Chapter XI
An Ontology for Secure Socio–Technical Systems

Fabio Massacci
University of Trento, Italy

John Mylopoulos
University of Trento, Italy

Nicola Zannone
University of Trento, Italy

ABSTRACT

Security is often compromised by exploiting vulnerabilities in the interface between the organization and the information systems that support it. This reveals the necessity of modeling and analyzing information systems together with the organizational setting where they will operate. In this chapter we address this problem by presenting a modeling language tailored to analyze the problem of security at an organizational level. This language proposes a set of concepts founded on the notions of permission, delegation, and trust. The chapter also presents a semantics for these concepts, based on Datalog. A case study from the bank domain is employed to illustrate the proposed language.

INTRODUCTION

The last years have seen the emergence of standards for capturing security and privacy aspects of information systems (Ashley, Hada, Karjoth, Powers, & Schnuter, 2003; Cranor, Langheinrich, Marchiori, & Reagle, 2002; OASIS, 2005). Those standards provide language constructs but offer no methodological tool for actually making design decisions. In this setting, the inclusion of security features within the system design is usually done after the functional design phase. This is a critical issue since security services
An Ontology for Secure Socio-Technical Systems

and related protection mechanisms have to be fitted into an existing design that might be not able to accommodate them.

It is generally accepted in the requirements engineering (RE) research community that system development requires models that represent the system-to-be along with its intended operational environment. This is even more important when the system has to meet security requirements, since security breaches often occur at an organizational level, rather than a technical one (Anderson, 1994). Even though there are mature methodologies for modeling and analyzing enterprises and their organizational structure, their focus is mostly on process and marketing aspects rather than security (AMICE Consortium, 1993; Bryce & Associates, 2006; Dignum, 2004; Hübnner, Sichman, & Boissier, 2002; Stader, 1996; Yu, 1996).

Socio-technical system analysis has been proposed to overcome this issue (Emery & Trist, 1960). This approach aims at capturing the interactions between people and technology in workplaces. In this setting, security is the ability of the system to protect itself against deliberate misbehavior by actors of the organizations involved in the application scenario while still providing expected services when requested by benign actors. For instance, an actor may abuse his position within the organization to gain personal advantages (House of Lords, 1999; Michaely & Womack, 1999). Therefore, modeling and analyzing the organizational environment where the system will act is crucial for building secure systems. This allows designers to identify security mechanisms that can best protect the system, and their impacts on the system.

This chapter aims at analyzing the problem of modeling security at an organizational level. Based on such an analysis, we identify and formally define basic ontological primitives for modeling organizational and security concepts, paying particular attention to the security relevant social interaction within organizations.

To allow for a systematic design of security in organization, we have developed an agent-oriented requirements engineering methodology, Secure Tropos (Giorgini, Massacci, Mylopoulos, & Zannone, 2006; Giorgini, Massacci, & Zannone, 2005), tailored to describe both the organizational environment of a system and the system itself. The methodology provides a requirements analysis process that drives system designers from the acquisition of the requirements model up to its verification and validation. One of its main features is the prominent role given to early requirements analysis phase that precedes a prescriptive requirements specification. The main advantage in having such a phase is that one can capture not only the “what” or the “how”, but also “why” a software system is developed. Secure Tropos was originally based on the i* modeling framework (Yu, 1996). This framework has already been used to model and analyze security requirements (Liu, Yu, & Mylopoulos, 2003). In this work, security requirements are treated as nonfunctional requirements. This approach supports the representation of design decisions that can contribute to a security goal and the modeling of attackers (both internal and external) who prevent the fulfillment of goals.

However, our work revealed early on that the i* ontology needs to be extended in order to adequately model security because it lacks fundamental concepts needed in order to talk about security within an organization (Giorgini et al., 2006). To this end, we have proposed an enhanced ontology with three main notions, namely ownership, delegation, and trust, which together form the very foundation of all security concerns (Giorgini et al., 2005). Ownership is used to identify goals, tasks, and resources that an actor controls; delegation is used to model the transfer of entitlements and responsibilities between actors; finally, trust represents the belief of actors about the behavior of other actors (Mayer, Davis, & Schoorman, 1995; Rousseau, Sitkin, Burt, & Camerer, 1998). Once basic ontological primitives have been identified, we develop a comprehensive ontology tailored to model security at an organizational level. To this end, we provide an axiomatic characterization of their intended semantics using answer set programming (Leone et al., 2006). The proposed ontology is intended to serve as