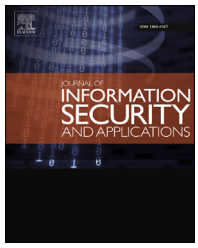
Available online at www.sciencedirect.com

ScienceDirect

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



Mining a high level access control policy in a network with multiple firewalls

Safaà Hachana [a,b,*], Nora Cuppens-Boulahia [a], Frédéric Cuppens [a]

[a] Dépt. LUSSI, Institut Télécom-Mines/Télécom Bretagne, France
[b] LIAS Labs, École Nationale Supérieure de Mécanique et d'Aérotechnique, France

ARTICLE INFO

Article history:
Available online 11 November 2014

Keywords:
Access control
Network security
Policy mining
Role mining
Multiple firewalls
Net-RBAC

ABSTRACT

A policy mining approach that aims to automatically extract a high level of abstraction policy from the rules configured on a firewall has been recently proposed (Hachana et al., 2013). This technique is likely to considerably facilitate firewall management. However, protecting the information system of a business organization usually requires the enforcement of more than one firewall. In this paper, we augment the policy mining approach by an additional processing for a network access control policy mining. We develop the problem of integration of Net-RBAC (Hachana, 2014) policies resulting from policy mining over several firewalls in order to mine a high level network policy. Moreover, we show how to verify security properties related to the deployment consistency over the firewalls. We illustrate the network policy mining approach by a realistic example, and we experimentally evaluate the performance of our merger algorithms.

1. Introduction

Today's corporations rely entirely on their information systems, usually connected to the Internet. Network access control, mainly ensured by firewalls, has become a paramount necessity. Yet, the management of manually configured firewall rules is complex, error prone, and costly for large networks. Using high abstract models for the definition and update of the access control policies is much more efficient and safer than manipulating the firewall configuration at low level using the constructor languages directly. The *Network Role Based Access Control (Net-RBAC)* model is adapted to the specification of network access control policies. Moreover, there exist safe automatic methods to deploy a policy modeled with Net-RBAC on firewalls (Preda et al., 2010). Still, the biggest challenge to adopt such a model is the initial definition of the high level policy, especially when a configuration of the firewalls already exists. For most security administrators, it is not worth throwing away the deployed filtering rules and starting a new policy definition from scratch. Providing a bottom-up approach that automatically extracts instances of the Net-RBAC policy from the deployed rules on a firewall is likely to highly promote the usage of this model. Recently, Hachana et al. have proposed such a policy mining technique (Hachana et al., 2013). They have defined a generic algorithm based on matrix factorization, that could adapt most of the existing data mining and role mining techniques (Hachana et al.; Fuchs and Meier, 2011) to extract from firewall rules the corresponding policy modeled with Net-RBAC. Nevertheless, large and medium networks are usually protected by more than one firewall, and the policy mining algorithm in Hachana et al. (2013) has been designed for a single firewall. In order to provide a complete automatic bottom-up framework for

* *Corresponding author*. Institut Telecom-Mines/Telecom Bretagne, 2 Rue de la Chataigneraie, 35510 Cesson Sévigné, France.
E-mail address: safaa.hachana@telecom-bretagne.eu (S. Hachana).
http://dx.doi.org/10.1016/j.jisa.2014.10.010

network policy mining, we still need a further processing of policy mining performed on each firewall into a global network policy. Proceeding in this modular way has several benefits. We can individually examine and analyze the configuration of each firewall apart, and detect intra-firewall misconfigurations. This could be performed on a regular basis to check the current configuration, without necessarily running the bottom-up process for the whole network. Moreover, we can verify consistency of deployment between the firewalls. For instance, we can check the accessibility of a permission over all the firewalls on the path before we add it to the final network policy.

In this paper, we handle the problem of integration of Net-RBAC policies resulting from policy mining over several firewalls to mine a high level network policy. We propose a two-staged process. In the first stage, we unify the hierarchies of the abstract entities of all the firewalls. We assimilate the problem to the general mathematic problem of partially ordered set merging. In the second stage, we build the effective deployed network policy rules. We integrate the highly abstracted rules from the firewalls while checking several security properties. We detect irrelevance anomalies consisting of rules that never apply because they are enforced in a firewall that is not on the path between the source and the destination. We also detect inaccessibility anomalies due to inconsistency between the configuration of firewalls on the path of the same flow. The correctly deployed rules are aggregated into the network policy, whereas the detected anomalies are reported.

Paper organization. Section 2 reviews the related work about policy mining techniques and the Net-RBAC model for network security policy expression. Then, it introduces the problem of Net-RBAC policies integration, and explains the followed methodology to solve it. Section 3 proposes an algorithm that tackles abstract entities integration. Section 4 presents a methodology for network access control rules mining through abstract rules integration while verifying accessibility and relevance properties in the deployed policy. Section 5 illustrates the network policy mining approach by a realistic example. Section 6 presents experimental results. Section 7 provides a comparison with related work. Section 8 concludes the paper.

2. A bottom-up framework to mine a model based network security policy

2.1. Firewall policy mining

Policy mining (Hachana et al., 2013) is inspired from the intense research realized in the *role mining* field recently. Role mining is the discipline of automating the extraction of the *Role Based Access Control (RBAC)* (Ferraiolo et al., 2001) roles from the already deployed set of direct authorizations or access control list (ACL) in a system, by using data mining tools. Several role mining techniques are proposed in the literature, with different assumptions and optimization objectives (Hachana et al.; Fuchs and Meier, 2011). However, traditional role mining techniques cannot be directly applied to firewall rules. This is because the targeted model, RBAC, is not well suited for application to network security. Indeed, the RBAC model is centered on the *role* (Fuchs et al., 2011), so the rules are modeled with the pattern: [*allow role r to access to privilege p*], where a privilege is a combination of an operation over and object. On the other side, a typical network access control rule follows the pattern: [*allow source_host sh to send service of type s to destination_host dh*] where *sh* is an IP address or a panel of addresses that send packets of service *s* defined by: protocol, source_port, and destination_port, to *dh* that is also an IP address or a panel of addresses. The three entities are semantically at the same level of importance from the network access control perspective. As the RBAC model does not allow to emphasize this ternary relation, Net-RBAC is an extension of the RBAC model defined to meet network access control policy specification requirements (Cuppens et al., 2004). Net-RBAC considers a three tuple security rules [*allow user u to perform operation op on object ob*] (Hachana, 2014). It retains the concept of *role* to structure the users, and generalizes it by adding two new abstract entities: *activity* that structures the operations, and *view* that structures the objects. The fact that the three concrete entities are structured induces the definition of the *abstract rules*. An abstract rule is of the form [*role r is permitted to perform activity a over view v*]. The concrete access control rule involving a given user *u*, operation *op* and object *ob* exists if *u* is assigned to a role *r*, *op* is assigned to an activity *a*, and *ob* is assigned to a view *v*, and the triplet (*r*, *a*, *v*) belongs to the relation of abstract rules *RAV*. The model can be easily used to express network access control policies if we assimilate the *source_host* to user, the *service* to operation and the *destination_host* to object, in the terminology of Net-RBAC (Cuppens et al., 2004).

Policy mining is an extension of role mining to extract a high level policy modeled with Net-RBAC from a firewall configuration. The method presented in Hachana et al. (2013) is based on two phases (see Fig. 2). First, in a preprocessing phase, the firewall rules are flattened, i.e. transformed into a non-order sensitive and a positive only set of rules. This is a prerequisite for the following step. There are solutions in literature that perform this transformation, such as the approach presented in (Tongaonkar, 2004) that is based on a Directed Acyclic Graph (DAG) representation of the rules, followed by DAG pruning. Then, the flattened firewall rules are parsed, and the different instances of source_hosts, services and destination_hosts are saved respectively in the sets of users *U*, operations *OPS*, and objects *OBJ*. The relation of concrete rules *UOO* is built as an $m \times n \times k$ 3-dimensional Boolean matrix for m users, n operations and k objects. The matrix is initiated with zeroes, and for each firewall rule where user i is allowed to perform operation j on object l, the cell $\{ijl\}$ in *UOO* is set to 1. These relations constitute the concrete level of the Net-RBAC policy. The second phase (see Fig. 2) is the factorization of the concrete rules relation *UOO* to extract the abstract rules relation *RAV*, in addition to the structures of roles, activities and views. Policy mining problem is assimilated to a three-dimensional matrix factorization problem where the traditional role mining is usually assimilated to a problem of factorization of a two-dimensional matrix of user-to-permission into user-to-role and role-to-permission assignment relations. The output of policy mining is the assignment of the initial source_hosts, services and