

Fundamentals of Secure System Modelling

Raimundas Matulevičius

Fundamentals of Secure System Modelling

Raimundas Matulevičius
Institute of Computer Science
University of Tartu
Tartu, Estonia

ISBN 978-3-319-61716-9 ISBN 978-3-319-61717-6 (eBook)
DOI 10.1007/978-3-319-61717-6

Library of Congress Control Number: 2017944165

© Springer International Publishing AG 2017

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, express or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Printed on acid-free paper

This Springer imprint is published by Springer Nature
The registered company is Springer International Publishing AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

*To Sigita, Mantvydas and Vygantas.
To my parents for all their trust, love
and support.*

Foreword by Andreas L. Opdahl

The security of ICT systems is becoming more important by the day. In the last decades, cyber crime has established itself as a branch of international organised crime. Computer and network security breaches—often combined with social engineering attacks—have become tools for industrial and political espionage, and electronic warfare has moved computer and information security into the realms of international politics and terrorism.

The new security threats have emerged as modern societies have become increasingly reliant on information and communication technologies. Industrial corporations depend on computing and information systems to store and process business-critical information about customers, processes, products, markets, and employees, and reliable ICT systems are needed to support essential public infrastructures such as energy, health, transportation, waste, and water. Besides being an important concern in itself, security is also a prerequisite for other aspects of dependability, such as safety and privacy. Safety-critical systems that used to run bespoke software on specialised hardware in isolation from the Internet have been re-engineered into or replaced by networked, standards-based systems, making them vulnerable to a broader range of security threats than before. And without the information confidentiality and integrity provided by secure ICT, there can be no personal information privacy.

In the old days, computer security was often treated as an implementation and infrastructural concern. Software was secure if it was securely coded, tested and maintained, and if it ran in a secure operating environment: on secure computers, basic software, and networks—preferably behind a firewall. Information was secure if it was encrypted. Modern ICT systems have long since become too complex for handling security only on the software and infrastructure levels. In a modern system, a single weakness can be used as an entry point to incrementally expand an attack to any of that system's parts: the only thing a prospective attacker needs is a single weak link in the security chain, and the chain keeps growing longer as system complexity increases. The emergence of systems-of-systems that span smart cities and multi-national corporations has only added weight to the problem.

The new situation calls for defence in depth, designing security into every component and every level of modern organisations. In addition to hardware, networks, and basic software, security must be woven into all the organisation's information systems, business processes, and its enterprise architectures—cross-cutting technological, individual, organisational, and social concerns. Such defence in depth cannot be added as an afterthought, but must be ingrained in every organisational development, redevelopment, and maintenance activity that somehow involves information management, information processing, or ICT. The new situation also calls for broader collaboration about security than before, starting from the earliest project planning stages. Whereas security of the past could be treated as a technical issue to be left to the experts, defence in depth requires collaboration between new groups of stakeholders: not only security experts, but also involving software developers and experts from many other domains, bringing new types of expertise, perspectives and vocabularies into the security work.

Future generations of security experts, risk analysts and software developers need new security skills to deal with the challenges. Dr. Raimundas Matulevičius' book provides a coherent core around which such skill sets can form. It combines perspectives and techniques from security requirements engineering—appropriately placing it in a security risk context—with techniques for secure system development—including pattern-based and model-driven security. Secure software systems modelling, underpinned by a coherent security meta model, is the glue that ties it all together. In Matulevičius' framework, modelling serves to assess security in a wider organisational context, which hopefully also makes it easier for stakeholders from different domains of expertise to collaborate. Modelling is also used as a link from security issues to risk assessment, necessary for prioritising and selecting among security alternatives. Modelling even offers a bridge into secure software development and ICT operations, a bridge made even more streamlined by the use of domain-specific, pattern-based, and model-driven security modelling techniques.

Dr. Matulevičius' book gives a coherent account of the most important modelling-related security techniques today, and shows how to combine them. It describes an integrated set of systematic practices that can be used to deliver increased security to software projects already from the outset. It combines practical ways of working with practical ways of distilling, managing, and making security knowledge operational. Integrated organisation-level security approaches such as the ones presented here will become increasingly important components of corporate ICT security ecologies of the future. His book is well suited for educating the next generations of security experts. While being written primarily for students, it should also interest industrialists and researchers alike. It deserves a broad readership in both academia and industry.

Well done, Raimundas!

University of Bergen
Bergen, Norway
April 2017

Andreas L. Opdahl

Foreword by Nicolas Mayer

Digitalisation of classical industries (e.g., FinTech, Smart Cities, e-Health, etc.) as well as the growth of new data intensive sectors (e.g., robotics, Internet of Things, genomics, etc.) leads to the necessity of securing data and services. In his book about the industries of the future, the innovative technology leader Alec Ross reports that if any college student asked him what career would most assure 50 years of steady, well-paying employment, he would respond “Cybersecurity”. Being ‘only’ \$3.5 billion a dozen years ago, the size of the cybersecurity market is expected to be more than \$100 billion by 2018.

While organisations and policy-makers being aware of the criticality but also of the cost of security, nowadays, a strong emphasis is put on the management of security risks. Modern day enterprises consider their risk management capabilities as an opportunity to drive their competitive advantage. From a security perspective, risk management supports enterprises to adopt cost-effective security measures because security threats are so numerous that it is impossible to act on all of them. In addition, enterprises are looking for a positive Return On Security Investment (ROSI). In this sense, security risk management plays an important role in alignment of a company’s business with its IT strategy. The same paradigm is used by the policy-makers who propose security-related regulations. For example, in the telecommunications sector, the service providers have to comply with the EU Directive 2009/140/EC where the Article 13a speaks about security and integrity of networks and services. This means that the Member States must ensure that their providers would manage the security risks of the public communication networks and services.

A similar approach has been chosen in international security standards, like, for example, ISO/IEC 27001, which provides requirements for an information security management system (ISMS), or PCI DSS, which provides security requirements for organisations that handle credit cards. While being aware of these concerns, the first focus of the book by Dr. Raimundas Matulevičius places the particular interest on security risk management.

In collaboration with some colleagues, we have developed the TISRIM tool, which directly implements the ISSRM (Information System Security Risk Management) domain model depicted in this book. This tool has successfully been used in dozens of companies, going from SMEs of 5–10 employees to larger organisations, such as European institutions. It has especially been used in some of the initial ISO/IEC 27001 certifications in Luxembourg and has been selected as the reference tool for the national law about security measures, to be taken by the telecommunications service providers. This shows the relevance and soundness of the underlying domain model. However, based on the 10 year-experience while using this tool, also taking into account the feedback received from the risk assessment practitioners both from public and private organisations, the current approaches of security risk management suffer from a number of limitations. One of the most common ones concerns the product, which results from the different steps of the risk management process. The outcome is usually a huge matrix composed of hundreds of lines of risks. Today this result is no more sustainable while considering the complexity of current information systems, the extent number of threats, and the fast and continuous evolution of organisations over time. The introduction of modelling languages to deal with (specific parts of) risk management is daring. Additionally I consider that training of the current and future risk management professionals in model-based approaches is promising for the better consideration of security in companies. I am pleased that a large part of this book is dedicated to the accurate and insightful consideration of the relevant and innovative modelling approaches for the risk and security management.

In his book, Dr. Matulevičius introduces a fundamental set of knowledge for the advanced management of risk and security. While going from the conceptual aspects to the practical tools, this book gives a broad coverage of the field. The learning approach is based on the extensive use of examples and exercises; thus, it insures an efficient learning. The further readings guarantee that learners will be able to enhance his or her knowledge on some specific topics.

Congratulations, Raimundas, for this book that I will certainly use as a reference book at the Master-level courses and for professional training!

Luxembourg Institute of Science and Technology
Luxembourg
May 2017

Nicolas Mayer

Preface

Computer systems play an important role in everyday life. If we look around we see that everyone is using computers for editing documents, managing financial data, banking, communicating and other various activities that improve our way of living. However, this also means that we need to deal with the certain risks that affect data and information, such as bank account data, educational qualifications, health records and others. In many cases this data and information needs to be kept private, confidential, integral and available only for the intended audience. This means that the need to secure systems and software becomes a necessity rather than an option.

Although the importance of introducing security engineering practices early in the development cycle has been acknowledged, the current practices take security consideration only after implementing the software systems. However, on one hand, this makes security engineering costly. Even more, it might mean that some critical security risk potentially might be overlooked. On the other hand, early consideration of security allows analysts to envision security threats, their consequences and countermeasures. It also helps in considering system design alternatives and determining the ones, which do not offer a sufficient security level. Finally, early security consideration could contribute to the re-scoping or cancelling of the project if the security risks are estimated as too costly to handle. The **scope** of this book is:

- *security requirements engineering*, including security risk management, major activities, asset identification, security risk analysis and security requirements elicitation;
- *secure software system modelling*, including modelling of context and protected assets, security risks, and decisions of security risk treatment using various modelling languages;
- *secure system development*, including secure system development approaches, pattern-driven development, and model-driven security.

In this book, therefore, we analyse different secure software system engineering techniques with emphasis on security modelling. We emphasise security modelling including the determination and modelling of security requirements, which could

be derived through systematic application of the principles for security risk management. Such requirements should be implemented in the security controls, which become assets in the protected software systems. In the book we illustrate how to combined different security modelling perspectives in order to complement generic secure software development.

Audience The reader of this book should be familiar with: (i) software system development, (ii) requirements engineering, and (iii) system modelling. The book could be used as a textbook in university-level courses, fully or partially supporting teaching of principles for secure software system modelling, engineering and development.

The primary target of this book, therefore, is *graduate students* (master and doctorate), who are studying cyber security, software engineering and system security engineering. Major benefits of the books are: (i) learning how to identify causes and consequences of (or the lack of) system and software security, (ii) learning how to master essential techniques to reduce and avoid system and software security problems, and (iii) learning how to introduce and to reason about security requirements, controls and the overall security solution.

The book might be interesting to *practitioners*, especially to the ones who wish to learn about the necessity to reason about decisions behind secure software systems. The book will consider (i) the importance of security engineering at early stages of software system development, (ii) the importance of the trade-off analysis, and (iii) the principles of model-driven security.

How to Read This Book The book consists of four parts and includes twelve chapters. In the introduction chapter (Chap. 1) we define what is meant by security engineering in software systems. Then the chapter provides overview of security and security risk management standards, security modelling approaches, domain-specific security languages and principles of model-driven security. Next, the chapter offers some insight into the multi-perspective secure system analysis. Finally, it presents the running example, which is use through the remainder of the book.

The first part of the book introduces the conceptual bases for security risk management. The part consists of three chapters. In Chap. 2, on *Domain Model for Information Systems Security Risk Management*, we discuss the ISSRM domain model, including definitions of asset-related, security risk-related, and security risk treatment-related concepts. This chapter also discusses concept relationships, multiplicities, processes as well as the metrics used to assess security risks.

In Chap. 3, on *Security Risk*, we define the major constituencies of the security risk. The discussion includes issues on asset harm using malicious software, common security error types and threats to distributed information systems. Next, the chapter discusses aspects of the threat agent profile and presents a number of techniques which could be used for threat model development. In Chap. 4, on *Security Requirements*, firstly, we differentiate between security problem, i.e., security criterion, and security solution, i.e., security requirements. Next, chapter

presents the taxonomy of security requirements and discusses the principles of security requirements representation and specification.

The second part of the book focusses on security risk-oriented modelling languages and their means to represent and specify security requirements as well as to reason about why these security requirements should be introduced in the considered software system. Security modelling helps developers to envision potential security solutions before building the system. It can also be used to discuss these solutions among the system stakeholders. Modelling could contribute to the trade-off analysis, thus helping to discard ineffective security solutions. In this part of the book we introduce four languages for security modelling. More specifically and following the previous part of the book, we discuss how general-purpose modelling languages are extended for security risk management. The part consists of four chapters.

Chapter 5, on *Security Risk-Oriented BPMN*, discusses how the modelling language of business process model and notation (a.k.a., BPMN) is extended with security criteria, vulnerability, security requirements and other security risk management concepts. The outcome of this extension is the security risk-oriented BPMN. Chapter 6, on *Security Risk-Aware Secure Tropos*, discusses the Secure Tropos approach—a modelling language and method to deal with actor dependencies and goals. The Secure Tropos language is mapped to the ISSRM domain model, resulting in the security risk-aware Secure Tropos. Chapter 7, on *Security Risk-Oriented Misuse Cases* introduces how use cases and misuse cases are aligned to the ISSRM domain model. The chapter mainly focusses on the graphical language extensions. However, it also briefly discusses the textual use/misuse case templates and their means to support security risk management. Chapter 8, on *Mal-activities for Security Risk Management*, introduces security risk management extensions to mal-activity diagrams, another languages of the UML family. The chapter illustrates how to analyse dynamic aspects of secure software system development.

The third part of this book is dedicated to the model-driven development of secure software systems. The use of models could stimulate and support stakeholder discussions, contribute to security requirements validation, guide software coding and even automate the coding processes. Models could also be used for the testing of the security solutions, or be used to reverse-engineer system design from implementation. In this part we discuss few of these aspects. The part consists of three chapters:

In Chap. 9, on *Transformations Between Security Risk-Oriented Modelling Languages*, we discuss how modelling languages considered in the second part of this book could be translated among themselves. Sets of transformation rules and guidelines, based on language alignments to the ISSRM domain model, are introduced and illustrated in four transformation cases. In Chap. 10, on *Role-Based Access Control*, we discuss the principles of role-based access control. Two security extensions of the generic UML language—SecureUML and UMLsec—are considered to show various RBAC concerns and application principles. Based on the RBAC domain, a set of transformation rules are defined to link both approaches together and to support the static and dynamic RBAC perspectives. The chapter

ends with discussion on an RBAC model application to restrict access to data storage systems. In Chap. 11, on *Secure System Development Using Patterns*, secure software system development using security patterns is discussed. The chapter presents a taxonomy of the security patterns. Next it discusses how security risk-oriented patterns could be applied to extract security requirements from the business processes.

The last part consists of one chapter. In Chap. 12, *Secure System Development*, we present the three lifecycles of the secure software systems development. In the end, we shortly discuss how different security modelling techniques could be used in the various stages of secure software system development.

Acknowledgements I would like to thank my family: Sigita for her patience and encouragement, Mantvydas and Vygantas for their joyfulness and playfulness, which gave me minutes of thought and relaxation while preparing this book. I thank my parents for their continuous trust, love and support.

Moreover, I am thankful for the many colleagues at different places who gave me a lot of input through discussions, encouragement, joint contributions and active support. Firstly, I wish to thank Prof. Marlon Dumas (from University of Tartu, Estonia) for his continuous encouragement and supportive comments. Secondly, I am grateful to Prof. Patrick Heymans (University of Namur, Belgium), Prof. Eric Dubois (LIST, Luxembourg), Dr. Nicolas Mayer (LIST, Luxembourg), Prof. Guttorm Sindre (University of Science and Technology, Norway), Prof. Andreas Opdahl (University of Bergen, Norway), Prof. Haralambos Mouratidis (University of Brighton, UK), Prof. Kurt Sandkuhl (University of Rostock, Germany), and Prof. Māriķe Kirikova (Riga Technical University, Latvia) for the joint contributions, emphasising discussions and joint research, which contributed to different parts of this book.

I would like to thank to the students of the University of Tartu: Dr. Naved Ahmed, Morshed Chowdhury, Olga Altuhhova, Henri Lakk, Inam Soomro, Naiad Khan, Anastasiia Onchukova, Eduard Sing, Andrei Proskurin, Silver Jūrimāe, Karl Kolk, Andrey Sergeev, and Silver Samarūtel. Your research contributions and results are valuable inputs to the different parts of this book. I also thank all the participants of the Master-level courses on Principles of Secure Software Design. You have tested the different book chapters by providing your solutions to the exercises and discussing various aspects related to secure software systems modelling.

I would like to thank the company No Magic for its generous permit to use the MagicDraw modelling tool. This help a lot in modelling book's illustrative examples using the BPMN and UML modelling languages. The tool's flexibility and extensibility allowed visualising important principles of secure software systems modelling, model transformation, and technique application.

Last but not least I would like to thank Ralf Gerstner from Springer for his professional help in making this book a reality.

Contents

1	Introduction	1
1.1	System and Security Engineering	1
1.2	Security and Security Risk Management Standards	2
1.3	Security Development Approaches	4
1.4	Domain-Specific Languages for Security Modelling	4
1.5	Model-Driven Security	5
1.6	Modelling Perspectives of Secure Software Systems.....	6
1.7	Running Example	9
1.8	Exercises.....	12
 Part I Security Risk Management		
2	Domain Model for Information Systems Security Risk Management	17
2.1	Domain Model.....	17
2.1.1	Asset-Related Concepts	17
2.1.2	Risk-Related Concepts	19
2.1.3	Risk Treatment-Related Concepts	20
2.2	Relationships and Multiplicities	20
2.3	Metrics	22
2.4	Process	22
2.5	ISSRM Application Example	23
2.6	Further Reading	27
2.7	Exercises	29
3	Security Risk	31
3.1	System Assets	31
3.2	Risk Analysis	33
3.3	Harm: Malicious Software	34
3.4	Taxonomy of Security Errors	36
3.5	Security Threats	37

3.6	Threat Agent	39
3.7	Further Reading	41
3.8	Exercises	41
4	Security Requirements	43
4.1	Security Criterion	43
4.2	Requirements Definition	44
4.3	Security Requirements Classification	45
4.4	How to Specify Security Requirements	50
4.5	Related (to Security) Requirements	52
4.6	Further Reading	56
4.7	Exercises	58
 Part II Modelling Languages for Security Risk Management		
5	Security Risk-Oriented BPMN	63
5.1	Business Process Model and Notation	63
5.2	Security Risk Management Using BPMN	64
5.2.1	Semantics	65
5.2.2	Abstract Syntax	65
5.2.3	Concrete Syntax	68
5.3	Example.....	69
5.4	Further Reading	72
5.5	Exercises	75
6	Security Risk-Aware Secure Tropos	77
6.1	Tropos and Secure Tropos	77
6.2	Security Risk Management Using Secure Tropos	79
6.2.1	Semantics and Concrete Syntax.....	79
6.2.2	Abstract Syntax	81
6.3	Examples	86
6.4	Further Reading	89
6.5	Exercises	91
7	Security Risk-Oriented Misuse Cases	93
7.1	Use and Misuse Cases.....	93
7.2	Security Risk Management Using Misuse Cases	94
7.2.1	Semantics and Concrete Syntax.....	94
7.2.2	Abstract Syntax	95
7.3	Examples	98
7.4	Textual Misuse Cases	101
7.5	Further Reading	103
7.6	Exercises	104
8	Mal-activities for Security Risk Management	107
8.1	Activity and Mal-activity Diagrams	107
8.2	Security Risk Management Using Mal-activities	108

8.2.1	Semantics and Concrete Syntax.....	108
8.2.2	Abstract Syntax	110
8.3	Example.....	112
8.4	Further Reading	113
8.5	Exercises	113

Part III Model-Driven Security Development and Application

9	Transformations Between Security Risk-Oriented Modelling Languages	119
9.1	Transformation Basis.....	119
9.1.1	Transformation Method	119
9.1.2	Comparison of Modelling Languages	120
9.2	Transforming from Security Risk-Oriented BPMN to Security Risk-Aware Secure Tropos	125
9.3	Transforming from Security Risk-Aware Secure Tropos to Security Risk-Oriented Misuse Cases	129
9.4	Transforming from Security Risk-Oriented Misuse Cases to Mal-activities for Security Risk Management	135
9.5	Further Reading	141
9.6	Exercises	144
10	Role-Based Access Control	147
10.1	Family of RBAC Models.....	147
10.2	RBAC Administration.....	149
10.3	RBAC Modelling Languages	150
10.3.1	SecureUML	150
10.3.2	UMLsec	153
10.3.3	Comparison	156
10.3.4	Transformation.....	158
10.4	Model-Driven Security	162
10.5	Further Reading	165
10.6	Exercises	167
11	Secure System Development Using Patterns.....	171
11.1	Security Patterns.....	171
11.2	Security Pattern Taxonomy	172
11.3	Security Risk-Oriented Patterns	174
11.4	Security Requirements Elicitation from Business Processes	180
11.4.1	SREBP Method	182
11.4.2	Pattern Application	185
11.5	Further Reading	193
11.6	Exercises	194

Part IV Concluding Remarks

12 Secure System Development	199
12.1 Secure System Development Processes	199
12.1.1 Microsoft Secure System Development Lifecycle	200
12.1.2 OWASP CLASP	201
12.1.3 Seven Touchpoints	202
12.1.4 Comparison	204
12.2 Security Approaches in Secure Systems Development Processes	204
12.3 Tools	206
12.4 Exercises	207
References	209

Acronyms

ABAC	Attribute-Based Access Control
API	Application Programming Interface
AURUM	Automatic Risk and Utility Management
BPMN	Business Process Model and Notation
BSI	(<i>In German</i>) Bundesamt für Sicherheit in der Informationstechnik
CAPEC	Common Attack Pattern Enumeration and Classification
CC	Common Criteria
CCTA	Central Computer and Telecommunications Agency
CORAS	It is the name of the approach; “it is not, and has never been, an acronym” [122]
CRAMM	CCTA Risk Analysis and Management Method
CySeMol	Cyber Security Modelling language
CLASP	Comprehensive Lightweight Application Security Process
DAC	Discretionary Access Control
DITSCAP	Defence Information Technology Security Certification and Accreditation Process
DNS	Domain Name System
EBIOS	(<i>In French</i>) Expression des Besoins et Identification des Objectifs de Sécurité
ERIS	Electronic Registration Information System
FSR	Final Security Review
HTML	HyperText Markup Language
ICMP	Internet Control Message Protocol
IOI	Items of Interest
IS	Information System
ISO/IEC	International Organisation for Standardisation and the International Electrotechnical Commission
ISSRM	Information Systems Security Risk Management
<i>i*</i>	Intentional Distribution (Modelling Language)
KAOS	Knowledge Acquisition in automated Specification
MAC	Mandatory Access Control

MEHARi	(<i>In French</i>): Methode Harmonisée d'Analyse du Risque informatique
MEMO	Multi-Perspective Enterprise Modelling
MUCM	Misuse Case Maps
NIST	National Institute of Standards and Technology
OCL	Object Constraint Language
OCTAVE	Operationally Critical Threat, Asset, and Vulnerability Evaluation
OWASP	Open Web Application Security Project
RAdAC	Risk-Adaptive Access Control
RBAC	Role-Based Access Control
RE	Requirements Engineering
SEAM	Security Enhanced Actor Model
SEGM	Security Enhanced Goal Model
SQUARE	Security Quality Requirements Engineering
SREBP	Security Requirements Elicitation from Business Processes
SROMUC	Security Risk-Oriented Misuse Cases
SRP	Security Risk-Oriented Patterns
SSDL	Secure System Development Lifecycle
STRIDE	Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of privileges
TCP	Transmission Control Protocol
UCON	Usage CONtrol Model
UML	Unified Modelling Language
XACML	eXtensible Access Control Markup Language
XML	eXtensible Markup Language

Fundamentals of Secure System Modelling

Matulevičius, R.

2017, XX, 218 p. 112 illus., 62 illus. in color., Hardcover

ISBN: 978-3-319-61716-9