Eurosec Alarms Instruction Manual

Learn to Program Android Apps in Less Than 24 Hours! This Book Android Programming & Android App Development teaches you everything you need to become an Android App Developer from scratch. This book explains How You Can Get Started with Android App Programming by explaining the System & Software Requirements, Creating the environment for Java, Android Studio & Android SDK Manager & Most Importantly This Book Guides You In "Learning Your First Android App Development"! Want to learn an exciting Android App? Want to learn the history of Android? Want to learn the advantages of Android Programming? Want to learn the different between Android Apps & other OS Apps? Want to learn the different versions of Android? Want to learn the important skills you need to develop an Android App? Want to know the Career Options In Android Programming? This book has "Answers" for all your questions!!! What You'll Learn From This Book? Chapter 1: Introduction Chapter 2: Choosing App Development As A Career Option Chapter 3: History Of Android App Development Chapter 4: Advantages Of Android Programming Chapter 5: Android Apps Vs other OS Apps Chapter 6: Different Versions In Android Chapter 7: The Skills You Need To Develop An Android App Chapter 8: Getting Started - System & Software Requirements - How To Set Java Environment - How To Set Android Studio Chapter 9: Let's Build Your First Android App - R.Java & String.XML - Learn About Manifest.XML - Learn About Layouts - Learn About Databases Chapter 10: How To Publish Your Android App Chapter 11: Rooting Android App Chapter 12: How To Use Your Mobile As AVD Chapter 13: Why Should You Become An Android Developer? Chapter 14: Conclusion - Future Of Android App Development This book's been prepared for the beginners to help them understand basic Android programming. After completing this book from start to end, you will find yourself at a moderate level of expertise in Android programming from where you can take yourself to next levels. Get started TODAY! Learn to develop Your First Android App! We teach you not just to develop an app but also take you through the step by step guide of publishing your Android App in Google PlayStore!

This book constitutes the refereed proceedings of the 21st International Symposium on Research in Attacks, Intrusions, and Defenses, RAID 2018, held in Heraklion, Crete, Greece, in September 2018. The 32 revised full papers were carefully reviewed and selected from 145 submissions. They are organized in the following topical sections: attacks; intrusion detection and prevention; DDoS attacks; passwords, accounts, and users; machine learning for computer security; hardware-assisted security; software security; malware; IoT/CPS security; security measurements; and defenses.

The current crisis in Europe is being labelled, in mainstream media and politics, as a ‘public debt crisis’. The present book draws a markedly different picture. What is happening now is rooted, in a variety of different ways, in the destabilisation of national models of capitalism due to the predominance of neoliberalism since the demise of the post-war ‘golden age’. Ten country analyses provide insights into national ways of coping – or failing to cope – with the ongoing crisis. They reveal the extent to which the respective socio-economic development models are unsustainable, either for the country in question, or for other countries. The bottom-line of the book is twofold. First, there will be no European reform agenda at all unless each country does its own homework. Second, and equally urgent, is a new European reform agenda without which alternative approaches in individual countries will inevitably be suffocated. This message, delivered by the country chapters, is underscored by more general chapters on the prospects of trade union policy in Europe and on current austerity policies and how they interact with the new approaches to economic governance at the EU level. These insights are aimed at providing a better understanding across borders at a time when European rhetoric is being used as a smokescreen for national egoism.

This book constitutes the refereed proceedings of the 13th International Conference on

Detection of Intrusions and Malware, and Vulnerability Assessment, DIMVA 2016, held in San Sebastián, Spain, in July 2016. The 19 revised full papers and 2 extended abstracts presented were carefully reviewed and selected from 66 submissions. They present the state of the art in intrusion detection, malware analysis, and vulnerability assessment, dealing with novel ideas, techniques, and applications in important areas of computer security including vulnerability detection, attack prevention, web security, malware detection and classification, authentication, data leakage prevention, and countering evasive techniques such as obfuscation.

This book highlights a collection of high-quality peer-reviewed research papers presented at the Sixth International Conference on Information System Design and Intelligent Applications (INDIA 2019), held at Lendi Institute of Engineering & Technology, Vizianagaram, Andhra Pradesh, India, from 1 to 2 November 2019. It covers a wide range of topics in computer science and information technology, from wireless networks, social networks, wireless sensor networks, information and network security, to web security, Internet of Things, bioinformatics, geoinformatics and computer networks.

The book is a timely report on advanced methods and applications of computational intelligence systems. It covers a long list of interconnected research areas, such as fuzzy systems, neural networks, evolutionary computation, evolving systems and machine learning. The individual chapters are based on peer-reviewed contributions presented at the 17th Annual UK Workshop on Computational Intelligence, held on September 6-8, 2017, in Cardiff, UK. The book puts a special emphasis on novels methods and reports on their use in a wide range of applications areas, thus providing both academics and professionals with a comprehensive and timely overview of new trends in computational intelligence.

This book constitutes the thoroughly refereed post-conference proceedings of the Second International Workshop on Smart Grid Security, SmartGridSec 2014, held in Munich, Germany, in February 2014. The volume contains twelve corrected and extended papers presented at the workshop which have undergone two rounds of reviewing and improvement. The engineering, deployment and operation of the future Smart Grid will be an enormous project that will require the active participation of many stakeholders with different interests and views regarding the security and privacy goals, technologies, and solutions. There is an increasing need for workshops that bring together researchers from different communities, from academia and industry, to discuss open research topics in the area of future Smart Grid security.

This edited volume features a wide spectrum of the latest computer science research relating to cyber deception. Specifically, it features work from the areas of artificial intelligence, game theory, programming languages, graph theory, and more. The work presented in this book highlights the complex and multi-facted aspects of cyber deception, identifies the new scientific problems that will emerge in the domain as a result of the complexity, and presents novel approaches to these problems. This book can be used as a text for a graduate-level survey/seminar course on cutting-edge computer science research relating to cyber-security, or as a supplemental text for a regular graduate-level course on cyber-security.

This book covers diverse aspects of advanced computer and communication engineering, focusing specifically on industrial and manufacturing theory and applications of electronics, communications, computing and information technology. Experts in research, industry, and academia present the latest developments in technology, describe applications involving cutting-edge communication and computer systems, and explore likely future trends. In addition, a wealth of new algorithms that assist in solving computer and communication engineering problems are presented. The book is based on presentations given at ICOCOE 2015, the 2nd International Conference on

Communication and Computer Engineering. It will appeal to a wide range of professionals in the field, including telecommunication engineers, computer engineers and scientists, researchers, academics and students.

This book constitutes the thoroughly refereed post-conference proceedings of the 18th International Conference on Financial Cryptography and Data Security (FC 2014), held in Christ Church, Barbados, in March 2014. The 19 revised full papers and 12 short papers were carefully selected and reviewed from 165 abstract registrations and 138 full papers submissions. The papers are grouped in the following topical sections: payment systems, case studies, cloud and virtualization, elliptic curve cryptography, privacy-preserving systems, authentication and visual encryption, network security, mobile system security, incentives, game theory and risk, and bitcoin anonymity.

This book constitutes the proceedings of the 16th International Symposium on Research in Attacks, Intrusions and Defenses, former Recent Advances in Intrusion Detection, RAID 2013, held in Rodney Bay, St. Lucia in October 2013. The volume contains 22 full papers that were carefully reviewed and selected from 95 submissions, as well as 10 poster papers selected from the 23 submissions. The papers address all current topics in computer security ranged from hardware-level security, server, web, mobile, and cloud-based security, malware analysis, and web and network privacy.

This book reviews the challenging issues that present barriers to greater implementation of the cloud computing paradigm, together with the latest research into developing potential solutions. Topics and features: presents a focus on the most important issues and limitations of cloud computing, covering cloud security and architecture, QoS and SLAs; discusses a methodology for cloud security management, and proposes a framework for secure data storage and identity management in the cloud; introduces a simulation tool for energy-aware cloud environments, and an efficient congestion control system for data center networks; examines the issues of energy-aware VM consolidation in the IaaS provision, and software-defined networking for cloud related applications; reviews current trends and suggests future developments in virtualization, cloud security, QoS data warehouses, cloud federation approaches, and DBaaS provision; predicts how the next generation of utility computing infrastructures will be designed.

This book examines the nature of Russia’s relations with the former Soviet states (FSS), in particular with countries which formed the Commonwealth of Independent States, in order to assess whether there has been a resurgence of Russian imperialism since the collapse of the USSR. The book sets out to determine whether Russian leaders have attempted to restore a sphere of influence over the former Soviet republics or whether Russia’s policies reflect a genuine desire to establish normal state-to-state relations with the new states. It adopts a comprehensive approach, analysing Russia’s policies towards the FSS across a broad range of areas: energy, trade and investment; military assistance,

security provision and peacekeeping; conflict management, political support, and alliance formation. While not denying the Kremlin's assertive role in the FSS, this book challenges the assumption that Russia has always intended to restore a sphere of influence over its 'Near Abroad'. Rather, it argues that Russia's policies are much more complex, multi-faceted, and often more incoherent than is often assumed. In essence, Russia's actions generally reflect a combination of legitimate state interests, enduring Soviet legacies, and genuine concerns over events unfolding along Russia's borders. This book also shows that, at times, Great-Power nostalgia and a real difficulty with discarding Russia's imperial legacy shapes Russia's behaviour towards the FSS. This book will be of great interest to students of Russian politics and foreign policy, east European politics, and International Relations in general.

While the Cold War is long past, the importance of arms control in Russo-American relations and the related issue of nuclear weapons for Russia remain vital concerns. Indeed, without an appreciation of the multiple dimensions of the latter, progress in the former domain is inconceivable. With this in mind, following essays explore many, if not all, of the issues connected with Russia's relatively greater reliance on nuclear weapons for its security. As such, they constitute an important contribution to the analysis of the Obama administration's reset policy, Russo-American relations, Russian foreign and defense policy, and international security in both Europe and Asia. Additionally, questions concerning the approach taken by other nuclear power nations in reference to the arms control agenda provide a crucial backdrop for the progress toward curbing the proliferation of nuclear weapons, a long-standing central goal of U.S. security policy.

This book constitutes the refereed proceedings oft he 19th International Symposium on Research in Attacks, Intrusions, and Defenses, RAID 2016, held in Evry, France, in September 2016. The 21 full papers presented were carefully reviewed and selected from 85 submissions. They are organized around the following topics: systems security; low-level attacks and defenses; measurement studies; malware analysis; network security; systematization of knowledge and experience reports; Web and mobile security.

This book constitutes the refereed proceedings of the 12th International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment, DIMVA 2015, held in Milan, Italy, in July 2015. The 17 revised full papers presented were carefully reviewed and selected from 75 submissions. The papers are organized in topical sections on attacks, attack detection, binary analysis and mobile malware protection, social networks and large-scale attacks, Web and mobile security, and provenance and data sharing.

Explores the history of mankind's use of steroids, and reveals how these drugs affect the body and brain. Details the process by which users become addicted to these substances, and offers tips on overcoming addiction. Includes full-color photographs, a glossary, and further reading sources.

This book volume contains 31 papers presented at ICICT 2016: Second International Congress on Information and Communication Technology. The conference was held during 12-13 December 2016, Bangkok, Thailand and organized communally by G R Foundation, and Computer Society of India Division IV – Communication and Division V – Education and Research. This volume contains papers mainly focused on ICT for computation, algorithms and data analytics, and IT security.

The book provides insights into International Conference on Smart Innovations in Communications and Computational Sciences (ICSICCS 2017) held at North West Group of Institutions, Punjab, India. It presents new advances and research results in the fields of computer and communication written by leading researchers, engineers and scientists in the domain of interest from around the world. The book includes research work in all the areas of smart innovation, systems and technologies, embedded knowledge and intelligence, innovation and sustainability, advance computing, networking and informatics. It also focuses on the knowledge-transfer methodologies and innovation strategies employed to make this happen effectively. The combination of intelligent systems tools and a broad range of applications introduce a need for a synergy of disciplines from science and technology. Sample areas include, but are not limited to smart hardware, software design, smart computing technologies, intelligent communications and networking, web and informatics and computational sciences.

Mobile devices, such as smart phones, have achieved computing and networking capabilities comparable to traditional personal computers. Their successful consumerization has also become a source of pain for adopting users and organizations. In particular, the widespread presence of information-stealing applications and other types of mobile malware raises substantial security and privacy concerns. Android Malware presents a systematic view on state-of-the-art mobile malware that targets the popular Android mobile platform. Covering key topics like the Android malware history, malware behavior and classification, as well as, possible defense techniques.

This book constitutes the thoroughly refereed post-conference proceedings of the 8th International Conference on Wireless Internet, WICON 2014, held in Lisbon, Portugal, in November 2014. The 45 revised full papers were carefully reviewed and selected from numerous submissions. The papers cover topics such as 5G mobile communications, Internet of Things (IoT), super Wi-Fi and V2V/V21.

Maritime Supply Chains breaks the maritime chain into components, consistently relating them to the overall integrated supply chain. The book not only analyzes and provides solutions to frequently encountered problems and key operational issues, it also applies cutting-edge scientific techniques on the maritime supply chain. Sections consider shipping, ports and terminals, hinterland and the issues that intersect different parts of the chain. Readers will find discussions of the various actors at play and how they relate to the overall function of the supply chain. Finally, the book offers solutions to the most pressing problems, thus providing a unique, well-balanced account.

This book constitutes the refereed proceedings of the 24th Nordic Conference on Secure IT Systems, NordSec 2019, held in Aalborg, Denmark, in November 2019. The 17 full papers presented in this volume were carefully reviewed and selected from 32 submissions. They are organized in topical sections named: privacy; network security;

platform security and malware; and system and software security.

This book presents the latest trends in attacks and protection methods of Critical Infrastructures. It describes original research models and applied solutions for protecting major emerging threats in Critical Infrastructures and their underlying networks. It presents a number of emerging endeavors, from newly adopted technical expertise in industrial security to efficient modeling and implementation of attacks and relevant security measures in industrial control systems; including advancements in hardware and services security, interdependency networks, risk analysis, and control systems security along with their underlying protocols. Novel attacks against Critical Infrastructures (CI) demand novel security solutions. Simply adding more of what is done already (e.g. more thorough risk assessments, more expensive Intrusion Prevention/Detection Systems, more efficient firewalls, etc.) is simply not enough against threats and attacks that seem to have evolved beyond modern analyses and protection methods. The knowledge presented here will help Critical Infrastructure authorities, security officers, Industrial Control Systems (ICS) personnel and relevant researchers to (i) get acquainted with advancements in the field, (ii) integrate security research into their industrial or research work, (iii) evolve current practices in modeling and analyzing Critical Infrastructures, and (iv) moderate potential crises and emergencies influencing or emerging from Critical Infrastructures.

This book constitutes the proceedings of the 16th International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment, DIMVA 2019, held in Gothenburg, Sweden, in June 2019. The 23 full papers presented in this volume were carefully reviewed and selected from 80 submissions. The contributions were organized in topical sections named: wild wild web; cyber-physical systems; malware; software security and binary analysis; network security; and attack mitigation.

This volume constitutes the refereed proceedings of the 4th IFIP WG 11.2 International Workshop on Information Security Theory and Practices: Security and Privacy of Pervasive Systems and Smart Devices, WISTP 2010, held in Passau, Germany, in April 2010. The 20 revised full papers and 10 short papers were carefully reviewed and selected from 69 submissions. They are organized in topical sections on embedded security, protocols, highly constrained embedded systems, security, smart card security, algorithms, hardware implementations, embedded systems and anonymity/database security.

Networking for Big Data supplies an unprecedented look at cutting-edge research on the networking and communication aspects of Big Data. Starting with a comprehensive introduction to Big Data and its networking issues, it offers deep technical coverage of both theory and applications. The book is divided into four sections: introduction to Big Data, networking theory and design for Big Data, networking security for Big Data, and platforms and systems for Big Data applications. Focusing on key networking issues in Big Data, the book explains network design and implementation for Big Data. It examines how network topology impacts data collection and explores Big Data storage and resource management. Addresses the virtual machine placement problem Describes

widespread network and information security technologies for Big Data Explores network configuration and flow scheduling for Big Data applications Presents a systematic set of techniques that optimize throughput and improve bandwidth for efficient Big Data transfer on the Internet Tackles the trade-off problem between energy efficiency and service resiliency The book covers distributed Big Data storage and retrieval as well as security, trust, and privacy protection for Big Data collection, storage, and search. It discusses the use of cloud infrastructures and highlights its benefits to overcome the identified issues and to provide new approaches for managing huge volumes of heterogeneous data. The text concludes by proposing an innovative user data profile-aware policy-based network management framework that can help you exploit and differentiate user data profiles to achieve better power efficiency and optimized resource management.

This timely text presents a comprehensive overview of fault tolerance techniques for high-performance computing (HPC). The text opens with a detailed introduction to the concepts of checkpoint protocols and scheduling algorithms, prediction, replication, silent error detection and correction, together with some application-specific techniques such as ABFT. Emphasis is placed on analytical performance models. This is then followed by a review of general-purpose techniques, including several checkpoint and rollback recovery protocols. Relevant execution scenarios are also evaluated and compared through quantitative models. Features: provides a survey of resilience methods and performance models; examines the various sources for errors and faults in large-scale systems; reviews the spectrum of techniques that can be applied to design a fault-tolerant MPI; investigates different approaches to replication; discusses the challenge of energy consumption of fault-tolerance methods in extreme-scale systems.

Planning is a critical stage of radiotherapy. Careful consideration of the complex variables involved and critical assessment of the techniques available are fundamental to good and effective practice. First published in 1985, Practical Radiotherapy Planning has, over three editions, established itself as the popular choice for the trainee raditation oncologist and radiographer, providing the 'nuts and bolts' of planning in a practical and accessible manner. This fourth edition encompasses a wealth of new material, reflecting the radical change in the practice of radiotherapy in recent years. The information contained within the introductory chapters has been expanded and brought up to date, and a new chapter on patient management has been added. CT stimulators, MLC shieldings and dose profiles, principles of IMRT, and use of MRI, PET and ultrasound are all included, amongst other new developments in this field. The aim of the book remains unchanged. Complexity of treatment planning has increased greatly, but the fourth edition continues to emphasise underlying principles of treatment that can be applied for conventional, conformal and novel treatments, taking into account advances in imaging and treatment delivery.

The two-volume set, LNCS 11098 and LNCS 11099 constitutes the refereed proceedings of the 23nd European Symposium on Research in Computer Security, ESORICS 2018, held in Barcelona, Spain, in September 2018. The 56 revised full papers presented were carefully reviewed and selected from 283 submissions. The papers address issues such as software security, blockchain and machine learning, hardware security, attacks, malware and vulnerabilities, protocol security, privacy, CPS and IoT security, mobile security, database and web security, cloud security, applied crypto, multi-party computation, SDN security.

This Festschrift is in honor of Sushil Jajodia, Professor in the George Mason University, USA, on the occasion of his 70th birthday. This book contains papers written in honor of Sushil Jajodia, of his vision and his achievements. Sushil has sustained a highly active research agenda spanning several important areas in computer security and privacy, and established himself as a leader in the security research community through unique scholarship and service. He has extraordinarily impacted the scientific and academic community, opening and pioneering new directions of research, and significantly influencing the research and development of security solutions worldwide. Also, his excellent record of research funding shows his commitment to sponsored research and the practical impact of his work. The research areas presented in this Festschrift include membrane computing, spiking neural networks, phylogenetic networks, ant colonies optimization, work bench for bio-computing, reaction systems, entropy of computation, rewriting systems, and insertion-deletion systems.

This book constitutes the refereed proceedings of the 15th International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment, DIMVA 2018, held in Saclay, France, in June 2018. The 17 revised full papers and 1 short paper included in this book were carefully reviewed and selected from 59 submissions. They present topics such as malware analysis; mobile and embedded security; attacks; detection and containment; web and browser security; and reverse engineering.

This handbook provides comprehensive knowledge and includes an overview of the current state-of-the-art of Big Data Privacy, with chapters written by international world leaders from academia and industry working in this field. The first part of this book offers a review of security challenges in critical infrastructure and offers methods that utilize acritical intelligence (AI) techniques to overcome those issues. It then focuses on big data security and privacy issues in relation to developments in the Industry 4.0. Internet of Things (IoT) devices are becoming a major source of security and privacy concern in big data platforms. Multiple solutions that leverage machine learning for addressing security and privacy issues in IoT environments are also discussed this handbook. The second part of this handbook is focused on privacy and security issues in different layers of big data systems. It discusses about methods for evaluating security and privacy of big data systems on network, application and physical layers. This handbook elaborates on existing methods to use data analytic and AI techniques at different layers of big data platforms to identify privacy and security attacks. The final part of this handbook is focused on analyzing cyber threats applicable to the big data environments. It offers an in-depth review of attacks applicable to big data platforms in smart grids, smart

farming, FinTech, and health sectors. Multiple solutions are presented to detect, prevent and analyze cyber-attacks and assess the impact of malicious payloads to those environments. This handbook provides information for security and privacy experts in most areas of big data including; FinTech, Industry 4.0, Internet of Things, Smart Grids, Smart Farming and more. Experts working in big data, privacy, security, forensics, malware analysis, machine learning and data analysts will find this handbook useful as a reference. Researchers and advanced-level computer science students focused on computer systems, Internet of Things, Smart Grid, Smart Farming, Industry 4.0 and network analysts will also find this handbook useful as a reference.

This book introduces fundamental concepts of cyber resilience, drawing expertise from academia, industry, and government. Resilience is defined as the ability to recover from or easily adjust to shocks and stresses. Unlike the concept of security - which is often and incorrectly conflated with resilience -- resilience refers to the system's ability to recover or regenerate its performance after an unexpected impact produces a degradation in its performance. A clear understanding of distinction between security, risk and resilience is important for developing appropriate management of cyber threats. The book presents insightful discussion of the most current technical issues in cyber resilience, along with relevant methods and procedures. Practical aspects of current cyber resilience practices and techniques are described as they are now, and as they are likely to remain in the near term. The bulk of the material is presented in the book in a way that is easily accessible to non-specialists. Logical, consistent, and continuous discourse covering all key topics relevant to the field will be of use as teaching material as well as source of emerging scholarship in the field. A typical chapter provides introductory, tutorial-like material, detailed examples, in-depth elaboration of a selected technical approach, and a concise summary of key ideas.

The guide that helps students study faster, learn better, and get top grades More than 40 million students have trusted Schaum's to help them study faster, learn better, and get top grades. Now Schaum's is better than ever-with a new look, a new format with hundreds of practice problems, and completely updated information to conform to the latest developments in every field of study. Fully compatible with your classroom text, Schaum's highlights all the important facts you need to know. Use Schaum's to shorten your study time-and get your best test scores! Schaum's Outlines-Problem Solved.

An info. security assessment (ISA) is the process of determining how effectively an entity being assessed (e.g., host, system, network, procedure, person) meets specific security objectives. This is a guide to the basic tech. aspects of conducting ISA. It presents tech. testing and examination methods and techniques that an org. might use as part of an ISA, and offers insights to assessors on their execution and the potential impact they may have on systems and networks. For an ISA to be successful, elements beyond the execution of testing and examination must support the tech. process. Suggestions for these activities ¿ including a robust planning process, root cause analysis, and tailored reporting ¿ are also presented in this guide. Illus.

This book includes high impact papers presented at the International Conference on Communication, Computing and Electronics Systems 2019, held at the PPG Institute of Technology, Coimbatore, India, on 15-16 November, 2019. Discussing recent trends in cloud computing, mobile computing, and advancements of electronics systems, the book covers topics such as automation, VLSI, embedded systems, integrated device technology, satellite communication, optical communication, RF communication, microwave engineering, artificial intelligence, deep learning, pattern recognition, Internet of Things, precision models, bioinformatics, and healthcare informatics.

As human activities moved to the digital domain, so did all the well-known malicious behaviors including fraud, theft, and other trickery. There is no silver bullet, and each security threat calls

for a specific answer. One specific threat is that applications accept malformed inputs, and in many cases it is possible to craft inputs that let an intruder take full control over the target computer system. The nature of systems programming languages lies at the heart of the problem. Rather than rewriting decades of well-tested functionality, this book examines ways to live with the (programming) sins of the past while shoring up security in the most efficient manner possible. We explore a range of different options, each making significant progress towards securing legacy programs from malicious inputs. The solutions explored include enforcement-type defenses, which excludes certain program executions because they never arise during normal operation. Another strand explores the idea of presenting adversaries with a moving target that unpredictably changes its attack surface thanks to randomization. We also cover tandem execution ideas where the compromise of one executing clone causes it to diverge from another thus revealing adversarial activities. The main purpose of this book is to provide readers with some of the most influential works on run-time exploits and defenses. We hope that the material in this book will inspire readers and generate new ideas and paradigms.