Chapter 8.7
Inegrating Security and Software Engineering:
Future Vision and Challenges

H. Mouratidis
University of East London, UK

P. Giorgini
University of Trento, Italy

ABSTRACT

The previous chapters of this book have presented promising approaches in the secure software engineering field. However, the field is still in its infancy and a number of challenges still need to be answered. The main aim of this chapter is to list and discuss nine challenges that we find important for the advance of the secure software engineering field. The main idea behind each challenge is presented in a short sentence followed by a discussion, which indicates why the challenge is important. In some cases, the discussion provides some ideas of how the challenge could be met.

INTRODUCTION

It has been widely argued in the literature, and throughout this book, that although the need to integrate security within software engineering practises has been identified at least for the last three decades, up to few years ago most of the efforts to solve such problem were random approaches initiated from individual researchers. However, and as it is evidence from the chapters of this book, the last few years the number of researchers working towards approaches to solve this problem has increased substantially. This evolving situation is the result of two main factors. Firstly, the broad awareness of the need to secure software systems has resulted in the identification of the situation as a key challenge for software and security engineers. Secondly, the appearance of specialised research events, which emphasise the need to integrate security issues within the software system development practice (see for example www.sreis.org and http://www.jmu.edu/iiia/issse/).

Most of the researchers and practitioners involved in such research and/or events mainly have the same future vision. The maturity of secure software engineering in such a degree that software developers will be able to model, construct, test, deploy, and maintain secure software systems through well defined and structured processes and with the aid of appropriate modelling languages. In such a vision, development is made even easier with the aid of computer-aided tools that enable to accurately track the security solution to the initial system requirements and therefore validate it against the security goals of the organisation where the system is deployed.

The previous chapters of this book have discussed work that brings us closer to that vision. In particular, the previous chapters have presented approaches and frameworks that allow reasoning about security requirements, methodologies, and pattern languages to model security requirements and support the development of secure software systems.

However, many challenges still need to be answered by researchers and practitioners working in the field. The rest of this chapter list and discusses nine challenges that we find important for the advance of the secure software engineering field.

THE CHALLENGES

Challenge 1: Unify Efforts to Integrate Security and Software Engineering

Although the need for such unification has been recognised by various researchers (see for example the literature review presented in Chapter I or the discussions in the previous chapters of this book), work on integrating security and software engineering is mainly carried out independently either by members of the security research community or by members of the software engineering community. It is important to unify the efforts on the two fields. Only then we will be able to precisely identify the technical as well as the social issues that surround the development of secure information systems and produce solutions that truly work.

Challenge 2: Consider the Social Dimension of Security

Security is mainly considered as a technical issue by software and security engineers alike. However, it is now widely accepted that a technical only approach in the development of secure software systems will not produce the expected results, since security is a multidimensional issue that cannot be considered in isolation. Especially, with the advances on software systems and the transition towards open and autonomous systems, issues such as sociality, trust, privacy, and delegation of responsibilities are closely related to the security of software systems.

This argument is also supported by recent research, which has shown that the human factor has a significant impact on security. For example, one of the main threats to medical private records is social engineering. Social engineering is a non-technical kind of intrusion that relies on human interaction and involves tricking other people (doctors, or nurses in the case of medical records) to break normal security procedures. A mature solution that integrates security and software engineering should consider not only the technical dimension of security but also the social dimension. It is only when we consider both dimensions that we will be able to develop secure enough information systems.

Challenge 3: Develop Complete Security Ontology

The need for sound and complete security ontology is well recognized as an important issue for the development of widely accepted solutions on