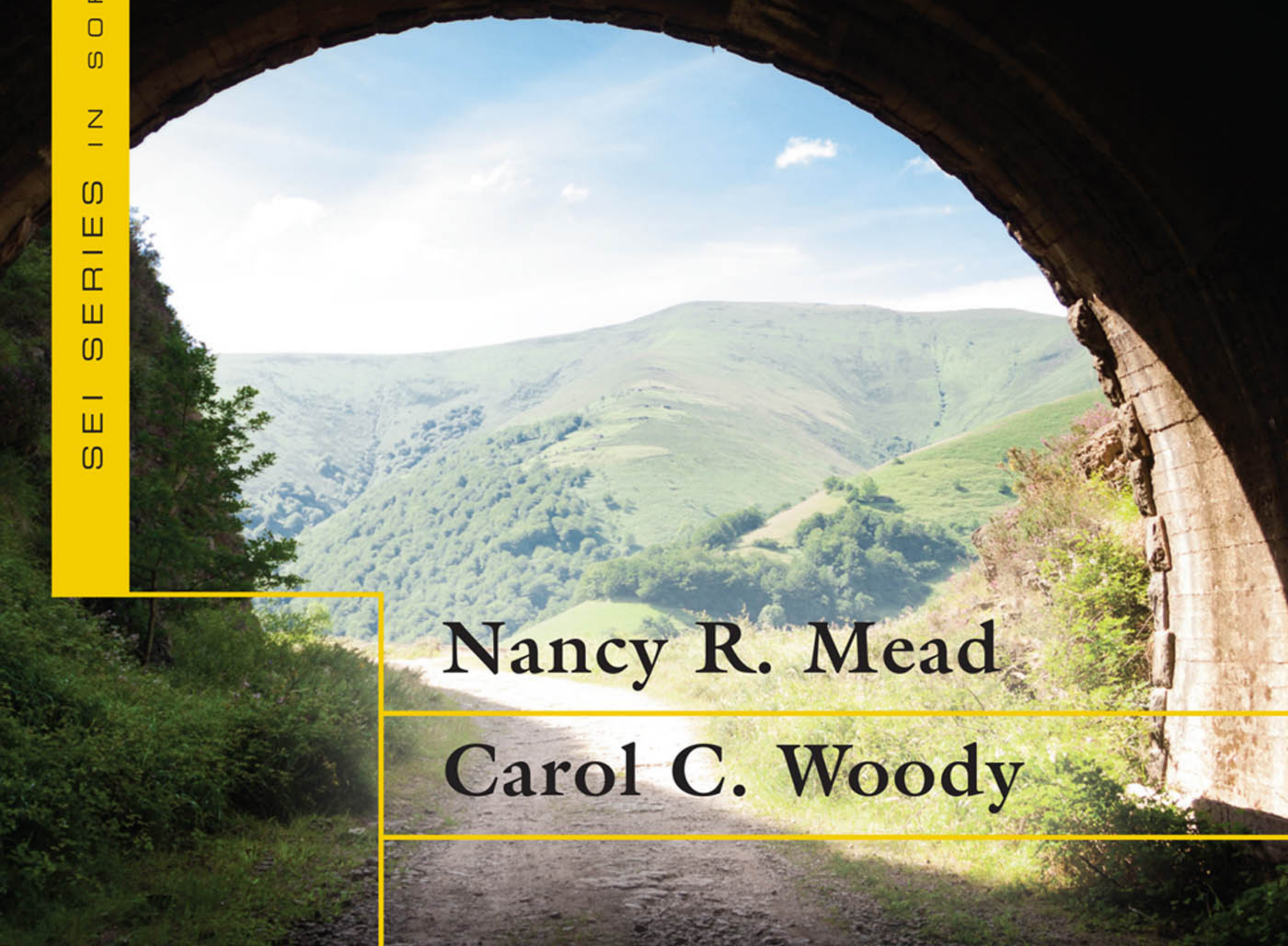
SEI SERIES IN SOFTWARE ENGINEERING

Cyber Security Engineering

A Practical Approach for Systems and Software Assurance



Nancy R. Mead

Carol C. Woody

Praise for *Cyber Security Engineering*

"This book presents a wealth of extremely useful material and makes it available from a single source."

—Nadya Bartol, Vice President of Industry Affairs and Cybersecurity Strategist, Utilities Technology Council

"Drawing from more than 20 years of applied research and use, CSE serves as both a comprehensive reference and a practical guide for developing assured, secure systems and software—addressing the full lifecycle; manager and practitioner perspectives; and people, process, and technology dimensions."

—Julia Allen, Principal Researcher, Software Engineering Institute

Cyber Security Engineering: A Practical Approach for Systems and Software Assurance

Table of Contents

Cover

Title Page

Copyright Page

Acknowledgments

About the Authors

Contents

Foreword

Preface

Chapter 1: Cyber Security Engineering: Lifecycle Assurance of Systems and Software

- 1.1 Introduction
- 1.2 What Do We Mean by Lifecycle Assurance?
- 1.3 Introducing Principles for Software Assurance
- 1.4 Addressing Lifecycle Assurance
- 1.5 Case Studies Used in This Book
  - 1.5.1 Wireless Emergency Alerts Case Study
  - 1.5.2 Fly-By-Night Airlines Case Study
  - 1.5.3 GoFast Automotive Corporation Case Study

Chapter 2: Risk AnalysisIdentifying and Prioritizing Needs

- 2.1 Risk Management Concepts

Pearson

Table of Contents

2.2 Mission Risk

2.3 Mission Risk Analysis

2.3.1 Task 1: Identify the Mission and Objective(s)

2.3.2 Task 2: Identify Drivers

2.3.3 Task 3: Analyze Drivers

2.4 Security Risk

2.5 Security Risk Analysis

2.6 Operational Risk AnalysisComparing Planned to Actual

2.7 Summary

Chapter 3: Secure Software Development Management and Organizational Models

3.1 The Management Dilemma

3.1.1 Background on Assured Systems

3.2 Process Models for Software Development and Acquisition

3.2.1 CMMI Models in General

3.2.2 CMMI for Development (CMMI-DEV)

3.2.3 CMMI for Acquisition (CMMI-ACQ)

3.2.4 CMMI for Services (CMMI-SVC)

3.2.5 CMMI Process Model Uses

3.3 Software Security Frameworks, Models, and Roadmaps

3.3.1 Building Security In Maturity Model (BSIMM)

3.3.2 CMMI Assurance Process Reference Model

3.3.3 Open Web Application Security Project (OWASP) Software Assurance Maturity Model (SAMM)

3.3.4 DHS SwA Measurement Work

3.3.5 Microsoft Security Development Lifecycle (SDL)

3.3.6 SEI Framework for Building Assured Systems

3.3.7 SEI Research in Relation to the Microsoft SDL

Table of Contents

3.3.8 CERT Resilience Management Model Resilient Technical Solution Engineering Process Area

3.3.9 International Process Research Consortium (IPRC) Roadmap

3.3.10 NIST Cyber Security Framework

3.3.11 Uses of Software Security Frameworks, Models, and Roadmaps

3.4 Summary

Chapter 4: Engineering Competencies

4.1 Security Competency and the Software Engineering Profession

4.2 Software Assurance Competency Models

4.3 The DHS Competency Model

4.3.1 Purpose

4.3.2 Organization of Competency Areas

4.3.3 SwA Competency Levels

4.3.4 Behavioral Indicators

4.3.5 National Initiative for Cybersecurity Education (NICE)

4.4 The SEI Software Assurance Competency Model

4.4.1 Model Features

4.4.2 SwA Knowledge, Skills, and Effectiveness

4.4.3 Competency Designations

4.4.4 A Path to Increased Capability and Advancement

4.4.5 Examples of the Model in Practice

4.4.6 Highlights of the SEI Software Assurance Competency Model

4.5 Summary

Chapter 5: Performing Gap Analysis

5.1 Introduction

5.2 Using the SEIs SwA Competency Model

5.3 Using the BSIMM

5.3.1 BSIMM Background

Table of Contents

5.3.2 BSIMM Sample Report

5.4 Summary

Chapter 6: Metrics

6.1 How to Define and Structure Metrics to Manage Cyber Security Engineering

6.1.1 What Constitutes a Good Metric?

6.1.2 Metrics for Cyber Security Engineering

6.1.3 Models for Measurement

6.2 Ways to Gather Evidence for Cyber Security Evaluation

6.2.1 Process Evidence

6.2.2 Evidence from Standards

6.2.3 Measurement Management

Chapter 7: Special Topics in Cyber Security Engineering

7.1 Introduction

7.2 Security: Not Just a Technical Issue

7.2.1 Introduction

7.2.2 Two Examples of Security Governance

7.2.3 Conclusion

7.3 Cyber Security Standards

7.3.1 The Need for More Cyber Security Standards

7.3.2 A More Optimistic View of Cyber Security Standards

7.4 Security Requirements Engineering for Acquisition

7.4.1 SQUARE for New Development

7.4.2 SQUARE for Acquisition

7.4.3 Summary

7.5 Operational Competencies (DevOps)

7.5.1 What Is DevOps?

7.5.2 DevOps Practices That Contribute to Improving Software Assurance

Table of Contents

7.5.3 DevOpsSec Competencies

7.6 Using Malware Analysis

7.6.1 Code and Design Flaw Vulnerabilities

7.6.2 Malware-AnalysisDriven Use Cases

7.6.3 Current Status and Future Research

7.7 Summary

Chapter 8: Summary and Plan for Improvements in Cyber Security Engineering Performance

8.1 Introduction

8.2 Getting Started on an Improvement Plan

8.3 Summary

References

Bibliography

Appendix A: WEA Case Study: Evaluating Security Risks Using Mission Threads

Appendix B: The MSwA Body of Knowledge with Maturity Levels Added

Appendix C: The Software Assurance Curriculum Project

Appendix D: The Software Assurance Competency Model Designations

Appendix E: Proposed SwA Competency Mappings

Appendix F: BSIMM Assessment Final Report

Appendix G: Measures from Lifecycle Activities, Security Resources, and Software Assurance Principles

Index

Pearson