Although the concepts of security and trust play an important issue in the development of information systems, they have been mainly neglected by software engineering methodologies. In this chapter, we present an approach that considers security and trust throughout the software development process. Our approach integrates two prominent software engineering approaches, one that provides a security-oriented process and one that provides a trust management process. The result is the development of a methodology that considers security and trust issues as part of its development process. Such integration represents an advance over the current state of the art by providing the first effort to consider security and trust issues under a single software engineering methodology. A case study from the health domain is employed to illustrate our approach.
INTRODUCTION

It has been identified in many cases that securing information systems is not only about providing a set of standard security mechanisms such as authentication or confidentiality. Providing adequate security requires the capability of reasoning about security and its related concepts. Some related concepts, and in particular trust, have been identified by recent research (DeTreville, 2002; Li, Mitchell, & Winsborough, 2002; Samarati & di Vimercati, 2001) as an important aspect to be considered when reasoning about security.

Anderson (2001) has recognised the need to integrate an in-depth analysis of security and trust issues during the development of information systems. Such analysis should allow developers not only to model security and trust but also, and most importantly, to reason about these concepts. In other words, securing information systems needs to evolve from a “one fits all” solution, where developers introduce standard security mechanisms such as authentication to various parts of the system without taking into account any interrelation and even conflicts with other requirements of the system, to completed and integrated solutions according to the real security requirements of the system, which also take into account any trust relationships that might affect the security of the system. However, up to now, the current state of the art does not provide modelling languages and methodologies to assist developers to consider security and trust when they develop information systems. This statement provides the main motivation behind our work. Our goal is to provide such languages and methodologies.

In this chapter, we describe how the integration of two prominent software engineering approaches, one that provides a security-oriented process (Mouratidis, 2004; Mouratidis, Giorgini, & Manson, 2005) and one that provides a trust management process (Giorgini, Massacci, Mylopoulos, & Zannone, 2004, 2005a, 2005b; Giorgini, Massacci, & Zannone, 2005d) results in the development of a methodology that considers security and trust issues as part of its development process. Such integration represents an advance over the current state of the art by providing the first effort to consider security and trust issues under a single software engineering methodology.

The chapter is structured as follows. Next section provides an overview of the Tropos methodology and discusses the issues of using the Tropos methodology for modelling security concerns. The following section describes the Secure Tropos concepts and modelling activities, whereas the next section presents the revised Secure Tropos process. The two subsequent sections discuss the formalisation of the Secure Tropos concepts and present an application of the Secure Tropos methodology to a case study from the health care domain. The last two sections present related work and conclude the chapter.
Critical Evaluation of Hazards Operability Versus Safety Integrity Risk Analysis Techniques