Chapter 4
Organizational Patterns for Security and Dependability: From Design to Application

Yudis Asnar
University of Trento, Italy

Fabio Massacci
University of Trento, Italy

Ayda Saidane
University of Trento, Italy

Carlo Riccucci
Engineering Ingegneria Informatica S.p.A, Italy

Massimo Felici
Deep Blue, Italy

Alessandra Tedeschi
Deep Blue, Italy

Paul El-Khoury
SAP Research, France

Keqin Li
SAP Research, France

Magali Séguran
SAP Research, France

Nicola Zannone
Eindhoven University of Technology, The Netherlands

ABSTRACT

Designing secure and dependable IT systems requires a deep analysis of organizational as well as social aspects of the environment where the system will operate. Domain experts and analysts often face security and dependability (S&D) issues they have already encountered before. These concerns require the design of S&D patterns to facilitate designers when developing IT systems. This article presents the experience in designing S&D organizational patterns, which was gained in the course of an industry lead EU project. The authors use an agent-goal-oriented modeling framework (i.e., the SI framework) to analyze organizational settings jointly with technical functionalities. This framework can assist domain experts and analysts in designing S&D patterns from their experience, validating them by proof-of-concept implementations, and applying them to increase the security level of the system.*

DOI: 10.4018/978-1-4666-2482-5.ch004

INTRODUCTION

Security and Dependability (S&D) are critical aspects in the development of IT systems (Anderson, 2001). The usual approach towards the inclusion of S&D concerns within a system is to identify security requirements after system design. Unfortunately, this makes the process inefficient and error-prone, mainly because security mechanisms have to be fitted into a pre-existing design which may not be able to accommodate them.

The literature in requirements engineering has highlighted the importance of analyzing S&D aspects since the early phases of the software development process (Giorgini et al., 2005a; Liu et al., 2003). It is also well accepted that S&D cannot be considered as purely technical issues but should be analyzed together with the organizational environment (Anderson, 1993). In this direction, goal-oriented approaches (Dardenne et al., 1993; Bresciani et al., 2004) have gained momentum in the community showing their relevance to model and analyze security issues within the organizational setting. This has spurred the definition of several goal-oriented frameworks for security requirements engineering (e.g., Giorgini et al., 2005a; Elahi et al., 2007). Requirements analysis, thus, is an iterative process where domain experts and analysts have to collaborate to elicit and analyze S&D requirements, besides the functional requirements of socio-technical systems. Often these security needs are common or "similar" to problems that security experts have seen before, and consequently the solution can be "similar" as well. The idea of using S&D patterns to provide solution to security requirements stems from this simple observation above. Patterns have been adopted into software engineering as a method for object-based reuse (Gamma et al., 1994) and security patterns (Yoder et al., 1997; Schumacher, 2003) have been proposed to capture and structure collective experience in the S&D domains and make this know-how available and exploitable for application designers. This transfer of knowledge is intended to improve the quality of the developed systems from an S&D point of view. However, most S&D patterns presents in the literature are technical patterns. Here we focus on organizational patterns where we consider the overall interactions between human and software components and the relative dependencies.

This article presents the process for capturing, validating, and applying S&D organizational patterns. Our proposed patterns have been used in widely different industrial contexts: Air Traffic Management (ATM) and e-Health Smart Items. In our work, we have adopted the *SI** modeling framework (Massacci et al., 2008), an agent, goal-oriented framework that extends the *i** framework (Yu, 1997) with the concepts of ownership, trust, delegation, and event for capturing and analyzing security and trust requirements of socio-technical systems (Giorgini et al., 2005a), designing access control policies (Massacci et al., 2008), and risk analysis (Asnar et al., 2008). In this article, we show how the *SI** framework has been used by industries for the capturing of S&D organizational patterns and their validation by proof-of-concept implementation. We also discuss how patterns can be applied to a system so that it has a sufficient level of security.

The article is organized as follows. Next, we introduce S&D organizational-patterns, their elicitation process using the *SI** modeling language (§2) and the formal frameworks underlying *SI** for pattern validation (§3). We present an excerpt of our library of S&D organizational patterns (§4) and describe how these patterns can be used in real systems (§5). Finally, we discuss related work and conclude with lessons learned from the case studies (§6).

Designing S&D Organizational Patterns

At the organizational level, a system can be seen as a set of interacting actors (e.g., humans, organizations, software agents), each of them is in charge