Byod Le Security Crowd Research Partners

Learning Technology for Education ChallengesComputers Helping People with Special NeedsManagement Information SystemsBuild a Next-Generation Digital WorkplaceDigital HealthThe Cyber Risk HandbookEconomics of Information SecurityCloud AtlasIBM MobileFirst in Action for mGovernment and Citizen Mobile ServicesSecurity and Privacy in Communication NetworksManaging Risk and Information SecurityThe Academic Book of the FutureThe Internet of ThingsAdvances in Internet, Data and Web TechnologiesHCI for Cybersecurity, Privacy and TrustManaged Code RootkitsMobile LearningDigital VortexHacking Exposed MobileFundamentals of StrategyIt's ComplicatedWhen Gadgets Betray UsMobile Cloud ComputingInformation Security HandbookAdvances in Digital Forensics XIICreating Business AgilityMalware DetectionDigital Phenotyping and Mobile SensingGuide to Vulnerability Analysis for Computer Networks and SystemsSecurity IntelligenceIntegration, Interconnection, and Interoperability of IoT SystemsBlockchain Technology for Industry 4.0ICT Systems Security and Privacy ProtectionMobile Apps EngineeringECCWS2014-Proceedings of the 13th European Conference on Cyber warefare and SecurityCybersecurity LeadershipSmart Cities of Today and TomorrowTen Strategies of a World-Class Cybersecurity Operations CenterThe Authentic Wild WestInternet of Things A to Z

Learning Technology for Education Challenges

Ten Strategies of a World-Class Cyber Security Operations Center conveys MITRE's accumulated expertise on enterprise-grade computer network defense. It covers ten key qualities of leading Cyber Security Operations Centers (CSOCs), ranging from their structure and organization, to processes that best enable smooth operations, to approaches that extract maximum value from key CSOC technology investments. This book offers perspective and context for key decision points in structuring a CSOC, such as what capabilities to offer, how to architect large-scale data collection and analysis, and how to prepare the CSOC team for agile, threat-based response. If you manage, work in, or are standing up a CSOC, this book is for you. It is also available on MITRE's website, www.mitre.org.

Computers Helping People with Special Needs

Managed Code Rootkits is the first book to cover application-level rootkits and other types of malware inside the application VM, which runs a platform-independent programming environment for processes. The book, divided into four parts, points out high-level attacks, which are developed in intermediate language. The initial part of the book offers an overview of managed code rootkits. It explores environment models of managed code and the relationship of managed code to rootkits by studying how they use application VMs. It also discusses attackers of managed code rootkits and various attack scenarios. The second part of the book covers the development of managed code rootkits, starting with the tools used in producing managed code rootkits through their deployment. The next part focuses on countermeasures that can possibly be used against managed code rootkits, including technical solutions, prevention, detection, and response tactics. The book concludes by presenting techniques that are somehow similar to managed code rootkits, which can be used in solving problems. Named a 2011 Best Hacking and Pen Testing Book by InfoSec Reviews Introduces the reader briefly to managed code environments and rootkits in general Completely details a new type of rootkit hiding in the application level and demonstrates how a hacker can change language runtime implementation Focuses on managed code including Java, .NET, Android Dalvik and reviews malware development scanarios

Management Information Systems

Developed for students on short courses in strategy for example, doing an initial course at undergraduate, postgraduate or post-experience level, or studying strategy as part of a wider degree in the arts, sciences or engineering, this book focuses on the analysis and formulation of strategy.

Build a Next-Generation Digital

Workplace

Mobile technology is changing the way government interacts with the public anytime and anywhere. mGovernment is the evolution of eGovernment. Like the evolution of web applications, mobile applications require a process transformation, and not by simply creating wrappers to mobile-enable existing web applications. This IBM® RedpaperTM publication explains what the key focus areas are for implementing a successful mobile government, how to address these focus areas with capabilities from IBM MobileFirstTM enterprise software, and what guidance and preferred practices to offer the IT practitioner in the public sector. This paper explains the key focus areas specific to governments and public sector clients worldwide in terms of enterprise mobility and describes the typical reference architecture for the adoption and implementation of mobile government solutions. This paper provides practical examples through typical use cases and usage scenarios for using the capabilities of the IBM MobileFirst products in the overall solution and provides guidance, preferred practices, and lessons learned to IT consultants and architects working in public sector engagements. The intended audience of this paper includes the following individuals: Client decision makers and solution architects leading mobile enterprise adoption projects in the public sector A wide range of IBM services and sales professionals who are involved in selling IBM software and designing public sector client solutions that include the IBM MobileFirst product suite Solution architects, consultants, and IBM Business Partners responsible for designing and deploying solutions that include the integration of the IBM MobileFirst product suite

Digital Health

Hackers, cyber-criminals, Dark Web users, and techno-terrorists beware! This book should make you think twice about attempting to do your dirty work in the smart cities of tomorrow. Scores of cities around the world have begun planning what are known as “smart cities.” These new or revamped urban areas use the latest technology to make the lives of residents easier and more enjoyable.They will have automated infrastructures such as the Internet of Things, “the Cloud,” automated industrial controls, electronic money, mobile and communication satellite systems, wireless texting and networking. With all of these benefits come new forms of danger, and so these cities will need many safeguards to prevent cyber criminals from wreaking havoc. This book explains the advantages of smart cities and how to design and operate one. Based on the practical experience of the authors in projects in the U.S. and overseas in Dubai, Malaysia, Brazil and India, it tells how such a city is planned and analyzes vital security concerns that must be addressed along the way. Most of us will eventually live in smart cities. What are the advantages and the latest design strategies for such ventures? What are the potential drawbacks? How will they change the lives of everyday citizens? This book offers a preview of our future and how you can help prepare yourself for the changes to come.

The Cyber Risk Handbook

This book constitutes the refereed proceedings of the 7th International Workshop on Learning Technology for Education Challenges, LTEC 2018, held in Žilina, Slovakia, in August 2018. The 25 revised full papers presented were carefully reviewed and selected from 54 submissions. The papers are organized in the following topical sections: Gamification and learning; learning and knowledge transfer; learning technologies applications; virtual learning environments; and mobile learning and MOOCs. LTEC 2018 examines how these technologies and pedagogical advances can be used to change the way teachers teach and students learn, while giving special emphasis to the pedagogically effective ways we can harness these new technologies in education.

Economics of Information Security

Minimize Power Consumption and Enhance User ExperienceEssential for high-speed fifth-generation mobile networks, mobile cloud computing (MCC) integrates the power of cloud data centers with the portability of mobile computing devices. Mobile Cloud Computing: Architectures, Algorithms and Applications covers the latest technological and architectura

Cloud Atlas

Digital forensics deals with the acquisition, preservation, examination, analysis and presentation of electronic evidence. Networked computing, wireless communications and portable electronic devices have expanded the role of digital forensics beyond traditional computer crime investigations. Practically every crime now involves some aspect of digital evidence; digital forensics provides the techniques and tools to articulate this evidence. Digital forensics also has myriad intelligence applications. Furthermore, it has a vital role in information assurance -- investigations of security breaches yield valuable information that can be used to design more secure systems. Advances in Digital Forensics XII describes original research results and innovative applications in the discipline of digital forensics. In addition, it highlights some of the major technical and legal issues related to digital evidence and electronic crime investigations. The areas of coverage include: Themes and Issues, Mobile Device Forensics, Network Forensics, Cloud Forensics, Social Media Forensics, Image Forensics, Forensic Techniques, and Forensic Tools. This book is the twelfth volume in the annual series produced by the International Federation for Information Processing (IFIP) Working Group 11.9 on Digital Forensics, an international community of scientists, engineers and practitioners dedicated to advancing the state of the art of research and practice in digital forensics. The book contains a selection of twenty edited papers from the Twelfth Annual IFIP WG 11.9 International Conference on Digital Forensics, held in New Delhi, India in the winter of 2016. Advances in Digital Forensics XII is an important resource for researchers, faculty members and graduate students, as well as for practitioners and individuals engaged in research and development efforts for the law enforcement and intelligence communities. Gilbert Peterson, Chair, IFIP WG 11.9 on Digital Forensics, is a Professor of Computer Engineering at the Air Force Institute of Technology, Wright-Patterson Air Force Base, Ohio, USA. Sujeet Shenoi is the F.P. Walter Professor of Computer Science and a Professor of Chemical Engineering at the University of Tulsa, Tulsa, Oklahoma, USA.

IBM MobileFirst in Action for mGovernment and Citizen Mobile Services

Actionable guidance and expert perspective for real-world cybersecurity The Cyber Risk Handbook is the practitioner's guide to implementing, measuring and improving the counter-cyber capabilities of the modern enterprise. The first resource of its kind, this book provides authoritative guidance for real-world situations, and cross-functional solutions for enterprise-wide improvement. Beginning with an overview of counter-cyber evolution, the discussion quickly turns practical with design and implementation guidance for the range of capabilities expected of a robust cyber risk management system that is integrated with the enterprise risk management (ERM) system. Expert contributors from around the globe weigh in on specialized topics with tools and techniques to help any type or size of organization create a robust system tailored to its needs. Chapter summaries of required capabilities are aggregated to provide a new cyber risk maturity model used to benchmark capabilities and to road-map gap-improvement. Cyber risk is a fast-growing enterprise risk, not just an IT risk. Yet seldom is guidance provided as to what this means. This book is the first to tackle in detail those enterprise-wide capabilities expected by Board, CEO and Internal Audit, of the diverse executive management functions that need to team up with the Information Security function in order to provide integrated solutions. Learn how cyber risk management can be integrated to better protect your enterprise Design and benchmark new and improved practical counter-cyber capabilities Examine planning and implementation approaches, models, methods, and more Adopt a new cyber risk maturity model tailored to your enterprise needs The need to manage cyber risk across the enterprise—inclusive of the IT operations—is a growing concern as massive data breaches make the news on an alarmingly frequent basis. With a cyber risk management system now a business-necessary requirement, practitioners need to assess the effectiveness of their current system, and measure its gap-improvement over time in response to a dynamic and fast-moving threat landscape. The Cyber Risk Handbook brings the world's best thinking to bear on aligning that system to the enterprise and vice-a-versa. Every functional head of any organization must have a copy at-hand to understand their role in achieving that alignment.

Security and Privacy in Communication

Networks

Technology is evolving faster than we are. As our mobile phones, mp3 players, cars, and digital cameras become more and more complex, we understand less and less about how they actually work and what personal details these gadgets might reveal about us. Robert Vamosi, an award-winning journalist and analyst who has been covering digital security issues for more than a decade, shows us the dark side of all that digital capability and convenience. Hotel-room TV remotes can be used to steal our account information and spy on what we've been watching, toll-booth transponders receive unencrypted EZ Pass or FasTrak info that can be stolen and cloned, and our cars monitor and store data about our driving habits that can be used in court against us. When Gadgets Betray Usgives us a glimpse into the secret lives of our gadgets and helps us to better understand--and manage--these very real risks.

Managing Risk and Information Security

This volume constitutes the thoroughly refereed post-conference proceedings of the 11th International Conference on Security and Privacy in Communication Networks, SecureComm 2015, held in Dallas, TX, USA, in October 2015. The 29 regular and 10 poster papers presented were carefully reviewed and selected from 107 submissions. It also presents 9 papers accepted of the workshop on Applications and Techniques in Cyber Security, ATCS 2015. The papers are grouped in the following topics: mobile, system, and software security; cloud security; privacy and side channels; Web and network security; crypto, protocol, and model.

The Academic Book of the Future

The two volume set LNCS 9758 and 9759, constitutes the refereed proceedings of the 15th International Conference on Computers Helping People with Special Needs, ICCHP 2015, held in Linz, Austria, in July 2016. The 115 revised full papers and 48 short papers presented were carefully reviewed and selected from 239 submissions. The papers included in the first volume are organized in the following topical sections: Art Karshmer lectures in access to mathematics, science and engineering; technology for inclusion and participation; mobile apps and platforms; accessibility of web and graphics; ambient assisted living (AAL) for aging and disability; the impact of PDF/UA on accessible PDF; standard tools and procedures in accessible e-book production; accessible e-learning – e-learning for accessibility/AT; inclusive settings, pedagogies and approaches in ICT-based learning for disabled and non-disabled people; digital games accessibility; user experience and emotions for accessibility (UEE4A).

The Internet of Things

Drawing on newspaper, eyewitness, and government accounts and the words of the gunfighters themselves, the author presents myth-shattering profiles of Billy the Kid, Wild Bill Hickok, Ben Thompson, John Wesley Hardin, Kid Curry, Tom Horn, and Harry Tracy

Advances in Internet, Data and Web Technologies

This professional guide and reference examines the challenges of assessing security vulnerabilities in computing infrastructure. Various aspects of vulnerability assessment are covered in detail, including recent advancements in reducing the requirement for expert knowledge through novel applications of artificial intelligence. The work also offers a series of case studies on how to develop and perform vulnerability assessment techniques using start-of-the-art intelligent mechanisms. Topics and features: provides tutorial activities and thought-provoking questions in each chapter, together with numerous case studies; introduces the fundamentals of vulnerability assessment, and reviews the state of the art of research in this area; discusses vulnerability assessment frameworks, including frameworks for industrial control and cloud systems; examines a range of applications that make use of artificial intelligence to enhance the vulnerability assessment processes; presents visualisation techniques that can be used to assist the vulnerability assessment process. In addition to serving the needs of security practitioners and researchers, this accessible volume is also ideal for students and instructors seeking a primer on artificial intelligence for vulnerability assessment, or a supplementary text for courses on computer security, networking, and artificial intelligence.

HCI for Cybersecurity, Privacy and Trust

Proven security tactics for today's mobile apps, devices, and networks "A great overview of the new threats created by mobile devices. The authors have heaps of experience in the topics and bring that to every chapter." -- Slashdot Hacking Exposed Mobile continues in the great tradition of the Hacking Exposed series, arming business leaders and technology practitioners with an in-depth understanding of the latest attacks and countermeasures--so they can leverage the power of mobile platforms while ensuring that security risks are contained." -- Jamil Farshchi, Senior Business Leader of Strategic Planning and Initiatives, VISA Identify and evade key threats across the expanding mobile risk landscape. Hacking Exposed Mobile: Security Secrets & Solutions covers the wide range of attacks to your mobile deployment alongside ready-to-use countermeasures. Find out how attackers compromise networks and devices, attack mobile services, and subvert mobile apps. Learn how to encrypt mobile data, fortify mobile platforms, and eradicate malware. This cutting-edge guide reveals secure mobile development guidelines, how to leverage mobile OS features and MDM to isolate apps and data, and the techniques the pros use to secure mobile payment systems. Tour the mobile risk ecosystem with expert guides to both attack and defense Learn how cellular network attacks compromise devices over-the-air See the latest Android and iOS attacks in action, and learn how to stop them Delve into mobile malware at the code level to understand how to write resilient apps Defend against server-side mobile attacks, including SQL and XML injection Discover mobile web attacks, including abuse of custom URI schemes and JavaScript bridges Develop stronger mobile authentication routines using OAuth and SAML Get comprehensive mobile app development security guidance covering everything from threat modeling to iOS- and Android-specific tips Get started quickly using our mobile pen testing and consumer security checklists

Managed Code Rootkits

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.

Mobile Learning

By the New York Times bestselling author of The Bone Clocks | Shortlisted for the Man Booker Prize A postmodern visionary and one of the leading voices in twenty-first-century fiction, David Mitchell combines flat-out adventure, a Nabokovian love of puzzles, a keen eye for character, and a taste for mind-bending, philosophical and scientific speculation in the tradition of Umberto Eco, Haruki Murakami, and Philip K. Dick. The result is brilliantly original fiction as profound as it is playful. In this groundbreaking novel, an influential favorite among a new generation of writers, Mitchell explores with daring artistry fundamental questions of reality and identity. Cloud Atlas begins in 1850 with Adam Ewing, an American notary voyaging from the Chatham Isles to his home in California. Along the way, Ewing is befriended by a physician, Dr. Goose, who begins to treat him for a rare species of brain parasite. . . . Abruptly, the action jumps to Belgium in 1931, where Robert Frobisher, a disinherited bisexual composer, contrives his way into the household of an infirm maestro who has a beguiling wife and a nubile daughter. . . . From there we jump to the West Coast in the 1970s and a troubled reporter named Luisa Rey, who stumbles upon a web of corporate greed and murder that threatens to claim her life. . . . And onward, with dazzling virtuosity, to an inglorious present-day England; to a Korean superstate of the near future where neocapitalism has run amok; and, finally, to a postapocalyptic Iron Age Hawaii in the last days of history. But the story doesn’t end even there. The narrative then boomerangs back through centuries and space, returning by the same route, in reverse, to its starting point. Along the way, Mitchell reveals how his disparate characters connect, how their fates intertwine, and how their souls drift across time like clouds across the sky. As wild as a videogame, as mysterious as a Zen koan, Cloud Atlas is an unforgettable tour de force that, like its incomparable author, has transcended its cult classic status to become a worldwide phenomenon. Praise for Cloud Atlas “[David] Mitchell is, clearly, a genius. He writes as though at the helm of some perpetual dream machine, can evidently do anything, and his ambition is written in magma across this novel’s every page.”—The New York Times Book Review “One of those how-the-holy-hell-did-he-do-it? modern classics that no doubt is—and should be—read by any student of contemporary literature.”—Dave Eggers “Wildly entertaining . . . a head rush, both action-packed and chillingly ruminative.”—People “The novel as series of nested dolls or Chinese boxes, a puzzle-book, and yet—not just dazzling, amusing, or clever but heartbreaking and passionate, too. I’ve never read anything quite like it, and I’m grateful to have lived, for a while, in all its many worlds.”—Michael Chabon “Cloud Atlas ought to make [Mitchell] famous on both sides of the Atlantic as a writer whose fearlessness is matched by his talent.”—The Washington Post Book World “Thrilling . . . One of the biggest joys in Cloud Atlas is watching Mitchell sashay from genre to genre without a hitch in his dance step.”—Boston Sunday Globe “Grand and elaborate . . . [Mitchell] creates a world and language at once foreign and strange, yet strikingly familiar and intimate.”—Los Angeles Times From the Hardcover edition.

Digital Vortex

Designed for managers struggling to understand the risks in organizations dependent on secure networks, this book applies economics not to generate breakthroughs in theoretical economics, but rather breakthroughs in understanding the problems of security.

Hacking Exposed Mobile

This book offers a snapshot of cutting-edge applications of mobile sensing for digital phenotyping in the field of Psychoinformatics. The respective chapters, written by authoritative researchers, cover various aspects related to the use of these technologies in health, education, and cognitive science research. They share insights both into established applications of mobile sensing (such as predicting personality or mental and behavioral health on the basis of smartphone usage patterns) and emerging trends. Machine learning and deep learning approaches are discussed, and important considerations regarding privacy risks and ethical issues are assessed. In addition to essential background information on various technologies and theoretical methods, the book also presents relevant case studies and good scientific practices, thus addressing researchers and professionals alike. To cite Thomas R. Insel, who wrote the foreword to this book: “Patients will only use digital phenotyping if it solves a problem, perhaps a digital smoke alarm that can prevent a crisis. Providers will only use digital phenotyping if it fits seamlessly into their crowded workflow. If we can earn public trust, there is every reason to be excited about this new field. Suddenly, studying human behavior at scale, over months and years, is feasible."

Fundamentals of Strategy

This edited book investigates the lack of interoperability in the IoT realm, including innovative research as well as technical solutions to interoperability, integration, and interconnection of heterogeneous IoT systems, at any level. It also explores issues caused by lack of interoperability such as impossibility to plug non-interoperable IoT devices into heterogeneous IoT platforms, impossibility to develop IoT applications exploiting multiple platforms in homogeneous and/or cross domains, slowness of IoT technology introduction at large-scale: discouragement in adopting IoT technology, increase of costs; scarce reusability of technical solutions and difficulty in meeting user satisfaction.

It's Complicated

Evolve your traditional intranet platform into a next-generation digital workspace with this comprehensive book. Through in-depth coverage of strategies, methods, and case studies, you will learn how to design and build an employee experience platform (EXP) for improved employee productivity, engagement, and collaboration. In Build a Next-Generation Digital Workplace, author Shailesh Kumar Shivakumar takes you through the advantages of EXPs and shows you how to successfully implement one in your organization. This book provides extensive coverage of topics such as EXP design, user experience, content strategy, integration, EXP development, collaboration, and EXP governance. Real-world case studies are also presented to explore practical applications. Employee experience platforms play a vital role in engaging, empowering, and retaining the employees of an organization. Next-generation workplaces demand constant innovation and responsiveness, and this book readies you to fulfill that need with an employee experience platform. You will: Understand key design elements of EXP, including the visual design, EXP strategy, EXP transformation themes, information architecture, and navigation design. Gain insights into end-to-end EXP topics needed to successfully design, implement, and maintain next-generation digital workplace platforms. Study methods used in the EXP lifecycle, such as requirements and design, development, governance, and maintenance Execute the main steps involved in digital transformation of legacy intranet platforms to EXP. Discover emerging trends in digital workplace such as gamification, machine-led operations model and maintenance model, employee-centric design (including persona based design and employee journey mapping), cloud transformation, and design transformation. Comprehend proven methods for legacy Intranet modernization, collaboration, solution validation, migration, and more. Who This Book Is For Digital enthusiasts, web developers, digital architects, program managers, and more.

When Gadgets Betray Us

Surveys the online social habits of American teens and analyzes the role technology and social media plays in their lives, examining common misconceptions about such topics as identity, privacy, danger, and bullying.

Mobile Cloud Computing

A comprehensive overview of the Internet of Things' core concepts, technologies, and applications Internet of Things A to Z offers a holistic approach to the Internet of Things (IoT) model. The Internet of Things refers to uniquely identifiable objects and their virtual representations in an Internet-like structure. Recently, there has been a rapid growth in research on IoT communications and networks, that confirms the scalability and broad reach of the core concepts. With contributions from a panel of international experts, the text offers insight into the ideas, technologies, and applications of this subject. The authors discuss recent developments in the field and the most current and emerging trends in IoT. In addition, the text is filled with examples of innovative applications and real-world case studies. Internet of Things A to Z fills the need for an up-to-date volume on the topic. This important book: Covers in great detail the core concepts, enabling technologies, and implications of the Internet of Things Addresses the business, social, and legal aspects of the Internet of Things Explores the critical topic of security and privacy challenges for both individuals and organizations Includes a discussion of advanced topics such as the need for standards and interoperability Contains contributions from an international group of experts in academia, industry, and research Written for ICT researchers, industry professionals, and lifetime IT learners as well as academics and students, Internet of Things A to Z provides a much-needed and comprehensive resource to this burgeoning field.

Information Security Handbook

"Focuses on the technology innovations that may help in building virtual businesses and making existing businesses smarter and efficient in their operations. Intended to help key decision makers understand more about introducing new technologies into businesses"--

Advances in Digital Forensics XII

This book presents a comprehensive state-of the-art approach to digital health technologies and practices within the broad confines of healthcare practices. It provides a canvas to discuss emerging digital health solutions, propelled by the ubiquitous availability of miniaturized, personalized devices and affordable, easy to use wearable sensors, and innovative technologies like 3D printing, virtual and augmented reality and driverless robots and vehicles including drones. One of the most significant promises the digital health solutions hold is to keep us healthier for longer, even with limited resources, while truly scaling the delivery of healthcare. Digital Health: Scaling Healthcare to the World addresses the emerging trends and enabling technologies contributing to technological advances in healthcare practice in the 21st Century. These areas include generic topics such as mobile health and telemedicine, as well as specific concepts such as social media for health, wearables and quantified-self trends. Also covered are the psychological models leveraged in design of solutions to persuade us to follow some recommended actions, then the design and educational facets of the proposed innovations, as well as ethics, privacy, security, and liability aspects influencing its acceptance. Furthermore, sections on economic aspects of the proposed innovations are included, analyzing the potential business models and entrepreneurship opportunities in the domain.

Creating Business Agility

This book captures the state of the art research in the area of malicious code detection, prevention and mitigation. It contains cutting-edge behavior-based techniques to analyze and detect obfuscated malware. The book analyzes current trends in malware activity online, including botnets and malicious code for profit, and it proposes effective models for detection and prevention of attacks using. Furthermore, the book introduces novel techniques for creating services that protect their own integrity and safety, plus the data they manage.

Malware Detection

Digital Phenotyping and Mobile Sensing

This book explores recent advances in blockchain technology and its impact on Industry 4.0 via advanced technologies. It provides an in-depth analysis of the step by step evolution of Industry 4.0 and blockchain technologies for creating the next-generation, secure, decentralized, distributed and trusted industry environment and enhancing the productivity of industries. The book describes how blockchain technology makes the industrial internet (Industry 4.0) a transparent, reliable and secure environment for people, processes, systems, and services, presenting a strong, technological and conceptual framework and roadmap for decision-makers involved in the transformation of any area of industry.

Guide to Vulnerability Analysis for Computer Networks and Systems

As more and more devices become interconnected through the Internet of Things (IoT), there is an even greater need for this book,which explains the technology, the internetworking, and applications that are making IoT an everyday reality. The book begins with a discussion of IoT "ecosystems" and the technology that enables them, which includes: Wireless Infrastructure and Service Discovery Protocols Integration Technologies and Tools

Application and Analytics Enablement Platforms A chapter on next-generation cloud infrastructure explains hosting IoT platforms and applications. A chapter on data analytics throws light on IoT data collection, storage, translation, real-time processing, mining, and analysis, all of which can yield actionable insights from the data collected by IoT applications. There is also a chapter on edge/fog computing. The second half of the book presents various IoT ecosystem use cases. One chapter discusses smart airports and highlights the role of IoT integration. It explains how mobile devices, mobile technology, wearables, RFID sensors, and beacons work together as the core technologies of a smart airport. Integrating these components into the airport ecosystem is examined in detail, and use cases and real-life examples illustrate this IoT ecosystem in operation. Another in-depth look is on envisioning smart healthcare systems in a connected world. This chapter focuses on the requirements, promising applications, and roles of cloud computing and data analytics. The book also examines smart homes, smart cities, and smart governments. The book concludes with a chapter on IoT security and privacy. This chapter examines the emerging security and privacy requirements of IoT environments. The security issues and an assortment of surmounting techniques and best practices are also discussed in this chapter.

Security Intelligence

Managing Risk and Information Security: Protect to

Enable, an ApressOpen title, describes the changing risk environment and why a fresh approach to information security is needed. Because almost every aspect of an enterprise is now dependent on technology, the focus of IT security must shift from locking down assets to enabling the business while managing and surviving risk. This compact book discusses business risk from a broader perspective, including privacy and regulatory considerations. It describes the increasing number of threats and vulnerabilities, but also offers strategies for developing solutions. These include discussions of how enterprises can take advantage of new and emerging technologies—such as social media and the huge proliferation of Internet-enabled devices—while minimizing risk. With ApressOpen, content is freely available through multiple online distribution channels and electronic formats with the goal of disseminating professionally edited and technically reviewed content to the worldwide community. Here are some of the responses from reviewers of this exceptional work: “Managing Risk and Information Security is a perceptive, balanced, and often thought-provoking exploration of evolving information risk and security challenges within a business context. Harkins clearly connects the needed, but often-overlooked linkage and dialog between the business and technical worlds and offers actionable strategies. The book contains eye-opening security insights that are easily understood, even by the curious layman.” Fred Wettling, Bechtel Fellow, IS&T Ethics & Compliance Officer, Bechtel “As disruptive technology innovations and escalating cyber threats continue to create enormous information security challenges, Managing

Risk and Information Security: Protect to Enable provides a much-needed perspective. This book compels information security professionals to think differently about concepts of risk management in order to be more effective. The specific and practical guidance offers a fast-track formula for developing information security strategies which are lock-step with business priorities." Laura Robinson, Principal, Robinson Insight Chair, Security for Business Innovation Council (SBIC) Program Director, Executive Security Action Forum (ESAF) "The mandate of the information security function is being completely rewritten. Unfortunately most heads of security haven't picked up on the change, impeding their companies' agility and ability to innovate. This book makes the case for why security needs to change, and shows how to get started. It will be regarded as marking the turning point in information security for years to come." Dr. Jeremy Bergsman, Practice Manager, CEB "The world we are responsible to protect is changing dramatically and at an accelerating pace. Technology is pervasive in virtually every aspect of our lives. Clouds, virtualization and mobile are redefining computing – and they are just the beginning of what is to come. Your security perimeter is defined by wherever your information and people happen to be. We are attacked by professional adversaries who are better funded than we will ever be. We in the information security profession must change as dramatically as the environment we protect. We need new skills and new strategies to do our jobs effectively. We literally need to change the way we think. Written by one of the best in the business, Managing Risk and Information

Security challenges traditional security theory with clear examples of the need for change. It also provides expert advice on how to dramatically increase the success of your security strategy and methods – from dealing with the misperception of risk to how to become a Z-shaped CISO. Managing Risk and Information Security is the ultimate treatise on how to deliver effective security to the world we live in for the next 10 years. It is absolute must reading for anyone in our profession – and should be on the desk of every CISO in the world." Dave Cullinane, CISSP CEO Security Starfish, LLC "In this overview, Malcolm Harkins delivers an insightful survey of the trends, threats, and tactics shaping information risk and security. From regulatory compliance to psychology to the changing threat context, this work provides a compelling introduction to an important topic and trains helpful attention on the effects of changing technology and management practices." Dr. Mariano-Florentino Cuéllar Professor, Stanford Law School Co-Director, Stanford Center for International Security and Cooperation (CISAC), Stanford University "Malcolm Harkins gets it. In his new book Malcolm outlines the major forces changing the information security risk landscape from a big picture perspective, and then goes on to offer effective methods of managing that risk from a practitioner's viewpoint. The combination makes this book unique and a must read for anyone interested in IT risk." Dennis Devlin AVP, Information Security and Compliance, The George Washington University "Managing Risk and Information Security is the first-to-read, must-read book on information security for C-Suite executives. It is accessible, understandable and actionable. No sky-is-falling scare tactics, no techno-babble – just straight talk about a critically important subject. There is no better primer on the economics, ergonomics and psycho-behaviourals of security than this." Thornton May, Futurist, Executive Director & Dean, IT Leadership Academy "Managing Risk and Information Security is a wake-up call for information security executives and a ray of light for business leaders. It equips organizations with the knowledge required to transform their security programs from a "culture of no" to one focused on agility, value and competitiveness. Unlike other publications, Malcolm provides clear and immediately applicable solutions to optimally balance the frequently opposing needs of risk reduction and business growth. This book should be required reading for anyone currently serving in, or seeking to achieve, the role of Chief Information Security Officer." Jamil Farshchi, Senior Business Leader of Strategic Planning and Initiatives, VISA "For too many years, business and security – either real or imagined – were at odds. In Managing Risk and Information Security: Protect to Enable, you get what you expect – real life practical ways to break logjams, have security actually enable business, and marries security architecture and business architecture. Why this book? It's written by a practitioner, and not just any practitioner, one of the leading minds in Security today." John Stewart, Chief Security Officer, Cisco "This book is an invaluable guide to help security professionals address risk in new ways in this alarmingly fast changing environment. Packed with examples which makes it a pleasure to read, the book captures practical ways a forward thinking CISO can turn information security into a competitive advantage for their business. This book provides a new framework for managing risk in an entertaining and thought provoking way. This will change the way security professionals work with their business leaders, and help get products to market faster. The 6 irrefutable laws of information security should be on a stone plaque on the desk of every security professional." Steven Proctor, VP, Audit & Risk Management, Flextronics

Integration, Interconnection, and Interoperability of IoT Systems

This book constitutes the thoroughly refereed proceedings of the First International Conference on HCI for Cybersecurity, Privacy and Trust, HCI-CPT 2019, which was held as part of the 21st HCI International Conference, HCII 2019, in Orlando, FL, USA, in July 2019. The total of 1275 papers and 209 posters included in the 35 HCII 2019 proceedings volumes were carefully reviewed and selected from 5029 submissions. HCI-CPT 2019 includes a total of 32 papers; they were organized in topical sections named: Authentication; cybersecurity awareness and behavior; security and usability; and privacy and trust.

Blockchain Technology for Industry 4.0

Digital disruption: seemingly out of nowhere, startups and other tech-savvy disruptors attack. In Digital Vortex, you will learn how to use the business models and strategies of startups to your own advantage.

Most importantly, you will learn how to build the agility to anticipate threats, sense opportunities, and seize them before your rivals do.

ICT Systems Security and Privacy Protection

"The insights go beyond cyber security alone to examine the critical concepts and often misunderstood distinction between leadership and management. This should be required reading on every college campus." - Collin Smith, CISSP - Cybersecurity Professional. "this book will change both the way we think about leadership and the way we understand information technology. I recommend this book highly to everyone." - Eric Schwartz - Executive Director at Advena World LLC and Adjunct Professor in Economics at Montgomery College. "explains what an organization needs to know to implement cybersecurity governance." Council of Graduate Schools Testimony at the US Senate Appropriations Committee Meeting, April 29, 2014. "exposes the common faults with which we are all struggling in this industry. It's humorous engaging, and I feel helps a reader question their own approaches. I was originally looking for a compendium that works as collateral reading for Cyber Security training courses, and I found it. I genuinely recommend this work tool." - David Bickel - Chief Information Security Officer, Department of Health and Mental Hygiene, State of Maryland. Written by one of the leading global thought leaders in cybersecurity with 30 years of practical experience in the field, this book addresses the most neglected area of cybersecurity -- cybersecurity governance -- the management, leadership, and engagement of people for the purposes of cybersecurity. This book is an essential book for anyone interested in understanding how cybersecurity should be led in an organization. All business executives or students at any level will benefit from this book. Cybersecurity can be a source of productivity and innovation and be a revenue driver. The leadership principles are applicable in any field and in any organization.

Mobile Apps Engineering

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

ECCWS2014-Proceedings of the 13th European Conference on Cyber warefare and Security

This book explores the use of mobile devices for teaching and learning language and literacies, investigating the ways in which these technologies open up new educational possibilities. Pegrum builds up a rich picture of contemporary mobile learning and outlines of likely future developments.

Cybersecurity Leadership

This book constitutes the refereed proceedings of the 32nd IFIP TC 11 International Conference on ICT Systems Security and Privacy Protection, SEC 2017, held in Rome, Italy, in May 2017. The 38 revised full papers presented were carefully reviewed and selected from 199 submissions. The papers are organized in the following topical sections: network security and cyber attacks; security and privacy in social applications and cyber attacks defense; private queries and aggregations; operating systems and firmware security; user authentication and policies; applied cryptography and voting schemes; software security and privacy; privacy; and digital signature, risk management, and code reuse attacks.

Smart Cities of Today and Tomorrow

Implement information security effectively as per your organization's needs. About This Book Learn to build your own information security framework, the best fit for your organization Build on the concepts of threat modeling, incidence response, and security analysis Practical use cases and best practices for information security Who This Book Is For This book is for security analysts and professionals who deal with security mechanisms in an organization. If you are looking for an end to end guide on information security and risk analysis with no prior knowledge of this domain, then this book is for you. What You Will Learn Develop your own information security framework Build your incident response mechanism Discover cloud security considerations Get to know the system development life cycle Get your security operation center up and running Know the various security testing types Balance security as per your business needs Implement information security best practices In Detail Having an information security mechanism is one of the most crucial factors for any organization. Important assets of organization demand a proper risk management and threat model for security, and so information security concepts are gaining a lot of traction. This book starts with the concept of information security and shows you why it's important. It then moves on to modules such as threat modeling, risk management, and mitigation. It also covers the concepts of incident response systems, information rights management, and more. Moving on, it guides you to build your own information security framework as the best fit for your organization. Toward the end, you'll discover some best practices that can be implemented to make your security framework strong. By the end of this book, you will be well-versed with all the factors involved in information security, which will help you build a security framework that is a perfect fit your organization's requirements. Style and approach This book takes a practical approach, walking you through information security fundamentals, along with information security best practices.

Ten Strategies of a World-Class Cybersecurity Operations Center

This book presents original contributions on the theories and practices of emerging Internet, Data and Web technologies and their applications in businesses, engineering and academia. As a key feature, it addresses advances in the life-cycle exploitation of data generated by digital ecosystem technologies. The Internet has become the most proliferative platform for emerging large-scale computing paradigms. Among these, Data and Web technologies are two of the most prominent paradigms, manifesting in a variety of forms such as Data Centers, Cloud Computing, Mobile Cloud, Mobile Web Services, and so on. These technologies altogether create a digital ecosystem whose cornerstone is the data cycle, from capturing to processing, analysis and visualization. The need to investigate various research and development issues in this digital ecosystem has been made even more pressing by the ever-increasing demands of real-life applications, which are based on storing and processing large amounts of data. Given its scope, the book offers a valuable asset for all researchers, software developers, practitioners and students interested in the field of Data and Web technologies.

The Authentic Wild West

This book is open access under a CC-BY licence. What makes a book 'academic'? What spaces, physical and digital, can they be found in? How are they made, bought, and read? These questions are tackled by a cross-section of thirteen experts from the fields of bookselling, publishing, university libraries, and academic research in this volume of essays, which was produced in conjunction with the team from the AHRC/British Library Academic Book of the Future Project as an accelerated publishing challenge for the first ever Academic Book Week. The topics include campus bookshops and bookselling, the role of national libraries, Open Access, the Research Excellence Framework, and publishing innovation. The approaches explore the realities of the present and venture all the way through to possible futures. There is something here for everyone who is connected to academic books - however these are defined, and whatever shape they are read in. This work was published by Saint Philip Street Press pursuant to a Creative Commons license permitting commercial use. All rights not granted by the work's license are retained by the author or authors.

Internet of Things A to Z