

# Preface

Information security management is a challenging topic, due to the difficulty of exhaustively modeling attackers for an entire system and the threats they cause to it. The idea of security standards and their respective certification schemes is an excellent one. Companies can use a security analysis process in a standard and establish a security product, e.g., a secure software or a process for information security. Security standards are based on best practices from industry and agreed upon in respective consortiums. After a security standard is established, a certification body checks the security product for compliance with the standard. The certification body shall either certify the successful efforts with an official document or provide guidance on how to improve their security product to achieve certification.

The alternative to a security certification process is to deal with security problems at random points in a system. These isolated efforts can prevent the exploitation of vulnerabilities of several parts of a system, but without a structured and systematic method the security level of the entire organization cannot be determined. Furthermore, inventing an effective process with regard to security not based on best practices or standards is extremely difficult. Not to mention the missing certification option, which includes an outside review of the security analysis. A security standard with a certification infrastructure has the potential to help with these problems effectively.

In 2013 the International Organization for Standardization (ISO) registered in total 22 293 ISO 27001 (ISO/IEC, 2005b) certifications<sup>2</sup> and 246 Common Criteria certifications.<sup>3</sup> These numbers show a low adoption rate of security standards in comparison to other standards such as ISO 9001 for which ISO registered 1 129 446 certifications<sup>4</sup> in 2013. These numbers suggest that security standards are still in the early stages of industrial adoption. Note also that the numbers published by ISO do

---

<sup>2</sup>ISO statistic: [http://www.iso.org/iso/iso\\_survey\\_executive-summary.pdf](http://www.iso.org/iso/iso_survey_executive-summary.pdf)

<sup>3</sup>Common Criteria Statistic: <https://www.commoncriteriaportal.org/products/stats/>

<sup>4</sup>ISO statistic: [http://www.iso.org/iso/iso\\_survey\\_executive-summary.pdf](http://www.iso.org/iso/iso_survey_executive-summary.pdf)

not reflect the size of the organization. It can be assumed that the numbers are even lower when only considering small and medium businesses, due to the required efforts to establish a security standard.

A scientific analysis of understanding why these standards are not largely adopted in industry and what we can do to improve the situation would be a timely research effort with relevance for our society. We can only encourage researchers to look into this problem in a more detailed analysis than we do in this book. We assume, based on discussions with practitioners, that the root cause for the low adoption of security standards is the ambiguity of their texts. Identifying and removing ambiguities is a timely research subject in the requirements engineering community, which is of particular relevance for information security standards. The reason is that these shall be applicable to all kinds of current and future hardware and software products. This requires the standards to be more ambiguous than other standards, due to the frequent changes in these information technology products. This situation should be addressed by providing structured methods, tools, and other support for resolving the ambiguity issues with information security standards. This book provides several such artifacts as examples for how to address this problem.

## **Who is This Book For**

This book is for software engineers, security analysts, and other professionals that are tasked with establishing a security standard, as well as researchers who aim to investigate the problems with establishing security standards. Furthermore, this book can be used to teach undergraduate students about security standards, security requirements engineering methods, context-patterns, and the relations between these topics. The numerous examples and explanations in this book are meant to be understandable by all these readers.

## **What Is the Reward for Reading This Book**

The book presents an analysis of the construction of security standards and the elementary concepts of security requirements engineering methods. We explain how to use this knowledge to build customized methods supporting security standard establishment. Note that this book does not focus on a single approach, but instead shows how to create step-by-step support using different security requirements engineering methods. The methods can be chosen by individual preferences such as familiarity with a particular method. Providing these multiple ways of achieving security standard support makes this book unique.

In addition, we acknowledge the fundamental importance of context elicitation and analysis for security standards. Numerous security issues in the past were

possible due to incomplete context descriptions. Our context-patterns approach helps to close this gap and also to ease the reuse of analysis results. Once readers have understood how to use this approach including describing their own context-patterns, they are empowered to utilize this approach to ease their work with security standards and to improve the results of security standard establishments.

## How to Use This Book

This book can be used in one or more of the activities explained below.

**Understand and Compare Security Standards** using our CAST methodology including available tool support for comparing standards (see Chap. 4). We show a way to describe standards in a high-level and comparable fashion. We described all the standards used in this book using CAST and present the results of a structured comparison. Moreover, the conceptual model CAST is based upon provides insights into the general construction of security standards. In addition, the reader can apply CAST to further standards with little effort.

**Use our Methods for Security Standard Establishment** presented in this book (see Chaps. 6–8). Each of these methods supports a particular standard and focuses on different aspects of security analysis. Hence, readers can choose the method that supports their demands best. The methods also serve as examples on how different the methodologies for security standards can be, due to their ambiguity. The numerous examples in this book even help readers to discover their preferences and identify the right type of method for their needs.

**Create Customized Methods for Establishing Security Standards** by using our relations between security standards and security requirements engineering methods (see Chap. 5). This enables engineers to tailor a given SRE method to support security standard establishment. The methods can be selected by any criteria, such as personal preferences or specific analysis demands.

**Apply Pattern-Based Security Standard Establishment** based on our context-pattern approach, which helps to reuse domain knowledge and support the identification of security analysis tasks that have the potential to be partially automatized (see Chaps. 10–13). Our context-pattern language and example methodology show how to use this approach, which includes the option for the readers to describe their own context-patterns and to create methodologies based on these.

In summary, this book can be used to learn about security standards and security requirements engineering. In addition, it shows how to apply several step-by-step SRE-based methodologies for security standard establishment. Moreover, readers can develop the skills for understanding security standards and create methodologies for supporting their establishment. All this is possible by learning about the fundamental concepts of security standards and security requirements engineering

methods presented in conceptual models in this book. The reader learns how existing standards and methods relate to these models and how to use these relations to create supporting approaches for security standard establishment. Furthermore, our context-pattern approach illustrates how to create supporting methods with a focus on the reuse of analysis results for particular domains and identifying analysis tasks that can be computer-aided.

Dortmund, Germany, February 2015

Kristian Beckers

<http://www.springer.com/978-3-319-16663-6>

Pattern and Security Requirements  
Engineering-Based Establishment of Security Standards  
Beckers, K.  
2015, XXV, 474 p. 186 illus., Hardcover  
ISBN: 978-3-319-16663-6