



SEI SERIES • A CERT® BOOK



SOFTWARE SECURITY SERIES

# Software Security Engineering

A Guide for Project Managers



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



# Software Security Engineering

# Software Security Engineering: A Guide for Project Managers

## Table of Contents

Contents

Foreword

Preface

About the Authors

Chapter 1: Why Is Security a Software Issue?

1.1 Introduction

1.2 The Problem

1.2.1 System Complexity: The Context within Which Software Lives

1.3 Software Assurance and Software Security

1.3.1 The Role of Processes and Practices in Software Security

1.4 Threats to Software Security

1.5 Sources of Software Insecurity

1.6 The Benefits of Detecting Software Security Defects Early

1.6.1 Making the Business Case for Software Security: Current State

1.7 Managing Secure Software Development

1.7.1 Which Security Strategy Questions Should I Ask?

1.7.2 A Risk Management Framework for Software Security

1.7.3 Software Security Practices in the Development Life Cycle

1.8 Summary

Chapter 2: What Makes Software Secure?

2.1 Introduction

2.2 Defining Properties of Secure Software

# **Table of Contents**

2.2.1 Core Properties of Secure Software

2.2.2 Influential Properties of Secure Software

## **2.3 How to Influence the Security Properties of Software**

2.3.1 The Defensive Perspective

2.3.2 The Attackers Perspective

## **2.4 How to Assert and Specify Desired Security Properties**

2.4.1 Building a Security Assurance Case

2.4.2 A Security Assurance Case Example

2.4.3 Incorporating Assurance Cases into the SDLC

2.4.4 Related Security Assurance and Compliance Efforts

2.4.5 Maintaining and Benefitting from Assurance Cases

## **2.5 Summary**

# **Chapter 3: Requirements Engineering for Secure Software**

## **3.1 Introduction**

3.1.1 The Importance of Requirements Engineering

3.1.2 Quality Requirements

3.1.3 Security Requirements Engineering

## **3.2 Misuse and Abuse Cases**

3.2.1 Security Is Not a Set of Features

3.2.2 Thinking About What You Cant Do

3.2.3 Creating Useful Misuse Cases

3.2.4 An Abuse Case Example

## **3.3 The SQUARE Process Model**

3.3.1 A Brief Description of SQUARE

3.3.2 Tools

3.3.3 Expected Results

## **3.4 SQUARE Sample Outputs**

3.4.1 Output from SQUARE Steps

3.4.2 SQUARE Final Results

# **Table of Contents**

## **3.5 Requirements Elicitation**

3.5.1 Overview of Several Elicitation Methods

3.5.2 Elicitation Evaluation Criteria

## **3.6 Requirements Prioritization**

3.6.1 Identify Candidate Prioritization Methods

3.6.2 Prioritization Technique Comparison

3.6.3 Recommendations for Requirements Prioritization

## **3.7 Summary**

## **Chapter 4: Secure Software Architecture and Design**

### **4.1 Introduction**

4.1.1 The Critical Role of Architecture and Design

4.1.2 Issues and Challenges

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

4.2.1 Software Characterization

4.2.2 Threat Analysis

4.2.3 Architectural Vulnerability Assessment

4.2.4 Risk Likelihood Determination

4.2.5 Risk Impact Determination

4.2.6 Risk Mitigation Planning

4.2.7 Recapping Architectural Risk Analysis

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

4.3.1 Security Principles

4.3.2 Security Guidelines

4.3.3 Attack Patterns

### **4.4 Summary**

## **Chapter 5: Considerations for Secure Coding and Testing**

### **5.1 Introduction**

# **Table of Contents**

## **5.2 Code Analysis**

5.2.1 Common Software Code Vulnerabilities

5.2.2 Source Code Review

## **5.3 Coding Practices**

5.3.1 Sources of Additional Information on Secure Coding

## **5.4 Software Security Testing**

5.4.1 Contrasting Software Testing and Software Security Testing

5.4.2 Functional Testing

5.4.3 Risk-Based Testing

## **5.5 Security Testing Considerations Throughout the SDLC**

5.5.1 Unit Testing

5.5.2 Testing Libraries and Executable Files

5.5.3 Integration Testing

5.5.4 System Testing

5.5.5 Sources of Additional Information on Software Security Testing

## **5.6 Summary**

# **Chapter 6: Security and Complexity: System Assembly Challenges**

## **6.1 Introduction**

## **6.2 Security Failures**

6.2.1 Categories of Errors

6.2.2 Attacker Behavior

## **6.3 Functional and Attacker Perspectives for Security Analysis: Two Examples**

6.3.1 Web Services: Functional Perspective

6.3.2 Web Services: Attackers Perspective

6.3.3 Identity Management: Functional Perspective

6.3.4 Identity Management: Attackers Perspective

6.3.5 Identity Management and Software Development

# **Table of Contents**

## **6.4 System Complexity Drivers and Security**

### **6.4.1 Wider Spectrum of Failures**

### **6.4.2 Incremental and Evolutionary Development**

### **6.4.3 Conflicting or Changing Goals Complexity**

## **6.5 Deep Technical Problem Complexity**

## **6.6 Summary**

# **Chapter 7: Governance, and Managing for More Secure Software**

## **7.1 Introduction**

## **7.2 Governance and Security**

### **7.2.1 Definitions of Security Governance**

### **7.2.2 Characteristics of Effective Security Governance and Management**

## **7.3 Adopting an Enterprise Software Security Framework**

### **7.3.1 Common Pitfalls**

### **7.3.2 Framing the Solution**

### **7.3.3 Define a Roadmap**

## **7.4 How Much Security Is Enough?**

### **7.4.1 Defining Adequate Security**

### **7.4.2 A Risk Management Framework for Software Security**

## **7.5 Security and Project Management**

### **7.5.1 Project Scope**

### **7.5.2 Project Plan**

### **7.5.3 Resources**

### **7.5.4 Estimating the Nature and Duration of Required Resources**

### **7.5.5 Project and Product Risks**

### **7.5.6 Measuring Software Security**

## **7.6 Maturity of Practice**

### **7.6.1 Protecting Information**

### **7.6.2 Audits Role**

# **Table of Contents**

7.6.3 Operational Resilience and Convergence

7.6.4 A Legal View

7.6.5 A Software Engineering View

7.6.6 Exemplars

7.7 Summary

## **Chapter 8: Getting Started**

8.1 Where to Begin

8.2 In Closing

## **Glossary**

A

B

C

D

E

F

H

I

M

N

P

R

S

T

U

V

W

Z



# **Table of Contents**

References

Build Security In Web Site References

Index