Chapter 2.16
Policy-Based Security Engineering of Service Oriented Systems

Antonio Maña
University of Málaga, Spain

Gimena Pujol
University of Málaga, Spain

Antonio Muñoz
University of Málaga, Spain

ABSTRACT

In this chapter the authors present a policy-based security engineering process for service oriented applications, developed in the SERENITY and MISTICO projects. Security and dependability (S&D) are considered as first-class citizens in the proposed engineering process, which is based on the precise description of reusable security and dependability solutions. The authors' process is based on the concept of S&D Pattern as the means to capture the specialized knowledge of security engineers and to make it available for automated processing, both in the development process (the focus of this chapter) and later at runtime. In particular, in this chapter they focus on the verification of the compliance with security policies, based on the formal specification of S&D Properties. The main advantages of the approach presented in this chapter are precisely that it allows us to define high-level policies and to verify that a secure oriented system complies with such policy (developed following the SERENITY approach). They also describe the application of the proposed approach to the verification of S&D properties in the web services (WS) environment. Concretely, the authors describe the use of SERENITY framework to facilitate the development of applications that use standard security mechanisms (such WS-Security, WS-Policy, WS-Security Policy, etc) and to ensure the correct application of these standard mechanisms, based on predefined policies. Finally, they show how to verify that the application complies with one or several S&D policies.

DOI: 10.4018/978-1-60566-950-2.ch006

INTRODUCTION

The popularization of open and distributed computing environments like mobile and ubiquitous computing, service oriented computing, ambient intelligence and sensor networks among others, indicates an irreversible trend towards distributed computing. This trend, along with the ever-growing number and importance of the computer-supported aspects of our daily lives, has raised the demands for security and dependability and has exposed the limitations of the current security and dependability solutions. Moreover, we exposed the limitations of current security engineering and software engineering methodologies and tools. In particular, the shift toward service-oriented computing increases the emphasis on relationships, negotiations, and agreements. This brings particular challenges for the area of security and dependability, which are traditionally very difficult to manage and measure. Additionally, it introduces accountability and liability issues, which are topics widely debated.

According to the conclusions of the ESFORS group of experts the state of the art of development processes for secure systems in open communication environments has to be considerably improved. Such improvements should include methods for precise specification of security policies and requirements, as well as the automated tools for classifying, selecting, adapting, and reorganizing existing security services, for integrating them into software systems under development, and last but not least for verifying the compliance of systems with security regulations and policies. Furthermore, special specification for the expression of security requirements have to be integrated into existing modelling languages to support rigorous treatment of security issues throughout the entire development process.

Although, security is an essential aspect in computing and communication, it has been traditionally overlooked and considered supplementary instead of a core element in the design and development of such systems. This concern has implied consequences and has been undermined the users' confidence in computer systems. Corporate scandals and breakdowns like the recent loss of 45 Million credit and debit card numbers and other personal data by the TJX Corporation, which have flourished in the last years, highlights the need for stronger compliance regulations for publicly listed companies.

One of the most significant regulations in this context is the Sarbanes-Oxley Act, developed in 2002, which defines significant tighter personal responsibility of corporate top management for the accuracy of reported financial statements. Last case shows how many of the best known initiatives for enhancing the security of computer systems have been based on guidelines, recommendations, best practices, certification, compliance and similar approaches lacking the necessary rigour and precision that one would expect when dealing with "security". Other relevant examples are: Common criteria, Federal Information Processing Standards (FIPS), traditional security patterns, Gramm-Leach-Bliley Act (GLBA), Federal Information Security Management Act (FISMA), and Health Insurance Portability and Accountability Act (HIPAA). In some cases other compliance frameworks, such as Control Objectives for Information and related Technology (COBIT), or standards as National Institute of Standards and Technology (NIST) inform on how to comply with the regulations.

The fact that all these regulations and policies are expressed informally or semi-formally make practically impossible to rigorously verify that an application complies with a specific regulation. In fact, several initiatives have been launched with the goal of verifying that applications comply with certain security policies. However, in these proposals, the concept of "security policy" refers to a set of low-level restriction. However, one common drawback of all these approaches is that they are strongly related with the low-level details (language, OS, development framework, etc.) of the application to be checked.