Review of the book

"Security Engineering for Service-Oriented Architectures"

by Michael Hafner and Ruth Breu

Springer, 2009

ISBN: 978-3-540-79538-4

Luigi Lo Iacono

1 Summary

The book by Hafner and Breu gives an overview on how to systematically design and realize security-critical service-based applications following the model-driven development methodology. Whenever the book talks about SOA or services, it is talking about the technical realisation of SOA using SOAP and related technologies and standards.

The book is divided into three main parts. In the first part, the necessary foundations are introduced. Since the focus of the book relies on the model-driven development of secured SOAP-based Web Services, the initial part deals with SOAP and the related standards and technology stack as well as the model-driven software development methodology. In the second part, the design and realisation of security-critical service-based applications following the model-driven security methodology is presented. The approaches developed by the authors for the management of security requirements (called ProSecO) and to perform the model-driven security engineering (called SECTET) are discussed. These explanations are guided by an example scenario from the e-government domain. The book closes by discussing the usage of model-driven security in general and ProSecO and SECTET more specifically in a case study from the healthcare domain.

2 Detailed description

This book of 230 pages (including the appendices) begins with an introduction to the required foundations. SOAP-based Web Services are introduced as a mean to implement SOA-based information systems. The book limits itself to this technology stack for realizing service-based systems. Before the related standards to secure SOAP-based systems (mainly focusing on WS-Security and XACML) are briefly introduced, some general security concepts and terms are presented. This introductory part closes with a primer on model-driven development and the definition for model-driven security used in remainder of the book.

In the second part, the authors approach the topic of model driven security for SOAP-based inter-organizational workflows by discussing two concrete developments they did. The first is related to the engineering of security requirements and is called ProSecO. The second is a framework for the model-driven configuration and management of security infrastructures and is called SECTET. While referring to an example scenario from the e-government domain, the book goes through the typical high-level (security) engineering steps (analysis, design, implementation and monitoring) and shows how these steps can be performed by adopting the model-driven development principles and concepts and by using ProSecO and SECTET.

In the final part of the book, the model-driven security development based on ProSecO and SECTET is illustrated through the presentation and discussion of a case study from the healthcare domain.

3 Recommendation

The book touches a very important topic, which will become even more important in the future, namely the security of SOA-based information systems which span across multiple distinct organizational domains. Overall, the book is a good starting point for people who want to learn how to engineer a security system for a SOAP-based inter-organizational workflow using the model-driven development principles and concepts. It gives a brief overview on the required foundations with adequate references to further readings and approaches this topic by introducing two concrete developments carried out by the authors. The book is written and structured in a clear and well-formed manner using a continuous example to motivate the authors' developments as well as a case study to illustrate the adoption of model driven security.

The title of the book is very misleading and unfortunately there is neither an adequate subtitle nor a hint on the back cover explaining that by SOA Hafner and Breu mean SOAP-based Web Services. A reader looking for a more general book on SOA security engineering or on other technologies to implement a SOA-based system such ESB or REST will not find anything related in this book.

Another drawback lies in the fact, that the discussions are not comprehensive enough from a security perspective. The focus is very much on the standard security services such as confidentiality, integrity, authentication and authorization (incl. delegation). Other equally important aspects in inter-organisational SOA-based workflows not discussed in this book include trust federation and management, identity management and auditing.

Finally it is not clear, whether the presented approaches ProSecO and SECTET—both developed by the authors—are already in a stage for the development of productive systems. This makes the contribution of the book somewhat useless for practitioners.

Due to these drawbacks, the book fails to deliver the expected content as given by the book's title and to meet the demands of practitioners. Thus, currently the audience mainly benefiting from this book is regarded as students and researchers.

The reviewer is a senior researcher at NEC Laboratories Europe.