This book constitutes the refereed proceedings of the Workshops and Symposiums of the 15th International Conference on Algorithms and Architectures for Parallel Processing, ICA3PP 2015, held in Zhangjiajie, China, in November 2015. The program of this year consists of 6 symposiums/workshops that cover a wide range of research topics on parallel processing technology: the Sixth International Workshop on Trust, Security and Privacy for Big Data, TrustData 2015; the Fifth International Symposium on Trust, Security and Privacy for Emerging Applications, TSP 2015; the Third International Workshop on Network Optimization and Performance Evaluation, NOPE 2015; the Second International Symposium on Sensor-Cloud Systems, SCS 2015; the Second International Workshop on Security and Privacy Protection in Computer and Network Systems, SPPCN 2015; and the First International Symposium on Dependability in Sensor, Cloud, and Big Data Systems and Applications, DependSys 2015. The aim of these symposiums/workshops is to provide a forum to bring together practitioners and researchers from academia and industry for discussion and presentations on the current research and future directions related to parallel processing technology. The themes and topics of these symposiums/workshops are a valuable complement to the overall scope of ICA3PP 2015 and give additional values and interests.

Cloud computing has experienced explosive growth and is expected to continue to rise in popularity as new services and applications become available. As with any new technology, security issues continue to be a concern, and developing effective methods to protect sensitive information and data on the cloud is imperative. Cloud Security: Concepts, Methodologies, Tools, and Applications explores the difficulties and challenges of securing user data and information on cloud platforms. It also examines the current approaches to cloud-based technologies and assesses the possibilities for future advancements in this field. Highlighting a range of topics such as cloud forensics, information privacy, and standardization and security in the cloud, this
The objective of this edited book is to gather best practices in the development and management of mobile apps projects. Mobile Apps Engineering aims to provide software engineering lecturers, students and researchers of mobile computing a starting point for developing successful mobile apps. To achieve these objectives, the book’s contributors emphasize the essential concepts of the field, such as apps design, testing and security, with the intention of offering a compact, self-contained book which shall stimulate further research interest in the topic. The editors hope and believe that their efforts in bringing this book together can make mobile apps engineering an independent discipline inspired by traditional software engineering, but taking into account the new challenges posed by mobile computing.
Some copies of CompTIA Security+ Study Guide: Exam SY0-501 (9781119416876) were printed without discount exam vouchers in the front of the books. If you did not receive a discount exam voucher with your book, please visit http://media.wiley.com/product_ancillary/5X/111941688/COMP/CompTIA_Coupon.pdf to download one. Expert preparation covering 100% of Security+ exam SY0-501 objectives CompTIA Security+ Study Guide, Seventh Edition offers invaluable preparation for Exam SY0-501. Written by an expert author team, this book covers 100% of the exam objectives with clear, concise explanation. You’ll learn how to handle threats, attacks, and vulnerabilities using industry-standard tools and technologies, while understanding the role of architecture and design. From everyday tasks like identity and access management to complex topics like risk management and cryptography, this study guide helps you consolidate your knowledge base in preparation for the Security+ exam. Practical examples illustrate how these processes play out in real-world scenarios, allowing you to immediately translate essential concepts to on-the-job application. You also gain access to the Sybex online learning environment, which features a robust toolkit for more thorough prep: flashcards, glossary of key terms, practice questions, and a pre-assessment exam equip you with everything you need to enter the exam confident in your skill set. This study guide is approved and endorsed by CompTIA, and has been fully updated to align with the latest version of the exam. Master essential security technologies, tools, and tasks Understand how Security+ concepts are applied in the real world Study on the go with electronic flashcards and more Test your knowledge along the way with hundreds of practice questions To an employer, the CompTIA Security+ certification proves that you have the knowledge base and skill set to secure applications, devices, and networks; analyze and respond to threats; participate in risk mitigation, and so much more. As data threats loom larger every day, the demand for qualified security professionals will only continue to grow. If you’re ready to take the first step toward a rewarding career, CompTIA Security+ Study Guide, Seventh Edition is the ideal companion for thorough exam preparation.
Read Book Securing Application Deployment With Obfuscation And Code Signing How To Create 3 Layers Of Protection For Net Release Build Application Security Series

This book presents a collection of diverse perspectives on cloud computing and its vital role in all components of organizations, improving the understanding of cloud computing and tackling related concerns such as change management, security, processing approaches, and much more. –Provided by publisher.

This book constitutes the refereed proceedings of the 26th IFIP WG 11.3 International Conference on Data and Applications Security and Privacy, DBSec 2012, held in Paris, France in July 2012. The 17 revised full and 15 short papers presented together with 1 invited paper were carefully reviewed and selected from 49 submissions. The papers are organized in topical sections on access control, confidentiality and privacy, smart cards security, privacy-preserving technologies, data management, intrusion and malware, probabilistic attacks and protection, and cloud computing.

This book gives thorough, scholarly coverage of an area of growing importance in computer security and is a ‘must have’ for every researcher, student, and practicing professional in software protection. –Mikhail Atallah, Distinguished Professor of Computer Science at Purdue University Theory, Techniques, and Tools for Fighting Software Piracy, Tampering, and Malicious Reverse Engineering The last decade has seen significant progress in the development of techniques for resisting software piracy and tampering. These techniques are indispensable for software developers seeking to protect vital intellectual property. Surreptitious Software is the first authoritative, comprehensive resource for researchers, developers, and students who want to understand these approaches, the level of security they afford, and the performance penalty they incur. Christian Collberg and Jasvir Nagra bring together techniques drawn from related areas of computer science, including cryptography, steganography, watermarking, software metrics, reverse engineering, and compiler optimization. Using extensive sample code, they show readers how to implement protection schemes ranging from code obfuscation and software fingerprinting to tamperproofing and birthmarking, and discuss the theoretical and practical limitations of these techniques. Coverage includes

Mastering techniques that both attackers and defenders use to analyze programs
Using code obfuscation to make software harder to analyze and understand
Fingerprinting software to identify its author and to trace software pirates
Tamperproofing software using guards that detect and respond to illegal modifications of code and data
Strengthening content protection through dynamic watermarking and dynamic obfuscation
Detecting code theft via software similarity analysis and birthmarking algorithms
Using hardware techniques to defend software and media against piracy and tampering
Detecting software tampering in distributed system
Understanding the theoretical limits of code obfuscation

CompTIA Security+ SY0-501 Exam Cram, Fifth Edition, is the perfect study guide to help you pass CompTIA’s newly updated version of the Security+ exam. It provides coverage and practice questions for every exam topic. The book contains a set of 150 questions. The powerful Pearson Test Prep practice test software provides real-time practice and feedback with all the questions so you can simulate the exam. Covers the critical information you need to know to score higher on your Security+ exam! · Analyze indicators of compromise and determine types of attacks, threats, and risks to systems · Minimize the impact associated with types of attacks and vulnerabilities · Secure devices, communications, and network infrastructure · Effectively manage risks associated with a global business environment · Differentiate between control methods used to secure the physical domain · Identify solutions for the implementation of secure network architecture · Compare techniques for secure application development and deployment · Determine relevant identity and access management procedures · Implement security policies, plans, and procedures related to organizational security · Apply principles of cryptography and effectively deploy related solutions
Blockchain technologies, as an emerging distributed architecture and computing paradigm, have accelerated the development/application of the Cloud/GPU/Edge Computing, Artificial Intelligence, cyber physical systems, social networking, crowdsourcing and crowdsensing, 5G, trust management, and finance. The popularity and rapid development of Blockchain brings many technical and regulatory challenges for research and academic communities. This book will feature contributions from experts on topics related to performance, benchmarking, durability, robustness, as well data gathering and management, algorithms, analytics techniques for transactions processing, and implementation of applications.

This book presents a range of cloud computing security challenges and promising solution paths. The first two chapters focus on practical considerations of cloud computing. In Chapter 1, Chandramouli, Iorga, and Chokani describe the evolution of cloud computing and the current state of practice, followed by the challenges of cryptographic key management in the cloud. In Chapter 2, Chen and Sion present a dollar cost model of cloud computing and explore the economic viability of cloud computing with and without security mechanisms involving cryptographic mechanisms. The next two chapters address security issues of the cloud infrastructure. In Chapter 3, Szefer and Lee describe a hardware-enhanced security architecture that protects the confidentiality and integrity of a virtual machine’s memory from an untrusted or malicious hypervisor. In Chapter 4, Tsugawa et al. discuss the security issues introduced when Software-Defined Networking (SDN) is deployed within and across clouds. Chapters 5-9 focus on the protection of data stored in the cloud. In Chapter 5, Wang et al. present two storage isolation schemes that enable cloud users with high security requirements to verify that their disk storage is isolated from some or all other users, without any cooperation from cloud service providers. In Chapter 6, De Capitani di Vimercati, Foresti, and Samarati describe emerging approaches for protecting data stored externally and for enforcing fine-grained and selective accesses on them, and illustrate how the combination of these approaches can introduce new privacy risks. In Chapter 7, Le, Kant, and Jajodia explore data access challenges in collaborative enterprise computing environments where multiple parties formulate their own authorization rules, and discuss the problems of rule consistency, enforcement, and dynamic updates. In Chapter 8, Smith et al. address key challenges to the practical realization of a system that supports query execution over remote encrypted data without exposing decryption keys or plaintext at the server. In Chapter 9, Sun et al. provide an overview of secure search techniques over encrypted data, and then elaborate on a scheme that can achieve privacy-preserving multi-keyword text search. The next three chapters focus on the secure deployment of computations to the cloud. In Chapter 10, Oktay el al. present a risk-based approach for workload partitioning in hybrid clouds that selectively outsources data and computation based on their level of sensitivity. The chapter also describes a vulnerability assessment framework for cloud computing environments. In Chapter 11, Albanese et al. present a solution for deploying a mission in the cloud while...
Chapter 12: Kontaxis et al. describe a system that generates computational decoys to introduce uncertainty and deceive adversaries as to which data and computation is legitimate.

Chapter 13: Zhou presents a secure, provenance-based capability that captures dependencies between system states, tracks state changes over time, and answers attribution questions about the existence, or change, of a system's state at a given time.

Chapter 14: Wu et al. present a monitoring capability for multicore architectures that runs monitoring threads concurrently with user or kernel code to constantly check for security violations.

Chapter 15: Hasan Cam describes how to manage the risk and resilience of cyber-physical systems by employing controllability and observability techniques for linear and non-linear systems.

Cloud technologies have revolutionized the way we store information and perform various computing tasks. With the rise of this new technology, the ability to secure information stored on the cloud becomes a concern.

The Handbook of Research on Securing Cloud-Based Databases with Biometric Applications explores the latest innovations in promoting cloud security through human authentication techniques. Exploring methods of access by identification, including the analysis of facial features, fingerprints, DNA, dental characteristics, and voice patterns, this publication is designed especially for IT professionals, academicians, and upper-level students seeking current research surrounding cloud security.

The information you need to avoid security threats on corporate mobile devices:

Mobile devices have essentially replaced computers for corporate users who are on the go and there are millions of networks that have little to no security. This essential guide walks you through the steps for securing a network and building a bulletproof framework that will protect and support mobile devices in the enterprise. Featuring real-world case scenarios, this straightforward guide shares invaluable advice for protecting mobile devices from the loss of sensitive and confidential corporate information.

Provides a practical, fast-track approach to protecting a mobile device from security threats:

- Discusses important topics such as specific hacker protection, loss/theft protection, backing up and restoring data, and more.
- Offers critical advice for deploying enterprise network protection for mobile devices.
- Walks you through the advantages of granular application access control and enforcement with VPN.

Business can be mobile without being vulnerable—and Mobile Device Security For Dummies shows you how.
Enterprise security is an important area since all types of organizations require secure and robust environments, platforms and services to work with people, data and computing applications. The book provides selected papers of the Second International Workshop on Enterprise Security held in Vancouver, Canada, November 30-December 3, 2016 in conjunction with CloudCom 2015. The 11 papers were selected from 24 submissions and provide a comprehensive research into various areas of enterprise security such as protection of data, privacy and rights, data ownership, trust, unauthorized access and big data ownership, studies and analysis to reduce risks imposed by data leakage, hacking and challenges of Cloud forensics.

Similar to unraveling a math word problem, Security Intelligence: A Practitioner’s Guide to Solving Enterprise Security Challenges guides you through a deciphering process that translates each security goal into a set of security variables, substitutes each variable with a specific security technology domain, formulates the equation that is the deployment strategy, then verifies the solution against the original problem by analyzing security incidents and mining hidden breaches, ultimately refines the security formula iteratively in a perpetual cycle. You will learn about: Secure proxies – the necessary extension of the endpoints Application identification and control – visualize the threats Malnets – where is the source of infection and who are the pathogens Identify the security breach – who was the victim and what was the lure Security in Mobile computing – SNAFU With this book, you will be able to: Identify the relevant solutions to secure the infrastructure Construct policies that provide flexibility to the users so to ensure productivity Deploy effective defenses against the ever evolving web threats Implement solutions that are compliant to relevant rules and regulations Offer insight to developers who are building new security solutions and products

The only official study guide for the new CCSP exam CCSP (ISC)2 Certified Cloud Security Professional Official Study Guide is your ultimate resource for the CCSP exam. As the only official study guide reviewed and endorsed by (ISC)2, this guide helps you prepare faster and smarter with the Sybex study tools that include pre-test assessments that show you what you know, and areas you need further review. Objective maps, exercises, and chapter review questions help you gauge your progress along the way, and the Sybex interactive online learning environment includes access to a PDF glossary, hundreds of flashcards, and two complete practice exams. Covering all CCSP domains, this book walks you through Architectural Concepts and Design Requirements, Cloud Data Security, Cloud Platform and Infrastructure Security, Cloud Application Security, Operations, and Legal and Compliance with real-world scenarios to help you apply your skills along the way. The CCSP is the latest credential from (ISC)2 and the Cloud Security Alliance, designed to show employers that you have what it takes to keep their organization safe in the cloud. Learn the skills you need to be confident on exam day and beyond. Review 100% of all CCSP exam objectives Practice applying essential concepts and skills Access the industry-leading online study tool set Test your knowledge with bonus practice exams and more As organizations become increasingly reliant on cloud-based IT, the threat to data security looms larger. Employers are seeking qualified professionals with a proven cloud security skillset, and the CCSP credential brings your resume to the top of the pile. CCSP (ISC)2 Certified Cloud Security Professional Official Study Guide gives you the tools and information you need to earn that certification, and apply your skills in a real-world setting.

This book provides insight and expert advice on the challenges of Trust, Identity, Privacy, Protection, Safety and Security (TIPPSS) for the growing Internet of Things (IoT) in our connected world. Contributors cover physical, legal, financial and reputational risk in connected products and services for citizens and institutions including industry, academia, scientific research, healthcare and smart cities. As an important part of the Women in Science and Engineering book series, the work highlights the contribution of women leaders in TIPPSS for IoT, inspiring women and men, girls and boys to enter and apply themselves to secure our future in an increasingly connected world. The book features contributions from prominent female engineers, scientists, business and technology leaders, policy and legal experts in IoT from academia, industry and government. Provides insight into women’s contributions to the field of Trust, Identity, Privacy, Protection, Safety and Security (TIPPSS) for IoT Presents information from academia, research, government and
Read Book Securing Application Deployment With Obfuscation And Code Signing How To Create 3 Layers Of Protection For Net Release Build Application Security Series

Explains the components, development tools, and programming model of the Microsoft .NET platform. How we can evade, protest, and sabotage today's pervasive digital surveillance by deploying more data, not less—and why we should. With Obfuscation, Finn Brunton and Helen Nissenbaum mean to start a revolution. They are calling us not to the barricades but to our computers, offering us ways to fight today's pervasive digital surveillance—the collection of our data by governments, corporations, advertisers, and hackers. To the toolkit of privacy protecting techniques and projects, they propose adding obfuscation: the deliberate use of ambiguous, confusing, or misleading information to interfere with surveillance and data collection projects. Brunton and Nissenbaum provide tools and a rationale for evasion, noncompliance, refusal, even sabotage—especially for average users, those of us not in a position to opt out or exert control over data about ourselves. Obfuscation will teach users to push back, software developers to keep their user data safe, and policy makers to gather data without misusing it. Brunton and Nissenbaum present a guide to the forms and formats that obfuscation has taken and explain how to craft its implementation to suit the goal and the adversary. They describe a series of historical and contemporary examples, including radar chaff deployed by World War II pilots, Twitter bots that hobbled the social media strategy of popular protest movements, and software that can camouflage users' search queries and stymie online advertising. They go on to consider obfuscation in more general terms, discussing why obfuscation is necessary, whether it is justified, how it works, and how it can be integrated with other privacy practices and technologies.

- This is the latest practice test to pass the CSSLP ISC Certified Secure Software Lifecycle Professional Exam. - It contains 349 Questions and Answers. - All the questions are 100% valid and stable. - You can reply on this practice test to pass the exam with a good mark and in the first attempt.

This book constitutes the refereed proceedings of the 25th Australasian Conference on Information Security and Privacy, ACISP 2020, held in Perth, WA, Australia, in November 2020. The 31 revised full papers and 5 short papers presented were carefully revised and selected from 151 submissions. The
papers present and discuss the latest research, trends, breakthroughs, and challenges in the domain of information security, privacy and cybersecurity on a variety of topics such as post-quantum cryptography; symmetric cipher; signature; network security and blockchain; cryptographic primitives; mathematical foundation; machine learning security, among others. *The conference was held virtually due to COVID-19 pandemic.