

Secure And Resilient Software Development Format

Secure and Resilient Software: Requirements, Test Cases, and Testing Methods provides a comprehensive set of requirements for secure and resilient software development and operation. It supplies documented test cases for those requirements as well as best practices for testing nonfunctional requirements for improved information assurance. This resource-rich book includes: Pre-developed nonfunctional requirements that can be reused for any software development project Documented test cases that go along with the requirements and can be used to develop a Test Plan for the software Testing methods that can be applied to the test cases provided A CD with all security requirements and test cases as well as MS Word versions of the checklists, requirements, and test cases covered in the book Offering ground-level, already-developed software nonfunctional requirements and corresponding test cases and methods, this book will help to ensure that your software meets its nonfunctional requirements for security and resilience. The accompanying CD filled with helpful checklists and reusable documentation provides you with the tools needed to integrate security into the requirements analysis, design, and testing phases of your software development lifecycle. Some Praise for the Book: This book pulls together the state of the art in thinking about this important issue in a holistic way with several examples. It takes you through the entire lifecycle from conception to implementation ... —Doug Cavit, Chief Security Strategist, Microsoft Corporation ...provides the reader with the tools necessary to jump-start and mature security within the software development lifecycle (SDLC). —Jeff Weekes, Sr. Security Architect at Terra Verde Services ... full of useful insights and practical advice from two authors who have lived this process. What you get is a tactical application security roadmap that cuts through the noise and is immediately applicable to your projects. —Jeff Williams, Aspect Security CEO and Volunteer Chair of the OWASP Foundation

Describes how to put software security into practice, covering such topics as risk analysis, coding policies, Agile Methods, cryptographic standards, and threat tree patterns.

The 7 Qualities of Highly Secure Software provides a framework for designing, developing, and deploying hacker-resilient software. It uses engaging anecdotes and analogies—ranging from Aesop's fables, athletics, architecture, biology, nursery rhymes, and video games—to illustrate the qualities that are essential for the development of highly secure

This book introduces a cross-layer design to achieve security and resilience for CPSs (Cyber-Physical Systems). The authors interconnect various technical tools and methods to capture the different properties between cyber and physical layers. Part II of this book bridges the gap between cryptography and control-theoretic tools. It develops a bespoke crypto-control framework to address security and resiliency in control and estimation problems where the outsourcing of computations is possible. Part III of this book bridges the gap between game theory and control theory and develops interdependent impact-aware security defense strategies and cyber-aware resilient control strategies. With the rapid development of smart cities, there is a growing need to integrate the physical systems, ranging from large-scale infrastructures to small embedded systems, with networked communications. The integration of the physical and cyber systems forms Cyber-Physical Systems (CPSs), enabling the use of digital information and control technologies to improve the monitoring, operation, and planning of the systems. Despite these advantages, they are vulnerable to cyber-physical attacks, which aim to damage the physical layer through the cyber network. This book also uses case studies from autonomous systems, communication-based train control systems, cyber manufacturing, and robotic systems to illustrate the proposed methodologies. These case studies aim to motivate readers to adopt a cross-layer system perspective toward security and resilience issues of large and complex systems and develop domain-specific solutions to address CPS challenges. A comprehensive suite of solutions to a broad range of technical challenges in secure and resilient control systems are described in this book (many of the findings in this book are useful to anyone working in cybersecurity). Researchers, professors, and advanced-level students working in computer science and engineering will find this book useful as a reference or secondary text. Industry professionals and military workers interested in cybersecurity will also want to purchase this book.

Security and Resilience in Intelligent Data-Centric Systems and Communication Networks presents current, state-of-the-art work on novel research in theoretical and practical resilience and security aspects of intelligent data-centric critical systems and networks. The book analyzes concepts and technologies that are successfully used in the implementation of intelligent data-centric critical systems and communication networks, also touching on future developments. In addition, readers will find in-demand information for domain experts and developers who want to understand and realize the aspects (opportunities and challenges) of using emerging technologies for designing and developing more secure and resilient intelligent data-centric critical systems and communication networks. Topics covered include airports, seaports, rail transport systems, plants for the provision of water and energy, and business transactional systems. The book is well suited for researchers and PhD interested in the use of security and resilient computing technologies. Includes tools and techniques to prevent and avoid both accidental and malicious behaviors Explains the state-of-the-art technological solutions for main issues hindering the development of monitoring and reaction solutions Describes new methods and technologies, advanced prototypes, systems, tools and techniques of future direction

“At Cisco, we have adopted the CERT C Coding Standard as the internal secure coding standard for all C developers. It is a core component of our secure development lifecycle. The coding standard described in this book breaks down complex software security topics into easy-to-follow rules with excellent real-world examples. It is an essential reference for any developer who wishes to write secure and resilient software in C and C++.” —Edward D. Paradise, vice president, engineering, threat response, intelligence, and development, Cisco Systems Secure programming in C can be more difficult than even many experienced programmers realize. To help programmers write more secure code, The CERT® C Coding Standard, Second Edition, fully documents the second official release of the CERT standard for secure coding in C. The rules laid forth in this new edition will help ensure that programmers' code fully complies with the new C11 standard; it also addresses earlier versions, including C99. The new standard itemizes those coding errors that are the root causes of current software vulnerabilities in C, prioritizing them by severity, likelihood of exploitation, and remediation costs. Each of the text's 98 guidelines includes examples of insecure code as well as secure, C11-conforming, alternative implementations. If uniformly applied, these guidelines will eliminate critical coding errors that lead to buffer overflows, format-string vulnerabilities, integer overflow, and other common vulnerabilities. This book reflects numerous experts' contributions to the open development and review of the rules and recommendations that comprise this standard. Coverage includes Preprocessor Declarations and Initialization Expressions Integers Floating Point Arrays Characters and Strings Memory Management Input/Output Environment Signals Error Handling Concurrency Miscellaneous Issues

The 7 Qualities of Highly Secure Software provides a framework for designing, developing, and deploying hacker-resilient software. It uses engaging anecdotes and analogies—ranging from Aesop's fables, athletics, architecture, biology, nursery rhymes, and video games—to illustrate the qualities that are essential for the development of highly secure software. Each chapter details one of the seven qualities that can make your software highly secure and less susceptible to hacker threats. Leveraging real-world experiences and examples, the book: Explains complex security concepts in language that is easy to understand for professionals involved in management, software development, and operations Specifies the qualities and skills that are essential for building secure software Highlights the parallels between the habits of effective people and qualities in terms of software security Praise for the Book: This will be required reading for my executives, security team, software architects and lead developers. —David W. Stender, CISSP, CSSLP, CAP, CISO of the US Internal Revenue Service Developing highly secure software should be at the forefront of organizational strategy and this book provides a framework to do so.

—Troy Leach, CTO, PCI Security Standards Council This book will teach you the core, critical skills needed to raise the security bar on the attackers and swing the game in your favor. —Michael Howard, Principal Cyber Security Program Manager, Microsoft As a penetration tester, my job will be a lot harder as people read this book! —Kevin Johnson, Security Consultant, Secure Ideas As the global leader in information security education and certification, (ISC)2 has a proven track record of educating and certifying information security professionals. Its newest certification, the Certified Secure Software Lifecycle Professional (CSSLP) is a testament to the organization's ongoing commitment to information and software security

Cyber-attacks continue to rise as more individuals rely on storing personal information on networks. Even though these networks are continuously checked and secured, cybercriminals find new strategies to break through these protections. Thus, advanced security systems, rather than simple security patches, need to be designed and developed. Exploring Security in Software Architecture and Design is an essential reference source that discusses the development of security-aware software systems that are built into every phase of the software architecture. Featuring research on topics such as migration techniques, service-based software, and building security, this book is ideally designed for computer and software engineers, ICT specialists, researchers, academicians, and field experts.

The only comprehensive set of guidelines for secure Java programming - from the field's leading organizations, CERT and Oracle • •Authoritative, end-to-end code-level requirements for building secure systems with any recent version of Java, including the new Java 7 •Presents techniques that also improve safety, reliability, dependability, robustness, availability, maintainability, and other attributes of quality. •Includes extensive risk assessment guidance, plus references for further information. This is the first authoritative, comprehensive compilation of code-level requirements for building secure systems in Java. Organized by CERT's pioneering software security experts, with support from Oracle's own Java platform developers, it covers every facet of secure software coding with Java 7 SE and Java 6 SE, and offers value even to developers working with other Java versions. The authors itemize the most common coding errors leading to vulnerabilities in Java programs, and provide specific guidelines for avoiding each of them. They show how to produce programs that are not only secure, but also safer, more reliable, more robust, and easier to maintain. After a high-level introduction to Java application security, eighteen consistently-organized chapters detail specific guidelines for each facet of Java development. Each set of guidelines defines conformance, presents both noncompliant examples and corresponding compliant solutions, shows how to assess risk, and offers references for further information. To limit this book's size, the authors focus on 'normative requirements': strict rules for what programmers must do for their work to be secure, as defined by conformance to specific standards that can be tested through automated analysis software. (Note: A follow-up book will present 'non-normative requirements': recommendations for what Java developers typically 'should' do to further strengthen program security beyond testable 'requirements'.)

Secure and Resilient Software: Requirements, Test Cases, and Testing Methods provides a comprehensive set of requirements for secure and resilient software development and operation. It supplies documented test cases for those requirements as well as best practices for testing nonfunctional requirements for improved information assurance. This resource-rich book includes: Pre-developed nonfunctional requirements that can be reused for any software development project. Documented test cases that go along with the requirements and can be used to develop a Test Plan for the software, Testing methods that can be applied to the test cases provided. Offering ground-level, already-developed software nonfunctional requirements and corresponding test cases and methods, this book will help to ensure that your software meets its nonfunctional requirements for security and resilience.

Developing Climate-Resilient Crops: Improving Global Food Security and Safety is timely, as the world is gradually waking up to the fact that a global food crisis of enormous proportions is brewing. Climate change is creating immense problems for agricultural productivity worldwide, resulting in higher food prices. This book elucidates the causative aspects of climate modification related to agriculture, soil, and plants, and discusses the relevant resulting mitigation process and also how new tools and resources can be used to develop climate-resilient crops. Features: Addresses the limits of the anthropogenic global warming theory advocated by the Intergovernmental Panel on Climate Change Presents the main characters (drought tolerance, heat tolerance, water-use efficiency, disease resistance, nitrogen-use efficiency, nitrogen fixation, and carbon sequestration) necessary for climate-resilient agriculture Delivers both theoretical and practical aspects, and serves as baseline information for future research Provides valuable resource for those students engaged in the field of environmental sciences, soil sciences, agricultural microbiology, plant pathology, and agronomy Highlights factors that are threatening future food production

IBM® has long been recognized as a leading provider of hardware, software, and services that are of the highest quality, reliability, function, and integrity. IBM products and services are used around the world by people and organizations with mission-critical demands for high performance, high stress tolerance, high availability, and high security. As a testament to this long-standing attention at IBM, demonstration of this attention to security can be traced back to the Integrity Statement for IBM mainframe software, which was originally published in 1973: IBM's long-term commitment to System Integrity is unique in the industry, and forms the basis of MVS (now IBM z/OS) industry leadership in system security. IBM MVS (now IBM z/OS) is designed to help you protect your system, data, transactions, and applications from accidental or malicious modification. This is one of the many reasons IBM 360 (now IBM Z) remains the industry's premier data server for mission-critical workloads. This commitment continues to apply to IBM's mainframe systems and is reiterated at the Server RACF General User's Guide web page. The IT market transformed in 40-plus years, and so have product development and information security practices. The IBM commitment to continuously improving product security remains a constant differentiator for the company. In this IBM Redguide™ publication, we describe

secure engineering practices for software products. We offer a description of an end-to-end approach to product development and delivery, with security considered. IBM is producing this IBM Redguide publication in the hope that interested parties (clients, other IT companies, academics, and others) can find these practices to be a useful example of the type of security practices that are increasingly a must-have for developing products and applications that run in the world's digital infrastructure. We also hope this publication can enrich our continued collaboration with others in the industry, standards bodies, government, and elsewhere, as we seek to learn and continuously refine our approach.

Software update is an important mechanism by which security changes and improvements are made in software, and this seemingly simple concept encompasses a wide variety of practices, mechanisms, policies, and technologies. To explore the landscape further, the Forum on Cyber Resilience hosted a workshop featuring invited speakers from government, the private sector, and academia. This publication summarizes the presentations and discussions from the workshop.

Most security books on Java focus on cryptography and access control, but exclude key aspects such as coding practices, logging, and web application risk assessment.

Encapsulating security requirements for web development with the Java programming platform, *Secure Java: For Web Application Development* covers secure programming, risk assessment, and threat modeling—explaining how to integrate these practices into a secure software development life cycle. From the risk assessment phase to the proof of concept phase, the book details a secure web application development process. The authors provide in-depth implementation guidance and best practices for access control, cryptography, logging, secure coding, and authentication and authorization in web application development. Discussing the latest application exploits and vulnerabilities, they examine various options and protection mechanisms for securing web applications against these multifarious threats. The book is organized into four sections: Provides a clear view of the growing footprint of web applications Explores the foundations of secure web application development and the risk management process Delves into tactical web application security development with Java EE Deals extensively with security testing of web applications This complete reference includes a case study of an e-commerce company facing web application security challenges, as well as specific techniques for testing the security of web applications. Highlighting state-of-the-art tools for web application security testing, it supplies valuable insight on how to meet important security compliance requirements, including PCI-DSS, PA-DSS, HIPAA, and GLBA. The book also includes an appendix that covers the application security guidelines for the payment card industry standards.

Security protections for critical infrastructure nodes are intended to minimize the risks resulting from an initiating event, whether it is an intentional malevolent act or a natural hazard. With an emphasis on protecting an infrastructure's ability to perform its mission or function, *Critical Infrastructure System Security and Resiliency* presents a practical methodology for developing an effective protection system that can either prevent undesired events or mitigate the consequences of such events. Developed at Sandia National Labs, the authors' analytical approach and methodology enables decision-makers and security experts to perform and utilize risk assessments in a manner that extends beyond the theoretical to practical application. These protocols leverage expertise in modeling dependencies—optimizing system resiliency for effective physical protection system design and consequence mitigation. The book begins by focusing on the design of protection strategies to enhance the robustness of the infrastructure components. The authors present risk assessment tools and necessary metrics to offer guidance to decision-makers in applying sometimes limited resources to reduce risk and ensure operational resiliency. Our critical infrastructure is vast and made up of many component parts. In many cases, it may not be practical or affordable to secure every infrastructure node. For years, experts—as a part of the risk assessment process—have tried to better identify and distinguish higher from lower risks through risk segmentation. In the second section of the book, the authors present examples to distinguish between high and low risks and corresponding protection measures. In some cases, protection measures do not prevent undesired events from occurring. In others, protection of all infrastructure components is not feasible. As such, this section describes how to evaluate and design resilience in these unique scenarios to manage costs while most effectively ensuring infrastructure system protection. With insight from the authors' decades of experience, this book provides a high-level, practical analytical framework that public and private sector owners and operators of critical infrastructure can use to better understand and evaluate infrastructure security strategies and policies. Strengthening the entire homeland security enterprise, the book presents a significant contribution to the science of critical infrastructure protection and resilience.

The overwhelming majority of a software system's lifespan is spent in use, not in design or implementation. So, why does conventional wisdom insist that software engineers focus primarily on the design and development of large-scale computing systems? In this collection of essays and articles, key members of Google's Site Reliability Team explain how and why their commitment to the entire lifecycle has enabled the company to successfully build, deploy, monitor, and maintain some of the largest software systems in the world. You'll learn the principles and practices that enable Google engineers to make systems more scalable, reliable, and efficient—lessons directly applicable to your organization. This book is divided into four sections: Introduction—Learn what site reliability engineering is and why it differs from conventional IT industry practices Principles—Examine the patterns, behaviors, and areas of concern that influence the work of a site reliability engineer (SRE) Practices—Understand the theory and practice of an SRE's day-to-day work: building and operating large distributed computing systems Management—Explore Google's best practices for training, communication, and meetings that your organization can use

This book constitutes the refereed proceedings of the International Workshop on Software Engineering for Resilient Systems, SERENE 2017, held in Geneva, Switzerland, in September 2017. The 11 papers presented together with 2 invited talks were carefully reviewed and selected from 16 submissions. They cover the following areas: modeling and specification; safety and

security; fault tolerance, resilience and robustness software.

Presenting a fundamental definition of resilience, the book examines the concept of resilience as it relates to space system design. The book establishes the required definitions, relates its place to existing state-of-the-art systems engineering practices, and explains the exact process and mathematical tools used to achieve a resilient design. It discusses a variety of potential threats and their impact upon a space system. By providing multiple, real-world examples to illustrate the application of the design methodology, the book covers the necessary techniques and tools, while guiding the reader through the entirety of the process. The book begins with space systems basics to ensure the reader is versed in the functions and components of the system prior to diving into the details of resilience. However, the text does not assume that the reader has an extensive background in the subject matter of resilience. This book is aimed at engineers and architects in the areas of aerospace, space systems, and space communications.

For Resilience Engineering, 'failure' is the result of the adaptations necessary to cope with the complexity of the real world, rather than a breakdown or malfunction. The performance of individuals and organizations must continually adjust to current conditions and, because resources and time are finite, such adjustments are always approximate. This definitive new book explores this groundbreaking new development in safety and risk management, where 'success' is based on the ability of organizations, groups and individuals to anticipate the changing shape of risk before failures and harm occur. Featuring contributions from many of the world's leading figures in the fields of human factors and safety, Resilience Engineering provides thought-provoking insights into system safety as an aggregate of its various components, subsystems, software, organizations, human behaviours, and the way in which they interact. The book provides an introduction to Resilience Engineering of systems, covering both the theoretical and practical aspects. It is written for those responsible for system safety on managerial or operational levels alike, including safety managers and engineers (line and maintenance), security experts, risk and safety consultants, human factors professionals and accident investigators. Handbook of System Safety and Security: Cyber Risk and Risk Management, Cyber Security, Adversary Modeling, Threat Analysis, Business of Safety, Functional Safety, Software Systems, and Cyber Physical Systems presents an update on the world's increasing adoption of computer-enabled products and the essential services they provide to our daily lives. The tailoring of these products and services to our personal preferences is expected and made possible by intelligence that is enabled by communication between them. Ensuring that the systems of these connected products operate safely, without creating hazards to us and those around us, is the focus of this book, which presents the central topics of current research and practice in systems safety and security as it relates to applications within transportation, energy, and the medical sciences. Each chapter is authored by one of the leading contributors to the current research and development on the topic. The perspective of this book is unique, as it takes the two topics, systems safety and systems security, as inextricably intertwined. Each is driven by concern about the hazards associated with a system's performance. Presents the most current and leading edge research on system safety and security, featuring a panel of top experts in the field Includes several research advancements published for the first time, including the use of 'goal structured notation' together with a 'judgment calculus' and their automation as a 'rule set' to facilitate systems safety and systems security process execution in compliance with existing standards Presents for the first time the latest research in the field with the unique perspective that systems safety and systems security are inextricably intertwined Includes coverage of systems architecture, cyber physical systems, tradeoffs between safety, security, and performance, as well as the current methodologies and technologies and implantation practices for system safety and security

This book addresses the latest approaches to holistic Cyber-Physical System (CPS) resilience in real-world industrial applications. Ensuring the resilience of CPSs requires cross-discipline analysis and involves many challenges and open issues, including how to address evolving cyber-security threats. The book describes emerging paradigms and techniques from two main viewpoints: CPSs' exposure to new threats, and CPSs' potential to counteract them. Further, the chapters address topics ranging from risk modeling to threat management and mitigation. The book offers a clearly structured, highly accessible resource for a diverse readership, including graduate students, researchers and industry practitioners who are interested in evaluating and ensuring the resilience of CPSs in both the development and assessment stages.

Security practitioners must be able to build a cost-effective security program while at the same time meet the requirements of government regulations. This book lays out these regulations in simple terms and explains how to use the control frameworks to build an effective information security program and governance structure. It discusses how organizations can best ensure that the information is protected and examines all positions from the board of directors to the end user, delineating the role each plays in protecting the security of the organization.

As more companies move toward microservices and other distributed technologies, the complexity of these systems increases. You can't remove the complexity, but through Chaos Engineering you can discover vulnerabilities and prevent outages before they impact your customers. This practical guide shows engineers how to navigate complex systems while optimizing to meet business goals. Two of the field's prominent figures, Casey Rosenthal and Nora Jones, pioneered the discipline while working together at Netflix. In this book, they expound on the what, how, and why of Chaos Engineering while facilitating a conversation from practitioners across industries. Many chapters are written by contributing authors to widen the perspective across verticals within (and beyond) the software industry. Learn how Chaos Engineering enables your organization to navigate complexity Explore a methodology to avoid failures within your application, network, and infrastructure Move from theory to practice through real-world stories from industry experts at Google, Microsoft, Slack, and LinkedIn, among others Establish a framework for thinking about complexity within software systems Design a Chaos Engineering program around game days and move toward highly targeted, automated experiments Learn how to design continuous collaborative chaos experiments

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.

With the prevalence of cyber crime and cyber warfare, software developers must be vigilant in creating systems which are impervious to cyber attacks. Thus, security issues are an integral part of every phase of software development and an essential component of software design. *Security-Aware Systems Applications and Software Development Methods* facilitates the promotion and understanding of the technical as well as managerial issues related to secure software systems and their development practices. This book, targeted toward researchers, software engineers, and field experts, outlines cutting-edge industry solutions in software engineering and security research to help overcome contemporary challenges.

Today's high-speed and rapidly changing development environments demand equally high-speed security practices. Still, achieving security remains a human endeavor, a core part of designing, generating and verifying software. Dr. James Ransome and Brook S.E. Schoenfield have built upon their previous works to explain that security starts with people; ultimately, humans generate software security. People collectively act through a particular and distinct set of methodologies, processes, and technologies that the authors have brought together into a newly designed, holistic, generic software development lifecycle facilitating software security at Agile, DevOps speed. —Eric. S. Yuan, Founder and CEO, Zoom Video Communications, Inc. It is essential that we embrace a mantra that ensures security is baked in throughout any development process. Ransome and Schoenfield leverage their abundance of experience and knowledge to clearly define why and how we need to build this new model around an understanding that the human element is the ultimate key to success. —Jennifer Sunshine Steffens, CEO of IOActive Both practical and strategic, *Building in Security at Agile Speed* is an invaluable resource for change leaders committed to building secure software solutions in a world characterized by increasing threats and uncertainty. Ransome and Schoenfield brilliantly demonstrate why creating robust software is a result of not only technical, but deeply human elements of agile ways of working. —Jorgen Hesselberg, author of *Unlocking Agility* and Cofounder of Comparative Agility The proliferation of open source components and distributed software services makes the principles detailed in *Building in Security at Agile Speed* more relevant than ever. Incorporating the principles and detailed guidance in this book into your SDLC is a must for all software developers and IT organizations.

—George K Tsantes, CEO of Cyberphos, former partner at Accenture and Principal at EY Detailing the people, processes, and technical aspects of software security, *Building in Security at Agile Speed* emphasizes that the people element remains critical because software is developed, managed, and exploited by humans. This book presents a step-by-step process for software security that is relevant to today's technical, operational, business, and development environments with a focus on what humans can do to control and manage the process in the form of best practices and metrics.

A collection of best practices and effective implementation recommendations that are proven to work, *Secure, Resilient, and Agile Software Development* leaves the boring details of software security theory out of the discussion as much as possible to concentrate on practical applied software security for practical people. Written to aid your career as well as your organization, the book shows how to gain skills in secure and resilient software development and related tasks. The book explains how to integrate these development skills into your daily duties, thereby increasing your professional value to your company, your management, your community, and your industry. *Secure, Resilient, and Agile Software Development* was written for the following professionals: AppSec architects and program managers in information security organizations Enterprise architecture teams with application development focus Scrum teams DevOps teams Product owners and their managers Project managers Application security auditors With a detailed look at Agile and Scrum software development methodologies, this book explains how security controls need to change in light of an entirely new paradigm on how software is developed. It focuses on ways to educate everyone who has a hand in any software development project with appropriate and practical skills to Build Security In. After covering foundational and fundamental principles for secure application design, this book dives into concepts, techniques, and design goals to meet well-understood acceptance criteria on features an application must implement. It also explains how the design sprint is adapted for proper consideration of security as well as defensive programming techniques. The book concludes with a look at white box application analysis and sprint-based activities to improve the security and quality of software under development.

Cyber Security Engineering is the definitive modern reference and tutorial on the full range of capabilities associated with modern cyber security engineering. Pioneering software assurance experts Dr. Nancy R. Mead and Dr. Carol C. Woody bring together comprehensive best practices for building software systems that exhibit superior operational security, and for considering security throughout your full system development and acquisition lifecycles. Drawing on their pioneering work at the Software Engineering Institute (SEI) and Carnegie Mellon University, Mead and Woody introduce seven core principles of software assurance, and show how to apply them coherently and systematically. Using these principles, they help you prioritize the wide range of possible security actions available to you, and justify the required investments. *Cyber Security Engineering* guides you through risk analysis, planning to manage secure software development, building organizational models, identifying required and missing competencies, and defining and structuring metrics. Mead and Woody address important topics, including the use of standards, engineering security requirements for acquiring COTS software, applying DevOps, analyzing malware to anticipate future vulnerabilities, and planning ongoing improvements. This book will be valuable to wide audiences of practitioners and managers with responsibility for systems, software, or quality engineering, reliability, security, acquisition, or operations. Whatever your role, it can help you reduce operational problems,

eliminate excessive patching, and deliver software that is more resilient and secure.

CERT® Resilience Management Model (CERT-RMM) is an innovative and transformative way to manage operational resilience in complex, risk-evolving environments. CERT-RMM distills years of research into best practices for managing the security and survivability of people, information, technology, and facilities. It integrates these best practices into a unified, capability-focused maturity model that encompasses security, business continuity, and IT operations. By using CERT-RMM, organizations can escape silo-driven approaches to managing operational risk and align to achieve strategic resilience management goals. This book both introduces CERT-RMM and presents the model in its entirety. It begins with essential background for all professionals, whether they have previously used process improvement models or not. Next, it explains CERT-RMM's Generic Goals and Practices and discusses various approaches for using the model. Short essays by a number of contributors illustrate how CERT-RMM can be applied for different purposes or can be used to improve an existing program. Finally, the book provides a complete baseline understanding of all 26 process areas included in CERT-RMM. Part One summarizes the value of a process improvement approach to managing resilience, explains CERT-RMM's conventions and core principles, describes the model architecturally, and shows how it supports relationships tightly linked to your objectives. Part Two focuses on using CERT-RMM to establish a foundation for sustaining operational resilience management processes in complex environments where risks rapidly emerge and change. Part Three details all 26 CERT-RMM process areas, from asset definition through vulnerability resolution. For each, complete descriptions of goals and practices are presented, with realistic examples. Part Four contains appendices, including Targeted Improvement Roadmaps, a glossary, and other reference materials. This book will be valuable to anyone seeking to improve the mission assurance of high-value services, including leaders of large enterprise or organizational units, security or business continuity specialists, managers of large IT operations, and those using methodologies such as ISO 27000, COBIT, ITIL, or CMMI.

Can a system be considered truly reliable if it isn't fundamentally secure? Or can it be considered secure if it's unreliable? Security is crucial to the design and operation of scalable systems in production, as it plays an important part in product quality, performance, and availability. In this book, experts from Google share best practices to help your organization design scalable and reliable systems that are fundamentally secure. Two previous O'Reilly books from Google—Site Reliability Engineering and The Site Reliability Workbook—demonstrated how and why a commitment to the entire service lifecycle enables organizations to successfully build, deploy, monitor, and maintain software systems. In this latest guide, the authors offer insights into system design, implementation, and maintenance from practitioners who specialize in security and reliability. They also discuss how building and adopting their recommended best practices requires a culture that's supportive of such change. You'll learn about secure and reliable systems through: Design strategies Recommendations for coding, testing, and debugging practices Strategies to prepare for, respond to, and recover from incidents Cultural best practices that help teams across your organization collaborate effectively

Application vulnerabilities continue to top the list of cyber security concerns. While attackers and researchers continue to expose new application vulnerabilities, the most common application flaws are previous, rediscovered threats. For example, SQL injection and cross-site scripting (XSS) have appeared on the Open Web Application Security Project

"This book challenges the concept of 'urban resilience' by exploring its impact and limitations in three cities. Resilience has become a buzzword in science, industry and policy, and this volume offers a fresh perspective on urban resilience as a regulatory and constitutive principle of governance in cities. Cities constitute an extremely relevant playground for resilience, as they are exposed to various disruptions from natural disasters and pandemics to political conflicts and terrorism. This book traces the evolution of urban resilience, from international development organizations to local governments and communities. It explores how this concept was adopted and mobilized by different actors for different purposes, and analyses the resulting resilience momentum in Barcelona, San Francisco, and Santiago. The book outlines the extent to which resilience has become a universal policy tool and a desired end-state, despite its clearly problematic definition. It also contributes to the discussion about contemporary governance, safety and security in times when their very nature and feasibility are being questioned. This book will be of much interest to students of resilience studies, urban studies, development studies, human geography, and International Relations"--

If you're an information security professional today, you are being forced to address growing cyber security threats and ever-evolving compliance requirements, while dealing with stagnant and decreasing budgets. The Frugal CISO: Using Innovation and Smart Approaches to Maximize Your Security Posture describes techniques you can immediately put to u

Cloud services are just as susceptible to network outages as any other platform. This concise book shows you how to prepare for potentially devastating interruptions by building your own resilient and reliable applications in the public cloud. Guided by engineers from 9apps—an independent provider of Amazon Web Services and Eucalyptus cloud solutions—you'll learn how to combine AWS with open source tools such as PostgreSQL, MongoDB, and Redis. This isn't a book on theory. With detailed examples, sample scripts, and solid advice, software engineers with operations experience will learn specific techniques that 9apps routinely uses in its cloud infrastructures. Build cloud applications with the "rip, mix, and burn" approach Get a crash course on Amazon Web Services Learn the top ten tips for surviving outages in the cloud Use elasticsearch to build a dependable NoSQL data store Combine AWS and PostgreSQL to build an RDBMS that scales well Create a highly available document database with MongoDB Replica Set and SimpleDB Augment Redis with AWS to provide backup/restore, failover, and monitoring capabilities Work with CloudFront and Route 53 to safeguard global content delivery

Although many software books highlight open problems in secure software development, few provide easily actionable, ground-level solutions. Breaking the mold, Secure and Resilient Software Development teaches you how to apply best practices and standards for consistent and secure software development. It details specific quality software developmen

Cyber Strategy: Risk-Driven Security and Resiliency provides a process and roadmap for any company to develop its unified Cybersecurity and Cyber Resiliency strategies. It demonstrates a methodology for companies to combine their disassociated efforts into one corporate plan with buy-in from senior management that will efficiently utilize resources, target high risk threats, and evaluate risk assessment methodologies and the efficacy of resultant risk mitigations. The book discusses all the steps required from conception of the plan from preplanning (mission/vision, principles, strategic objectives, new initiatives derivation), project management directives, cyber threat and vulnerability analysis, cyber risk and controls assessment to reporting and measurement techniques for plan success and overall strategic plan performance. In addition, a methodology is presented to aid in new initiative selection for the following year by identifying all relevant inputs. Tools utilized include: Key Risk Indicators (KRI) and Key Performance Indicators (KPI) National Institute of Standards and Technology (NIST) Cyber Security Framework (CSF) Target State Maturity interval mapping per initiative Comparisons of current and target state business goals and critical success factors A quantitative NIST-based risk assessment of initiative technology components Responsible, Accountable, Consulted, Informed (RACI) diagrams for Cyber Steering Committee tasks and Governance Boards' approval processes Swimlanes, timelines, data flow diagrams (inputs, resources, outputs), progress report templates, and Gantt charts for project management The last chapter provides downloadable checklists, tables, data flow diagrams, figures, and assessment tools to help develop your company's cybersecurity and cyber resiliency strategic plan.

This book focuses on software architecture and the value of architecture in the development of long-lived, mission-critical, trustworthy software-systems. The author introduces and demonstrates the powerful strategy of "Managed Evolution," along with the engineering best practice known as "Principle-based Architecting." The book examines in detail architecture principles for e.g., Business Value, Changeability, Resilience, and Dependability. The author argues that the software development community has a strong responsibility to produce and operate useful, dependable, and trustworthy software. Software should at the same time provide business value and guarantee many quality-of-service properties, including security, safety, performance, and integrity. As Dr. Furrer states, "Producing dependable software is a balancing act between investing in the implementation of business functionality and investing in the quality-of-service properties of the software-systems." The book presents extensive coverage of such concepts as: Principle-Based Architecting Managed Evolution Strategy The Future Principles for Business Value Legacy Software Modernization/Migration Architecture Principles for Changeability Architecture Principles for Resilience Architecture Principles for Dependability The text is supplemented with numerous figures, tables, examples and illustrative quotations. Future-Proof Software-Systems provides a set of good engineering practices, devised for integration into most software development processes dedicated to the creation of software-systems that incorporate Managed Evolution.

[Copyright: e8a81d05ce5fa9d1fd3c3d2667a91c12](https://www.pdfdrive.com/secure-and-resilient-software-development-format-pdf/e8a81d05ce5fa9d1fd3c3d2667a91c12)