Modelling Security Using Trust Based Concepts

Michalis Pavlidis, University of East London, UK

Haralambos Mouratidis, University of East London, UK

Shareeful Islam, University of East London, UK

ABSTRACT

Security modelling and analysing not only require solving technical problems but also reasoning on the organization as a whole for the development of a secure system. Assumptions exist about trust relationships among actors within the system environment, which play an important role in modelling and analysing security. Such assumptions are critical and must be analysed systematically for ensuring the overall system security. In this paper, the authors introduce trust-based concepts to identify these trust assumptions, and integrate the trust concepts with security concepts for the development of secure software systems. For this purpose, Secure Tropos' security modelling activities are extended with trust modelling activities based on the trust-based concepts. The CASE tool SecTro was extended to include the notation of the trust-based concepts to support the methodology. Finally, a running example from the UK National Health Service (NHS) domain is used to demonstrate how trust can be used for security modelling.

Keywords: *Control, Secure Tropos, Security Modelling, Trust, Trust Modelling, Trustworthiness, Trustworthy Systems*

INTRODUCTION

Modern society heavily depends on software systems to process and manage sensitive information. It is expected that such systems should have the capability to ensure the overall system security. If security is violated, then it can result in any potential loss such as money, time, reputation, and disclosure of sensitive information. A careful security analysis is necessary for the development of secure software systems. Modelling supports the security analysis by reasoning about security, so that developers can understand the relevant security concepts such as security requirements, goals, resources and mechanisms for a specific system context. The consideration of security though, should not be done in an ad-hoc way but in a systematic and proactive way. It should be considered throughout the development process, and in particular from the early stages of the development process and along with the functional requirements. This allows avoiding potential conflicts that lead to security vulnerabilities and identifying possible tradeoffs that are required between the functional and security requirements.

DOI: 10.4018/jsse.2012040102

The size and complexity of software systems has increased significantly and systems are not isolated any more, but interact with external components to meet the objectives. Security of such systems depends on overall organizational settings where actors perform actions to achieve goals. Identifying security issues in such organizational settings is difficult and very likely that some important security information might be omitted or not properly treated. Security modelling plays an effective role for capturing and analysing security issues (Houmb et al., 2010). Rasmusson and Janssen (1996) define two types of security, i.e., hard and soft. Hard security is the security mechanisms that protect the system against any potential attack. However, users are sometimes more concerned about the quality of the received resource even though the security mechanism is implemented. Soft security contributes on this context; in particular it deals with the quality of a resource by ensuring that a resource should be received with the appropriate quality. There exist trust assumptions for the proper operation of the security mechanisms and for the appropriate quality of the receiving resources. Therefore, security mechanisms and resource providers need to be trustworthy to satisfy the goals. If such trust assumptions are left unreasoned and proved to be wrong, they can pose potential security vulnerabilities.

Within the given context, the main contribution of this paper is to introduce a set of trust-based concepts and to integrate them with security concepts to support security modelling activities. A running example from the health care domain is used to demonstrate the applicability of the trust concepts for modelling security. We propose trust-based concepts such as trust types (reported, experiential, normative, and external trust), control, resolution and entailment and integrate these concepts with the security concepts. We adopt Secure Tropos' security concepts such as secure dependency, constraint, goal, plan, and resource and extend it with the trust-based concepts so that trust modelling activities can support security modelling activities. Secure Tropos is an appropriate candidate in our case, since it models not only the system itself, but also the overall system environment (Mouratidis & Giorgini, 2007; Islam et al., 2011). Secure Tropos captures the system environment through actors who perform actions to achieve goals by using resources and by depending on other actors. Security requirements are represented as security constraints and satisfied by secure goals. These dependencies allow integrating the trust concepts so that we can reason about the trustworthiness of the actor to fulfill the dependency. Secure Tropos identifies and assigns security responsibilities to the actors without analysing whether an actor is trusted or not for that specific purpose. Our work supports the analysis of whether an actor can be trustworthy to fulfill the assigned secure goal, to carry out a secure plan, or to deliver a quality resource. The security modeling activities model the security concepts, while the trust modeling activities model the trust concepts. The trust modeling activities justify the existing trust relationships among the dependencies to ensure the overall system security. The proposed trust concepts are visually represented using notation within the existing SecTro CASE tool of Secure Tropos (Pavlidis & Islam, 2011; Pavlidis et al., in press). A running example from the National Health Service (NHS) system in United Kingdom is used to demonstrate the applicability of using trust for security modelling.

The paper is organized as follows. In the following section there is a brief overview of Secure Tropos followed by sections that introduce the trust-based concepts and the process that extends the Secure Tropos modelling activities. The running example is presented, which is followed by the related work and discussion. The last section concludes the paper and presents future work.

AN OVERVIEW OF SECURE TROPOS

Secure Tropos is an extension of Tropos methodology (Bresciani et al., 2004) in terms of