Essay Information Security

MADILYNN ARCHER

Principles of Information Security John Wiley & Sons
High-level overview of the information security field. Covers key concepts like confidentiality, integrity, and availability, then dives into practical applications of these ideas in the areas of operational, physical, network, application, and operating system security. In this high-level survey of the information security field, best-selling author Jason Andress covers the basics of a wide variety of topics, from authentication and authorization to maintaining confidentiality and performing penetration testing. Using real-world security breaches as examples, Foundations of Information Security explores common applications of these concepts, such as operations security, network design, hardening and patching operating systems, securing mobile devices, as well as tools for assessing the security of hosts and applications. You'll also learn the basics of topics like: Multifactor authentication and how biometrics and hardware tokens can be used to harden the authentication process The principles behind modern cryptography, including symmetric and asymmetric algorithms, hashes, and certificates The laws and regulations that protect systems and data Anti-malware tools, firewalls, and intrusion detection systems Vulnerabilities such as buffer overflows and race conditions A valuable resource for beginning security professionals, network systems administrators, or anyone new to the field, Foundations of Information Security is a great place to start your journey into the dynamic and rewarding field of information security.
Information Security Management Handbook on CD-ROM, 2006 Edition Institute of Electrical & Electronics Engineers(IEEE)
Anthology from the year 2014 in the subject Business economics - Business Management, Corporate Governance, grade: 70%, University of Portsmouth (Institute of Criminal Justice Studies), course: BSc Security and Risk Management, language: English, abstract: This collection of essays outlines the work of one BSc student in Security and Risk Management from the University of Portsmouth, UK. It provides useful insights towards a better understanding of the topics of security, risk and organised crime. This book will be of particular relevance for BSc students in security and risk management and for security professionals who would like to deepen their academic knowledge. List of essays: What are the main influences on the function of a security manager in the retail and aviation sectors? Is there such a thing as an unified theory of risk and does the academic literature account for such principle adequately? There has been a move away from risk as probability to risk as accountability and liability which place the emphasis upon the individual Business continuity management has evolved as a business function Critically discuss how corporate security management is evolving The introduction of more privatisation into public policing will bring lower standards and risk greater corruption Critically examine the appropriateness of the term ‘organised crime’
Database Security CRC Press
In today's hyper-connected society, understanding the mechanisms of trust is crucial. Issues of trust are critical to solving problems as diverse as corporate responsibility, global warming, and the political system. In this insightful and entertaining book, Schneier weaves together ideas from across the social and biological sciences to explain how society induces trust. He shows the unique

role of trust in facilitating and stabilizing human society. He discusses why and how trust has evolved, why it works the way it does, and the ways the information society is changing everything.

We Have Root No Starch Press

The need for information security management has never been greater. With constantly changing technology, external intrusions, and internal thefts of data, information security officers face threats at every turn. The Information Security Management Handbook on CD-ROM, 2006 Edition is now available. Containing the complete contents of the Information Security Management Handbook, this is a resource that is portable, linked and searchable by keyword. In addition to an electronic version of the most comprehensive resource for information security management, this CD-ROM contains an extra volume's worth of information that is not found anywhere else, including chapters from other security and networking books that have never appeared in the print editions. Exportable text and hard copies are available at the click of a mouse. The Handbook's numerous authors present the ten domains of the Information Security Common Body of Knowledge (CBK) ®. The CD-ROM serves as an everyday reference for information security practitioners and an important tool for any one preparing for the Certified Information System Security Professional (CISSP) ® examination. New content to this Edition: Sensitive/Critical Data Access Controls Role-Based Access Control Smartcards A Guide to Evaluating Tokens Identity Management-Benefits and Challenges An Examination of Firewall Architectures The Five "W's" and Designing a Secure Identity Based Self-Defending Network Maintaining Network Security-Availability via Intelligent Agents PBX Firewalls: Closing the Back Door Voice over WLAN Spam Wars: How to Deal with Junk E-Mail Auditing the Telephony System: Defenses against Communications Security Breaches and Toll Fraud The "Controls" Matrix Information Security Governance

Essays on information assurance CRC Press

We depend on information and information technology (IT) to make many of our day-to-day tasks easier and more convenient. Computers play key roles in transportation, health care, banking, and energy. Businesses use IT for payroll and accounting, inventory and sales, and research and development. Modern military forces use weapons that are increasingly coordinated through computer-based networks. Cybersecurity is vital to protecting all of these functions. Cyberspace is vulnerable to a broad spectrum of hackers, criminals, terrorists, and state actors. Working in cyberspace, these malevolent actors can steal money, intellectual property, or classified information; impersonate law-abiding parties for their own purposes; damage important data; or deny the availability of normally accessible services. Cybersecurity issues arise because of three factors taken together - the presence of malevolent actors in cyberspace, societal reliance on IT for many important functions, and the presence of vulnerabilities in IT systems. What steps can policy makers take to protect our government, businesses, and the public from those would take advantage of system vulnerabilities? At the Nexus of Cybersecurity and Public Policy offers a wealth of information on practical measures, technical and nontechnical challenges, and potential policy responses. According to this report, cybersecurity is a never-ending battle; threats will evolve as adversaries adopt new tools and techniques to compromise security. Cybersecurity is therefore an ongoing process that needs to evolve as new threats are identified. At the Nexus of Cybersecurity and Public Policy is a call for action to make cybersecurity a public safety priority. For a number of years, the cybersecurity issue has received increasing public attention; however, most policy focus has been on the short-term costs of improving systems. In its explanation of the fundamentals of cybersecurity and the discussion of potential policy responses, this book will be a resource for policy makers, cybersecurity and IT professionals, and anyone who wants to understand threats to cyberspace.

Cybersecurity Law CRC Press

Presenting invaluable advice from the world?s most famous computer security expert, this intensely readable collection features some of the most insightful and informative coverage of the strengths and weaknesses of computer security and the price people pay -- figuratively and literally -- when security fails. Discussing the issues surrounding things such as airplanes, passports, voting machines, ID cards, cameras, passwords, Internet banking, sporting events, computers, and castles, this book is a must-read for anyone who values security at any level -- business, technical, or personal.

Cybersecurity and Information Security Analysts Course Technology

This textbook presents a proven, mature Model-Based Systems Engineering (MBSE) methodology that has delivered success in a wide range of system and enterprise programs. The authors introduce MBSE as the state of the practice in the vital Systems Engineering discipline that manages complexity and integrates technologies and design approaches to achieve effective, affordable, and balanced system solutions to the needs of a customer organization and its personnel. The book begins with a summary of the background and nature of MBSE. It summarizes the theory behind Object-Oriented Design applied to complex system architectures. It then walks through the phases of the MBSE methodology, using system examples to illustrate key points. Subsequent chapters broaden the application of MBSE in Service-Oriented Architectures (SOA), real-time systems, cybersecurity, networked enterprises, system simulations, and prototyping. The vital subject of system and architecture governance completes the discussion. The book features exercises at the end of each chapter intended to help readers/students focus on key points, as well as extensive appendices that furnish additional detail in particular areas. The self-contained text is ideal for students in a range of courses in systems architecture and MBSE as well as for practitioners seeking a highly practical presentation of MBSE principles and techniques.

Department of Defense Sponsored Information Security Research Grin Publishing

CYBERSECURITY LAW Learn to protect your clients with this definitive guide to cybersecurity law in this fully-updated third edition Cybersecurity is an essential facet of modern society, and as a result, the application of security measures that ensure the confidentiality, integrity, and availability of data is crucial. Cybersecurity can be used to protect assets of all kinds, including data, desktops, servers, buildings, and most importantly, humans. Understanding the ins and outs of the legal rules governing this important field is vital for any lawyer or other professionals looking to protect these interests. The thoroughly revised and updated Cybersecurity Law offers an authoritative guide to the key statutes, regulations, and court rulings that pertain to cybersecurity, reflecting the latest legal developments on the subject. This comprehensive text deals with all aspects of cybersecurity law, from data security and enforcement actions to anti-hacking laws, from surveillance and privacy laws to national and international cybersecurity law. New material in this latest edition includes many expanded sections, such as the addition of more recent FTC data security consent decrees, including Zoom, SkyMed, and InfoTrax. Readers of the third edition of Cybersecurity Law will also find: An all-new chapter focused on laws related to ransomware and the latest attacks that compromise the availability of data and systems New and updated sections on new data security laws in New York and Alabama, President Biden’s cybersecurity executive order, the Supreme Court’s first opinion interpreting the Computer Fraud and Abuse Act, American Bar Association guidance on law firm cybersecurity, Internet of Things cybersecurity laws and guidance, the Cybersecurity Maturity Model Certification, the NIST Privacy Framework, and more New cases that feature the latest findings in the constantly evolving cybersecurity law space An article by the author of this textbook, assessing the major gaps in U.S. cybersecurity law A companion website for instructors that features expanded case studies, discussion questions by chapter, and exam questions by chapter Cybersecurity Law is an ideal textbook for undergraduate and graduate level courses in cybersecurity, cyber operations, management-oriented information technology (IT), and computer science. It is also a useful reference for IT professionals, government personnel, business managers, auditors, cybersecurity insurance agents, and academics in these fields, as well as academic and corporate libraries that support these professions.

Security in Cyberspace Springer

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.

Safeguarding Your Technology GRIN Verlag

This book presents high-quality research papers presented at the Second International Conference on Smart Computing and Cyber Security: Strategic Foresight, Security Challenges and Innovation (SMARTCYBER 2021) held during June 16–17, 2021, in the Department of Smart Computing, Kyungdong University, Global Campus, South Korea. The book includes selected works from academics and industrial experts in the field of computer science, information technology, and electronics and telecommunication. The content addresses challenges of cyber security.

Service and Advanced Technology Addison-Wesley Longman

A collection of popular essays from security guru Bruce Schneier In his latest collection of essays, security expert Bruce Schneier tackles a range of cybersecurity, privacy, and real-world security issues ripped from the headlines. Essays cover the ever-expanding role of technology in national security, war, transportation, the Internet of Things, elections, and more. Throughout, he challenges the status quo with a call for leaders, voters, and consumers to make better security and privacy decisions and investments. Bruce's writing has previously appeared in some of the world's best-known and most-respected publications, including The Atlantic, the Wall Street Journal, CNN, the New York Times, the Washington Post, Wired, and many others. And now you can enjoy his essays in one place—at your own speed and convenience. Timely security and privacy topics The impact of security and privacy on our world Perfect for fans of Bruce's blog and newsletter Lower price than his previous essay collections The essays are written for anyone who cares about the future and implications of security and privacy for society.

Emerging Technologies in Data Mining and Information Security Springer

The Information Security Management Handbook continues its tradition of consistently communicating the fundamental concepts of security needed to be a true CISSP. In response to new developments, Volume 4 supplements the previous volumes with new information covering topics such as wireless, HIPAA, the latest hacker attacks and defenses, intrusion

Building an Information Security Awareness Program Cornell University Press

In his latest book, a pre-eminent information security pundit confessed that he was wrong about the solutions to the problem of information security. It's not technology that's the solution, but the human factor-people. But even infosec policies and procedures are insufficient if employees don't know about them, or why they're important, or what ca

Information Security CRC Press

Starting with the inception of an education program and progressing through its development, implementation, delivery, and evaluation, Managing an Information Security and Privacy Awareness and Training Program, Second Edition provides authoritative coverage of nearly everything needed to create an effective training program that is compliant with applicable laws, regulations, and policies. Written by Rebecca Herold, a well-respected information security and privacy expert named one of the "Best Privacy Advisers in the World" multiple times by Computerworld magazine as well as a "Top 13 Influencer in IT Security" by IT Security Magazine, the text supplies a proven framework for creating an awareness and training program. It also: Lists the laws and associated excerpts of the specific passages that require training and awareness Contains a plethora of forms, examples, and samples in the book’s 22 appendices Highlights common mistakes that many organizations make Directs readers to additional resources for more specialized information Includes 250 awareness activities ideas and 42 helpful tips for trainers Complete with case studies and examples from a range of businesses and industries, this all-in-one resource provides the holistic and practical understanding needed to identify and implement the training and awareness methods best suited to, and most effective for, your organization. Praise for: The first edition was outstanding. The new second edition is even better ... the definitive and indispensable guide for information security and privacy awareness and training professionals, worth every cent. As with the first edition, we recommend it unreservedly.. —NoticeBored.com

Information Security Management Handbook, Sixth Edition John Wiley & Sons

The book features research papers presented at the International Conference on Emerging Technologies in Data Mining and Information Security (IEMIS 2018) held at the University of Engineering & Management, Kolkata, India, on February 23–25, 2018. It comprises high-quality research by academics and industrial experts in the field of computing and communication, including full-length papers, research-in-progress papers, case studies related to all the areas of

data mining, machine learning, IoT and information security.

Liars and Outliers Springer Science & Business Media

This thesis is composed of four essays addressing problems in the domain of information systems (IS). In the first essay, we study methods for improving propagation of messages in both consumer and enterprise social networks. We present the formal definition and analysis of the problem, and use the hop-constrained minimum spanning tree (HMST) model to find cost-effective seeds and possible new connections that result in networks with improved propagation properties. Moreover, we present new heuristic algorithms that substantially improve the solution quality for the HMST problem, as tested on both random and real-world networks. In the second essay, we study the decision making of publisher websites in using third parties. We propose a two-sided economic model that captures the interaction between users, publisher websites, and third parties. Specifically, we focus on the effect of user privacy concerns on information sharing behavior of publisher websites. We then analyze welfare aspects and provide insights on the impact of industry regulations on stakeholders. The model is validated using an exploratory empirical analysis of publisher websites' third party sharing. Following this topic, in the third essay, we examine the impact of user privacy concerns as the self-regulatory mechanism that induces the website publisher to respect user privacy concerns. We conduct experiments designed to test the impact of users' privacy concerns, and find that the privacy concerns do affect the sharing intensity of user information by the websites. We analyze the effectiveness of passive "Do Not Track" and active "AdBlock Plus" privacy tools in a self-regulated environment. Interestingly, we find that the "Do Not Track" request does not always serve its intended purpose, but is actually being used by many websites as a signal to substantially increase the user information sharing intensity. Finally, in the fourth essay, we examine a firm's choice of information technology supplier, where customers' demand changes in response to adverse events or incidents that occur at the firms. We specifically model the strategic choice of firms choosing between either a shared supplier versus an independent supplier. In a symmetric duopoly setting, we show that this choice depends on the customer demand reactions to adverse events as well as relative risks of the suppliers. We also analyze the effectiveness of regulation and cooperation in improving firms' profit.

E-Commerce Security Threats John Wiley & Sons

Welcome to the cybersecurity (also called information security or InfoSec) field! If you are interested in a career in cybersecurity, you've come to the right book. So what exactly do these people do on the job, day in and day out? What kind of skills and educational background do you need to succeed in this field? How much can you expect to make, and what are the pros and cons of these various professions? Is this even the right career path for you? How do you avoid burnout and deal with stress? This book can help you answer these questions and more. Cybersecurity and Information Security Analysts: A Practical Career Guide, which includes interviews with professionals in the field, covers the following areas of this field that have proven to be stable, lucrative, and growing professions. Security Analysts/Engineers Security Architects Security Administrators Security Software Developers Cryptographers/Cryptologists/Cryptanalysts

Security and Risk Management. Selected Academic Essays Springer

The Handbook of Information Security is a definitive 3-volume handbook that offers coverage of both established and cutting-edge theories and developments on information and computer security. The text contains 180 articles from over 200 leading experts, providing the benchmark resource for information security, network security, information privacy, and information warfare.

Handbook of Information Security, Threats, Vulnerabilities, Prevention, Detection, and Management GRIN Verlag

To what extent does hacking become legal and can be done as a legal business under the concept of penetration testing? This essay examines the impacts of ethical hacking as a business.

From Database to Cyber Security Rowman & Littlefield

This volume in the Advances in Management Information Systems series covers the managerial landscape of information security.

Related with Essay Information Security:

• Chemistry Printable Periodic Table : click here