Security In Computing Pfleeger 4th Edition

Thank you very much for downloading **Security In Computing Pfleeger 4th Edition** . Maybe you have knowledge that, people have look hundreds times for their favorite readings like this Security In Computing Pfleeger 4th Edition , but end up in infectious downloads.
Rather than enjoying a good book with a cup of coffee in the afternoon, instead they juggled with some infectious virus inside their laptop.

Security In Computing Pfleeger 4th Edition is available in our digital library an online access to it is set as public so you can get it instantly.
Our digital library saves in multiple locations, allowing you to get the most less latency time to download any of our books like this one.
Kindly say, the Security In Computing Pfleeger 4th Edition is universally compatible with any devices to read

Security in Computing - Charles P. Pfleeger 2003
This third edition of the all time classic computer security book provides an overview of all types of computer security from centralized systems to distributed networks. The book has been updated to make the most current information in the field available and accessible to today's professionals.
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.

Handbook of Security and Networks - Yang Xiao 2011

This valuable handbook is a comprehensive compilation of state-of-art advances on security in computer networks. More than 40 internationally recognized authorities in the field of security and networks contribute articles in their areas of expertise. These international researchers and practitioners are from highly-respected universities, renowned research institutions

and IT companies from all over the world. Each self-contained chapter covers one essential research topic on security in computer networks. Through the efforts of all the authors, all chapters are written in a uniformed style; each containing which contains a comprehensive overview, the latest pioneering work and future research direction of a research topic.

Introduction to Network Security - Jie Wang 2015-07-10

Introductory textbook in the important area of network security for undergraduate and graduate students Comprehensively covers fundamental concepts with newer topics such as electronic cash, bit-coin, P2P, SHA-3, E-voting, and Zigbee security Fully updated to reflect new developments in network security Introduces a chapter on Cloud security, a very popular and essential topic Uses everyday examples that most computer users experience to illustrate important principles and mechanisms Features a companion website with Powerpoint slides for lectures and solution manuals to selected exercise problems, available at http://www.cs.uml.edu/~wang/NetSec

Information Security Management Professional based on ISO/IEC 27001 Courseware revised Edition–English - Ruben Zeegers 2018

Information is crucial for the continuity and proper functioning of both individual organizations and the economies they fuel; this information must be protected against access by unauthorized people, protected against accidental or malicious modification or destruction and must be available when it is needed. The EXIN Information Security Management (based on ISO/IEC 27001) certification program consist out of three Modules: Foundation, Professional and Expert.This book is the officially by Exin accredited courseware for the Information Security Management Professional

training. It includes:• Trainer presentation handout• Sample exam questions• Practical assignments • Exam preparation guide The module Information Security Management Professional based on ISO/IEC 27001 tests understanding of the organizational and managerial aspects of information security. The subjects of this module are Information Security Perspectives (business, customer, and the service provider) Risk Management (Analysis of the risks, choosing controls, dealing with remaining risks) and Information Security Controls (organizational, technical and physical controls).The program and this courseware are intended for everyone who is involved in the implementation, evaluation, and reporting of an information security program, such as an Information Security Manager (ISM), Information Security Officer (ISO) or a Line Manager, Process Manager or Project Manager with security responsibilities. Basic knowledge of Information Security is recommended, for instance through the EXIN Information Security Foundation based on ISO/IEC 27001 certification.

ECCWS2015-Proceedings of the 14th European Conference on Cyber Warfare and Security 2015 - Dr Nasser Abouzakhar 2015-07-01

Complete proceedings of the 14th European Conference on Cyber Warfare and Security Hatfield UK Published by Academic Conferences and Publishing International Limited

Vertrauen für föderiertes Identitätsmanagement - Christian Broser 2016-04-29

Moderne und erfolgreiche Unternehmen verlangen nach Möglichkeiten, Dienste und Applikationen flexibel in der Cloud anbieten oder aus der Cloud für die eigenen Geschäftsprozesse nutzen zu können. In diesem Zusammenhang spielt der Bereich Identity- und Accessmanagement eine entscheidende Rolle.

Klassische Lösungen mit einer zentralisierten Benutzerverwaltung sind für diesen Zweck nicht ausreichend. Eine Erweiterung hin zum föderierten Identitätsmanagement (FIdM), welches hingegen auf eine verteilte Benutzerverwaltung setzt und den Zugriff auf eine entfernte Ressource mittels der digitalen Identität bei der Heimatorganisation regelt, ist erforderlich. Im Rahmen von föderiertem Identitätsmanagement gilt Vertrauen zwischen den beteiligten Parteien als zentrale Herausforderung. Existierende FIdM-Systeme berücksichtigen diese Thematik jedoch bislang unzureichend und sind deshalb häufig spezifisch auf die jeweilige Umgebung ausgerichtet und wenig flexibel ausgestaltet. Aktuelle Erkenntnisse zeigen, dass eine Integration von Ansätzen des Vertrauensmanagements und Techniken des föderierten Identitätsmanagements zu einer Dynamisierung und Flexibilisierung von FIdM führen kann. Dieses Buch bietet eine umfangreiche und systematische Betrachtung der Bereiche des Vertrauensmanagements und föderierten Identitätsmanagements. Dabei werden unterschiedliche Typen von FIdM klassifiziert und Einflussfaktoren auf Vertrauen analysiert. Darauf aufbauend, wird in diesem Buch zur Demonstration der Integration der beiden Bereiche ein generisches Modell präsentiert, das als Grundlage für die Implementierung von dynamischem und flexiblem FIdM verwendet werden kann, womit auch vertrauenswürdige Transaktionen zwischen vorher unbekannten Parteien ermöglicht werden.

Auditing Information Systems - Piattini, Mario 1999-07-01

Society's growing dependence on information technology for survival has elevated the importance of controlling and evaluating information systems. A sound plan for auditing information systems and the technology that

supports them is a necessity for organizations to improve the IS benefits and allow the organization to manage the risks associated with technology.Auditing Information Systems gives a global vision of auditing and control, exposing the major techniques and methods. It provides guidelines for auditing the crucial areas of IT--databases, security, maintenance, quality, and communications.

Software Safety and Security - NATO Emerging Security Challenges Division 2012

Recent decades have seen major advances in methods and tools for checking the safety and security of software systems. Automatic tools can now detect security flaws not only in programs of the order of a million lines of code, but also in high-level protocol descriptions. There has also been something of a breakthrough in the area of operating system verification. This book presents the lectures from the NATO Advanced Study Institute on Tools for Analysis and Verification of Software Safety and Security; a summer school held at Bayrischzell, Germany, in 2011. This Advanced Study Institute was divided into three integrated modules: Foundations of Safety and Security, Applications of Safety Analysis and Security Analysis. Subjects covered include mechanized game-based proofs of security protocols, formal security proofs, model checking, using and building an automatic program verifier and a hands-on introduction to interactive proofs. Bringing together many leading international experts in the field, this NATO Advanced Study Institute once more proved invaluable in facilitating the connections which will influence the quality of future research and the potential to transfer research into practice. This book will be of interest to all those whose work depends on the safety and security of software systems.

Secure Software Design - Theodor Richardson 2013

Networking & Security.

Computer Security and the Internet - Paul C. van Oorschot 2021-10-13

This book provides a concise yet comprehensive overview of computer and Internet security, suitable for a one-term introductory course for junior/senior undergrad or first-year graduate students. It is also suitable for self-study by anyone seeking a solid footing in security – including software developers and computing professionals, technical managers and government staff. An overriding focus is on brevity, without sacrificing breadth of core topics or technical detail within them. The aim is to enable a broad understanding in roughly 350 pages. Further prioritization is supported by designating as optional selected content within this. Fundamental academic concepts are reinforced by specifics and examples, and related to applied problems and real-world incidents. The first chapter provides a gentle overview and 20 design principles for security. The ten chapters that follow provide a framework for understanding computer and Internet security. They regularly refer back to the principles, with supporting examples. These principles are the conceptual counterparts of security-related error patterns that have been recurring in software and system designs for over 50 years. The book is "elementary" in that it assumes no background in security, but unlike "soft" high-level texts it does not avoid low-level details, instead it selectively dives into fine points for exemplary topics to concretely illustrate concepts and principles. The book is rigorous in the sense of being technically sound, but avoids both mathematical proofs and lengthy source-code examples that typically make books inaccessible to general audiences. Knowledge of elementary operating system and networking concepts is helpful, but review sections summarize the essential background. For graduate

students, inline exercises and supplemental references provided in per-chapter endnotes provide a bridge to further topics and a springboard to the research literature; for those in industry and government, pointers are provided to helpful surveys and relevant standards, e.g., documents from the Internet Engineering Task Force (IETF), and the U.S. National Institute of Standards and Technology.

ISSE 2009 Securing Electronic Business Processes - Norbert Pohlmann 2010-07-23

This book presents the most interesting talks given at ISSE 2009 – the forum for the inter-disciplinary discussion of how to adequately secure electronic business processes. The topics include: - Economics of Security and Identity Management - Security Services and Large Scale Public Applications - Privacy and Data Protection and Awareness Raising - Standards and Technical Solutions - Secure Software, Trust and Assurance Adequate information security is one of the basic requirements of all electronic business processes. It is crucial for effective solutions that the possibilities offered by security technology can be integrated with the commercial requirements of the applications. The reader may expect state-of-the-art: best papers of the Conference ISSE 2009.

Insider Threats in Cyber Security - Christian W. Probst 2010-07-28

Insider Threats in Cyber Security is a cutting edge text presenting IT and non-IT facets of insider threats together. This volume brings together a critical mass of well-established worldwide researchers, and provides a unique multidisciplinary overview. Monica van Huystee, Senior Policy Advisor at MCI, Ontario, Canada comments "The book will be a must read, so of course I'll need a copy." Insider Threats in Cyber Security covers all aspects of insider threats, from motivation to mitigation. It includes how to monitor insider threats (and what to monitor

for), how to mitigate insider threats, and related topics and case studies. Insider Threats in Cyber Security is intended for a professional audience composed of the military, government policy makers and banking; financing companies focusing on the Secure Cyberspace industry. This book is also suitable for advanced-level students and researchers in computer science as a secondary text or reference book.

The Data Warehouse Lifecycle Toolkit - Ralph Kimball 2011-03-08

A thorough update to the industry standard for designing, developing, and deploying data warehouse and business intelligence systems The world of data warehousing has changed remarkably since the first edition of The Data Warehouse Lifecycle Toolkit was published in 1998. In that time, the data warehouse industry has reached full maturity and acceptance, hardware and software have made staggering advances, and the techniques promoted in the premiere edition of this book have been adopted by nearly all data warehouse vendors and practitioners. In addition, the term "business intelligence" emerged to reflect the mission of the data warehouse: wrangling the data out of source systems, cleaning it, and delivering it to add value to the business. Ralph Kimball and his colleagues have refined the original set of Lifecycle methods and techniques based on their consulting and training experience. The authors understand first-hand that a data warehousing/business intelligence (DW/BI) system needs to change as fast as its surrounding organization evolves. To that end, they walk you through the detailed steps of designing, developing, and deploying a DW/BI system. You'll learn to create adaptable systems that deliver data and analyses to business users so they can make better business decisions.

Information Security Management Professional based on ISO/IEC 27001 Courseware – English -

Ruben Zeegers 2018-01-22 Information is crucial for the continuity and proper functioning of both individual organizations and the economies they fuel; this information must be protected against access by unauthorized people, protected against accidental or malicious modification or destruction and must be available when it is needed. The EXIN Information Security Management (based on ISO/IEC 27001) certification program consist out of three Modules: Foundation, Professional and Expert. This book is the officially by Exin accredited courseware for the Information Security Management Professional training. It includes: • Trainer presentation handout • Sample exam questions • Practical assignments • Exam preparation guide • Summary of ISO/IEC 27001:2013 The module Information Security Management Professional based on ISO/IEC 27001 tests understanding of the organizational and managerial aspects of information security. The subjects of this module are Information Security Perspectives (business, customer, and the service provider) Risk Management (Analysis of the risks, choosing controls, dealing with remaining risks) and Information Security Controls (organizational, technical and physical controls). The program and this courseware are intended for everyone who is involved in the implementation, evaluation, and reporting of an information security program, such as an Information Security Manager (ISM), Information Security Officer (ISO) or a Line Manager, Process Manager or Project Manager with security responsibilities. Basic knowledge of Information Security is recommended, for instance through the EXIN Information Security Foundation based on ISO/IEC 27001 certification.

Encyclopedia of Information Science and Technology, Fourth Edition - Khosrow-Pour, D.B.A., Mehdi 2017-06-20 In recent years, our world has

experienced a profound shift and progression in available computing and knowledge sharing innovations. These emerging advancements have developed at a rapid pace, disseminating into and affecting numerous aspects of contemporary society. This has created a pivotal need for an innovative compendium encompassing the latest trends, concepts, and issues surrounding this relevant discipline area. During the past 15 years, the Encyclopedia of Information Science and Technology has become recognized as one of the landmark sources of the latest knowledge and discoveries in this discipline. The Encyclopedia of Information Science and Technology, Fourth Edition is a 10-volume set which includes 705 original and previously unpublished research articles covering a full range of perspectives, applications, and techniques contributed by thousands of experts and researchers from around the globe. This authoritative encyclopedia is an all-encompassing, well-established reference source that is ideally designed to disseminate the most forward-thinking and diverse research findings. With critical perspectives on the impact of information science management and new technologies in modern settings, including but not limited to computer science, education, healthcare, government, engineering, business, and natural and physical sciences, it is a pivotal and relevant source of knowledge that will benefit every professional within the field of information science and technology and is an invaluable addition to every academic and corporate library.

Information Security Management Handbook, Sixth Edition - Harold F. Tipton 2007-05-14

Considered the gold-standard reference on information security, the Information Security Management Handbook provides an authoritative compilation of the fundamental knowledge, skills,

techniques, and tools required of today's IT security professional. Now in its sixth edition, this 3200 page, 4 volume stand-alone reference is organized under the CISSP Common Body of Knowledge domains and has been updated yearly. Each annual update, the latest is Volume 6, reflects the changes to the CBK in response to new laws and evolving technology.

The Total CISSP Exam Prep Book - Thomas R. Peltier 2002-06-20

Until now, those preparing to take the Certified Information Systems Security Professional (CISSP) examination were not afforded the luxury of studying a single, easy-to-use manual. Written by ten subject matter experts (SMEs) - all CISSPs - this test prep book allows CISSP candidates to test their current knowledge in each of the ten security doma

Security in Vehicular Networks - Leila Benarous 2022-10-11

Vehicular networks were first developed to ensure safe driving and to extend the Internet to the road. However, we can now see that the ability of vehicles to engage in cyber-activity may result in tracking and privacy violations through the interception of messages, which are frequently exchanged on road. This book serves as a guide for students, developers and researchers who are interested in vehicular networks and the associated security and privacy issues. It facilitates the understanding of the technologies used and their various types, highlighting the importance of privacy and security issues and the direct impact they have on the safety of their users. It also explains various solutions and proposals to protect location and identity privacy, including two anonymous authentication methods that preserve identity privacy and a total of five schemes that preserve location privacy in the vehicular ad hoc networks and the cloud-enabled internet of vehicles, respectively. This book also presents a new privacy-aware blockchain-based pseudonym management framework.Vehicular networks

were first developed to ensure safe driving and to extend the Internet to the road. However, we can now see that the ability of vehicles to engage in cyber-activity may result in tracking and privacy violations through the interception of messages, which are frequently exchanged on road. This book serves as a guide for students, developers and researchers who are interested in vehicular networks and the associated security and privacy issues. It facilitates the understanding of the technologies used and their various types, highlighting the importance of privacy and security issues and the direct impact they have on the safety of their users. It also explains various solutions and proposals to protect location and identity privacy, including two anonymous authentication methods that preserve identity privacy and a total of five schemes that preserve location privacy in the vehicular ad hoc networks and the cloud-enabled internet of vehicles, respectively. This book also presents a new privacy-aware blockchain-based pseudonym management framework. Leila

FISMA and the Risk Management Framework - Stephen D. Gantz 2012-12-31 FISMA and the Risk Management Framework: The New Practice of Federal Cyber Security deals with the Federal Information Security Management Act (FISMA), a law that provides the framework for securing information systems and managing risk associated with information resources in federal government agencies. Comprised of 17 chapters, the book explains the FISMA legislation and its provisions, strengths and limitations, as well as the expectations and obligations of federal agencies subject to FISMA. It also discusses the processes and activities necessary to implement effective information security management following the passage of FISMA, and it describes the National Institute of Standards and Technology's Risk Management Framework. The book looks at how

information assurance, risk management, and information systems security is practiced in federal government agencies; the three primary documents that make up the security authorization package: system security plan, security assessment report, and plan of action and milestones; and federal information security-management requirements and initiatives not explicitly covered by FISMA. This book will be helpful to security officers, risk managers, system owners, IT managers, contractors, consultants, service providers, and others involved in securing, managing, or overseeing federal information systems, as well as the mission functions and business processes supported by those systems. Learn how to build a robust, near real-time risk management system and comply with FISMA Discover the changes to FISMA compliance and beyond Gain your systems the authorization they need

Handbook Of Electronic Security And Digital Forensics - Hamid Jahankhani 2010-03-31 The widespread use of information and communications technology (ICT) has created a global platform for the exchange of ideas, goods and services, the benefits of which are enormous. However, it has also created boundless opportunities for fraud and deception. Cybercrime is one of the biggest growth industries around the globe, whether it is in the form of violation of company policies, fraud, hate crime, extremism, or terrorism. It is therefore paramount that the security industry raises its game to combat these threats. Today's top priority is to use computer technology to fight computer crime, as our commonwealth is protected by firewalls rather than firepower. This is an issue of global importance as new technologies have provided a world of opportunity for criminals.This book is a compilation of the collaboration between the researchers and practitioners

in the security field; and provides a comprehensive literature on current and future e-security needs across applications, implementation, testing or investigative techniques, judicial processes and criminal intelligence. The intended audience includes members in academia, the public and private sectors, students and those who are interested in and will benefit from this handbook.

Handbook of Research on Emerging Developments in Data Privacy - Gupta, Manish 2014-12-31

Data collection allows today's businesses to cater to each customer's individual needs and provides a necessary edge in a competitive market. However, any breach in confidentiality can cause serious consequences for both the consumer and the company. The Handbook of Research on Emerging Developments in Data Privacy brings together new ideas on how to deal with potential leaks of valuable customer information. Highlighting the legal aspects of identity protection, trust and security, and detection techniques, this comprehensive work is a valuable resource for any business, legal, or technology professional looking to improve information security within their organization.

Large-Scale Distributed Computing and Applications: Models and Trends - Cristea, Valentin 2010-05-31

Many applications follow the distributed computing paradigm, in which parts of the application are executed on different network-interconnected computers. The extension of these applications in terms of number of users or size has led to an unprecedented increase in the scale of the infrastructure that supports them. Large-Scale Distributed Computing and Applications: Models and Trends offers a coherent and realistic image of today's research results in large scale distributed systems, explains state-of-the-art technological solutions for the main issues

regarding large scale distributed systems, and presents the benefits of using large scale distributed systems and the development process of scientific and commercial distributed applications.

Privacy, Intrusion Detection and Response: Technologies for Protecting Networks - Kabiri, Peyman 2011-10-31

Though network security has almost always been about encryption and decryption, the field of network security is moving towards securing the network environment rather than just stored or transferred data. Privacy, Intrusion Detection and Response: Technologies for Protecting Networks explores the latest practices and research works in the area of privacy, intrusion detection, and response. Increased interest on intrusion detection together with prevention and response proves that protecting data either in the storage or during transfer is necessary, but not sufficient, for the security of a network. This book discusses the latest trends and developments in network security and privacy, and serves as a vital reference for researchers, academics, and practitioners working in the field of privacy, intrusion detection, and response.

Elements of Computer Security - David Salomon 2010-08-05

As our society grows ever more reliant on computers, so it also becomes more vulnerable to computer crime. Cyber attacks have been plaguing computer users since the 1980s, and computer security experts are predicting that smart telephones and other mobile devices will also become the targets of cyber security threats in the future. Developed from the author's successful Springer guide to Foundations of Computer Security, this accessible textbook/reference is fully updated and enhanced with resources for students and tutors. Topics and features: examines the physical security of computer hardware, networks, and digital data; introduces the different forms

of rogue software (or malware), discusses methods for preventing and defending against malware, and describes a selection of viruses, worms and Trojans in detail; investigates the important threats to network security, and explores the subjects of authentication, spyware, and identity theft; discusses issues of privacy and trust in the online world, including children's privacy and safety; includes appendices which discuss the definition, meaning, and history of the term hacker, introduce the language of "l33t Speak", and provide a detailed virus timeline; provides numerous exercises and examples throughout the text, in addition to a Glossary of terms used in the book; supplies additional resources at the associated website, http://www.DavidSalomon.name/, including an introduction to cryptography, and answers to the exercises. Clearly and engagingly written, this concise textbook is an ideal resource for undergraduate classes on computer security. The book is mostly non-mathematical, and is suitable for anyone familiar with the basic concepts of computers and computations.

Principles, Methodologies, and Service-Oriented Approaches for Cloud Computing - Yang, Xiaoyu 2013-01-31

Innovations in cloud and service-oriented architectures continue to attract attention by offering interesting opportunities for research in scientific communities. Although advancements such as computational power, storage, networking, and infrastructure have aided in making major progress in the implementation and realization of cloud-based systems, there are still significant concerns that need to be taken into account. Principles, Methodologies, and Service-Oriented Approaches for Cloud Computing aims to present insight into Cloud principles, examine associated methods and technologies, and investigate the use of service-oriented computing

technologies. In addressing supporting infrastructure of the Cloud, including associated challenges and pressing issues, this reference source aims to present researchers, engineers, and IT professionals with various approaches in Cloud computing.

ISSE 2012 Securing Electronic Business Processes - Helmut Reimer 2012-12-11

This book presents the most interesting talks given at ISSE 2012 - the forum for the inter-disciplinary discussion of how to adequately secure electronic business processes. The topics include: - Information Security Strategy; Enterprise and Cloud Computing Security - Security and Privacy Impact of Green Energy; Human Factors of IT Security - Solutions for Mobile Applications; Identity & Access Management - Trustworthy Infrastructures; Separation & Isolation - EU Digital Agenda; Cyber Security: Hackers & Threats Adequate information security is one of the basic requirements of all electronic business processes. It is crucial for effective solutions that the possibilities offered by security technology can be integrated with the commercial requirements of the applications. The reader may expect state-of-the-art: best papers of the Conference ISSE 2012. Content Information Security Strategy - Enterprise and Cloud Computing Security - Security and Privacy - Impact of Green Energy - Human Factors of IT Security - Solutions for Mobile Applications - Identity & Access Management - Trustworthy Infrastructures - Separation & Isolation - EU Digital Agenda - Cyber Security - Hackers & Threats Target Group Developers of Electronic Business Processes IT Managers IT Security Experts Researchers The Editors Norbert Pohlmann: Professor for Distributed System and Information Security at Westfälische Hochschule Gelsenkirchen Helmut Reimer: Senior Consultant, TeleTrusT Wolfgang Schneider: Senior Adviser, Fraunhofer Institute SIT

Secure Messaging on the

Internet - Rolf Oppliger 2014-08-01
This book offers a comprehensive understanding of secure Internet messaging, and brings together all the relevant and critical information needed to use OpenPGP and S/MIME-compliant software. It explores the conceptual and technical approaches followed by the developers of both OpenPGP and S/MIME, and gives a thorough treatment of the latest and most-effective technologies for secure messaging. Ideal for security and network managers, as well as professional system and network administrators, this easy-to-understand book is a complete guide to OpenPGP, S/MIME, Web-based and gateway solutions, certified mail, delivery platforms, and instant messaging.

Strategic Adoption of Technological Innovations - Howard, Caroline 2013-01-31
Strategic Adoption of Technological Innovations brings together research from practitioners on the development, use, and importance of information technology in order to achieve organizational performance. This comprehensive collection is useful for academicians, scholars, researchers and other industry professionals to provide an understanding of strategy and use of information systems in organizations and entities.

Computer Security Handbook, Set - Seymour Bosworth 2012-07-18
The classic and authoritative reference in the field of computer security, now completely updated and revised With the continued presence of large-scale computers; the proliferation of desktop, laptop, and handheld computers; and the vast international networks that interconnect them, the nature and extent of threats to computer security have grown enormously. Now in its fifth edition, Computer Security Handbook continues to provide authoritative guidance to identify and to eliminate these threats where possible, as well

as to lessen any losses attributable to them. With seventy-seven chapters contributed by a panel of renowned industry professionals, the new edition has increased coverage in both breadth and depth of all ten domains of the Common Body of Knowledge defined by the International Information Systems Security Certification Consortium (ISC). Of the seventy-seven chapters in the fifth edition, twenty-five chapters are completely new, including: 1. Hardware Elements of Security 2. Fundamentals of Cryptography and Steganography 3. Mathematical models of information security 4. Insider threats 5. Social engineering and low-tech attacks 6. Spam, phishing, and Trojans: attacks meant to fool 7. Biometric authentication 8. VPNs and secure remote access 9. Securing Peer2Peer, IM, SMS, and collaboration tools 10. U.S. legal and regulatory security issues, such as GLBA and SOX Whether you are in charge of many computers or just one important one, there are immediate steps you can take to safeguard your computer system and its contents. Computer Security Handbook, Fifth Edition equips you to protect the information and networks that are vital to your organization.

Computer Security - Dieter Gollmann 2011-02-28

A completely up-to-date resource on computer security Assuming no previous experience in the field of computer security, this must-have book walks you through the many essential aspects of this vast topic, from the newest advances in software and technology to the most recent information on Web applications security. This new edition includes sections on Windows NT, CORBA, and Java and discusses cross-site scripting and JavaScript hacking as well as SQL injection. Serving as a helpful introduction, this self-study guide is a wonderful starting point for examining the variety of competing security systems and what makes them different

from one another. Unravels the complex topic of computer security and breaks it down in such a way as to serve as an ideal introduction for beginners in the field of computer security Examines the foundations of computer security and its basic principles Addresses username and password, password protection, single sign-on, and more Discusses operating system integrity, hardware security features, and memory Covers Unix security, Windows security, database security, network security, web security, and software security Packed with in-depth coverage, this resource spares no details when it comes to the critical topic of computer security.

Trust Modeling and Management in Digital Environments: From Social Concept to System Development - Yan, Zheng 2010-01-31

"This book investigates various definitions of trust and their characteristics in distributed systems and digital computing, and details how to model and implement trust in a digital system"--Provided by publisher.

IT-Sicherheit - Claudia Eckert 2014-10-29

Gesundheit, Mobilität, Handel oder Finanzen: moderne IT-Systeme sind heute in nahezu allen Bereichen von zentraler Bedeutung und mögliche Sicherheitsrisiken dieser Systeme von unmittelbarer Brisanz. Claudia Eckert stellt in diesem Standardwerk die zur Umsetzung der Sicherheitsanforderungen benötigten Verfahren und Protokolle detailliert vor und erläutert sie anschaulich anhand von Fallbeispielen. Im Vordergrund steht dabei, die Ursachen für Probleme heutiger IT-Systeme zu verdeutlichen und die grundlegenden Sicherheitskonzepte mit ihren jeweiligen Vor- und Nachteilen zu präsentieren. Der Leser entwickelt nicht nur ein Bewusstsein für IT-Sicherheitsrisiken, sondern erwirbt auch ein breites und grundlegendes Wissen zu deren Behebung. - Sicherheitsbedrohungen durch

unsichere Programmierung, Schadcode, Apps - Internet-(Un)Sicherheit - Security Engineering Vorgehen mit Bedrohungs- und Risiko-Analysen, Bewertungskriterien und Sicherheitsmodellen - Kryptografische Verfahren und Schlüsselmanagement - Authentifikation und digitale Identität - Zugriffskontrolle in zentralen und serviceorientierten (SOA) Systemen - Kommunikationssicherheit mit SSL/TLS, IPSec und sicherer Mail - Sichere mobile und drahtlose Kommunikation mit GSM/UMTS/LTE sowie, WLAN und Bluetooth Ein Muss für jeden, der sich mit dieser hochaktuellen Problematik beschäftigt!

CRYPTOGRAPHY AND INFORMATION SECURITY, THIRD EDITION - PACHGHARE, V. K. 2019-09-01

The main objective of this book is to cater to the need of a quality textbook for education in the field of information security. The present third edition of the book covers the principles, design, and implementation of various algorithms in cryptography and information security domain. The book is a comprehensive work with a perfect balance and systematic presentation of the theoretical and practical aspects. The pre-requisite of the cryptography are the fundamentals of the mathematical background. The book covers all such relevant methods and theorems, which are helpful to the readers to get the necessary mathematical base for the understanding of the cryptographic algorithms. It provides a clear analysis of different algorithms and techniques. NEW TO THE THIRD EDITION • New chapters on o Cyber Laws o Vulnerabilities in TCP/IP Model • Revised sections on o Digital signature o Attacks against digital signature • Introduction to some open source tools like Nmap, Zenmap, port scanner, network scanner and wireshark • Revised section on block cipher modes of operation • Coverage of Simplified Data Encryption Standard (S-DES)

and Simplified Advanced Encryption Standard (S-AES) with examples • Elaborated section on Linear Cryptanalysis and Differential Cryptanalysis • New solved problems and a topic “primitive roots” in number theory • Chapter on public key cryptosystems with various attacks against RSA algorithm • New topics on Ransomware, Darknet, and Darkweb as per the current academic requirement • Revised chapter on Digital Forensics The book is intended for the undergraduate and postgraduate students of computer science and engineering (B.Tech/M.Tech), undergraduate and postgraduate students of computer science (B.Sc. / M.Sc. Computer Science), and information technology (B.Sc. / M.Sc. IT) and the students of Master of Computer Applications (MCA).

Analyzing Computer Security - Charles P. Pfleeger 2012

In this book, the authors of the 20-year best-selling classic Security in Computing take a fresh, contemporary, and powerfully relevant new approach to introducing computer security. Organised around attacks and mitigations, the Pfleegers' new Analyzing Computer Security will attract students' attention by building on the high-profile security failures they may have already encountered in the popular media. Each section starts with an attack description. Next, the authors explain the vulnerabilities that have allowed this attack to occur. With this foundation in place, they systematically present today's most effective countermeasures for blocking or weakening the attack. One step at a time, students progress from attack/problem/harm to solution/protection/mitigation, building the powerful real-world problem solving skills they need to succeed as information security professionals. Analyzing Computer Security addresses crucial contemporary computer security themes throughout, including effective security

management and risk analysis; economics and quantitative study; privacy, ethics, and laws; and the use of overlapping controls. The authors also present significant new material on computer forensics, insiders, human factors, and trust.

Designing for Privacy and its Legal Framework - Aurelia Tamò-Larrieux 2018-11-03

This book discusses the implementation of privacy by design in Europe, a principle that has been codified within the European Data Protection Regulation (GDPR). While privacy by design inspires hope for future privacy-sensitive designs, it also introduces the need for a common understanding of the legal and technical concepts of privacy and data protection. By pursuing an interdisciplinary approach and comparing the problem definitions and objectives of both disciplines, this book bridges the gap between the legal and technical fields in order to enhance the regulatory and academic discourse. The research presented reveals the scope of legal principles and technical tools for privacy protection, and shows that the concept of privacy by design goes beyond the principle of the GDPR. The book presents an analysis of how current regulations delegate the implementation of technical privacy and data protection measures to developers and describes how policy design must evolve in order to implement privacy by design and default principles.

Pervasive Information Security and Privacy Developments: Trends and Advancements - Nemati, Hamid 2010-07-31

Privacy and security concerns are at the forefront of research and critical study in the prevalence of information technology. Pervasive Information Security and Privacy Developments: Trends and Advancements compiles research on topics such as technical, regulatory, organizational, managerial, cultural, ethical, and human aspects of information security

and privacy. This reference offers methodologies, research frameworks, theory development and validation, case studies, simulations, technological architectures, infrastructure issues in design, and implementation of secure and privacy preserving initiatives.

Handbook of Research on Digital Crime, Cyberspace Security, and Information Assurance - Cruz-Cunha, Maria Manuela 2014-07-31
In our hyper-connected digital world, cybercrime prevails as a major threat to online security and safety. New developments in digital forensics tools and an understanding of current criminal activities can greatly assist in minimizing attacks on individuals, organizations, and society as a whole. The Handbook of Research on Digital Crime, Cyberspace Security, and Information Assurance combines the most recent developments in data protection and information communication technology (ICT) law with research surrounding current criminal behaviors in the digital sphere. Bridging research and practical application, this comprehensive reference source is ideally designed for use by investigators, computer forensics practitioners, and experts in ICT law, as well as academicians in the fields of information security and criminal science.

Basiswissen Sichere Software - Sachar Paulus 2012-04-20
Sichere Software zeichnet sich dadurch aus, dass sie jedem möglichen Angriff standhalten können muss. Jeder Beteiligte im Softwareentwicklungsprozess sollte bewusst auf die Schaffung dieser Eigenschaft einer Software hinarbeiten. Dieses Buch vermittelt, welche Aspekte dabei zu berücksichtigen sind und zeigt für alle wichtigen Bereiche der Softwareentwicklung auf, was jeweils für Sicherheit getan werden kann - und muss. Es deckt den Lehrplan zum Certified Professional for Secure Software Engineering nach ISSECO-Standard ab, eignet sich zum Selbststudium

und als Begleitliteratur zu Schulungen.

Toward Better Usability, Security, and Privacy of Information Technology - National Research Council 2010-10-07

Despite many advances, security and privacy often remain too complex for individuals or enterprises to manage effectively or to use conveniently. Security is hard for users, administrators, and developers to understand, making it all too easy to use, configure, or operate systems in ways that are inadvertently insecure. Moreover, security and privacy technologies originally were developed in a context in which system administrators had primary responsibility for security and privacy protections and in which the users tended to be sophisticated. Today, the user base is much wider--including the vast majority of employees in many organizations and a large fraction of households--but the basic models for security and privacy are essentially unchanged. Security features can be clumsy and awkward to use and can present significant obstacles to getting work done. As a result, cybersecurity measures are all too often disabled or bypassed by the users they are intended to protect. Similarly, when security gets in the way of functionality, designers and administrators deemphasize it. The result is that end users often engage in actions, knowingly or unknowingly, that compromise the security of computer systems or contribute to the unwanted release of personal or other confidential information. Toward Better Usability, Security, and Privacy of Information Technology discusses computer system security and privacy, their relationship to usability, and research at their intersection.