Introduction To Reliable And Secure Distributed P

The perimeter defenses guarding your network perhaps are not as secure as you think. Hosts behind the firewall have no defenses of their own, so when a host in the "trusted" zone is breached, access to your data center is not far behind. That’s an all-too-familiar scenario today. With this practical book, you’ll learn the principles behind zero trust architecture, along with details necessary to implement it. The Zero Trust Model treats all hosts as if they’re internet-facing, and considers the entire network to be compromised and hostile. By taking this approach, you’ll focus on building strong authentication, authorization, and encryption throughout, while providing compartmentalized access and better operational agility. Understand how perimeter-based defenses have evolved to become the broken model we use today Explore two case studies of zero trust in production networks on the client side (Google) and on the server side (PagerDuty) Get example configuration for open source tools that you can use to build a zero trust network Learn how to migrate from a perimeter-based network to a zero trust network in production

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

The main goal of Internet of Things (IoT) is to make secure, reliable, and fully automated smart environments. However, there are many technological challenges in deploying IoT. This includes connectivity and networking, timeliness, power and energy consumption dependability, security and privacy, compatibility and longevity, and network/protocol standards. Internet of Things and Secure Smart Environments: Successes and Pitfalls provides a comprehensive overview of recent research and open problems in the area of IoT research. Features: Presents cutting edge topics and research in IoT Includes contributions from leading worldwide researchers Focuses on IoT architectures for smart environments Explores security, privacy, and trust Covers data handling and management (accumulation, abstraction, storage, processing, encryption, fast retrieval, security, and privacy) in IoT for smart environments This book covers state-of-the-art problems, presents solutions, and opens research directions for researchers and scholars in both industry and academia.

The First Expert Guide to Static Analysis for Software Security! Creating secure code requires more than just good intentions. Programmers need to know that their code will be safe in an almost infinite number of scenarios and configurations. Static source code analysis gives users the ability to review their work with a fine-toothed comb and uncover the kinds of errors that lead directly to security vulnerabilities. Now, there’s a complete guide to static analysis: how it works, how to integrate it into the software development processes, and how to make the most of it during security code review. Static analysis experts Brian Chess and Jacob West look at the most common types of security defects that occur today. They illustrate main points using Java and C code examples taken from real-world security incidents, showing how coding errors are exploited, how they could have been prevented, and how static analysis can rapidly uncover similar mistakes. This book is for everyone concerned with building more secure software: developers, security engineers, analysts, and testers.

Smart Energy Grid Engineering

Reliable, Secure and Resilient Logistics Networks

Handbook of Research on Blockchain Technology

Delivering Products in a Risky Environment

A Framework for Decision Makers

Best Practices for Designing, Implementing, and Maintaining Systems

Blockchain-Based Smart Grids presents emerging applications of blockchain in electrical system and looks to future developments in the use of blockchain technology in the energy market. Rapid growth of renewable energy resources in power systems and significant developments in the telecommunication systems has resulted in new market designs being employed to cover unpredictable and distributed generation of electricity. This book considers the marriage of blockchain and grid modernization, and discusses the transaction shifts in smart grids, from centralized to peer-to-peer structures. In addition, it addresses the effective application of these structures to speed up processes, resulting in more flexible electricity systems. Aimed at moving towards blockchain-based smart grids with renewable applications, this book is useful to researchers and practitioners in all sectors of smart grids, including renewable energy providers, manufacturers and professionals involved in electricity generation from renewable sources, grid modernization and smart grid applications.

Front Cover; Dedication; Embedded Systems Security: Practical Methods for Safe and Secure Softwareand Systems Development; Copyright; Contents; Foreword; Preface; About this

Book; Audience; Organization; Approach; Acknowledgements; Chapter 1 -- Introduction to Embedded Systems Security; 1.1What is Security?; 1.2What is an Embedded System?; 1.3Embedded Security Trends; 1.4Security Policies; 1.5Security Threats; 1.6Wrap-up; 1.7Key Points; 1.8 Bibliography and Notes; Chapter 2 -- Systems Software Considerations; 2.1The Role of the Operating System; 2.2Multiple Independent Levels of Security.

This book serves as a security practitioner ' s guide to today ' s most crucial issues in cyber security and IT infrastructure. It offers in-depth coverage of theory, technology, and practice as they relate to established technologies as well as recent advancements. It explores practical solutions to a wide range of cyber-physical and IT infrastructure protection issues. Composed of 11 chapters contributed by leading experts in their fields, this highly useful book covers disaster recovery, biometrics, homeland security, cyber warfare, cyber security, national infrastructure security, access controls, vulnerability assessments and audits, cryptography, and operational and organizational security, as well as an extensive glossary of security terms and acronyms. Written with instructors and students in mind, this book includes methods of analysis and problem-solving techniques through hands-on exercises and worked examples as well as questions and answers and the ability to implement practical solutions through real-life case studies. For example, the new format includes the following pedagogical elements: • Checklists throughout each chapter to gauge understanding • Chapter Review Questions/Exercises and Case Studies • Ancillaries: Solutions Manual; slide package; figure files This format will be attractive to universities and career schools as well as federal and state agencies, corporate security training programs, ASIS certification, etc. Chapters by leaders in the field on theory and practice of cyber security and IT infrastructure protection, allowing the reader to develop a new level of technical expertise Comprehensive and up-to-date coverage of cyber security issues allows the reader to remain current and fully informed from multiple viewpoints Presents methods of analysis and problem-solving techniques, enhancing the reader's grasp of the material and ability to implement practical solutions

When you first hear the term Information Assurance you tend to conjure up an image of a balanced set of reasonable measures that have been taken to protect the information after an assessment has been made of risks that are posed to it. In truth this is the Holy Grail that all organisations that value their information should strive to achieve, but which few even understand. Information Assurance is a term that has recently come into common use. When talking with old timers in IT (or at least those that are over 35 years old), you will hear them talking about information security, a term that has survived since the birth of the computer. In the more recent past, the term Information Warfare was coined to describe the measures that need to be taken to defend and attack information. This term, however, has military connotations - after all, warfare is normally their domain. Shortly after the term came into regular use, it was applied to a variety of situations encapsulated by Winn Schwartau as the three classes of Information Warfare: Class 1- Personal Information Warfare. Class 2 - Corporate Information Warfare. Class 3 - Global Information Warfare. Political sensitivities lead to "warfare" being replaced by "operations", a much more "politically correct" word. Unfortunately, "operations" also has an offensive connotation and is still the terminology of the military and governments.

Building Secure and Reliable Systems

Decrypting the Encryption Debate

Building Secure and Reliable Network Applications

Challenges and Solutions in Smart Environments

Database Reliability Engineering

Distributed Algorithms

How prepared are you to build fast and efficient web applications? This eloquent book provides what every web developer should know about the network, from fundamental limitations that affect performance to major innovations for building even more powerful browser applications—including HTTP 2.0 and XHR improvements, Server-Sent Events (SSE), WebSocket, and WebRTC. Author Ilya Grigorik, a web performance engineer at Google, demonstrates performance optimization best practices for TCP, UDP, and TLS protocols, and explains unique wireless and mobile network optimization requirements. You'll then dive into performance characteristics of technologies such as HTTP 2.0, client-side network scripting with XHR, real-time streaming with SSE and WebSocket, and P2P communication with WebRTC. Deliver superlative TCP, UDP, and TLS performance Speed up network performance over 3G/4G mobile networks Develop fast and energy-efficient mobile applications Address bottlenecks in HTTP 1.x and other browser protocols Plan for and deliver the best HTTP 2.0 performance Enable efficient real-time streaming in the browser Create efficient peer-to-peer videoconferencing and low-latency applications with real-time WebRTC transports

Practical methods for analysing mechanical designs with respect to their capability and reliability are combined in this volume. The book is written with postgraduate students and professional engineers in mind.

In modern computing a program is usually distributed among several processes. The fundamental challenge when developing reliable and secure distributed programs is to support the cooperation of processes required to execute a common task, even when some of these processes fail. Failures may range from crashes to adversarial attacks by malicious processes. Cachin, Guerraoui, and Rodrigues present an introductory description of fundamental distributed programming abstractions together with algorithms to implement them in distributed systems, where processes are subject to crashes and malicious attacks. The authors follow an incremental approach by first introducing basic abstractions in simple distributed environments, before moving to more sophisticated abstractions and more challenging environments. Each core chapter is devoted to one topic, covering reliable broadcast, shared memory, consensus, and extensions of consensus. For every topic, many exercises and their solutions enhance the understanding This book represents the second edition of "Introduction to Reliable Distributed Programming". Its scope has been extended to include security against *malicious actions by non-cooperating processes. This important domain has become widely known under the name "Byzantine fault-tolerance".*

This is the book for Gophers who want to learn how to build distributed systems. You know the basics of Go and are eager to put your knowledge to work. Build distributed services that are highly available, resilient, and scalable. This book is just what you need to apply Go to real-world situations. Level up your engineering skills today. Take your Go skills to the next level by learning how to design, develop, and deploy a distributed service. Start from the bare essentials of storage handling, then work your way through networking a client and server, and finally to distributing server instances, deployment, and testing. All this will make coding in your day job or side projects easier, faster, and more fun. Create your own distributed services and contribute to open source projects. Build networked, secure clients and servers with gRPC. Gain insights into your systems and debug issues with observable services instrumented with metrics, logs, and traces. Operate your own Certificate Authority to authenticate internal web services with TLS. Automatically handle when nodes are added or removed to your cluster with service discovery. Coordinate distributed systems with replicated state machines powered by the Raft consensus algorithm. Lay out your applications and libraries to be modular and easy to maintain. Write CLIs to configure and run your applications. Run your distributed system locally and deploy to the cloud with Kubernetes. Test and benchmark your applications to ensure they're correct and fast. Dive into writing Go and join the hundreds of thousands who are using it to build software for the real world. What You Need: Go 1.13+ and Kubernetes 1.16+

Designing Distributed Systems

Secure Programming with Static Analysis

Site Reliability Engineering

Smart, Secure, Green and Reliable

A Hands-On Guide to Reliable Security Audits

Designing Data-Intensive Applications

Smart Energy Grid Engineering provides in-depth detail on the various important engineering challenges of smart energy grid design and operation by focusing on advanced methods and practices for designing different components and their integration within the grid. Governments around the world are investing heavily in smart energy grids to ensure optimum energy use and supply, enable better planning for outage responses and recovery, and facilitate the integration of heterogeneous technologies such as renewable energy systems, electrical vehicle networks, and smart homes arour the grid. By looking at case studies and best practices that illustrate how to implement smart energy grid infrastructures and analyze the technical details involved in tackling emerging challenges, this valuable reference considers the important engineering aspects of design and implementation, energy generation, utilization and energy conservation, intelligent control and monitoring data analysis security, and asset integrity. Includes detailed support to integrate systems for smart grid infrastructures Features global case studies outlining design components and their integration within the grid Provides examples and best practices from industry that will assist in the migration to smart grids

Principles of Computer System Design is the first textbook to take a principles-based approach to the computer system design. It identifies, examines, and illustrates fundamental concepts in computer system design that are common across operating systems, networks, database systems, distributed systems, programming languages, software engineering, security, fault tolerance, and architecture. Through carefully analyzed case studies from each of these disciplines, it demonstrates how to apply these concepts to tackle practical system design problems. To support the focus on design, the text identifies and explains abstractions that have proven successful in practice such as remote procedure call, client/service organization, file systems, data integrity, consistency, and authenticated messages. Most computer systems are built using a handful of such abstractions. The text describes how these abstractions are implemented, demonstrates how they are used in different systems, and prepares the reader to apply them in future designs. The book is recommended for junior and senior undergraduate students in Operating Systems, Distributed Systems, Distributed Operating Systems and/or Computer Systems Design courses; and professional computer systems designers. Features: Concepts of computer system design guided by fundamental principles. Cross-cutting approach that identifies abstractions common to networking, operating systems, transaction systems, distributed systems, architecture, and software engineering. Case studies that make the abstractions real: naming (DNS and the URL); file systems (the UNIX file system); clients and services (NFS); virtualization (virtual machines); scheduling (disk arms); security (TLS). Numerous pseudocode fragments that provide concrete examples of abstract concepts. Extensive support. The authors and MIT OpenCourseWare provide on-line, free of charge, open educational resources, including additional chapters, course syllabi, board layouts and slides, lecture videos, and an archive of lecture schedules, class assignments, and design projects.

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

Dependence on computers has had a transformative effect on human society. Cybernetics is now woven into the core functions of virtually every basic institution, including our oldest ones. War is one such institution, and the digital revolution's impact on it has been profound. The American military, which has no peer, is almost completely reliant on high-tech computer systems. Given the Internet's potential for full-spectrum surveillance and information disruption, the marshaling of computer networks represents the next stage of cyberwar. Indeed, it is upon us already. The recent Stuxnet episode, in which Israel fed a malignant computer virus into Iran's nuclear facilities, is one such example. Penetration into US government computer systems by Chinese hackers-presumably sponsored by the Chinese government-is another. Together, they point to a new era in the evolution of human conflict. In Cybersecurity and Cyerbwar: What Everyone Needs to Know, noted experts Peter W. Singer and Allan Friedman lay out how the revolution in military cybernetics occurred and explain where it is headed. They begin with an explanation of what cyberspace is before moving on to discussions of how it can be exploited and why it is so hard to defend. Throughout, they discuss the latest developments in military and security technology. Singer and Friedman close with a discussion of how people and governments can protect themselves. In sum, Cybersecurity and Cyerbwar is the definitive account on the subject for the educated general reader who wants to know more about the nature of war, conflict, and security in the twenty-first century.

Lattices Applied to Coding for Reliable and Secure Communications

Reliable Distributed Systems

Cyber Security and IT Infrastructure Protection

Internet of Things and Secure Smart Environments

Building Secure Systems in Untrusted Networks

Technologies, Web Services, and Applications

Explains fault tolerance in clear terms, with concrete examples drawn from real-world settings Highly practical focus aimed at building "mission-critical" networked applications that remain secure

Handbook of Research on Blockchain Technology presents the latest information on the adaptation and implementation of Blockchain technologies in real world business, scientific, healthcare and biomedical applications. The book's editors present the rapid advancements in existing business models by applying Blockchain techniques. Novel architectural solutions in the deployment of Blockchain comprise the core aspects of this book. Several use cases with IoT, biomedical engineering, and smart cities are also incorporated. As Blockchain is a relatively new technology that exploits decentralized networks and is used in many sectors for reliable, cost-effective and rapid business transactions, this book is a welcomed addition on existing knowledge. Financial services, retail, insurance, logistics, supply chain, public sectors and biomedical industries are now investing in Blockchain research and technologies for their business growth. Blockchain prevents double spending in financial transactions without the need of a trusted authority or central server. It is a decentralized ledger platform that facilitates verifiable transactions between parties in a secure and smart way. Presents the evolution of blockchain, from fundamental theories, to present forms Explains the concepts of blockchain related to cloud/edge computing, smart healthcare, smart cities and Internet of Things (IoT) Provides complete coverage of the various tools, platforms and techniques used in blockchain Explores smart contract tools and consensus algorithms Covers a variety of applications with real world case studies in areas such as biomedical engineering, supply chain management, and tracking of goods and delivery

The perfect introduction to pen testing for all IT professionals and students · Clearly explains key concepts, terminology, challenges, tools, and skills · Covers the latest penetration testing standards from NSA, PCI, and NIST Welcome to today’s most useful and practical introduction to penetration testing. Chuck Easttom brings together up-to-the-minute coverage of all the concepts, terminology, challenges, and skills you’ll need to be effective. Drawing on decades of experience in cybersecurity and related IT fields, Easttom integrates theory and practice, covering the entire penetration testing life cycle from planning to reporting. You’ll gain practical experience through a start-to-finish sample project relying on free open source tools.

Throughout, quizzes, projects, and review sections deepen your understanding and help you apply what you’ve learned. Including essential pen testing standards from NSA, PCI, and NIST, Penetration Testing Fundamentals will help you protect your assets–and expand your career options. LEARN HOW TO · Understand what pen testing is and how it’s used · Meet modern standards for comprehensive and effective testing · Review cryptography essentials every pen tester must know · Perform reconnaissance with Nmap, Google searches, and ShodanHq · Use malware as part of your pen testing toolkit · Test for vulnerabilities in Windows shares, scripts, WMI, and the Registry · Pen test websites and web communication · Recognize SQL injection and cross-site scripting attacks · Scan for vulnerabilities with OWASP ZAP, Vega, Nessus, and MBSA · Identify Linux vulnerabilities and password cracks · Use Kali Linux for advanced pen testing · Apply general hacking technique ssuch as fake Wi-Fi hotspots and social engineering · Systematically test your environment with Metasploit · Write or customize sophisticated Metasploit exploits

In the race to compete in today’s fast-moving markets, large enterprises are busy adopting new technologies for creating new products, processes, and business models. But one obstacle on the road to digital transformation is placing too much emphasis on technology, and not enough on the types of processes technology enables. What if different lines of business could build their own services and applications—and decision-making was distributed rather than centralized? This report explores the concept of a digital business platform as a way of empowering individual business sectors to act on data in real time. Much innovation in a digital enterprise will increasingly happen at the edge, whether it involves business users (from marketers to data scientists) or IoT devices. To facilitate the process, your core IT team can provide these sectors with the digital tools they need to innovate quickly. This report explores: Key cultural and organizational changes for developing business capabilities through cross-functional product teams A platform for integrating applications, data sources, business partners, clients, mobile apps, social networks, and IoT devices Creating internal API programs for building innovative edge services in low-code or no-code environments Tools including Integration Platform as a Service, Application Platform as a Service, and Integration Software as a Service The challenge of integrating microservices and serverless architectures Event-driven architectures for processing and reacting to events in real time You’ll also learn about a complete pervasive integration solution as a core component of a digital business platform to serve every audience in your organization.

Blockchain-Based Smart Grids

Building a Secure Computer System

The Power Grid

SSH, The Secure Shell

Introduction to Reliable Distributed Programming

An Introduction to Predictive Maintenance

In Distributed Algorithms, Nancy Lynch provides a blueprint for designing, implementing, and analyzing distributed algorithms. She directs her book at a wide audience, including students, programmer system designers, and researchers. Distributed Algorithms contains the most significant algorithms and impossibility results in the area, all in a simple automata-theoretic setting. The algorithms are pro correct, and their complexity is analyzed according to precisely defined complexity measures. The problems covered include resource allocation, communication, consensus among distributed process consistency, deadlock detection, leader election, global snapshots, and many others. The material is organized according to the system model—first by the timing model and then by the interprocess communication mechanism. The material on system models is isolated in separate chapters for easy reference. The presentation is completely rigorous, yet is intuitive enough for immediate comprehe book familiarizes readers with important problems, algorithms, and impossibility results in the area: readers can then recognize the problems when they arise in practice, apply the algorithms to solve th use the impossibility results to determine whether problems are unsolvable. The book also provides readers with the basic mathematical tools for designing new algorithms and proving new impossibilit In addition, it teaches readers how to reason carefully about distributed algorithms—to model them formally, devise precise specifications for their required behavior, prove their correctness, and evalua performance with realistic measures.

Smart Cities Cybersecurity and Privacy examines the latest research developments and their outcomes for safe, secure, and trusting smart cities residents. Smart cities improve the quality of life of citi their energy and water usage, healthcare, environmental impact, transportation needs, and many other critical city services. Recent advances in hardware and software, have fueled the rapid growth a deployment of ubiquitous connectivity between a city’s physical and cyber components. This connectivity however also opens up many security vulnerabilities that must be mitigated. Smart Cities Cybe and Privacy helps researchers, engineers, and city planners develop adaptive, robust, scalable, and reliable security and privacy smart city applications that can mitigate the negative implications asso with cyber-attacks and potential privacy invasion. It provides insights into networking and security architectures, designs, and models for the secure operation of smart city applications. Consolidates in place state-of-the-art academic and industry research Provides a holistic and systematic framework for design, evaluating, and deploying the latest security solutions for smart cities Improves understa collaboration among all smart city stakeholders to develop more secure smart city architectures

This second edition of An Introduction to Predictive Maintenance helps plant, process, maintenance and reliability managers and engineers to develop and implement a comprehensive maintenance m program, providing proven strategies for regularly monitoring critical process equipment and systems, predicting machine failures, and scheduling maintenance accordingly. Since the publication of the edition in 1990, there have been many changes in both technology and methodology, including financial implications, the role of a maintenance organization, predictive maintenance techniques, variou analyses, and maintenance of the program itself. This revision includes a complete update of the applicable chapters from the first edition as well as six additional chapters outlining the most recent info available. Having already been implemented and maintained successfully in hundreds of manufacturing and process plants worldwide, the practices detailed in this second edition of An Introduction to Predictive Maintenance will save plants and corporations, as well as U.S. industry as a whole, billions of dollars by minimizing unexpected equipment failures and its resultant high maintenance cost wh increasing productivity. A comprehensive introduction to a system of monitoring critical industrial equipment Optimize the availability of process machinery and greatly reduce the cost of maintenance P the means to improve product quality, productivity and profitability of manufacturing and production plants

Since the first edition of Security and Loss Prevention was published in 1983, much has changed in security and loss prevention considerations. In the past five years alone, security awareness and th added business continuity and preparedness considerations has been uniquely highlighted given events such as Katrina, 9/11, the formation of the Department of Homeland Security, and the increase terrorist events. This edition of Security and Loss Prevention is fully updated and encompasses the breadth and depth of considerations involved in implementing general loss prevention concepts and programs within an organization. The book provides proven strategies to prevent and reduce incidents of loss due to legal issues, theft and other crimes, fire, accidental or intentional harm from employ well as the many ramifications of corporate mismanagement. The new edition contains a brand new terrorism chapter, along with coverage on background investigations, protection of sensitive informa internal threats, and considerations at select facilities (nuclear, DoD, government and federal). Author Philip Purpura once again demonstrates why students and professionals alike rely on this best-se as a timely, reliable resource. - Covers the latest professional security issues surrounding Homeland Security and risks presented by threats of terrorism - Recommended reading for ASIS Internationa prestigious CPP Certification - Cases provide real-world applications

The Big Ideas Behind Reliable, Scalable, and Maintainable Systems

Introduction to Reliable and Secure Distributed Programming

Security and Loss Prevention

Cybersecurity

AI Techniques for Reliability Prediction for Electronic Components

Practical Methods for Safe and Secure Software and Systems Development

The Power Grid: Smart, Secure, Green and Reliable offers a diverse look at the traditional engineering and physics aspects of power systems, also examining the issues affecting clean power generation, power distribution, and the new security issues that could potentially affect the availability and reliability of the grid. The book looks at growth in new loads that are consuming over 1% of all the electrical power produced, and how combining those load issues of getting power to the regions experiencing growth in energy demand can be addressed. In addition, it considers the policy issues surrounding transmission line approval by regulators. With truly multidisciplinary content, including failure analysis of various systems, photovoltaic, wind power, quality issues with clean power, high-voltage DC transmission, electromagnetic radiation, electromagnetic interference, privacy concerns, and data security, this reference is relevant to anyone interested in the broad area of power grid stability. Discusses state–of-the-art trends and issues in power grid reliability Offers guidance on purchasing or investing in new technologies Includes a technical document relevant to public policy that can help all stakeholders understand the technical issues facing a green, secure power grid

This book describes the essential components of the SCION secure Internet architecture, the first architecture designed foremost for strong security and high availability. Among its core features, SCION also provides route control, explicit trust information, multipath communication, scalable quality-of-service guarantees, and efficient forwarding. The book includes functional specifications of the network elements, communication protocols among these elements, data structures, and configuration files. In particular, the book offers a specification of a working prototype. The authors provide a comprehensive description of the main design features for achieving a secure Internet architecture. They facilitate the reader throughout, structuring the book so that the technical detail gradually increases, and supporting the text with a glossary, an index, a list of abbreviations, answers to frequently asked questions, and special highlighting for examples and for sections that explain important research, engineering, and deployment features. The book is suitable for researchers, practitioners, and graduate students who are interested in network security.

In modern computing a program is usually distributed among several processes. The fundamental challenge when developing reliable distributed programs is to support the cooperation of processes required to execute a common task, even when some of these processes fail. Guerraoui and Rodrigues present an introductory description of fundamental reliable distributed programming abstractions as well as algorithms to implement these abstractions. The authors follow an incremental approach by first introducing basic abstractions in simple distributed environments, before moving to more sophisticated abstractions and more challenging environments. Each core chapter is devoted to one specific class of abstractions, covering reliable delivery, shared memory, consensus and various forms of agreement. This textbook comes with a companion set of running examples implemented in Java. These can be used by students to get a better understanding of how reliable distributed programming abstractions can be implemented and used in practice. Combined, the chapters deliver a full course on reliable distributed programming. The book can also be used as a complete reference on the basic elements required to build reliable distributed applications.

Little prior knowledge is needed to use this long-needed reference. Computer professionals and software engineers will learn how to design secure operating systems, networks and applications.

Successes and Pitfalls

Zero Trust Networks

Distributed Services with Go

Surviving in the Information Environment

What every web developer should know about networking and web performance

Information Assurance

Are you serious about network security? Then check out SSH, the Secure Shell, which provides key-based authentication and transparent encryption for your network connections. It's reliable, robust, and reasonably easy to use, and both free and commercial implementations are widely available for most operating systems. While it doesn't solve every privacy and security problem, SSH eliminates several of them very effectively. Everything you want to know about SSH is in our second edition of SSH, The Secure Shell: The Definitive Guide. This updated book thoroughly covers the latest SSH-2 protocol for system administrators and end users interested in using this increasingly popular TCP/IP-based solution. How does it work? Whenever data is sent to the network, SSH automatically encrypts it. When data reaches its intended recipient, SSH decrypts it. The result is "transparent" encryption-users can work normally, unaware that their communications are already encrypted. SSH supports secure file transfer between computers, secure remote logins, and a unique "tunneling" capability that adds encryption to otherwise insecure network applications. With SSH, users can freely navigate the Internet, and system administrators can secure their networks or perform remote administration. Written for a wide, technical audience, SSH, The Secure Shell: The Definitive Guide covers several implementations of SSH for different operating systems and computing environments. Whether you're an individual running Linux machines at home, a corporate network administrator with thousands of users, or a PC/Mac owner who just wants a secure way to telnet or transfer files between machines, our indispensable guide has you covered. It starts with simple installation and use of SSH, and works its way to in-depth case studies on large, sensitive computer networks. No matter where or how you're shipping information, SSH, The Secure Shell: The Definitive Guide will show you how to do it securely.

This book synthesizes the current state of knowledge on logistics infrastructures and process modeling, especially for processes that are exposed to changing and uncertain environments. It then builds on this knowledge to present a new concept of dependable product delivery assurance. In order to quantitatively assess dependability, a service continuity oriented approach as well as an imperfect knowledge based concept of risk are employed. This approach is based on the methodology of service engineering and is closely related to the idea of the resilient enterprise, as well as the concept of disruption-tolerant operation. The practical advantages of this concept are subsequently illustrated in three sample applications: a modified FMECA method, an expert system with fuzzy reasoning, and a simulation agent-based model of logistic network resilience. The book will benefit a broad readership, including: researchers, especially in systems science, management science and operations research; professionals, especially managers; project managers and analysts; and undergraduate, postgraduate and MBA students in engineering.

This book provides a concise overview of the current state of the art in cybersecurity and shares novel and exciting ideas and techniques, along with specific cases demonstrating their practical application. It gathers contributions by both academic and industrial researchers, covering all aspects of cybersecurity and addressing issues in secure information systems as well as other emerging areas. The content comprises high-quality research articles and reviews that promote a multidisciplinary approach and reflect the latest advances, challenges, requirements and methodologies. Thus, the book investigates e.g. security vulnerabilities, cybercrime, and privacy issues related to big data analysis, as well as advances in digital forensics, secure smart city services, and risk mitigation strategies for devices employing cyber-physical systems. Given its scope, the book offers a valuable resource for students, researchers, IT professionals and providers, citizens, consumers and policymakers involved or interested in the modern security procedures needed to protect our information and communication resources. Its goal is to foster a community committed to further research and education, and one that can also translate its findings into concrete practices.

Data is at the center of many challenges in system design today. Difficult issues need to be figured out, such as scalability, consistency, reliability, efficiency, and maintainability. In addition, we have an overwhelming variety of tools, including relational databases, NoSQL datastores, stream or batch processors, and message brokers. What are the right choices for your application? How do you make sense of all these buzzwords? In this practical and comprehensive guide, author Martin Kleppmann helps you navigate this diverse landscape by examining the pros and cons of various technologies for processing and storing data. Software keeps changing, but the fundamental principles remain the same. With this book, software engineers and architects will learn how to apply those ideas in practice, and how to make full use of data in modern applications. Peer under the hood of the systems you already use, and learn how to use and operate them more effectively Make informed decisions by identifying the strengths and weaknesses of different tools Navigate the trade-offs around consistency, scalability, fault tolerance, and complexity Understand the distributed systems research upon which modern databases are built Peek behind the scenes of major online services, and learn from their architectures

The Definitive Guide

Embedded Systems Security

Smart Cities Cybersecurity and Privacy

Designing and Operating Resilient Database Systems

Patterns and Paradigms for Scalable, Reliable Services

What Everyone Needs to Know

The infrastructure-as-code revolution in IT is also affecting database administration. With this practical book, developers, system administrators, and junior to mid-level DBAs will learn ho the modern practice of site reliability engineering applies to the craft of database architecture and operations. Authors Laine Campbell and Charity Majors provide a framework for professionals looking to join the ranks of today’s database reliability engineers (DBRE). You’ll begin by exploring core operational concepts that DBREs need to master. Then you’ll examine a wide range of database persistence options, including how to implement key technologies to provide resilient, scalable, and performant data storage and retrieval. With a firm foundation in database reliability engineering, you’ll be ready to dive into the architecture and operations of any modern database. This book covers: Service-level requirements and risk management Building and evolving an architecture for operational visibility Infrastructure engineering and infrastructure management How to facilitate the release management process Data storage, indexing, and replication Identifying datastore characteristics and best use cases Datastore architectural components and data-driven architectures

The development of “intelligent” systems that can take decisions and perform autonomously might lead to faster and more consistent decisions. A limiting factor for a broader adoption of technology is the inherent risks that come with giving up human control and oversight to “intelligent” machines. For sensitive tasks involving critical infrastructures and affecting human well-being or health, it is crucial to limit the possibility of improper, non-robust and unsafe decisions and actions. Before deploying an AI system, we see a strong need to validate its beha and thus establish guarantees that it will continue to perform as expected when deployed in a real-world environment. In pursuit of that objective, ways for humans to verify the agreemen between the AI decision structure and their own ground-truth knowledge have been explored. Explainable AI (XAI) has developed as a subfield of AI, focused on exposing complex AI mo to humans in a systematic and interpretable manner. The 22 chapters included in this book provide a timely snapshot of algorithms, theory, and applications of interpretable and explaina AI and AI techniques that have been proposed recently reflecting the current discourse in this field and providing directions of future development. The book is organized in six parts: towa AI transparency; methods for interpreting AI systems; explaining the decisions of AI systems; evaluating interpretability and explanations; applications of explainable AI; and software for explainable AI.

Encryption protects information stored on smartphones, laptops, and other devices - in some cases by default. Encrypted communications are provided by widely used computing devices services - such as smartphones, laptops, and messaging applications - that are used by hundreds of millions of users. Individuals, organizations, and governments rely on encryption to counter threats from a wide range of actors, including unsophisticated and sophisticated criminals, foreign intelligence agencies, and repressive governments. Encryption on its own does solve the challenge of providing effective security for data and systems, but it is an important tool. At the same time, encryption is relied on by criminals to avoid investigation and prosecu including criminals who may unknowingly benefit from default settings as well as those who deliberately use encryption. Thus, encryption complicates law enforcement and intelligence investigations. When communications are encrypted "end-to-end," intercepted messages cannot be understood. When a smartphone is locked and encrypted, the contents cannot be rea phone is seized by investigators. Decrypting the Encryption Debate reviews how encryption is used, including its applications to cybersecurity; its role in protecting privacy and civil liberti the needs of law enforcement and the intelligence community for information; technical and policy options for accessing plaintext; and the international landscape. This book describes th context in which decisions about providing authorized government agencies access to the plaintext version of encrypted information would be made and identifies and characterizes poss mechanisms and alternative means of obtaining information.

This book provides a first course on lattices – mathematical objects pertaining to the realm of discrete geometry, which are of interest to mathematicians for their structure and, at the sam time, are used by electrical and computer engineers working on coding theory and cryptography. The book presents both fundamental concepts and a wealth of applications, including co and transmission over Gaussian channels, techniques for obtaining lattices from finite prime fields and quadratic fields, constructions of spherical codes, and hard lattice problems used in cryptography. The topics selected are covered in a level of detail not usually found in reference books. As the range of applications of lattices continues to grow, this work will appeal to mathematicians, electrical and computer engineers, and graduate or advanced undergraduate in these fields.

An Introduction

Cybersecurity and Secure Information Systems

High Performance Browser Networking

Introduction to Computer Networks and Cybersecurity

Designing Capable and Reliable Products

How Google Runs Production Systems

In the industry of manufacturing and design, one major constraint has been enhancing operating performance using less time. As technology continues to advance, manufacturers are looking for better methods in predicting the condition and residual lifetime of electronic devices in order to save repair costs and their reputation. Intelligent systems are a solution for predicting the reliability of these components; however, there is a lack of research on the advancements of this smart technology within the manufacturing industry. AI Techniques for Reliability Prediction for Electronic Components provides emerging research exploring the theoretical and practical aspects of prediction methods using artificial intelligence and machine learning in the manufacturing field. Featuring coverage on a broad range of topics such as data collection, fault tolerance, and health prognostics, this book is ideally designed for reliability engineers, electronic engineers, researchers, scientists, students, and faculty members seeking current research on the advancement of reliability analysis using AI.

If a network is not secure, how valuable is it? Introduction to Computer Networks and Cybersecurity takes an integrated approach to networking and cybersecurity, highlighting the interconnections so that you quickly understand the complex design issues in modern networks. This full-color book uses a wealth of examples and illustrations to effective

SCION: A Secure Internet Architecture

Explainable AI: Interpreting, Explaining and Visualizing Deep Learning

Penetration Testing Fundamentals

Principles of Computer System Design