



Software Security Engineering: A Guide for Project Managers

Julia H. Allen, Sean Barnum, Robert J. Ellison, Gary McGraw, Nancy R. Mead

Download now

[Click here](#) if your download doesn't start automatically

Software Security Engineering: A Guide for Project Managers

Julia H. Allen, Sean Barnum, Robert J. Ellison, Gary McGraw, Nancy R. Mead

Software Security Engineering: A Guide for Project Managers Julia H. Allen, Sean Barnum, Robert J. Ellison, Gary McGraw, Nancy R. Mead

“This book’s broad overview can help an organization choose a set of processes, policies, and techniques that are appropriate for its security maturity, risk tolerance, and development style. This book will help you understand how to incorporate practical security techniques into all phases of the development lifecycle.”

—Steve Riley, senior security strategist, Microsoft Corporation

“There are books written on some of the topics addressed in this book, and there are other books on secure systems engineering. Few address the entire life cycle with a comprehensive overview and discussion of emerging trends and topics as well as this one.”

—Ronda Henning, senior scientist-software/security queen, Harris Corporation

Software that is developed from the beginning with security in mind will resist, tolerate, and recover from attacks more effectively than would otherwise be possible. While there may be no silver bullet for security, there are practices that project managers will find beneficial. With this management guide, you can select from a number of sound practices likely to increase the security and dependability of your software, both during its development and subsequently in its operation.

***Software Security Engineering* draws extensively on the systematic approach developed for the Build Security In (BSI) Web site. Sponsored by the Department of Homeland Security Software Assurance Program, the BSI site offers a host of tools, guidelines, rules, principles, and other resources to help project managers address security issues in every phase of the software development life cycle (SDLC). The book’s expert authors, themselves frequent contributors to the BSI site, represent two well-known resources in the security world: the CERT Program at the Software Engineering Institute (SEI) and Cigital, Inc., a consulting firm specializing in software security.**

This book will help you understand why

- Software security is about more than just eliminating vulnerabilities and conducting penetration tests
- Network security mechanisms and IT infrastructure security services do not sufficiently protect application software from security risks
- Software security initiatives should follow a risk-management approach to identify priorities and to define what is “good enough”—understanding that software security risks will change throughout the SDLC
- Project managers and software engineers need to learn to think like an attacker in order to address the range of functions that software should not do, and how software can better resist, tolerate, and recover when under attack

Chapter 1: Why Is Security a Software Issue? 1

1.1 Introduction 1

1.2 The Problem 2

1.3 Software Assurance and Software Security 6

1.4 Threats to Software Security 9

1.5 Sources of Software Insecurity 11

1.6 The Benefits of Detecting Software Security Defects Early 13

1.7 Managing Secure Software Development 18

1.8 Summary 23

Chapter 2: What Makes Software Secure? 25

2.1 Introduction 25

2.2 Defining Properties of Secure Software 26

2.3 How to Influence the Security Properties of Software 36

2.4 How to Assert and Specify Desired Security Properties 61

2.5 Summary 71

Chapter 3: Requirements Engineering for Secure Software 73

3.1 Introduction 73

3.2 Misuse and Abuse Cases 78

3.3 The SQUARE Process Model 84

3.4 SQUARE Sample Outputs 91

3.5 Requirements Elicitation 99

3.6 Requirements Prioritization 106

3.7 Summary 112

Chapter 4: Secure Software Architecture and Design 115

4.1 Introduction 115

4.2 Software Security Practices for Architecture and Design: Architectural Risk Analysis 119

4.3 Software Security Knowledge for Architecture and Design: Security Principles, Security Guidelines, and Attack Patterns 137

4.4 Summary 148

Chapter 5: Considerations for Secure Coding and Testing 151

5.1 Introduction 151

5.2 Code Analysis 152

5.3 Coding Practices 160

5.4 Software Security Testing 163

5.5 Security Testing Considerations Throughout the SDLC 173

5.6 Summary 180

Chapter 6: Security and Complexity: System Assembly Challenges 183

6.1 Introduction 183

6.2 Security Failures 186

6.3 Functional and Attacker Perspectives for Security Analysis: Two Examples 189

6.4 System Complexity Drivers and Security 203

6.5 Deep Technical Problem Complexity 215

6.6 Summary 217

Chapter 7: Governance, and Managing for More Secure Software 221

7.1 Introduction 221

7.2 Governance and Security 223

7.3 Adopting an Enterprise Software Security Framework 226

7.4 How Much Security Is Enough? 236

7.5 Security and Project Management 244

7.6 Maturity of Practice 259

7.7 Summary 266

Chapter 8: Getting Started 267

8.1 Where to Begin 269

8.2 In Closing 281

 **Download** [Software Security Engineering: A Guide for Project ...pdf](#)

 **Read Online** [Software Security Engineering: A Guide for Proje ...pdf](#)

Download and Read Free Online Software Security Engineering: A Guide for Project Managers Julia H. Allen, Sean Barnum, Robert J. Ellison, Gary McGraw, Nancy R. Mead

From reader reviews:

Jesse Valles:

Do you certainly one of people who can't read satisfying if the sentence chained from the straightway, hold on guys this kind of aren't like that. This Software Security Engineering: A Guide for Project Managers book is readable simply by you who hate the perfect word style. You will find the data here are arrange for enjoyable reading through experience without leaving perhaps decrease the knowledge that want to give to you. The writer of Software Security Engineering: A Guide for Project Managers content conveys the idea easily to understand by a lot of people. The printed and e-book are not different in the content material but it just different by means of it. So , do you still thinking Software Security Engineering: A Guide for Project Managers is not loveable to be your top checklist reading book?

Patsy Phan:

Information is provisions for individuals to get better life, information currently can get by anyone with everywhere. The information can be a knowledge or any news even an issue. What people must be consider while those information which is inside former life are hard to be find than now is taking seriously which one is appropriate to believe or which one the actual resource are convinced. If you receive the unstable resource then you get it as your main information there will be huge disadvantage for you. All those possibilities will not happen inside you if you take Software Security Engineering: A Guide for Project Managers as the daily resource information.

Johnny Sutton:

You may spend your free time to study this book this publication. This Software Security Engineering: A Guide for Project Managers is simple to develop you can read it in the park your car, in the beach, train along with soon. If you did not possess much space to bring typically the printed book, you can buy the e-book. It is make you better to read it. You can save the actual book in your smart phone. Consequently there are a lot of benefits that you will get when you buy this book.

Henry Heath:

A number of people said that they feel bored when they reading a guide. They are directly felt this when they get a half portions of the book. You can choose the particular book Software Security Engineering: A Guide for Project Managers to make your own reading is interesting. Your skill of reading proficiency is developing when you like reading. Try to choose simple book to make you enjoy to see it and mingle the idea about book and examining especially. It is to be first opinion for you to like to open up a book and go through it. Beside that the reserve Software Security Engineering: A Guide for Project Managers can to be a newly purchased friend when you're feel alone and confuse in what must you're doing of the time.

**Download and Read Online Software Security Engineering: A
Guide for Project Managers Julia H. Allen, Sean Barnum, Robert J.
Ellison, Gary McGraw, Nancy R. Mead #UKD6HXL43JG**

Read Software Security Engineering: A Guide for Project Managers by Julia H. Allen, Sean Barnum, Robert J. Ellison, Gary McGraw, Nancy R. Mead for online ebook

Software Security Engineering: A Guide for Project Managers by Julia H. Allen, Sean Barnum, Robert J. Ellison, Gary McGraw, Nancy R. Mead Free PDF d0wnl0ad, audio books, books to read, good books to read, cheap books, good books, online books, books online, book reviews epub, read books online, books to read online, online library, greatbooks to read, PDF best books to read, top books to read Software Security Engineering: A Guide for Project Managers by Julia H. Allen, Sean Barnum, Robert J. Ellison, Gary McGraw, Nancy R. Mead books to read online.

Online Software Security Engineering: A Guide for Project Managers by Julia H. Allen, Sean Barnum, Robert J. Ellison, Gary McGraw, Nancy R. Mead ebook PDF download

Software Security Engineering: A Guide for Project Managers by Julia H. Allen, Sean Barnum, Robert J. Ellison, Gary McGraw, Nancy R. Mead Doc

Software Security Engineering: A Guide for Project Managers by Julia H. Allen, Sean Barnum, Robert J. Ellison, Gary McGraw, Nancy R. Mead Mobipocket

Software Security Engineering: A Guide for Project Managers by Julia H. Allen, Sean Barnum, Robert J. Ellison, Gary McGraw, Nancy R. Mead EPub