White Paper Wannacry Ransomware Analysis

This book concentrates on a wide range of advances related to IT cybersecurity management. The topics covered in this book include, among others, management techniques in security, IT risk management, the impact of technologies and techniques on security management, regulatory techniques and issues, surveillance technologies, security policies, security for protocol management, location management, GOS management, resource management, channel management, and mobility management. The authors also discuss digital contents copyright protection, system security management, network security

management, security management in network equipment, storage area networks (SAN) management, information security management, government security policy, web penetration testing, security operations, and vulnerabilities management. The authors introduce the concepts, techniques, methods, approaches and trends needed by cybersecurity management specialists and educators for keeping current their cybersecurity management knowledge. Further, they provide a glimpse of future directions where cybersecurity management techniques, policies, applications, and theories are headed. The book is a rich collection of carefully selected and reviewed manuscripts written by diverse cybersecurity management experts in the listed fields and edited

by prominent cybersecurity management researchers and specialists.

The new edition of the highly influential Tallinn Manual, which outlines public international law as it applies to cyber operations.

Your one-stop guide to know digital extortion and it's prevention. Key Features A complete guide to how ransomware works Build a security mechanism to prevent digital extortion. A practical approach to knowing about, and responding to, ransomware. Book Description Ransomware has turned out to be the most aggressive malware and has affected numerous organizations in the recent past. The current need is to have a defensive mechanism in place for workstations and servers under one organization. This book starts by explaining the

basics of malware, specifically ransomware. The book provides some quick tips on malware analysis and how you can identify different kinds of malware. We will also take a look at different types of ransomware, and how it reaches your system, spreads in your organization, and hijacks your computer. We will then move on to how the ransom is paid and the negative effects of doing so. You will learn how to respond quickly to ransomware attacks and how to protect yourself. The book gives a brief overview of the internals of security software and Windows features that can be helpful in ransomware prevention for administrators. You will also look at practical use cases in each stage of the ransomware phenomenon. The book talks in detail about the latest ransomware attacks

involving WannaCry, Petya, and BadRabbit. By the end of this book, you will have end-to-end knowledge of the trending malware in the tech industry at present. What you will learn Understand malware types and malware techniques with examples Obtain a quick malware analysis Understand ransomware techniques, their distribution, and their payment mechanism Case studies of famous ransomware attacks Discover detection technologies for complex malware and ransomware Configure security software to protect against ransomware Handle ransomware infections Who this book is for This book is targeted towards security administrator, security analysts, or any stakeholders in the security sector who want to learn about the most trending malware in the current market:

ransomware.

This book constitutes the proceedings of the First International Conference on Science of Cyber Security, SciSec 2018, held in Beijing, China, in August 2018. The 11 full papers and 6 short papers presented in this volume were carefully reviewed and selected from 54 submissions. The papers focus on science of security; cybersecurity dynamics; attacks and defenses; network security; security metrics and measurements; and performance enhancements.

A Law Enforcement Practitioner ' s Perspective

With Forewords by Robert M. Lee and Tom Gilb

8th International Conference, SKM 2019, Goa, India, December 21–22, 2019, Proceedings

National Audit Office. Department of

Health; Investigation
Applications of Evolutionary Computation
New Dimensions of Information Warfare
This publication highlights the fast-moving technological advancement and infiltration of Artificial Intelligence into society. Concepts of evolution of society through interconnectivity are explored, together with how the fusion of human and technological interaction leading to Augmented Humanity is fast becoming more than just an endemic phase, but a cultural phase shift to digital societies. It aims to balance both the positive progressive outlooks such

developments bring with potential issues that may stem from innovation of this kind, such as the invasive procedures of bio hacking or ethical connotations concerning the usage of digital twins. This publication will also give the reader a good level of understanding on fundamental cyber defence principles, interactions with Critical National Infrastructure (CNI) and the Command, Control, Communications and Intelligence (C3I) decision-making framework. A detailed view of the cyber-attack landscape will be garnered; touching on the tactics,

techniques and procedures used, red and blue teaming initiatives, cyber resilience and the protection of larger scale systems. The integration of AI, smart societies, the human-centric approach and Augmented Humanity is discernible in the exponential growth, collection and use of [big] data; concepts woven throughout the diversity of topics covered in this publication; which also discusses the privacy and transparency of data ownership, and the potential dangers of exploitation through social media. As humans are become ever more interconnected, with the prolificacy of smart wearable

devices and wearable body area networks, the availability of and abundance of user data and metadata derived from individuals has grown exponentially. The notion of data ownership, privacy and situational awareness are now at the forefront in this new age. In today's modernized market, many fields are utilizing internet technologies in their everyday methods of operation. The industrial sector is no different as these technological solutions have provided several benefits including reduction of costs, scalability, and efficiency improvements. Despite this, cyber security remains a crucial

risk factor in industrial control systems. The same public and corporate solutions do not apply to this specific district because these security issues are more complex and intensive. Research is needed that explores new risk assessment methods and security mechanisms that professionals can apply to their modern technological procedures. Cyber Security of Industrial Control Systems in the Future Internet Environment is a pivotal reference source that provides vital research on current security risks in critical infrastructure schemes with the implementation of information and communication

technologies. While highlighting topics such as intrusion detection systems, forensic challenges, and smart grids, this publication explores specific security solutions within industrial sectors that have begun applying internet technologies to their current methods of operation. This book is ideally designed for researchers, system engineers, managers, networkers, IT professionals, analysts, academicians, and students seeking a better understanding of the key issues within securing industrial control systems that utilize internet technologies. This book presents high-quality

research on the concepts and developments in the field of information and communication technologies, and their applications. It features 134 rigorously selected papers (including 10 poster papers) from the Future of Information and Communication Conference 2020 (FICC 2020), held in San Francisco, USA, from March 5 to 6, 2020, addressing state-of-the-art intelligent methods and techniques for solving real-world problems along with a vision of future research Discussing various aspects of communication, data science, ambient intelligence, networking, computing, security and Internet

of Things, the book offers researchers, scientists, industrial engineers and students valuable insights into the current research and next generation information science and communication technologies.

This book revises the strategic objectives of Information Warfare, interpreting them according to the modern canons of information age, focusing on the fabric of society, the economy, and critical Infrastructures. The authors build plausible detailed real-world scenarios for each entity, showing the related possible threats from the Information Warfare point of view. In

addition, the authors dive into the description of the still open problems, especially when it comes to critical infrastructures, and the countermeasures that can be implemented, possibly inspiring further research in the domain. This book intends to provide a conceptual framework and a methodological guide, enriched with vivid and compelling use cases for the readers (e.g. technologists, academicians, military, government) interested in what Information Warfare really means, when its lenses are applied to current technology. Without sacrificing accuracy, rigor and, most importantly, the

big picture of Information Warfare, this book dives into several relevant and up-to-date critical domains. The authors illustrate how finance (an always green target of Information Warfare) is intertwined with Social Media, and how an opponent could exploit these latter ones to reach its objectives. Also, how cryptocurrencies are going to reshape the economy, and the risks involved by this paradigm shift. Even more compelling is how the very fabric of society is going to be reshaped by technology, for instance how our democratic elections are exposed to risks that are even

greater than what appears in the current public discussions. Not to mention how our Critical Infrastructure is becoming exposed to a series of novel threats, ranging from state-supported malware to drones. A detailed discussion of possible countermeasures and what the open issues are for each of the highlighted threats complete this book. This book targets a widespread audience that includes researchers and advanced level students studying and working in computer science with a focus on security. Military officers, government officials and professionals working in this

field will also find this book useful as a reference.

Preventing Ransomware

15th International Annual Conference, CNCERT 2018, Beijing, China, August 14-16, 2018, Revised Selected Papers

Security and Organization within IoT and Smart Cities

Explore the concepts, tools, and techniques to analyze and investigate Windows malware

WannaCry Cyber Attack and the NHS

Ransomware Revealed

This book constitutes the refereed proceedings of the 8th International Conference On Secure Knowledge Management In Artificial Intelligence Era, SKM 2019, held in Goa, India, in

December 2019. The 12 full papers presented were carefully reviewed and selected from 34 submissions. They were organized according to the following topical sections: cyber security; security and artifcial intelligence; access control models; and social networks.

This book examines the requirements, risks, and solutions to improve the security and quality of complex cyber-physical systems (C-CPS), such as production systems, power plants, and airplanes, in order to ascertain whether it is possible to protect engineering organizations against cyber threats and to ensure engineering project quality. The book consists of three parts that logically build upon each other. Part I "Product Engineering of Complex

Cyber-Physical Systems" discusses the structure and behavior of engineering organizations producing complex cyber-physical systems, providing insights into processes and engineering activities, and highlighting the requirements and border conditions for secure and high-quality engineering. Part II "Engineering Quality Improvement" addresses quality improvements with a focus on engineering data generation, exchange, aggregation, and use within an engineering organization, and the need for proper data modeling and engineering-result validation. Lastly, Part III "Engineering Security Improvement" considers security aspects concerning C-CPS engineering, including engineering organizations ' security assessments and engineering

data management, security concepts and technologies that may be leveraged to mitigate the manipulation of engineering data, as well as design and run-time aspects of secure complex cyber-physical systems. The book is intended for several target groups: it enables computer scientists to identify research issues related to the development of new methods, architectures, and technologies for improving quality and security in multi-disciplinary engineering, pushing forward the current state of the art. It also allows researchers involved in the engineering of C-CPS to gain a better understanding of the challenges and requirements of multi-disciplinary engineering that will guide them in their future research and development

activities. Lastly, it offers practicing engineers and managers with engineering backgrounds insights into the benefits and limitations of applicable methods, architectures, and technologies for selected use cases.
This book focuses on how advances in ICT have brought about a sea change in the way people work, live and share while also making them vulnerable. These advances exhibit a fundamentally reformed global context for development that has not just been restricted to the civilian domain but has simultaneously impacted the military domain. The exponential pace of advances in the field of Artificial Intelligence (AI), robotics, big data, quantum computing or IoT (Internet of Things) pioneers a significantly

different vision of work and society. The current trends in warfighting present a very blurred picture of the future operating environment, but they give some shape to its likely direction. Military forces are trying to become much more flexible and have been adapting to these changes while emphasizing the importance of innovation and improvisation in order to counter challenges emanating from future scenarios. In this context, the book highlights the changing military strategies and tactics across nations vis-à-vis the hanging and emerging ICT technologies. It also highlights the importance of looking at present institutions, legal frameworks and principles as well as at the restraining factors inherent in realpolitik in order

to understand if nation states are ready. Please note: Taylor & Francis does not sell or distribute the Hardback in India, Pakistan, Nepal, Bhutan, Bangladesh and Sri Lanka

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.

Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations

Cyber and Digital Forensic Investigations

5th International Conference, ICAIS 2019, New York, NY, USA, July 26 – 28, 2019, Proceedings, Part IV

An Artificial Intelligence Approach

Artificial Intelligence and Security

The Ethics of Cybersecurity

Malware analysis is big business, and attacks can cost a company dearly. When malware breaches your defenses, you need to act quickly to cure current infections and prevent future ones from occurring. For those who want to stay ahead of the latest malware,

Practical Malware Analysis will teach you the tools and techniques used by professional analysts. With this book as your guide, you'll be able to safely analyze, debug, and disassemble any malicious software that comes your way. You'll learn how to: – Set up a safe virtual environment to analyze malware – Quickly extract network signatures and host-based indicators – Use key analysis tools like IDA Pro, OllyDbg, and WinDbg – Overcome malware tricks like obfuscation, anti-disassembly, anti-debugging, and anti-virtual machine techniques – Use your newfound knowledge of Windows internals for malware analysis – Develop a methodology for unpacking malware and get practical experience with five of

the most popular packers – Analyze special cases of malware with shellcode, C++, and 64-bit code Hands-on labs throughout the book challenge you to practice and synthesize your skills as you dissect real malware samples, and pages of detailed dissections offer an over-the-shoulder look at how the pros do it. You'll learn how to crack open malware to see how it really works, determine what damage it has done, thoroughly clean your network, and ensure that the malware never comes back. Malware analysis is a cat-and-mouse game with rules that are constantly changing, so make sure you have the fundamentals. Whether you're tasked with securing one network or a thousand networks, or you're

making a living as a malware analyst, you'll find what you need to succeed in Practical Malware Analysis.

Understanding the latest capabilities in the cyber threat landscape as well as the cyber forensic challenges and approaches is the best way users and organizations can prepare for potential negative events. Adopting an experiential learning approach, this book describes how cyber forensics researchers, educators and practitioners can keep pace with technological advances, and acquire the essential knowledge and skills, ranging from IoT forensics, malware analysis, and CCTV and cloud forensics to network forensics and financial investigations. Given the growing

importance of incident response and cyber forensics in our digitalized society, this book will be of interest and relevance to researchers, educators and practitioners in the field, as well as students wanting to learn about cyber forensics.

Global events involving cybersecurity breaches have highlighted the ever-growing dependence on interconnected online systems in international business. The increasing societal dependence on information technology has pushed cybersecurity to the forefront as one of the most urgent challenges facing the global community today. Poor cybersecurity is the primary reason hackers are able to penetrate safeguards in business

computers and other networks, and the growing global skills gap in cybersecurity simply exacerbates the problem. Global Cyber Security Labor Shortage and International Business Risk provides emerging research exploring the theoretical and practical aspects of protecting computer systems against online threats as well as transformative business models to ensure sustainability and longevity. Featuring coverage on a broad range of topics such as cybercrime, technology security training, and labor market understanding, this book is ideally designed for professionals, managers, IT consultants, programmers, academicians, and students seeking current research on cyber security ' s influence on

business, education, and social networks.

The rate of cybercrimes is increasing because of the fast-paced advancements in computer and internet technology. Crimes employing mobile devices, data embedding/mining systems, computers, network communications, or any malware impose a huge threat to data security. Countering Cyber Attacks and Preserving the Integrity and Availability of Critical Systems addresses current problems and issues emerging in cyber forensics and investigations and proposes new solutions that can be adopted and implemented to counter security breaches within various organizations. The publication examines a variety of

topics such as advanced techniques for forensic developments in computer and communication-link environments and legal perspectives including procedures for cyber investigations, standards, and policies. It is designed for policymakers, forensic analysts, technology developers, security administrators, academicians, researchers, and students.

Detection of Intrusions and Malware, and Vulnerability Assessment

Cyber Security of Industrial Control Systems in the Future Internet Environment

Intelligent Computing & Optimization

Protecting Your Company and Society

Secure Knowledge Management In Artificial Intelligence Era

First International Conference, ISDDC 2017, Vancouver, BC, Canada, October 26-28, 2017, Proceedings

The non-technical handbook for cyber security risk management Solving Cyber Risk distills a decade of research into a practical framework for cyber security. Blending statistical data and cost information with research into the culture, psychology, and business models of the hacker community, this book provides business executives, policy-makers,

and individuals with a deeper understanding of existing future threats, and an action plan for safeguarding their organizations. Key Risk Indicators reveal vulnerabilities based on organization type, IT infrastructure and existing security measures, while expert discussion from leading cyber risk specialists details practical, real-world methods of risk reduction and mitigation. By the nature of the business, your organization's customer

database is packed with highly sensitive information that is essentially hacker-bait, and even a minor flaw in security protocol could spell disaster. This book takes you deep into the cyber threat landscape to show you how to keep your data secure. Understand who is carrying out cyber-attacks, and why Identify your organization's risk of attack and vulnerability to damage Learn the most cost-effective risk reduction measures Adopt a new cyber risk assessment and

quantification framework based on techniques used by the insurance industry By applying risk management principles to cyber security, non-technical leadership gains a greater understanding of the types of threat, level of threat, and level of investment needed to fortify the organization against attack. Just because you have not been hit does not mean your data is safe, and hackers rely on their targets' complacence to help maximize their haul. Solving Cyber Risk gives

you a concrete action plan for implementing top-notch preventative measures before you're forced to implement damage control. This collection explores organized crime and terror networks and the points at which they intersect. It analyses the close relationships between these criminalities, the prevalence and ambiguity of this nexus, the technological elements facilitating it, and the financial aspects embedded in this criminal partnership. Organized Crime and Terrorist

Networks is the outcome of empirical research, seminars, workshops and interviews carried out by a multinational consortium of researchers within 'TAKEDOWN', a Horizon 2020 project funded by the European Commission. The consortium's objective was to examine the perspectives, requirements and misgivings of front-line practitioners operating in the areas of organized crime and terrorism. The chapters collected in this volume are the outcome of such analytical efforts. The

topics addressed include the role of Information and Communication Technology in contemporary criminal organizations, terrorism financing, online transnational criminality, identity crime, the crime-terror nexus and tackling the nexus at supranational level. This book offers a compelling contribution to scholarship on organized crime and terrorism, and considers possible directions for future research. It will be of much interest to students and researchers engaged in

studies of criminology, criminal justice, crime control and prevention, organized crime, terrorism, political violence, and cybercrime. This book aims to provide the latest research developments and results in the domain of AI techniques for smart cyber ecosystems. It presents a holistic insight into AI-enabled theoretic approaches and methodology in IoT networking, security analytics using AI tools and network automation, which ultimately enable

intelligent cyber space. This book will be a valuable resource for students, researchers, engineers and policy makers working in various areas related to cybersecurity and privacy for Smart Cities. This book includes chapters titled "An Overview of the Artificial Intelligence Evolution and Its Fundamental Concepts, and Their Relationship with IoT Security", "Smart City: Evolution and Fundamental Concepts", "Advances in AI-Based Security for Internet of

Things in Wireless Virtualization Environment", "A Conceptual Model for Optimal Resource Sharing of Networked Microgrids Focusing Uncertainty: Paving Path to Eco-friendly Smart Cities", "A Novel Framework for a Cyber Secure Smart City", "Contemplating Security Challenges and Threats for Smart Cities", "Self-Monitoring Obfuscated IoT Network", "Introduction to Side Channel Attacks and Investigation of Power Analysis and Fault Injection Attack

Techniques", "Collaborative Digital Forensic Investigations Model for Law Enforcement: Oman as a Case Study", "Understanding Security Requirements and Challenges in the Industrial Internet of Things: A Review", "5G Security and the Internet of Things", "The Problem of Deepfake Videos and How to Counteract Them in Smart Cities", "The Rise of Ransomware Aided by Vulnerable IoT Devices", "Security Issues in Self-Driving Cars within Smart Cities", and "Trust-Aware

Crowd Associated Network-Based Approach for Optimal Waste Management in Smart Cities". This book provides state-of-the-art research results and discusses current issues, challenges, solutions and recent trends related to security and organization within IoT and Smart Cities. We expect this book to be of significant importance not only to researchers and practitioners in academia, government agencies and industries, but also for policy makers and system managers. We anticipate

this book to be a valuable resource for all those working in this new and exciting area, and a "must have" for all university libraries.
Translational Bioinformatics in Healthcare and Medicine offers an overview of main principles of bioinformatics, biological databases, clinical informatics, health informatics, viroinformatics and real-case applications of translational bioinformatics in healthcare. Written by

experts from both technology and clinical sides, the content brings together essential knowledge to make the best of recent advancements of the field. The book discusses topics such as next generation sequence analysis, genomics in clinical care, IoT applications, blockchain technology, patient centered interoperability of EHR, health data mining, and translational bioinformatics methods for drug discovery and drug repurposing. In addition, it discusses the role of

bioinformatics in cancer research and viroinformatics approaches to counter viral diseases through informatics. This is a valuable resource for bioinformaticians, clinicians, healthcare professionals, graduate students and several members of biomedical field who are interested in learning more about how bioinformatics can impact in their research and practice. Covers recent advancements in translational bioinformatics and its healthcare applications

Discusses integrative and multidisciplinary approaches to U-healthcare systems development and management Bridges the gap among various knowledge domains in the field, integrating both technological and clinical knowledge into practical content

Cyber Defence in the Age of AI, Smart Societies and Augmented Humanity

Advances in Computing and Data Sciences

IoT

Cybersecurity Issues in Emerging Technologies

Security and Quality in

Cyber-Physical Systems Engineering

Intelligent, Secure, and Dependable Systems in Distributed and Cloud Environments

The 4-volume set LNCS 11632 until LNCS 11635 constitutes the refereed proceedings of the 5th International Conference on Artificial Intelligence and Security, ICAIS 2019, which was held in New York, USA, in July 2019. The conference was formerly called "International Conference on Cloud Computing and Security" with the acronym ICCCS. The total of 230 full papers presented in this 4-volume proceedings was carefully reviewed and selected

from 1529 submissions. The papers were organized in topical sections as follows: Part I: cloud computing; Part II: artificial intelligence; big data; and cloud computing and security; Part III: cloud computing and security; information hiding; IoT security; multimedia forensics; and encryption and cybersecurity; Part IV: encryption and cybersecurity.

There is little doubt that cyber-space has become the battle space for confrontations. However, to conduct cyber operations, a new armory of weapons needs to be employed. No matter how many, or how sophisticated an aggressor's kinetic weapons are, they are useless in cyber-space. This book

looks at the milieu of the cyber weapons industry, as well as the belligerents who use cyber weapons. It discusses what distinguishes these hardware devices and software programs from computer science in general. It does this by focusing on specific aspects of the topic—contextual issues of why cyber-space is the new battleground, defensive cyber weapons, offensive cyber weapons, dual-use weapons, and the implications these weapons systems have for practice. Contrary to popular opinion, the use of cyber weapons is not limited to nation states; though this is where the bulk of news reporting focuses. The reality is that there isn't a sector of the

political-economy that is immune to cyber skirmishes. So, this book looks at cyber weapons not only by national security agencies and the military, but also by law enforcement, and the business sector—the latter includes administrations termed non-government organisations (NGOs). This book offers study material suitable for a wide-ranging audience—students, professionals, researchers, policy officers, and ICT specialists.
IOT: Security and Privacy Paradigm covers the evolution of security and privacy issues in the Internet of Things (IoT). It focuses on bringing all security and privacy related technologies into one source, so that students, researchers, and practitioners

can refer to this book for easy understanding of IoT security and privacy issues. This edited book uses Security Engineering and Privacy-by-Design principles to design a secure IoT ecosystem and to implement cyber-security solutions. This book takes the readers on a journey that begins with understanding the security issues in IoT-enabled technologies and how it can be applied in various aspects. It walks readers through engaging with security challenges and builds a safe infrastructure for IoT devices. The book helps readers gain an understand of security architecture through IoT and describes the state of the art of IoT countermeasures. It also differentiates security threats in

IoT-enabled infrastructure from traditional ad hoc or infrastructural networks, and provides a comprehensive discussion on the security challenges and solutions in RFID, WSNs, in IoT. This book aims to provide the concepts of related technologies and novel findings of the researchers through its chapter organization. The primary audience includes specialists, researchers, graduate students, designers, experts and engineers who are focused on research and security related issues. Souvik Pal, PhD, has worked as Assistant Professor in Nalanda Institute of Technology, Bhubaneswar, and JIS College of Engineering, Kolkata (NAAC "A" Accredited College). He is the

organizing Chair and Plenary Speaker of RICE Conference in Vietnam; and organizing co-convener of ICICIT, Tunisia. He has served in many conferences as chair, keynote speaker, and he also chaired international conference sessions and presented session talks internationally. His research area includes Cloud Computing, Big Data, Wireless Sensor Network (WSN), Internet of Things, and Data Analytics. Vicente García-Díaz, PhD, is an Associate Professor in the Department of Computer Science at the University of Oviedo (Languages and Computer Systems area). He is also the editor of several special issues in prestigious journals such as Scientific

Programming and International Journal of Interactive Multimedia and Artificial Intelligence. His research interests include eLearning, machine learning and the use of domain specific languages in different areas. Dac-Nhuong Le, PhD, is Deputy-Head of Faculty of Information Technology, and Vice-Director of Information Technology Apply and Foreign Language Training Center, Haiphong University, Vietnam. His area of research includes: evaluation computing and approximate algorithms, network communication, security and vulnerability, network performance analysis and simulation, cloud computing, IoT and image processing in biomedical. Presently, he is

serving on the editorial board of several international journals and has authored nine computer science books published by Springer, Wiley, CRC Press, Lambert Publication, and Scholar Press.

The result of a three-year project, this manual addresses the entire spectrum of international legal issues raised by cyber warfare.

Solving Cyber Risk

Translational Bioinformatics in Healthcare and Medicine

Third International Conference, ICACDS 2019, Ghaziabad, India, April 12–13, 2019, Revised Selected Papers, Part II

Proceedings of the 2020 Future of Information and Communication Conference (FICC), Volume 1

Cybercrimes et enjeux technologiques - Contexte et perspectives

Cyber Security

This open access book provides the first comprehensive collection of papers that provide an integrative view on cybersecurity. It discusses theories, problems and solutions on the relevant ethical issues involved. This work is sorely needed in a world where cybersecurity has become indispensable to protect trust and confidence in the digital infrastructure whilst respecting fundamental values like equality, fairness, freedom, or privacy. The book has a strong practical focus

as it includes case studies outlining ethical issues in cybersecurity and presenting guidelines and other measures to tackle those issues. It is thus not only relevant for academics but also for practitioners in cybersecurity such as providers of security software, governmental CERTs or Chief Security Officers in companies. Understand malware analysis and its practical implementation Key Features Explore the key concepts of malware analysis and memory forensics using real-world examples Learn the art of detecting, analyzing, and investigating malware threats

Understand adversary tactics and techniques Book Description Malware analysis and memory forensics are powerful analysis and investigation techniques used in reverse engineering, digital forensics, and incident response. With adversaries becoming sophisticated and carrying out advanced malware attacks on critical infrastructures, data centers, and private and public organizations, detecting, responding to, and investigating such intrusions is critical to information security professionals. Malware analysis and memory forensics have become must-have skills to fight

advanced malware, targeted attacks, and security breaches. This book teaches you the concepts, techniques, and tools to understand the behavior and characteristics of malware through malware analysis. It also teaches you techniques to investigate and hunt malware using memory forensics. This book introduces you to the basics of malware analysis, and then gradually progresses into the more advanced concepts of code analysis and memory forensics. It uses real-world malware samples, infected memory images, and visual diagrams to help you gain a better

understanding of the subject and to equip you with the skills required to analyze, investigate, and respond to malware-related incidents. What you will learn Create a safe and isolated lab environment for malware analysis Extract the metadata associated with malware Determine malware's interaction with the system Perform code analysis using IDA Pro and x64dbg Reverse-engineer various malware functionalities Reverse engineer and decode common encoding/encryption algorithms Reverse-engineer malware code injection and hooking techniques Investigate and hunt malware

using memory forensics Who this book is for This book is for incident responders, cyber-security investigators, system administrators, malware analyst, forensic practitioners, student, or curious security professionals interested in learning malware analysis and memory forensics. Knowledge of programming languages such as C and Python is helpful but is not mandatory. If you have written few lines of code and have a basic understanding of programming concepts, you'll be able to get most out of this book.

This open access book constitutes the refereed

proceedings of the 15th International Annual Conference on Cyber Security, CNCERT 2018, held in Beijing, China, in August 2018. The 14 full papers presented were carefully reviewed and selected from 53 submissions. The papers cover the following topics: emergency response, mobile internet security, IoT security, cloud security, threat intelligence analysis, vulnerability, artificial intelligence security, IPv6 risk research, cybersecurity policy and regulation research, big data analysis and industrial security.

Know how to mitigate and handle ransomware attacks via the

essential cybersecurity training in this book so you can stop attacks before they happen. Learn the types of ransomware, distribution methods, internal structure, families (variants), defense strategies, recovery methods, and legal issues related to reporting ransomware incidents to authorities and other affected parties. This book also teaches you how to develop a ransomware incident response plan to minimize ransomware damage and recover normal operations quickly. Ransomware is a category of malware that can encrypt your computer and mobile device files until you pay a

ransom to unlock them. Ransomware attacks are considered the most prevalent cybersecurity threats today—the number of new ransomware variants has grown 30-fold since 2015 and they currently account for roughly 40% of all spam messages. Attacks have increased in occurrence from one every 40 seconds to one every 14 seconds. Government and private corporations are targets. Despite the security controls set by organizations to protect their digital assets, ransomware is still dominating the world of security and will continue to do so in the future. Ransomware Revealed

discusses the steps to follow if a ransomware infection occurs, such as how to pay the ransom through anonymous payment methods, perform a backup and restore your affected files, and search online to find a decryption tool to unlock (decrypt) your files for free. Mitigation steps are discussed in depth for both endpoint devices and network systems. What You Will Learn Be aware of how ransomware infects your system Comprehend ransomware components in simple terms Recognize the different types of ransomware families Identify the attack vectors employed by

ransomware to infect computer systems Know how to prevent ransomware attacks from successfully comprising your system and network (i.e., mitigation strategies) Know what to do if a successful ransomware infection takes place Understand how to pay the ransom as well as the pros and cons of paying Set up a ransomware response plan to recover from such attacks Who This Book Is For Those who do not specialize in the cybersecurity field (but have adequate IT skills) and want to fully understand the anatomy of ransomware threats. Although most of the book's content will be

understood by ordinary computer users, it will also prove useful for experienced IT users aiming to understand the ins and outs of ransomware threats without diving deep into the technical jargon of the internal structure of ransomware.

The Hands-On Guide to Dissecting Malicious Software

Advances in Cybersecurity Management

Organized Crime and Terrorist Networks

Cyber Operations and International Law

Issues and Implications of Digital Arms

A Beginner's Guide to Protecting

and Recovering from Ransomware Attacks

This two-volume set (CCIS 1045 and CCIS 1046) constitutes the refereed proceedings of the Third International Conference on Advances in Computing and Data Sciences, ICACDS 2019, held in Ghaziabad, India, in April 2019. The 112 full papers were carefully reviewed and selected from 621 submissions. The papers are centered around topics like advanced computing, data sciences, distributed systems organizing principles, development frameworks and environments, software verification and validation, computational complexity and cryptography, machine learning theory, database theory, probabilistic representations.

Malgré l'impact qu'a eu l'informatisation de la société sur le crime, les connaissances sur le cybercrime n'abondent pas. Ce livre se veut une contribution à la synthèse des connaissances sur différents cybercrimes, notamment par l'examen des enjeux qu'ils soulèvent. Il étudie de façon approfondie quatorze phénomènes liés aux cybercrimes, allant des pratiques policières sur les médias sociaux à l'exploitation sexuelle des enfants sur Internet, en passant par la cyberintimidation, le piratage, les fraudes et l'utilisation des nouvelles technologies à des fins de propagande. Selon le sujet, les chapitres adoptent l'une de deux structures : les chapitres de type synthèse proposent une analyse des dernières connaissances

criminologiques, sociologiques, juridiques et technologiques relatives à un cybercrime donné tandis que les chapitres de type nouvelle recherche présentent les résultats d'une recherche récente. Dans tous les cas, les expériences professionnelles et universitaires des auteurs, à l'instar de la diversité de leur provenance géographique au sein de la Francophonie (Canada, Suisse, France), viennent enrichir le contenu. Cet ouvrage, qui s'adresse aussi bien à l'étudiant, au chercheur ou à l'intervenant du milieu de la justice qu'au citoyen, peut se lire d'une couverture à l'autre ou un chapitre - voire une section - à la fois.

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 book deals with questions of democracy and governance relating to new technologies. The deployment and application of new technologies is often accompanied with uncertainty as to their long-term (un)intended impacts. New technologies also raise questions about the limits of the law as the line

between harmful and beneficial effects is often difficult to draw. The volume explores overarching concepts on how to regulate new technologies and their implications in a diverse and constantly changing society, as well as the way in which regulation can address differing, and sometimes conflicting, societal objectives, such as public health and the protection of privacy. Contributions focus on a broad range of issues such as Citizen Science, Smart Cities, big data, and health care, but also on the role of market regulation for new technologies.The book will serve as a useful research tool for scholars and practitioners interested in the latest developments in the field of technology regulation. Leonie Reins is Assistant

Professor at the Tilburg Institute for Law, Technology, and Society (TILT) in The Netherlands.

Advances in ICT and the Likely Nature of Warfare

First International Conference, SciSec 2018, Beijing, China, August 12-14, 2018, Revised Selected Papers

23rd European Conference, EvoApplications 2020, Held as Part of EvoStar 2020, Seville, Spain, April 15–17, 2020, Proceedings

Regulating New Technologies in Uncertain Times

Practical Malware Analysis

Tallinn Manual on the International Law Applicable to Cyber Warfare

A comprehensive analysis of the international law applicable to cyber operations,

including a systematic study of attribution, lawfulness and remedies.

This book includes innovative research work presented at ICO'2018, the 1st International Conference on Intelligent Computing and Optimization, held in Pattaya, Thailand on October 4–5, 2018. The conference presented topics ranging from power quality, reliability, security assurance, cloud computing, smart cities, renewable energy, agro-engineering, smart vehicles, deep learning, block chain, power systems, AI, machine learning, manufacturing

systems, and big-data analytics. This volume focuses on subjects related to innovative computing, uncertainty management and optimization approaches to real-world problems in big-data, smart cities, sustainability, meta-heuristics, cyber-security, IoTs, economics and finance, renewable energy, energy and electricity systems, and block chain. Presenting cutting-edge methodologies with real-world application problems and their solutions, the book is useful for researchers, managers, executives, students,

academicians, practicing scientists, and decision makers from all around the globe. It offers the academic and the applied communities a compendium and a research resource with significant insights and inspiration for innovative scientific education, investigation and collaboration, to overcome “hard problems” among the emerging challenges today and in the future.

Covers issues arising out of advancing computer technology such as violations of personal privacy, difficulties in prosecution and legal

entanglements, computer intimidation, and considers the future of white-collar crime The threat landscape is evolving with tremendous speed. We are facing an extremely fast-growing attack surface with a diversity of attack vectors, a clear asymmetry between attackers and defenders, billions of connected IoT devices, mostly reactive detection and mitigation approaches, and finally big data challenges. The clear asymmetry of attacks and the enormous amount of data are additional arguments to make it

necessary to rethink cybersecurity approaches in terms of reducing the attack surface, to make the attack surface dynamic, to automate the detection, risk assessment, and mitigation, and to investigate the prediction and prevention of attacks with the utilization of emerging technologies like blockchain, artificial intelligence and machine learning. This book contains eleven chapters dealing with different Cybersecurity Issues in Emerging Technologies. The issues that are discussed and analyzed include smart

connected cars, unmanned ships, 5G/6G connectivity, blockchain, agile incident response, hardware assisted security, ransomware attacks, hybrid threats and cyber skills gap. Both theoretical analysis and experimental evaluation of state-of-the-art techniques are presented and discussed. Prospective readers can be benefitted in understanding the future implications of novel technologies and proposed security solutions and techniques. Graduate and postgraduate students, research scholars, academics, cybersecurity professionals,

and business leaders will find this book useful, which is planned to enlighten both beginners and experienced readers.

Cyber Weaponry

Global Cyber Security Labor Shortage and International Business Risk

Advances in Information and Communication

Guide to Vulnerability Analysis for Computer Networks and Systems

Learning Malware Analysis

Cyberspace in Peace and War, Second Edition

This book constitutes the refereed proceedings

of the First International Conference on Intelligent, Secure, and Dependable Systems in Distributed and Cloud Environments, ISDDC 2017, held in Vancouver, BC, Canada, in October 2017.The 12 full papers presented together with 1 short paper were carefully reviewed and selected from 43 submissions. This book also contains 3 keynote talks and 2 tutorials. The contributions included in this proceedings cover many

aspects of theory and application of effective and efficient paradigms, approaches, and tools for building, maintaining, and managing secure and dependable systems and infrastructures, such as botnet detection, secure cloud computing and cryptosystems, IoT security, sensor and social network security, behavioral systems and data science, and mobile computing.
This updated and expanded edition of

Cyberspace in Peace and War by Martin C. Libicki presents a comprehensive understanding of cybersecurity, cyberwar, and cyber-terrorism. From basic concepts to advanced principles, Libicki examines the sources and consequences of system compromises, addresses strategic aspects of cyberwar, and defines cybersecurity in the context of military operations while highlighting unique aspects of the digital battleground and

strategic uses of cyberwar. This new edition provides updated analysis on cyberespionage, including the enigmatic behavior of Russian actors, making this volume a timely and necessary addition to the cyber-practitioner's library. Cyberspace in Peace and War guides readers through the complexities of cybersecurity and cyberwar and challenges them to understand the topics in new ways.

Libicki provides the technical and geopolitical foundations of cyberwar necessary to understand the policies, operations, and strategies required for safeguarding an increasingly online infrastructure.
This book constitutes the refereed proceedings of the 23rd European Conference on Applications of Evolutionary Computation, EvoApplications 2020, held as part of

*Evo*2020, in Seville, Spain, in April 2020, co-located with the Evo*2020 events EuroGP, EvoMUSART and EvoCOP. The 44 full papers presented in this book were carefully reviewed and selected from 62 submissions. The papers cover a wide spectrum of topics, ranging from applications of bio-inspired techniques on social networks, evolutionary computation in digital healthcare and personalized medicine, soft-computing*

applied to games, applications of deep-bioinspired algorithms, parallel and distributed systems, and evolutionary machine learning.?
Science of Cyber Security
15th International Conference, DIMVA 2018, Saclay, France, June 28-29, 2018, Proceedings
Security and Privacy Paradigm
Crime by Computer
Countering Cyber Attacks and Preserving the Integrity and

Availability of Critical Systems