Chapter 3.16
Policy Technologies for Security Management in Coalition Networks

Seraphin B. Calo
IBM Research, USA

Clare-Marie Karat
IBM Research, USA

John Karat
IBM Research, USA

Jorge Lobo
IBM Research, USA

Robert Craven
Imperial College, UK

Emil Lupu
Imperial College, UK

Jiefei Ma
Imperial College, UK

Alessandra Russo
Imperial College, UK

Morris Sloman
Imperial College, UK

Arosha Bandara
The Open University, UK

ABSTRACT

The goal of policy-based security management is to enable military personnel to specify security requirements in terms of simple, intuitive goals. These goals are translated into the concrete system settings in a way that the system behaves in a consistent and desirable way. This technology minimizes the technical expertise required by military personnel and automates security management while allowing a high level control by the human in the loop. This chapter describes a framework for managing security policies, and an overview of two prototypes that simplify different aspects of policy management in the context of coalition operations.

DOI: 10.4018/978-1-60960-587-2.ch316

INTRODUCTION

Secure, reliable and adaptable communications is needed to support dynamic mission-based coalitions of partners from different military and

non-military organizations. If sensitive information is communicated to the wrong person/device, it could cost the lives of the personnel involved in the mission. Likewise, if necessary information is not communicated and shared with the right people, it could also lead to loss of lives. Policy-based security management should enable military personnel to specify security requirements in terms of simple, intuitive goals that are translated into the concrete system settings in such a way that the system behaves in a consistent and desirable way. The objective is to minimize the technical expertise required by military personnel, and to automate policy management as far as possible. This is dependent on being able to specify and analyze policies to ensure that they prescribe correct and desirable behavior. For example, inconsistencies should not arise because the available communication devices cannot support the specified policies. We assume that military personnel specify goals using a structured natural language aimed at non-technical people. Goals are automatically translated into a formal, logic-based abstract language for refinement and analysis. Our past experience has indicated that logic languages, while good for reasoning, are not amenable to efficient implementation, particularly on small hand-held devices. Thus abstract policies must be translated into concrete implementable policies described in languages such as Ponder2 (Twidle et al, 2008), XACML (OASIS XACML TC, 2005), or CIM-SPL (Agrawal et al, 2007).

We start with the presentation of a policy-based security management framework for complex, dynamic, ad hoc systems. This provides the platform supporting mechanisms for adapting system behaviors to meet high-level user-specified security policies through the enforcement of low-level controls in coalition networks. To accomplish this, end-to-end policy mechanisms are described that capture the security requirements of the system, transform them into constraints on the system resources and executable policies, which are then disseminated to and executed upon the appropriate distributed entities within the coalition network. Yet without analysis much of the benefit of using policy-based techniques and declarative policy languages may be lost. Arguably, the lack of effective analysis tools accounts in part for the lack of wider adoption of policy-based techniques. In order to perform analysis, policies must be expressed unambiguously in a manner that captures their semantic meaning. We describe an approach based upon a logical construct for the specification and analysis of security policies. This construct is developed over a very expressive policy language that may be used to represent policies and systems at many different levels of abstraction and stages during the refinement process.

In order to bring together and demonstrate the various policy technologies for security management, two concept prototypes are discussed. These served to integrate some capabilities and provided an end-to-end view of the policy lifecycle for coalition systems. They were based on user scenarios. The purpose of a user scenario is to provide sufficient context about a problem-space being investigated so that researchers can identify the scientific, technical, and feasibility questions they must address in the research. A user scenario can be a valuable research and design tool for scientists to employ to understand the trade-offs about different options in the context of the targeted end user. Details of these prototype demonstrations are presented, as are a number of research questions that arose during their development.

FRAMEWORK FOR SECURITY POLICIES

Our framework for policy analysis and refinement captures policies at various levels of abstraction (or layers), which identify the key stages in the process of refining policies from goals to implementations. The layered architecture is useful in identifying the architectural elements, software components, and system models that are needed