Security Patterns In Practice Designing Secure Architectures Using Software Patterns Wiley Series In Software Design Patterns By Fernandez Eduardo B Author 2013 Hardcover

If you ally craving such a referred **Security Patterns In Practice Designing Secure Architectures Using Software Patterns Wiley Series In Software Design Patterns By Fernandez Eduardo B Author 2013 Hardcover** ebook that will give you worth, get the no question best seller from us currently from several preferred authors. If you want to droll books, lots of novels, tale, jokes, and more fictions collections are next launched, from best seller to one of the most current released.

You may not be perplexed to enjoy all book collections Security Patterns In Practice Designing Secure Architectures Using Software Patterns Wiley Series In Software Design Patterns By Fernandez Eduardo B Author 2013 Hardcover that we will unconditionally offer. It is not around the costs. Its nearly what you dependence currently. This Security Patterns In Practice Designing Secure Architectures Using Software Patterns Wiley Series In Software Design Patterns By Fernandez Eduardo B Author 2013 Hardcover , as one of the most in action sellers here will utterly be accompanied by the best options to review.

The Practice of Enterprise Modeling - Ulrich Frank 2014-11-07
This volume constitutes the proceedings of the 7th IFIP WG 8.1 Conference on the Practice of Enterprise Modeling held in November 2014 in Manchester, UK. The focus of the PoEM conference series is on advances in the practice of enterprise modeling through a forum for sharing knowledge and experiences between the academic community and practitioners from industry and the public sector. The 16 full and four short papers accepted were carefully reviewed and selected from 39 submissions. They reflect different topics of enterprise modeling including business process modeling, enterprise architecture, investigation of enterprise modeling methods, requirements engineering, and specific aspects of enterprise modeling.
Model Management and Analytics for Large Scale Systems - Bedir Tekinerdogan 2019-09-14
Model Management and Analytics for Large Scale Systems covers the use of models and related artefacts (such as metamodels and model transformations) as central elements for tackling the complexity of building systems and managing data. With their increased use across diverse settings, the complexity, size, multiplicity and variety of those artefacts has increased. Originally developed for software engineering, these approaches can now be used to simplify the analytics of large-scale models and automate complex data analysis processes. Those in the field of data science will gain novel insights on the topic of model analytics that go beyond both model-based development and data analytics. This book is aimed at both researchers and practitioners who are interested in model-based development and the analytics of large-scale models, ranging from big data management and analytics, to enterprise domains. The book could also be used in graduate courses on model development, data analytics and data management. Identifies key problems and offers solution approaches and tools that have been developed or are necessary for model management and analytics Explores basic theory and background, current research topics, related challenges and the research directions for model management and analytics Provides a complete overview of model management and analytics frameworks, the different types of analytics (descriptive, diagnostics, predictive and prescriptive), the required modelling and method steps, and important future directions
Cyberspace Safety and Security - Yang Xiang 2012-12-02
This book constitutes the refereed proceedings of the 4th International Symposium on Cyberspace Safety and Security (CSS 2012), held in Melbourne, Australia, in December 2012. The 30 revised full papers presented together with 7 invited talks were carefully reviewed and selected from 105 submissions. The papers cover the following topics: mobile security, cyberspace attacks and defense, security application adn systems, network and cloud security, wireless security, security protocols and models.
Designing Secure IoT Devices with the Arm Platform Security Architecture and Cortex-M33 - Trevor Martin 2022-04-28
Designing Secure IoT devices with the Arm Platform Security Architecture and Cortex-M33 explains how to design and deploy secure IoT devices based on the Cortex-M23/M33 processor. The book is split into three parts. First, it introduces the Cortex-M33 and its architectural design and major processor peripherals. Second, it shows how to design secure software and secure communications to minimize the threat of both hardware and software hacking. And finally, it examines common IoT cloud systems and how to design and deploy a fleet of IoT devices. Example projects are provided for the Keil MDK-ARM and NXP LPCXpresso tool chains. Since their inception, microcontrollers have been designed as functional devices with a CPU, memory and peripherals that can be programmed to accomplish a huge range of tasks. With the growth of internet connected devices and the Internet of Things (IoT), “plain old microcontrollers are no longer suitable as they lack the features necessary to create both a secure and functional device. The recent development by ARM of the Cortex M23 and M33 architecture is intended for today’s IoT world. Shows how to design secure software and secure communications using the ARM Cortex M33-based microcontrollers Explains how to write secure code to minimize vulnerabilities using the CERT-C coding standard Uses the mbedTLS library to implement modern cryptography Introduces the TrustZone security peripheral PSA security model and Trusted Firmware Legal requirements and reaching device certification with PSA Certified
Security and Microservice Architecture on AWS - Gaurav Raje 2021-09-08
Security is usually an afterthought when organizations design microservices for cloud systems. Most companies today are exposed to potential security threats, but their responses are often more reactive than proactive. This leads to unnecessarily complicated systems that are hard to implement and even harder to manage and scale. Author Gaurav Raje shows you how to build highly secure systems on AWS without increasing overhead. Ideal for cloud solution architects and software developers with AWS experience, this practical book starts with a high-level architecture and design discussion, then explains how to implement your solution in the cloud while ensuring that the development and operational experience isn't compromised. By leveraging the AWS Shared Responsibility Model, you'll be able to: Develop a modular architecture using microservices that aims to simplify compliance with various regulations in finance, medicine, and legal services Introduce various AWS-based security controls to help protect your microservices from malicious actors Leverage the modularity of the architecture to independently scale security mechanisms on individual microservices Improve the security posture without compromising the autonomy or efficiency of software development teams
Secrets of a Cyber Security Architect - Brook S. E. Schoenfield 2019-12-15
Any organization with valuable data has been or will be attacked, probably successfully, at some point and with some damage. And, don't all digitally connected organizations have at least some data that can be considered "valuable"? Cyber security is a big, messy, multivariate, multidimensional arena. A reasonable "defense-in-depth" requires many technologies; smart, highly skilled people; and deep and broad analysis, all of which must come together into some sort of functioning whole, which is often termed a security architecture. Secrets of a Cyber Security Architect is about security architecture in practice. Expert security architects have dozens of tricks of their trade in their kips. In this book, author Brook S. E. Schoenfield shares his tips and tricks, as well as myriad tried and true bits of wisdom that his colleagues have shared with him. Creating and implementing a cyber security architecture can be hard, complex, and certainly frustrating work. This book is written to ease this pain and show how to express security requirements in ways that

make the requirements more palatable and, thus, get them accomplished. It also explains how to surmount individual, team, and organizational resistance. The book covers: What security architecture is and the areas of expertise a security architect needs in practice The relationship between attack methods and the art of building cyber defenses Why to use attacks and how to derive a set of mitigations and defenses Approaches, tricks, and manipulations proven successful for practicing security architecture Starting, maturing, and running effective security architecture programs Secrets of the trade for the practicing security architecture Tricks to surmount typical problems Filled with practical insight, Secrets of a Cyber Security Architect is the desk reference every security architect needs to thwart the constant threats and dangers confronting every digitally connected organization.

Software Technologies - Marten van Sinderen 2019-08-12

This book constitutes the thoroughly refereed post-conference proceedings of the 13th International Joint Conference on Software Technologies, ICSOFT 2018, held in Porto, Portugal, in July 2018. The 18 revised full papers were carefully reviewed and selected from 117 submissions. The topics covered in the papers include: business process modelling, IT service management, interoperability and service-oriented architecture, project management software, scheduling and estimating, software metrics, requirements elicitation and specification, software and systems integration, etc.

Exploring Security in Software Architecture and Design - Felderer, Michael 2019-01-25

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.

Guide to Efficient Software Design - David P. Voorhees 2020-01-01

This classroom-tested textbook presents an active-learning approach to the foundational concepts of software design. These concepts are then applied to a case study, and reinforced through practice exercises, with the option to follow either a structured design or object-oriented design paradigm. The text applies an incremental and iterative software development approach, emphasizing the use of design characteristics and modeling techniques as a way to represent higher levels of design abstraction, and promoting the model-view-controller (MVC) architecture. Topics and features: provides a case study to illustrate the various concepts discussed throughout the book, offering an in-depth look at the pros and cons of different software designs; includes discussion questions and hands-on exercises that extend the case study and apply the concepts to other problem domains; presents a review of program design fundamentals to reinforce understanding of the basic concepts; focuses on a bottom-up approach to describing software design concepts; introduces the characteristics of a good software design, emphasizing the model-view-controller as an underlying architectural principle; describes software design from both object-oriented and structured perspectives; examines additional topics on human-computer interaction design, quality assurance, secure design, design patterns, and persistent data storage design; discusses design concepts that may be applied to many types of software development projects; suggests a template for a software design document, and offers ideas for further learning. Students of computer science and software engineering will find this textbook to be indispensable for advanced undergraduate courses on programming and software design. Prior background knowledge and experience of programming is required, but familiarity in software design is not assumed.

Agile Software Engineering Skills - Julian Michael Bass 2023-04-14

This textbook is about working in teams to create functioning software. It covers skills in agile software development methods, team working, version control and continuous integration and shows readers how to apply some of the latest ideas from lean, agile and Kanban. Part I, which focuses on People, describes various project roles and the skills needed to perform each role. This includes members of self-organizing teams, scrum masters, product owners and activities for managing other stakeholders. The skills needed to create Product artefacts are detailed in Part II. These include skills to create agile requirements, architectures, designs as well as development and security artefacts. The agile development Process to coordinate with co-workers is described in Part III. It introduces the skills needed to facilitate an incremental process and to use software tools for version control and automated testing. Eventually some more advanced topics are explained in Part IV. These topics include large projects comprising multiple cooperating teams, automating deployment, cloud software services, DevOps and evolving live systems. This textbook addresses significant competencies in the IEEE/ACM Computing Curricula Task Force 2020. It includes nearly 100 exercises for trying out and applying the skills needed for agile software development. Hints, tips and further advice about tackling the exercises are presented at the end of each chapter, and a case study project, with downloadable source code from an online repository, integrates the skills learned across the chapters. In addition, further example software projects are also available there. This way, the book provides a hands-on guide to working on a development project as part of a team, and is inspired by the needs of early career practitioners as well as undergraduate software engineering and computer science students.

Safety and Security of Cyber-Physical Systems - Frank J. Furrer 2022-07-20

Cyber-physical systems (CPSs) consist of software-controlled computing devices communicating with each other and interacting with the physical world through sensors and actuators. A CPS has, therefore, two parts: The cyber part implementing most of the functionality and the physical part, i.e., the real world. Typical examples of CPS’s are a water treatment plant, an unmanned aerial vehicle, and a heart pacemaker. Because most of the functionality is implemented in software, the software is of crucial importance. The software determines the functionality and many CPS properties, such as safety, security, performance, real-time behavior, etc. Therefore, avoiding safety accidents and security incidents in the CPS requires highly dependable software. Methodology Today, many methodologies for developing safe and secure software are in use. As software engineering slowly becomes disciplined and mature, generally accepted construction principles have emerged. This monograph advocates principle-based engineering for the development and operation of dependable software. No new development process is suggested, but integrating security and safety principles into existing development processes is demonstrated. Safety and Security Principles At the core of this monograph are the engineering principles. A total of 62 principles are introduced and catalogized into five categories: Business & organization, general principles, safety, security, and risk management principles. The principles are rigorous, teachable, and enforceable. The terminology used is precisely defined. The material is supported by numerous examples and enriched by illustrative quotes from celebrities in the field. Final Words «In a cyber-physical system’s safety and security, any compromise is a planned disaster» Audience First, this monograph is for organizations that want to improve their methodologies to build safe and secure software for mission-critical cyber-physical systems. Second, the material is suitable for a two-semester, 4 hours/week, advanced computer science lecture at a Technical University. This textbook has been recommended and developed for university courses in Germany, Austria and Switzerland.

Building Secure and Reliable Systems - Heather Adkins 2020-03-16

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

Innovative Systems for Intelligent Health Informatics - Faisal Saeed 2021-05-05

This book presents the papers included in the proceedings of the 5th International Conference of Reliable

Information and Communication Technology 2020 (IRICT 2020) that was held virtually on December 21–22, 2020. The main theme of the book is “Innovative Systems for Intelligent Health Informatics”. A total of 140 papers were submitted to the conference, but only 111 papers were published in this book. The book presents several hot research topics which include health informatics, bioinformatics, information retrieval, artificial intelligence, soft computing, data science, big data analytics, Internet of things (IoT), intelligent communication systems, information security, information systems, and software engineering.

Cyberpatterns - Clive Blackwell 2014-05-13

Cyberspace in increasingly important to people in their everyday lives for purchasing goods on the Internet, to energy supply increasingly managed remotely using Internet protocols. Unfortunately, this dependence makes us susceptible to attacks from nation states, terrorists, criminals and hactivists. Therefore, we need a better understanding of cyberspace, for which patterns, which are predictable regularities, may help to detect, understand and respond to incidents better. The inspiration for the workshop came from the existing work on formalising design patterns applied to cybersecurity, but we also need to understand the many other types of patterns that arise in cyberspace.

Design Patterns for Cloud Native Applications - Kasun Indrasiri 2021-05-17

With the immense cost savings and scalability the cloud provides, the rationale for building cloud native applications is no longer in question. The real issue is how. With this practical guide, developers will learn about the most commonly used design patterns for building cloud native applications using APIs, data, events, and streams in both greenfield and brownfield development. You'll learn how to incrementally design, develop, and deploy large and effective cloud native applications that you can manage and maintain at scale with minimal cost, time, and effort. Authors Kasun Indrasiri and Sriskandarajah Suhothayan highlight use cases that effectively demonstrate the challenges you might encounter at each step. Learn the fundamentals of cloud native applications Explore key cloud native communication, connectivity, and composition patterns Learn decentralized data management techniques Use event-driven architecture to build distributed and scalable cloud native applications Explore the most commonly used patterns for API management and consumption Examine some of the tools and technologies you'll need for building cloud native systems

Designing Distributed Control Systems - Veli-Pekka Eloranta 2014-06-09

Designing Distributed Control Systems presents 80 patterns for designing distributed machine control system software architecture (forestry machinery, mining drills, elevators, etc.). These patterns originate from state-of-the-art systems from market-leading companies, have been tried and tested, and will address typical challenges in the domain, such as long lifecycle, distribution, real-time and fault tolerance. Each pattern describes a separate design problem that needs to be solved. Solutions are provided, with consequences and trade-offs. Each solution will enable piecemeal growth of the design. Finding a solution is easy, as the patterns are divided into categories based on the problem field the pattern tackles. The design process is guided by different aspects of quality, such as performance and extendibility, which are included in the pattern descriptions. The book also contains an example software architecture designed by leading industry experts using the patterns in the book. The example system introduces the reader to the problem domain and demonstrates how the patterns can be used in a practical system design process. The example architecture shows how useful a toolbox the patterns provide for both novices and experts, guiding the system design process from its beginning to the finest details. Designing distributed machine control systems with patterns ensures high quality in the final product. High-quality systems will improve revenue and guarantee customer satisfaction. As market need changes, the desire to produce a quality machine is not only a primary concern, there is also a need for easy maintenance, to improve efficiency and productivity, as well as the growing importance of environmental values; these all impact machine design. The software of work machines needs to be designed with these new requirements in mind. Designing Distributed Control Systems presents patterns to help tackle these challenges. With proven methodologies from the expert author team, they show readers how to improve the quality and efficiency of distributed control systems.

Engineering Secure Software and Systems - Eric Bodden 2017-06-23

This book constitutes the refereed proceedings of the 9th International Symposium on Engineering Secure Software and Systems, ESSoS 2017, held in Bonn, Germany in July 2017. The 12 full papers presented together with 3 short papers were carefully reviewed and selected from 32 submissions. The goal of this symposium is to bring together researchers and practitioners to advance the states of the art and practice in secure software engineering.

Real-time Design Patterns - Bruce Powel Douglass 2003

This revised and enlarged edition of a classic in Old Testament scholarship reflects the most up-to-date research on the prophetic books and offers substantially expanded discussions of important new insight on Isaiah and the other prophets.

Secure by Design - Daniel Sawano 2019-09-03

Summary Secure by Design teaches developers how to use design to drive security in software development. This book is full of patterns, best practices, and mindsets that you can directly apply to your real world development. You'll also learn to spot weaknesses in legacy code and how to address them. About the technology Security should be the natural outcome of your development process. As applications increase in complexity, it becomes more important to bake security-mindedness into every step. The secure-by-design approach teaches best practices to implement essential software features using design as the primary driver for security. About the book Secure by Design teaches you principles and best practices for writing highly secure software. At the code level, you’ll discover security-promoting constructs like safe error handling, secure validation, and domain primitives. You’ll also master security-centric techniques you can apply throughout your build-test-deploy pipeline, including the unique concerns of modern microservices and cloud-native designs. What's inside Secure-by-design concepts Spotting hidden security problems Secure code constructs Assessing security by identifying common design flaws Securing legacy and microservices architectures About the reader Readers should have some experience in designing applications in Java, C#, .NET, or a similar language. About the author Dan Bergh Johnsson, Daniel Deogun, and Daniel Sawano are acclaimed speakers who often present at international conferences on topics of high-quality development, as well as security and design.

Managed Software Evolution - Ralf Reussner 2019-06-26

This open access book presents the outcomes of the “Design for Future – Managed Software Evolution” priority program 1593, which was launched by the German Research Foundation (“Deutsche Forschungsgemeinschaft (DFG)”) to develop new approaches to software engineering with a specific focus on long-lived software systems. The different lifecycles of software and hardware platforms lead to interoperability problems in such systems. Instead of separating the development, adaptation and evolution of software and its platforms, as well as aspects like operation, monitoring and maintenance, they should all be integrated into one overarching process. Accordingly, the book is split into three major parts, the first of which includes an introduction to the nature of software evolution, followed by an overview of the specific challenges and a general introduction to the case studies used in the project. The second part of the book consists of the main chapters on knowledge carrying software, and cover tacit knowledge in software evolution, continuous design decision support, model-based round-trip engineering for software product lines, performance analysis strategies, maintaining security in software evolution, learning from evolution for evolution, and formal verification of evolutionary changes. In turn, the last part of the book presents key findings and spin-offs. The individual chapters there describe various case studies, along with their benefits, deliverables and the respective lessons learned. An overview of future research topics rounds out the coverage. The book was mainly written for scientific researchers and advanced professionals with an academic background. They will benefit from its comprehensive treatment of various topics related to problems that are now gaining in importance, given the higher costs for maintenance and evolution in comparison to the initial development, and the fact that today, most software is not developed from scratch, but as part of a continuum of former and future releases.

Fundamentals of Secure System Modelling - Raimundas Matulevičius 2017-08-17

This book provides a coherent overview of the most important modelling-related security techniques available today, and demonstrates how to combine them. Further, it describes an integrated set of systematic practices that can be used to achieve increased security for software from the outset, and combines practical ways of working with practical ways of distilling, managing, and making security

knowledge operational. The book addresses three main topics: (1) security requirements engineering, including security risk management, major activities, asset identification, security risk analysis and defining security requirements; (2) secure software system modelling, including modelling of context and protected assets, security risks, and decisions regarding security risk treatment using various modelling languages; and (3) secure system development, including effective approaches, pattern-driven development, and model-driven security. The primary target audience of this book is graduate students studying cyber security, software engineering and system security engineering. The book will also benefit practitioners interested in learning about the need to consider the decisions behind secure software systems. Overall it offers the ideal basis for educating future generations of security experts.

Fowler - Martin Fowler 2012-03-09

The practice of enterprise application development has benefited from the emergence of many new enabling technologies. Multi-tiered object-oriented platforms, such as Java and .NET, have become commonplace. These new tools and technologies are capable of building powerful applications, but they are not easily implemented. Common failures in enterprise applications often occur because their developers do not understand the architectural lessons that experienced object developers have learned. Patterns of Enterprise Application Architecture is written in direct response to the stiff challenges that face enterprise application developers. The author, noted object-oriented designer Martin Fowler, noticed that despite changes in technology--from Smalltalk to CORBA to Java to .NET--the same basic design ideas can be adapted and applied to solve common problems. With the help of an expert group of contributors, Martin distills over forty recurring solutions into patterns. The result is an indispensable handbook of solutions that are applicable to any enterprise application platform. This book is actually two books in one. The first section is a short tutorial on developing enterprise applications, which you can read from start to finish to understand the scope of the book's lessons. The next section, the bulk of the book, is a detailed reference to the patterns themselves. Each pattern provides usage and implementation information, as well as detailed code examples in Java or C#. The entire book is also richly illustrated with UML diagrams to further explain the concepts. Armed with this book, you will have the knowledge necessary to make important architectural decisions about building an enterprise application and the proven patterns for use when building them. The topics covered include · Dividing an enterprise application into layers · The major approaches to organizing business logic · An in-depth treatment of mapping between objects and relational databases · Using Model-View-Controller to organize a Web presentation · Handling concurrency for data that spans multiple transactions · Designing distributed object interfaces

Computer Safety, Reliability, and Security - Amund Skavhaug 2016-09-01

This book constitutes the refereed proceedings of four workshops co-located with SAFECOMP 2016, the 35th International Conference on Computer Safety, Reliability, and Security, held in Trondheim, Norway, in September 2016. The 30 revised full papers presented together with 4 short and 5 invited papers were carefully reviewed and selected from numerous submissions. This year’s workshop are: ASSURE 2016 - Assurance Cases for Software-intensive Systems; DECSoS 2016 - EWICS/ERCIM/ARTEMIS Dependable Cyber-physical Systems and Systems-of-Systems Workshop; SASSUR 2016 - Next Generation of System Assurance Approaches for Safety-Critical Systems; and TIPS 2016 – Timing Performance in Safety Engineering.

Designing Secure Software - Loren Kohnfelder 2021-12-21

What every software professional should know about security. Designing Secure Software consolidates Loren Kohnfelder’s more than twenty years of experience into a concise, elegant guide to improving the security of technology products. Written for a wide range of software professionals, it emphasizes building security into software design early and involving the entire team in the process. The book begins with a discussion of core concepts like trust, threats, mitigation, secure design patterns, and cryptography. The second part, perhaps this book’s most unique and important contribution to the field, covers the process of designing and reviewing a software design with security considerations in mind. The final section details the most common coding flaws that create vulnerabilities, making copious use of code snippets written in C and Python to illustrate implementation vulnerabilities. You’ll learn how to: • Identify important assets, the attack surface, and the trust boundaries in a system • Evaluate the effectiveness of various threat mitigation candidates • Work with well-known secure coding patterns and libraries • Understand and prevent vulnerabilities like XSS and CSRF, memory flaws, and more • Use security testing to proactively identify vulnerabilities introduced into code • Review a software design for security flaws effectively and without judgment Kohnfelder’s career, spanning decades at Microsoft and Google, introduced numerous software security initiatives, including the co-creation of the STRIDE threat modeling framework used widely today. This book is a modern, pragmatic consolidation of his best practices, insights, and ideas about the future of software.

Future-Proof Software-Systems - Frank J. Furrer 2019-09-25

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.

Software Architecture in Practice - Len Bass 2003

This is the eagerly-anticipated revision to one of the seminal books in the field of software architecture which clearly defines and explains the topic.

Software Architecture with Python - Anand Balachandran Pillai 2017-04-28

Architect and design highly scalable, robust, clean, and highly performant applications in Python About This Book Identify design issues and make the necessary adjustments to achieve improved performance Understand practical architectural quality attributes from the perspective of a practicing engineer and architect using Python Gain knowledge of architectural principles and how they can be used to provide accountability and rationale for architectural decisions Who This Book Is For This book is for experienced Python developers who are aspiring to become the architects of enterprise-grade applications or software architects who would like to leverage Python to create effective blueprints of applications. What You Will Learn Build programs with the right architectural attributes Use Enterprise Architectural Patterns to solve scalable problems on the Web Understand design patterns from a Python perspective Optimize the performance testing tools in Python Deploy code in remote environments or on the Cloud using Python Secure architecture applications in Python In Detail This book starts off by explaining how Python fits into an application architecture. As you move along, you will understand the architecturally significant demands and how to determine them. Later, you'll get a complete understanding of the different architectural quality requirements that help an architect to build a product that satisfies business needs, such as maintainability/reusability, testability, scalability, performance, usability, and security. You will use various techniques such as incorporating DevOps, Continuous Integration, and more to make your application robust. You will understand when and when not to use object orientation in your applications. You will be able to think of the future and design applications that can scale proportionally to the growing business. The focus is on building the business logic based on the business process documentation and which frameworks are to be used when. We also cover some important patterns that are to be taken into account while solving design problems as well as those in relatively new domains such as the Cloud. This book will help you understand the ins and outs of Python so that you can make those critical design decisions that not just live up to but also surpass the expectations of your clients. Style and approach Filled with examples and use cases, this guide takes a no-nonsense approach to help you with everything it takes to become a successful software architect.

Software Architecture Design Patterns in Java - Partha Kuchana 2004-04-27
Software engineering and computer science students need a resource that explains how to apply design patterns at the enterprise level, allowing them to design and implement systems of high stability and quality. Software Architecture Design Patterns in Java is a detailed explanation of how to apply design patterns and develop software architectures. It provides in-depth examples in Java, and guides students by detailing when, why, and how to use specific patterns. This textbook presents 42 design patterns, including 23 GoF patterns. Categories include: Basic, Creational, Collectional, Structural, Behavioral, and Concurrency, with multiple examples for each. The discussion of each pattern includes an example implemented in Java. The source code for all examples is found on a companion Web site. The author explains the content so that it is easy to understand, and each pattern discussion includes Practice Questions to aid instructors. The textbook concludes with a case study that pulls several patterns together to demonstrate how patterns are not applied in isolation, but collaborate within domains to solve complicated problems.
Software Architecture - Danny Weyns 2015-09-02
This book constitutes the proceedings of the 9th European Conference on Software Architecture, ECSA 2015, held in Cavtat, Croatia in September 2015. The 12 full papers and 15 short papers presented together with three education and training papers in this volume were carefully reviewed and selected from 100 submissions. They are organized in topical sections named: adaptation; design approaches; decisions and social aspects; education and training; cloud and green; agile and smart systems; analysis and automation; services and ecosystems.
Business Modeling and Software Design - Boris Shishkov 2016-06-13
This book contains revised and extended versions of selected papers from the Fifth International Symposium on Business Modeling and Software Design, BMSD 2015, held in Milan, Italy, in July 2015. The symposium was organized and sponsored by the Interdisciplinary Institute for Collaboration and Research on Enterprise Systems and Technology (IICREST), being co-organized by Politecnico di Milano and technically co-sponsored by BPM-D. Cooperating organizations were Aristotle University of Thessaloniki (AUTH), the U Twente Center for Telematics and Information Technology (CTIT), the BAS Institute of Mathematics and Informatics (IMI), the Dutch Research School for Information and Knowledge Systems (SIKS), and AMAKOTA Ltd. BMSD 2015 received 57 paper submissions from which 36 papers were selected for publication in the BMSD'15 proceedings. 14 of those papers were selected as full papers. Additional post-symposium reviewing was carried out reflecting both the qualities of the papers and the way they were presented. 10 best papers were selected for the Springer edition (mainly from the BMSD'15 full papers). The 10 papers published in this book were carefully revised and extended (following the reviewers' comments) from the papers presented. The selection considers a large number of BMSD-relevant research topics: from business-processes-related topics, such as process mining and discovery, (dynamic) business process management (and process-aware information systems), and business process models and ontologies (including reflections into the Business Model Canvas); through software-engineering-related topics, such as domain-specific languages and software quality (and technical debt); and semantics-related topics, such as semantic technologies and knowledge management (and knowledge identification); to topics touching upon cloud computing and IT-enabled capabilities for enterprises.
Web Information Systems Engineering – WISE 2015 - Jianyong Wang 2015-10-26
This two volume set LNCS 9418 and LNCS 9419 constitutes the proceedings of the 16th International Conference on Web Information Systems Engineering, WISE 2015, held in Miami, FL, USA, in November 2015. The 53 full papers, 17 short and 14 special sessions and invited papers, presented in these proceedings were carefully reviewed and selected from 189 submissions. The papers cover the areas of big data techniques and applications, deep/hidden web, integration of web and internet, linked open data, semantic web, social network computing, social web and applications, social web models, analysis and mining, web-based applications, web-based business processes and web services, web data integration and mashups, web data models, web information retrieval, web privacy and security, web-based recommendations, and web search.
Pattern and Security Requirements - Kristian Beckers 2015-04-15
Security threats are a significant problem for information technology companies today. This book focuses on how to mitigate these threats by using security standards and provides ways to address associated problems faced by engineers caused by ambiguities in the standards. The security standards are analysed, fundamental concepts of the security standards presented, and the relations to the elementary concepts of security requirements engineering (SRE) methods explored. Using this knowledge, engineers can build customised methods that support the establishment of security standards. Standards such as Common Criteria or ISO 27001 are explored and several extensions are provided to well-known SRE methods such as Si*, CORAS, and UML4PF to support the establishment of these security standards. Through careful analysis of the activities demanded by the standards, for example the activities to establish an Information Security Management System (ISMS) in compliance with the ISO 27001 standard, methods are proposed which incorporate existing security requirement approaches and patterns. Understanding Pattern and Security Requirements engineering methods is important for software engineers, security analysts and other professionals that are tasked with establishing a security standard, as well as researchers who aim to investigate the problems with establishing security standards. The examples and explanations in this book are designed to be understandable by all these readers.
Security Patterns in Practice - Eduardo Fernandez-Buglioni 2013-06-25
Learn to combine security theory and code to produce secure systems Security is clearly a crucial issue to consider during the design and implementation of any distributed software architecture. Security patterns are increasingly being used by developers who take security into serious consideration from the creation of their work. Written by the authority on security patterns, this unique book examines the structure and purpose of security patterns, illustrating their use with the help of detailed implementation advice, numerous code samples, and descriptions in UML. Provides an extensive, up-to-date catalog of security patterns Shares real-world case studies so you can see when and how to use security patterns in practice Details how to incorporate security from the conceptual stage Highlights tips on authentication, authorization, role-based access control, firewalls, wireless networks, middleware, VoIP, web services security, and more Author is well known and highly respected in the field of security and an expert on security patterns Security Patterns in Practice shows you how to confidently develop a secure system step by step.
Cybersecurity: Engineering a Secure Information Technology Organization - Dan Shoemaker 2014-01-29
Software is essential and pervasive in the modern world, but software acquisition, development, operation, and maintenance can involve substantial risk, allowing attackers to compromise millions of computers every year. This groundbreaking book provides a uniquely comprehensive guide to software security, ranging far beyond secure coding to outline rigorous processes and practices for managing system and software lifecycle operations. The book opens with a comprehensive guide to the software lifecycle, covering all elements, activities, and practices encompassed by the universally accepted ISO/IEEE 12207-2008 standard. The authors then proceed document proven management architecture and process framework models for software assurance, such as ISO 21827 (SSE-CMM), CERT-RMM, the Software Assurance Maturity Model, and NIST 800-53. Within these models, the authors present standards and practices related to key activities such as threat and risk evaluation, assurance cases, and adversarial testing. Ideal for new and experienced cybersecurity professionals alike in both the public and private sectors, this one-of-a-kind book prepares readers to create and manage coherent, practical, cost-effective operations to ensure defect-free systems and software. Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version.
Designing Software Architectures - Humberto Cervantes 2016-04-29
Designing Software Architectures will teach you how to design any software architecture in a systematic, predictable, repeatable, and cost-effective way. This book introduces a practical methodology for architecture design that any professional software engineer can use, provides structured methods supported by reusable chunks of design knowledge, and includes rich case studies that demonstrate how to use the methods. Using realistic examples, you'll master the powerful new version of the proven Attribute-Driven Design (ADD) 3.0 method and will learn how to use it to address key drivers, including quality attributes, such as modifiability, usability, and availability, along with functional requirements and architectural concerns. Drawing on their extensive experience, Humberto Cervantes and Rick Kazman guide you through crafting practical designs that support the full software life cycle, from requirements to maintenance and evolution. You'll learn how to successfully integrate design in your organizational context, and how to design

systems that will be built with agile methods. Comprehensive coverage includes Understanding what architecture design involves, and where it fits in the full software development life cycle Mastering core design concepts, principles, and processes Understanding how to perform the steps of the ADD method Scaling design and analysis up or down, including design for pre-sale processes or lightweight architecture reviews Recognizing and optimizing critical relationships between analysis and design Utilizing proven, reusable design primitives and adapting them to specific problems and contexts Solving design problems in new domains, such as cloud, mobile, or big data

Secrets of a Cyber Security Architect - Brook S. E. Schoenfield 2019-12-06

Any organization with valuable data has been or will be attacked, probably successfully, at some point and with some damage. And, don't all digitally connected organizations have at least some data that can be considered "valuable"? Cyber security is a big, messy, multivariate, multidimensional arena. A reasonable "defense-in-depth" requires many technologies; smart, highly skilled people; and deep and broad analysis, all of which must come together into some sort of functioning whole, which is often termed a security architecture. Secrets of a Cyber Security Architect is about security architecture in practice. Expert security architects have dozens of tricks of their trade in their kips. In this book, author Brook S. E. Schoenfield shares his tips and tricks, as well as myriad tried and true bits of wisdom that his colleagues have shared with him. Creating and implementing a cyber security architecture can be hard, complex, and certainly frustrating work. This book is written to ease this pain and show how to express security requirements in ways that make the requirements more palatable and, thus, get them accomplished. It also explains how to surmount individual, team, and organizational resistance. The book covers: What security architecture is and the areas of expertise a security architect needs in practice The relationship between attack methods and the art of building cyber defenses Why to use attacks and how to derive a set of mitigations and defenses Approaches, tricks, and manipulations proven successful for practicing security architecture Starting, maturing, and running effective security architecture programs Secrets of the trade for the practicing security architecture Tricks to surmount typical problems Filled with practical insight, Secrets of a Cyber Security Architect is the desk reference every security architect needs to thwart the constant threats and dangers confronting every digitally connected organization.

Foundations and Practice of Security - Jean Luc Danger 2014-03-20

This book constitutes the carefully refereed post-proceedings of the 6th Symposium on Foundations and Practice of Security, FPS 2013, held in La Rochelle, France, in October 2013. The 25 revised full papers presented together with a keynote address were carefully reviewed and selected from 65 submissions. The papers are organized in topical sections on security protocols, formal methods, physical security, attack classification and assessment, access control, cipher attacks, ad-hoc and sensor networks, resilience and intrusion detection.

Empirical Research for Software Security - Lotfi ben Othmane 2017-11-28

Developing secure software requires the integration of numerous methods and tools into the development process, and software design is based on shared expert knowledge, claims, and opinions. Empirical methods, including data analytics, allow extracting knowledge and insights from the data that organizations collect from their processes and tools, and from the opinions of the experts who practice these processes and methods. This book introduces the reader to the fundamentals of empirical research methods, and demonstrates how these methods can be used to hone a secure software development lifecycle based on empirical data and published best practices.

Security Patterns - Markus Schumacher 2013-07-12

Most security books are targeted at security engineers and specialists. Few show how build security into software. None breakdown the different concerns facing security at different levels of the system: the enterprise, architectural and operational layers. Security Patterns addresses the full spectrum of security in systems design, using best practice solutions to show how to integrate security in the broader engineering process. Essential for designers building large-scale systems who want best practice solutions to typical security problems Real world case studies illustrate how to use the patterns in specific domains For more information visit www.securitypatterns.org

5th International Symposium on Data Mining Applications - Mamdouh Alenezi 2018-03-28

The 5th Symposium on Data Mining Applications (SDMA 2018) provides valuable opportunities for technical collaboration among data mining and machine learning researchers in Saudi Arabia, Gulf Cooperation Council (GCC) countries and the Middle East region. This book gathers the proceedings of the SDMA 2018. All papers were peer-reviewed based on a strict policy concerning the originality, significance to the area, scientific vigor and quality of the contribution, and address the following research areas.• Applications: Applications of data mining in domains including databases, social networks, web, bioinformatics, finance, healthcare, and security.• Algorithms: Data mining and machine learning foundations, algorithms, models, and theory.• Text Mining: Semantic analysis and mining text in Arabic, semi-structured, streaming, multimedia data.• Framework: Data mining frameworks, platforms and systems implementation.• Visualizations: Data visualization and modeling.