Rule-Based Policies for Secured Defense Meetings

Pravin Shetty
Monash University, Australia

Seng Loke
La Trobe University, Australia

INTRODUCTION

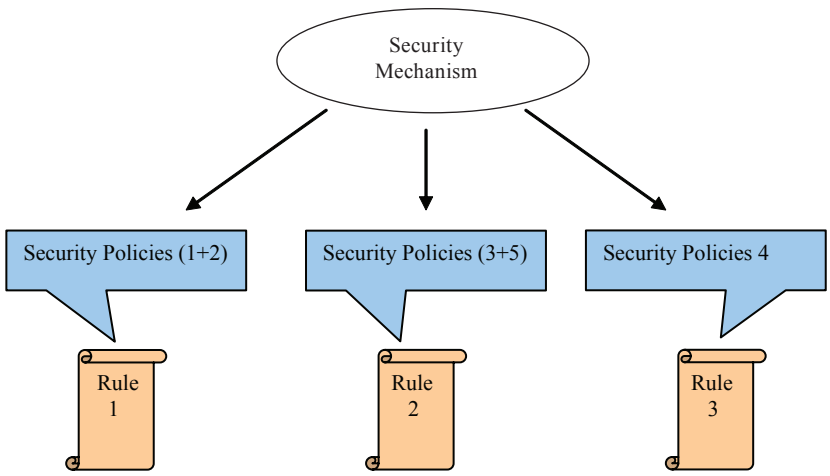
Security of the information in a defense department of any country is of utmost importance. And today, in this nuclear world, security and privacy of the various defense plans and other valuable strategies of a country's defense force is in focus. This security is of prime importance during war periods. The defense strategies are normally discussed in the meetings held at the various headquarters of the defense department. In today's computing world these meetings are conducted with the various concerned persons connected via a secured network in a room. If a person is unable to attend a meeting due to some important work, then he or she takes part in the discussion through his or her laptop. Such meetings involving technology have also become a part of research centers where innovation of new technologies is being carried out.

Such meetings involving technology are efficient when they have to be conducted in an emergency, but the question about the secured flow of data still remains. The main aim of this article is to strive for effective security solutions in such areas where the privacy of each and every piece of information is absolutely essential. The article provides a security infrastructure for such meetings. The security policies here are defined in a rule-based formalism. Figure 1 shows the approach used in this article.

'Security Policies' in Figure 1 refers to the security policies put forth by the integrated security model. The figure shows how the access rules make reference to the security policies that are also used in a similar fashion in the context-based security approach using context graphs. Each access rule can be a combination of one or more than one security policy depending on the context.

The rule-based technique provides the following two basic functions in achieving adaptive security solutions:

Figure 1. Access rules in the rule-based formalism



- capturing security policies and rules that are subject to frequent changes
- implementing those changes quickly and efficiently

Thus rule-based techniques play an important role in modeling security policies in any pervasive computing scenario. The article manifests the use of rule-based formalisms coupled with modular policy concepts.

SECURITY ARCHITECTURE

Figure 2 shows the overall security architecture in a military meeting scenario. The architecture is actually divided into two scenarios. The first one is for the access to the meeting network and the second is the access to the resources themselves. The basic steps that are performed are the same in both the cases. Further a user can access the network either physically or remotely. The access rules for all such cases are defined with policies (Cardelli & Gordon, 1998; Bugliesi, Castagna, & Crafa, 2001; Cardelli, 1999), declared with the help of rules (Mostefaoui & Brezillon, 2003) and stored in the policy server. The following subsections discuss the main components of the architecture.

Policy Server

The policy server has three main functions:

- storage of access rules
- authentication mechanism based on the access point
- validation of the request based on the information from the context storing area and the evaluation of the access rules

As shown in Figure 3, the policy server consists of three subcomponents:

- a **rule repository**, where all the access rules are stored;
- an **authentication mechanism**, which consists of the records of the valid usernames and the passwords; and
- a **rule evaluator**, which takes inputs from the context storing area and the authentication mechanism, and evaluates the request based on the access rules stored.

The access rules stated are based on the rule-based technique. The various situations in a military meeting

Figure 2. Overall architecture