Integrated manegement method for Network Security

Hiroshi Takechi

School of Information Science,
Japan Advanced Institute of Science and Technology

February 15, 2000

Keywords: Network security, Policy, Network management.

The tremendous growth of the Internet is making network systems increasingly important for many organizations to manage their own activities and interact with others. The network security is also becoming a issue along with the growth of the organizations' dependency on the network system.

The integration of the organizational network systems causes a fundamental problem for security management. That is, to ensure a consistent authorization state when multiple independent network entities are involved, each having an access control function of its own. In other words, how to ensure an organization-wide security policy.

Network system management is a task to achieve the organizational objectives which are represented as policies which are interpreted by the system managers. The organizational network management are moving toward a policy-based network management. Therefore, it is very important for the realization of the organizational objectives to provide the support of interpreting and applying the policies.

Polices are usually defined at a high level of abstraction. These polices are needed to be translate to the procedures which can be interpreted by

the computer system. For example, the security policies are translated into access control procedures.

The process of the translation often produces errors into the policies. The reason why these errors can be produced as follow:

1. Policies are often stated in natural language (e.g. English or Japanese). Then, various interpretation of the polices can be made depending the context.

2. The administrators translate the policies based on their experience and the knowledge of the network.

The ambiguity and imprecision of the policies and the errors during the translation lead to inconsistency of the network system. Therefore, the support of interpreting and applying the polices requires the way of describing precise polices and the method of the translation from the policies into the procedures which can not be introduce errors in the policies.

In this paper we have proposed a framework for integrating heterogeneous component systems (which support their own access control mechanism) into one policy-based management system which offer the system-wide integrated access control rules by simply changing access control policies to resolve the problems of networks security. Especially, we have developed the methods for mapping the access control policies to access control function onto the actual network entities by using the attribute calculation which are made to regard a network entity as a node of the syntax tree.

The methods enable generating the access control rules for the network entities from the polices and detecting the network entities of violating the polices.

In this framework we consider that the network systems are defined as the set of the services which are offered to the users in order to achieve their objectives. Service descriptions are described by the policy definitions that are represented as objects that specify a relationship between subjects (managers) and targets (managed objects).

First, a network manager defines the set of the Service descriptions to define the whole network as the set of policies by using tool, which is provided to assist with the editing and manipulation of policies. The merit to use such a tool is that it is easy to trace the derived policies that may also need to be changed.

Three kinds of the service attributions are generated with the access control policies within the Service description. a) The object service attribute , which is attached for the object of the polices. b) The positive subject service attribute, which is attached for the subject which can make access to the object of the polices. c) The negative subject service attribute, which is attached for the subject which are prohibited from making access to the object of the polices.

Attribute evaluation rules are also generated from the service descriptions, which are formulations to define the relation among attributions. These rules are used to evaluate the relation between the attribute of the ports for generating access control rules and detecting policy violations.

Secondly, to map the service attributions onto the actual network configuration, the network configuration description is generated from the actual network configuration information database by using a network management tool. The network configuration description is a modeling of the actual network. It is modeled with a layered structure. The attribution calculations are held on each layer separately, for which each layer's access control function can be treat to work separately.

At this point, the preparations of the attribution calculation are made. There are two applications of the attribution calculation: the generating access control rules of the network entities which are equipped with the access control function; and the detecting network entities which have violated any policies. The attribution calculation on the network configuration description is proceeded to regard network as a syntax tree. A port of a network entity and a link between ports are a node and a link of a syntax tree respectively.

The generating access control rules are made like below. At first, we calculate the attributions of the entities which do not have the access control function along with the whole network configuration description, by which result in the attributions of all ports of entities which have the access control function. Then we evaluate the attributions between ports of entities which have the access control function based on the attribute evaluation rules; if an attribution is prohibited to be inherited or composed between the ports, an access control rule which prohibit to inherit or compose the attribution is generated. Otherwise, an access control role to permit is generated.

The detecting network entities that have violated any policies are made like below. We calculate the attributions of the entities on the whole network configuration description with the current access control rules. After that for

all ports of all network entities, we check weather each attribution of them satisfy the attribute evaluation rules or not. If any attribution on an entity not to satisfy the rules exist, its entity has violated the policy.

We have implemented a prototype system as single layer network model and have verified that the proposed methods could generate the access control rules properly and detect the policy violation.

In this research, we consider that the policy-based network management are efficient framework to integrate the organizations' network security system but the methods to map high-level policy into the actual access control rules on the network entities are needed. Then we have proposed the methods to generate access control rules from the policy and detect the policy violation. As the future work, the implementation of full-proposed framework will be made and need to verify that the system can be applied to the large actual network system and work properly. And then we consider the research for a) the representation of various policies other than access control policies, b) the detection methods of the policy conflicts and c) the meta-filtering language.