@rutgers.edu

Abstract. Todays enterprises rely entirely on their information systems, usually connected to the internet. Network access control, mainly ensured by firewalls, has become a paramount necessity. Still, the management of manually configured firewall rules is complex, error prone, and costly for large networks. The use of high abstract models such as role based access control RBAC has proved to be very efficient in the definition and management of access control policies. The recent interest in role mining which is the bottom-up approach for automatic RBAC configuration from the already deployed authorizations is likely to further promote the development of this model. Recently, an extension of RBAC adapted to the specificities of network access control, which we refer to as NS-RBAC model, has been proposed. However, no effort has been made to extend the bottom-up approach to configure this model. In this paper, we propose an extension of role mining techniques to facilitate the adoption of a model based framework in the management of network access control. We present policy mining, a bottom-up approach that extracts instances of the NS-RBAC model from the deployed rules on a firewall. We provide a generic algorithm that could adapt most of the existing role mining solutions to the NS-RBAC model. We illustrate the feasibility of our solution by experimentations on real and synthetic data.

Keywords: IT Security, Access Control, Network Security, Firewall, RBAC, Role Mining.

1 Introduction

Nowadays, most of the enterprises are completely dependent on their information systems, either for their internal functioning, or for their commercial web interface. A reliable access control policy is essential to ensure the good and continuous working of these systems. The access control policy is mainly deployed on firewalls. The configuration and the management of these firewalls are hard tasks. Filtering rules are enforced in a vendor specific low level language, the
number of rules is usually high, and the rules are order sensitive. Performed manually, operations such as migration, updates, and delegation to a new administrator are real challenges. The firewall management problem becomes more and more urgent with the increasing complexity of modern security policies. One of the most important proposed approaches is to configure and manage firewalls from a high level language down to device specific low level language [1–3]. This methodology is likely to overcome the problems encountered when using low level languages by providing the administrator with the benefit of hindsight, decreasing the probability of human error and allowing a reliable configuration of a system of firewalls. The greatest stumbling block to the wholesale adoption of high level models is that no solution has been proposed to handle the already deployed rules on firewalls. This implies to throw away the already deployed rules, and start from scratch the specification of the whole access control policy. To bypass this problem, we advocate for a bottom-up approach that parses the configured rules in the firewalls and leverages data mining techniques to automatically reach an instance of the high level model corresponding to the deployed policy. Recently, the emergence of Role Mining [4] has become a new catalyst of the expansion of Role Based Access Control (RBAC) [5] in organizations. Role mining is the discipline of automating the extraction of RBAC roles from the already deployed set of direct authorizations in a system, using data mining tools. However, applying the role mining solutions proposed in literature directly to firewall rules can not provide interesting outcome. Indeed, though RBAC model has imposed itself as the standard high abstraction level access control policy model, and has proved to be very efficient in a wide area of access control applications such as physical security package, environmental security, operating system security, and staff security [6], it still does not fully capture the specificities of network access control policies. From the perspective of the RBAC model, the access control security rules are considered to follow the pattern: \( a \text{user} u \text{is allowed access to permission} p \), with \( p \) an operation over an object. The users are the central entities, and RBAC introduces the concept of role to structure them. However, when we focus on the structure of a network access control rule, it is of the form \( \text{allow source} \text{host} s \text{to send service of type} s \text{to destination} \text{host} d h \). In this pattern, the three involved entities are semantically at the same level of importance from the network access control perspective. Cuppens et al. have showed that a model that captures this ternary relation allows to define a network security policy efficiently [3]. The Network Security RBAC (NS-RBAC) model contains and generalizes the concept of role from RBAC by adding the concepts of activity to structure the services, and view to structure the destination hosts, the same as role structures the source hosts into higher level of abstraction entities. Role mining techniques do not fit the NS-RBAC model since they structure only one of the three entities. Applying role mining to structure each of the three entities separately is not feasible since it would output unconnected abstract entities that can not be related with security rules to express the original access control policy.