

Preface

In the coming years, information technology will continue to transform the way we think, work, communicate, and learn. The tremendous success of Internet-related technologies (web services, voice over IP, mobile telephony, etc.) coupled with advances both in hardware and software will invigorate the existing proliferation of software intensive systems. This will allow for new services, applications, and systems that will recede increasingly into the background of our lives. In this setting, the secure engineering of such software-intensive systems becomes a major concern. This is emphasized by the fact that security breaches of software systems keep appearing at an alarming rate in spite of numerous updates and patches that are constantly being issued.

Unfortunately, in many organizations, the emphasis on operational security usually leads most investments to be directed to network security measures, such as firewall, virtual private network, intrusion detection system, etc. However, in spite of significant efforts on network security, the scale and severity of security breaches have been increasing with no victory in sight in this arm race against attackers. Recently, new efforts have emerged in extending the defense by rooting the security in software itself. However, given the complexity and pervasiveness of today's software systems, building secure software is a challenging task. In most cases, the security of software widely depends on developers' awareness of security requirements, which is unfortunately not always present. To reduce the burden on developers, there is a clear need for practical tools and methods for secure software development.

Very often security practices are added to existing software either as an after-thought phase of the software development life cycle, or manually injected into software code or UML models. However, this practice is no longer acceptable for such an important aspect, especially with the increasing complexity and pervasiveness of today's software systems. Therefore, security must be addressed during the early phases of the software engineering process. A promising approach to early security hardening is to leverage prominent modeling languages, such as the Unified Modeling Language (UML) for the specification, verification, and hardening of software security. Indeed, using UML for secure software development

would have more practical significance considering the fact that UML is the de-facto standard for object-oriented modeling of software systems and there exist many tools for UML modeling. In addition, UML supports standard extension mechanisms that enable the language to be customized for different platforms or domains.

Besides, because of the pervasive nature of security, adding security manually into a UML design is tedious, may lead to additional security vulnerabilities, and security components may become tangled and scattered throughout the whole design. Consequently, the resulting UML design model will most likely become difficult to understand and maintain. In this respect, the aspect-oriented technology emerged as an appealing approach for security hardening. This paradigm has received considerable attention from researchers and industrial practitioners alike. It allows a more advanced modularization by separating crosscutting concerns, such as security, from the software functionalities. Due to the increasing interest, the aspect-oriented technology has stretched over earlier stages of the software development life cycle. Aspect-Oriented Modeling (AOM) applies aspect-oriented techniques to software models with the aim of modularizing crosscutting concerns. It carries over the advantages of aspect-oriented programming to the modeling level. Indeed, handling those concerns at the modeling level would significantly help in alleviating the complexity of software models and facilitate reuse of existing design models.

This book contributes to the secure engineering of software-intensive systems. To this end, it extends current model-driven engineering paradigms and prominent modeling languages, such as UML, to address security concerns throughout the development life cycle. Moreover, it leverages the AOM paradigm for the specification and the systematic execution of security hardening practices on UML models. In this regard, a UML profile has been developed for the specification of security hardening aspects on UML diagrams. In addition, a weaving framework, with the underlying theoretical foundations, has been elaborated for the systematic injection of security aspects into UML models. The book will benefit researchers in academia and industry as well as students in the field of software and systems engineering. The reader will find, in this book, an overview of the research advancements related to model-based software security hardening.

The book is organized as follows: Chapter 1 presents an introduction to software security, model-driven engineering, UML, and aspect-oriented technologies. Chapter 2 provides an overview of UML language. Chapter 3 describes the main concepts of AOM. Chapter 4 explores the area of model-driven architecture with a focus on model transformations. The main approaches that are adopted in the literature for security specification and hardening are presented in Chap. 5. Chapter 6 presents our AOM profile for security aspects specification. Afterwards, Chap. 7 details the design and implementation of the security weaving framework. In addition, several real-life case studies are illustrated to demonstrate the relevance

of the proposed framework for security hardening. Chapter 8 elaborates an operational semantics for the matching/weaving processes in activity diagrams. Moreover, Chaps. 9 and 10 elaborate a denotational semantics for aspect matching and weaving in executable models following a continuation-passing style. Finally, a summary and evaluation of the presented work are presented in Chap. 11.

March 2015

Djedjiga Mouheb
Mourad Debbabi
Makan Pourzandi
Lingyu Wang
Mariam Nouh
Raha Ziarati
Dima Alhadidi
Chamseddine Talhi
Vitor Lima

Aspect-Oriented Security Hardening of UML Design
Models

Mouheb, D.; Debbabi, M.; Pourzandi, M.; Wang, L.; Nouh,
M.; Ziarati, R.; Alhadidi, D.; Talhi, C.; Lima, V.

2015, XVIII, 237 p. 123 illus., Hardcover

ISBN: 978-3-319-16105-1