Read Book Network Security Attacks And Countermeasures By Dileep Kumar G Pdf For Free

Guide to Network Defense and Countermeasures *Phishing and Countermeasures* Improving Web Application Security *Internet of Things, Threats, Landscape, and Countermeasures* **Risk Analysis and Security Countermeasure Selection** Practical Hacking Techniques and Countermeasures **Analyzing Computer Security Internet of Things Security Security, Privacy, and Digital Forensics in the Cloud** Practical Hacking Techniques and Countermeasures, Second Edition Practical Hacking Techniques and Countermeasures *Surveillance Countermeasures Ethical Hacking and Countermeasures: Web Applications and Data Servers* Web Application Security **Threats, Countermeasures, and Advances in Applied Information Security** High G Flight **IoT Applications, Security Threats, and Countermeasures** *Guide to Network Defense and Countermeasures Viruses, Hardware and Software Trojans Electromagnetic Information Leakage and Countermeasure Technique* Security and Privacy in the Internet of Things *Information Hiding in Communication Networks Ethical Hacking and Countermeasures: Secure Network Operating Systems and Infrastructures (CEH)* **Distributed Denial of Service (DDoS) Attacks** Ethical Hacking: Techniques, Tools, and Countermeasures *Ethical Hacking and Countermeasures: Attack Phases* **Optimization of Exercise Countermeasures for Human Space Flight – Lessons from Terrestrial Physiology and Operational Implementation** Ethical Hacking and Countermeasures: Linux, Macintosh and Mobile Systems **Guide to Network Defense and Countermeasures** *Analysis of Return Oriented Programming and Countermeasures* **Network Defense and Countermeasures Network Defense and Countermeasures** *Driver Distraction and Inattention* **Ethical Hacking and Countermeasures: Threats and Defense Mechanisms** *Security of Internet of Things Nodes Social and Human Elements of Information Security* **GNSS Interference, Threats, and Countermeasures Guide to Network Defense and Countermeasures Side-Channel Attacks and Countermeasures** Debris Flow

Internet of Things (IoT) is an ecosystem comprised of heterogeneous connected devices that communicate to deliver capabilities making our living, cities, transport, energy, and other areas more intelligent. This book delves into the different cyber-security domains and their challenges due to the massive amount and the heterogeneity of devices. This book introduces readers to the inherent concepts of IoT. It offers case studies showing how IoT counteracts the cyber-security concerns for domains. It provides suggestions on how to mitigate cyber threats by compiling a catalogue of threats that currently comprise the contemporary threat landscape. It then examines different security measures that can be applied to system installations or operational environment and discusses how these measures may alter the threat exploitability level and/or the level of the technical impact. Professionals, graduate students, researchers, academicians, and institutions that are interested in acquiring knowledge in the areas of IoT and cyber-security, will find this book of interest. The EC-Council|Press Ethical Hacking and Countermeasures series is comprised of four books covering a broad base of topics in offensive network security, ethical hacking, and network defense and countermeasures. The content of this series is designed to immerse the reader into an interactive environment where they will be shown how to scan, test, hack, and secure information systems. A wide variety of tools, viruses, and malware is presented in these books, providing a complete understanding of the tactics and tools used by hackers. The full series of books helps prepare readers to take and succeed on the C|EH certification exam from EC-Council. Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version. The EC-Council | Press Ethical Hacking and Countermeasures Series is comprised of five books covering a broad base of topics in offensive network security, ethical hacking, and network defense and countermeasures. The content of this series is designed to immerse the reader into an interactive environment where they will be shown how to scan, test, hack and secure information systems. With the full series of books, the reader will gain in-depth knowledge and practical experience with essential security systems, and become prepared to succeed on the Certified Ethical Hacker, or C|EH, certification from EC-Council. This certification covers a plethora of offensive security topics ranging from how perimeter defenses work, to scanning and attacking simulated networks. A wide variety of tools, viruses, and malware is presented in this and the other four books, providing a complete understanding of the tactics and tools used by hackers. By gaining a thorough understanding of how hackers operate, an Ethical Hacker will be able to set up strong countermeasures and defensive systems to protect an organization's critical infrastructure and information. Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version. The EC-Council|Press Ethical Hacking and Countermeasures series is comprised of four books covering a broad base of topics in offensive network security, ethical hacking, and network defense and countermeasures. The content of this series is designed to immerse the reader into an interactive environment where they will be shown how to scan, test, hack, and secure information systems. A wide variety of tools, viruses, and malware is presented in these books, providing a complete understanding of the tactics and tools used by hackers. The full series of books helps prepare readers to take and succeed on the C|EH certification exam from EC-Council. Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version. A lot of devices which are daily used (i.e., credit card, pay-tv card, e-passport) have to guarantee the retention of sensible data. Sensible data are ciphered by a secure key by which only the key holder can get the data. For this reason, to protect the cipher key against possible attacks becomes a main issue. Many research activities have been directed in developing countermeasures to enhance the device resistance against attacks and, on the other side, many contributions aimed to enhance the attack itself have been reported in the technical literature. This book is a collection of the main results of a PhD in hardware cryptography about side-channel attacks and countermeasures in the design of secure IC's devices. About hardware countermeasures against power analysis, three new logic families for cryptographic applications are designed. With respect to the contributions aimed to enhance the attack methodologies, an active circuit which promises to improve the power attacks is proposed. Besides, a new side channel and a novel methodology to attack cryptographic circuits is studied. Finally, two activities focused on Random Numbers Generators are briefly described. Introduction: Attackers have relatively success in defeating modern defensive techniques by using an exploitation method known as "code reuse." This class of exploitation techniques makes use of the lack of memory safety in C which allows an attacker to redirect a program's control flow to pre-existing snippets of code. Code reuse attacks have historically been a powerful and ubiquitous exploitation technique [2]. Even as recently as 2014 there has been an outbreak of these code reuse attacks, targeting such applications as Adobe, Internet Explorer, and Firefox 15]. Many defensive countermeasures have been taken by the security community, ranging from data execution prevention to varying degrees of code randomization. This thesis can roughly be broken into two halves: 1. Show how code reuse attacks can leverage timing information in order to break many existing defenses. 2. Investigate how control flow integrity can be improved upon as a countermeasure to code reuse attacks ... The book Security of Internet of Things Nodes: Challenges, Attacks, and Countermeasures® covers a wide range of research topics on the security of the Internet of Things nodes along with the latest research development in the domain of Internet of Things. It also covers various algorithms, techniques, and schemes in the field of computer science with state-of-the-art tools and technologies. This book mainly focuses on the security challenges of the Internet of Things devices and the countermeasures to overcome security vulnerabilities. Also, it highlights trust management issues on the Internet of Things nodes to build secured Internet of Things systems. The book also covers the necessity of a system model for the Internet of Things devices to ensure security at the hardware level. Guide to Network Defense and Countermeasures, 2E is the second of two books that are required for Level One of the Security Certified Program (SCP). This edition has been revised with updated content and maps clearly to the exam objectives for the current Security Certified Network Professional (SCNP) exam. Although the primary emphasis is on intrusion detection, the book also covers such essential practices as developing a security policy and then implementing that policy by performing Network Address Translation, setting up packet filtering, and installing proxy servers, firewalls, and virtual private networks. Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version. Organizations are increasingly relying on electronic information to conduct business, which has caused the amount of personal information to grow exponentially. Threats, Countermeasures, and Advances in Applied Information Security addresses the fact that managing information security program while effectively managing risks has never been so critical. This book contains 24 chapters on the most relevant and important issues and advances in applied information security management. The chapters are authored by leading researchers and practitioners in the field of information security from across the globe. The chapters represent emerging threats and countermeasures for effective management of information security at organizations. SECURITY AND PRIVACY IN THE INTERNET OF THINGS Provides the authoritative and up-to-date information required for securing IoT architecture and applications The vast amount of data generated by the Internet of Things (IoT) has made information and cyber security vital for not only personal privacy, but also for the sustainability of the IoT itself. Security and Privacy in the Internet of Things brings together high-quality research on IoT security models, architectures, techniques, and application domains. This concise yet comprehensive volume explores state-of-the-art mitigations in IoT security while addressing important security and privacy challenges across different IoT layers. The book provides timely coverage of IoT architecture, security technologies and mechanisms, and applications. The authors outline emerging trends in IoT security and privacy with a focus on areas such as smart environments and e-health. Topics include authentication and access control, attack detection and prevention, securing IoT through traffic modeling, human aspects in IoT security, and IoT hardware security. Presenting the current body of knowledge in a single volume, Security and Privacy in the Internet of Things: Discusses a broad range of IoT attacks and defense mechanisms Examines IoT security and privacy protocols and approaches Covers both the logical and physical security of IoT devices Addresses IoT security through network traffic modeling Describes privacy preserving techniques in smart cities Explores current threat and vulnerability analyses Security and Privacy in the Internet of Things: Architectures, Techniques, and Applications is essential reading for researchers, industry practitioners, and students involved in IoT security development and IoT systems deployment. GUIDE TO NETWORK DEFENSE AND COUNTERMEASURES provides a thorough guide to perimeter defense fundamentals, including intrusion detection and firewalls. This trusted text also covers more advanced topics such as security policies, network address translation (NAT), packet filtering and analysis, proxy servers, virtual private networks (VPN), and network traffic signatures. Thoroughly updated, the new third edition reflects the latest technology, trends, and techniques including virtualization, VMware, IPv6, and ICMPv6 structure, making it easier for current and aspiring professionals to stay on the cutting edge and one step ahead of potential security threats. A clear writing style and numerous screenshots and illustrations make even complex technical material easier to understand, while tips, activities, and projects throughout the text allow you to hone your skills by applying what you learn. Perfect for students and professionals alike in this high-demand, fast-growing field, GUIDE TO NETWORK DEFENSE AND COUNTERMEASURES, Third Edition, is a must-have resource for success as a network security professional. Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version. The EC-Council|Press Ethical Hacking and Countermeasures series is comprised of four books covering a broad base of topics in offensive network security, ethical hacking, and network defense and countermeasures. The content of this series is designed to immerse the reader into an interactive environment where they will be shown how to scan, test, hack, and secure information systems. A wide variety of tools, viruses, and malware is presented in these books, providing a complete understanding of the tactics and tools used by hackers. The full series of books helps prepare readers to take and succeed on the C|EH certification exam from EC-Council. Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version. In a unique and systematic way, this book discusses the security and privacy aspects of the cloud, and the relevant cloud forensics. Cloud computing is an emerging yet revolutionary technology that has been changing the way people live and work. However, with the continuous growth of cloud computing and related services, security and privacy has become a critical issue. Written by some of the top experts in the field, this book specifically discusses security and privacy of the cloud, as well as the digital forensics of cloud data, applications, and services. The first half of the book enables readers to have a comprehensive understanding and background of cloud security, which will help them through the digital investigation guidance and recommendations found in the second half of the book. Part One of Security, Privacy and Digital Forensics in the Cloud covers cloud infrastructure security; confidentiality of data; access control in cloud IaaS; cloud security and privacy management; hacking and countermeasures; risk management and disaster recovery; auditing and compliance; and security as a service (SaaS). Part Two addresses cloud forensics – model, challenges, and approaches; cyberterrorism in the cloud; digital forensic process and model in the cloud; data acquisition; digital evidence management, presentation, and court preparation; analysis of digital evidence; and forensics as a service (FaaS). Thoroughly covers both security and privacy of cloud and digital forensics Contributions by top researchers from the U.S., the European and other countries, and professionals active in the field of information and network security, digital and computer forensics, and cloud and big data Of interest to those focused upon security and implementation, and incident management Logical, well-structured, and organized to facilitate comprehension Security, Privacy and Digital Forensics in the Cloud is an ideal book for advanced undergraduate and master's-level students in information systems, information technology, computer and network forensics, as well as computer science. It can also serve as a good reference book for security professionals, digital forensics practitioners and cloud service providers. Examining computer security from the hacker's perspective, Practical Hacking Techniques and Countermeasures employs virtual computers to illustrate how an attack is executed, including the script, compilation, and results. It provides detailed screen shots in each lab for the reader to follow along in a step-by-step process in order to duplicate and understand how the attack works. It enables experimenting with hacking techniques without fear of corrupting computers or violating any laws. Written in a lab manual style, the book begins with the installation of the VMware® Workstation product and guides the users through detailed hacking labs enabling them to experience what a hacker actually does during an attack. It covers social engineering techniques, footprinting techniques, and scanning tools. Later chapters examine spoofing techniques, sniffing techniques, password cracking, and attack tools. Identifying wireless attacks, the book also explores Trojans, Man-in-the-Middle (MTM) attacks, and Denial of Service (DoS) attacks. Learn how to secure your computers with this comprehensive guide on hacking techniques and countermeasures By understanding how an attack occurs the reader can better understand how to defend against it. This book shows how an attack is conceptualized, formulated, and performed. It offers valuable information for constructing a system to defend against attacks and provides a better understanding of securing your own computer or corporate network. The EC-Council | Press Ethical Hacking and Countermeasures Series is comprised of five books covering a broad base of topics in offensive network security, ethical hacking, and network defense and countermeasures. The content of this series is designed to immerse the reader into an interactive environment where they will be shown how to scan, test, hack and secure information systems. With the full series of books, the reader will gain in-depth knowledge and practical experience with essential security systems, and become prepared to succeed on the Certified Ethical Hacker, or C|EH, certification from EC-Council. This certification covers a plethora of offensive security topics ranging from how perimeter defenses work, to scanning and attacking simulated networks. A wide variety of tools, viruses, and malware is presented in this and the other four books, providing a complete understanding of the tactics and tools used by hackers. By gaining a thorough understanding of how hackers operate, an Ethical Hacker will be able to set up strong countermeasures and defensive systems to protect an organization's critical infrastructure and information. Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version. Everything you need to know about modern network attacks and defense, in one book Clearly explains core network security concepts, challenges, technologies, and skills Thoroughly updated for the latest attacks and countermeasures The perfect beginner’s guide for anyone interested in a network security career ¿ Security is the IT industry’s hottest topic–and that’s where the hottest opportunities are, too. Organizations desperately need professionals who can help them safeguard against the most sophisticated attacks ever created–attacks from well-funded global criminal syndicates, and even governments. ¿ Today, security begins with defending the organizational network. Network Defense and Countermeasures, Second Edition is today’s most complete, easy-to-understand introduction to modern network attacks and their effective defense. From malware and DDoS attacks to firewalls and encryption, Chuck Easttom blends theoretical foundations with up-to-the-minute best-practice techniques. Starting with the absolute basics, he discusses crucial topics many security books overlook, including the emergence of network-based espionage and terrorism. ¿ If you have a basic understanding of networks, that’s all the background you’ll need to succeed with this book: no math or advanced computer science is required. You’ll find projects, questions, exercises, case studies, links to expert resources, and a complete glossary–all designed to deepen your understanding and prepare you to defend real-world networks. ¿ Learn how to Understand essential network security concepts, challenges, and careers Learn how modern attacks work Discover how firewalls, intrusion detection systems (IDS), and virtual private networks (VPNs) combine to protect modern networks Select the right security technologies for any network environment Use encryption to protect information Harden Windows and Linux systems and keep them patched Securely configure web browsers to resist attacks Defend against malware Define practical, enforceable security policies Use the “6 Ps” to assess technical and human aspects of system security Detect and fix system vulnerability Apply proven security standards and models, including Orange Book, Common Criteria, and Bell-LaPadula Ensure physical security and prepare for disaster recovery Know your enemy: learn basic hacking, and see how to counter it Understand standard forensic techniques and prepare for investigations of digital crime ¿ In this book, the authors of the 20-year best-selling classic Security in Computing take a fresh, contemporary, and powerfully relevant new approach to introducing computer security. Organised around attacks and mitigations, the Pfleegers' new Analyzing Computer Security will attract students' attention by building on the high-profile security failures they may have already encountered in the popular media. Each section starts with an attack description. Next, the authors explain the vulnerabilities that have allowed this attack to occur. With this foundation in place, they systematically present today's most effective countermeasures for blocking or weakening the attack. One step at a time, students progress from attack/problem/harm to solution/protection/mitigation, building the powerful real-world problem solving skills they need to succeed as information security professionals. Analyzing Computer Security addresses crucial contemporary computer security themes throughout, including effective security management and risk analysis; economics and quantitative study; privacy, ethics, and laws; and the use of overlapping controls. The authors also present significant new material on computer forensics, insiders, human factors, and trust. Human spaceflight has required space agencies to study and develop exercise countermeasure (CM) strategies to manage the profound, multi-system adaptation of the human body to prolonged microgravity (?G). Future space exploration will present new challenges in terms of adaptation management that will require the attention of both exercise physiologists and operational experts. In the short to medium-term, all exploration missions will be realised using relatively small vehicles/habitats, with some exploration scenarios including surface operations in low (1G) gravity conditions. The evolution of CM hardware has allowed modern-day astronauts to return to Earth with, on average, relatively moderate levels ?G-induced adaptation of the musculoskeletal (MS) and cardiovascular (CV) systems. However, although the intense use of CM has attenuated many aspects of MS and CV adaptation, on an individual level, there remains wide variation in the magnitude of these

changes. Innovations in CM programs have been largely engineering-driven, with new hardware providing capability for new modes of exercise and a wider range of exercise protocols, which, in turn, has facilitated the transfer of traditional, but effective, terrestrial concepts based around high frequency resistance (multiple-set, multiple repetition) and mediumintensity continuous aerobic training. As a result, International Space Station (ISS) CM specialists have focused their efforts in these domains, taking advantage of hardware innovations as and when they became available. However, terrestrial knowledge in human and exercise physiology has expanded rapidly during the lifetime of the ISS and, consequently, there is potential to optimize current approaches by re-examining terrestrial knowledge and identifying opportunities to implement this knowledge into operational practices. Current terrestrial knowledge in exercise physiology is the product of a large number of intervention studies in which the variables that contribute to the effects of physical activity (mode, frequency, duration, intensity, recovery) have been controlled and systematically manipulated. However, due to limited opportunities to perform intervention studies in both spaceflight analogues – head-down bed rest (HDBR) being considered the 'gold standard' – and spaceflight itself, it will not be possible to systematically investigate the contribution of these factors to the efficacy of in-flight CM. As such, it will be necessary to draw on terrestrial evidence to identify solutions/strategies that may be best suited to the constraints of exploration and prioritise specific solutions/strategies for evaluation in HDBR and in flight. "The book represents a compilation of articles on technology, processes, management, governance, research and practices on human and social aspects of information security"--Provided by publisher. When properly conducted, risk analysis enlightens, informs, and illuminates, helping management organize their thinking into properly prioritized, cost-effective action. Poor analysis, on the other hand, usually results in vague programs with no clear direction and no metrics for measurement. Although there is plenty of information on risk analysis, it is rare to find a book that explains this highly complex subject with such startling clarity. Very few, if any, focus on the art of critical thinking and how to best apply it to the task of risk analysis. The first comprehensive resource to explain how to evaluate the appropriateness of countermeasures, from a cost-effectiveness perspective, Risk Analysis and Security Countermeasure Selection details the entire risk analysis process in language that is easy to understand. It guides readers from basic principles to complex processes in a step-by-step fashion, evaluating DHS–approved risk assessment methods, including CARVER, API/NPRA, RAMCAP, and various Sandia methodologies. Using numerous case illustrations, the text clearly explains the five core principles of the risk analysis lifecycle—determining assets, threats, vulnerabilities, risks, and countermeasures. It also supplies readers with a completely adaptable graphic risk analysis tool that is simple to use, can be applied in public or private industries, and works with all DHS–approved methods. This reader-friendly guide provides the tools and insight needed to effectively analyze risks and secure facilities in a broad range of industries, including DHS designated critical infrastructure in the chemical, transportation, energy, telecommunications, and public health sectors. All you need to know about defending networks, in one book · Clearly explains concepts, terminology, challenges, tools, and skills · Covers key security standards and models for business and government · The perfect introduction for all network/computer security professionals and students Welcome to today's most useful and practical introduction to defending modern networks. Drawing on decades of experience, Chuck Easttom brings together updated coverage of all the concepts, terminology, techniques, and solutions you'll need to be effective. Easttom thoroughly introduces the core technologies of modern network security, including firewalls, intrusion-detection systems, and VPNs. Next, he shows how encryption can be used to safeguard data as it moves across networks. You'll learn how to harden operating systems, defend against malware and network attacks, establish robust security policies, and assess network security using industry-leading standards and models. You'll also find thorough coverage of key issues such as physical security, forensics, and cyberterrorism. Throughout, Easttom blends theory and application, helping you understand both what to do and why. In every chapter, quizzes, exercises, projects, and web resources deepen your understanding and help you use what you've learned–in the classroom and in your career. Learn How To · Evaluate key network risks and dangers · Choose the right network security approach for your organization · Anticipate and counter widespread network attacks, including those based on "social engineering" · Successfully deploy and apply firewalls and intrusion detection systems · Secure network communication with virtual private networks · Protect data with cryptographic public/private key systems, digital signatures, and certificates · Defend against malware, including ransomware, Trojan horses, and spyware · Harden operating systems and keep their security up to date · Define and implement security policies that reduce risk · Explore leading security standards and models, including ISO and NIST standards · Prepare for an investigation if your network has been attacked · Understand the growing risks of espionage and cyberterrorism This book presents a model of electromagnetic (EM) information leakage based on electromagnetic and information theory. It discusses anti-leakage, anti-interception and anti-reconstruction technologies from the perspectives of both computer science and electrical engineering. In the next five years, the threat posed by EM information leakage will only become greater, and the demand for protection will correspondingly increase. The book systematically introduces readers to the theory of EM information leakage and the latest technologies and measures designed to counter it, and puts forward an EM information leakage model that has established the foundation for new research in this area, paving the way for new technologies to counter EM information leakage. As such, it offers a valuable reference guide for all researchers and engineers involved in EM information leakage and countermeasures. Ethical Hacking: Techniques, Tools, and Countermeasures, Fourth Edition, covers the basic strategies and tools that prepare students to engage in proactive and aggressive cyber security activities, with an increased focus on Pen testing and Red Teams. Written by subject matter experts, with numerous real-world examples, the Fourth Edition provides readers with a clear, comprehensive introduction to the many threats on the security of our cyber environments and what can be done to combat them. The text begins with an examination of the landscape, key terms, and concepts that a security professional needs to know about hackers and computer criminals who break into networks, steal information, and corrupt data. Part II provides a technical overview of hacking: how attackers target cyber resources and the methodologies they follow. Part III studies those methods that are most effective when dealing with hacking attacks, especially in an age of increased reliance on distributed devices. Surveillance Countermeasures By: Aden C. Magee In today's prolific hostile threat environment, surveillance countermeasures expertise is a necessary component of security knowledge. The wide range of increasingly unconstrained threats to the personal privacy and security of average citizens include common criminals and stalkers, private and corporate investigators, government-sponsored espionage and other covert agencies, and international crime and terrorist organizations. In virtually all cases, the elements that threaten individual, corporate, or national security conduct surveillance operations to further their objectives, or as the primary means to an end Surveillance countermeasures are actions taken by an individual or security detail to identify the presence of surveillance and, if necessary, to elude or evade the individual or group conducting the surveillance. Understanding how the surveillance threat thinks and reacts is the basis of effective surveillance countermeasures. This manual details surveillance countermeasures concepts, techniques, and procedures that are proven effective against the spectrum of surveillance capabilities ranging from the very basic to the world's most sophisticated. This manual now supersedes the previous industry standards as the authoritative resource on surveillance countermeasures principles, procedures, and practices. This manual is a compilation of the most relevant details from two of the all-time classics and best-sellers in the genre – Surveillance Countermeasures and Countering Hostile Surveillance. It also draws precise threat/surveillance perspective from another of the all-time greats – Secrets of Surveillance. The fact that this manual consolidates the knowledge derived from these three unparalleled classics demonstrates that this manual now represents the full-spectrum amalgam of surveillance countermeasures methodologies ranging from the foundational baseline of tactics and techniques to the most advanced concepts and procedures. This revised instant classic for the genre also includes many additional details and special-interest topics to form an informational/educational resource like no other. Written by one of the rare breed who has actually stalked the streets and stood in the shadows, this manual presents surveillance countermeasures tradecraft from the theoretical to the practical levels in terms of the "art" and "science." The execution of techniques as components of methodical procedures to effectively manipulate and exploit a hostile surveillance effort is representative of a security professional or security-conscious individual operating at the master's level of surveillance countermeasures tradecraft. The information and instruction in this manual begins with the basics and then takes the practitioner to that level execution. Phishing and Counter-Measures discusses how and why phishing is a threat, and presents effective countermeasures. Showing you how phishing attacks have been mounting over the years, how to detect and prevent current as well as future attacks, this text focuses on corporations who supply the resources used by attackers. The authors subsequently deliberate on what action the government can take to respond to this situation and compare adequate versus inadequate countermeasures. The Internet of Things (IoT), with its technological advancements and massive innovations, is building the idea of inter-connectivity among everyday life objects. With an explosive growth in the number of Internet-connected devices, the implications of the idea of IoT on enterprises, individuals, and society are huge. IoT is getting attention from both academia and industry due to its powerful real-time applications that raise demands to understand the entire spectrum of the field. However, due to increasing security issues, safeguarding the IoT ecosystem has become an important concern. With devices and information becoming more exposed and leading to increased attack possibilities, adequate security measures are required to leverage the benefits of this emerging concept. Internet of Things Security: Principles, Applications, Attacks, and Countermeasures is an extensive source that aims at establishing an understanding of the core concepts of IoT among its readers and the challenges and corresponding countermeasures in the field. Key features: Containment of theoretical aspects, as well as recent empirical findings associated with the underlying technologies Exploration of various challenges and trade-offs associated with the field and approaches to ensure security, privacy, safety, and trust across its key elements Vision of exciting areas for future research in the field to enhance the overall productivity This book is suitable for industrial professionals and practitioners, researchers, faculty members, and students across universities who aim to carry out research and development in the field of IoT security. The book explores modern sensor technologies while also discussing security issues, which is the dominant factor for many types of Internet of Things (IoT) applications. It also covers recent (IoT) applications such as the Markovian Arrival Process, fog computing, real-time solar energy monitoring, healthcare, and agriculture. Fundamental concepts of gathering, processing, and analyzing different Artificial Intelligence (AI) models in IoT applications are covered along with recent detection mechanisms for different types of attacks for effective network communication. On par with the standards laid out by international organizations in related fields, the book focuses on both core concepts of IoT along with major application areas. Designed for technical developers, academicians, data scientists, industrial researchers, professionals, and students, this book is useful in uncovering the latest innovations in the field of IoT. The complexity and severity of the Distributed Denial of Service (DDoS) attacks are increasing day-by-day. The Internet has a highly inconsistent structure in terms of resource distribution. Numerous technical solutions are available, but those involving economic aspects have not been given much consideration. The book, DDoS Attacks – Classification, Attacks, Challenges, and Countermeasures, provides an overview of both types of defensive solutions proposed so far, exploring different dimensions that would mitigate the DDoS effectively and show the implications associated with them. Features: Covers topics that describe taxonomies of the DDoS attacks in detail, recent trends and classification of defensive mechanisms on the basis of deployment location, the types of defensive action, and the solutions offering economic incentives. Introduces chapters discussing the various types of DDoS attack associated with different layers of security, an attacker's motivations, and the importance of incentives and liabilities in any defensive solution. Illustrates the role of fair resource-allocation schemes, separate payment mechanisms for attackers and legitimate users, negotiation models on cost and types of resources, and risk assessments and transfer mechanisms. DDoS Attacks – Classification, Attacks, Challenges, and Countermeasures is designed for the readers who have an interest in the cybersecurity domain, including students and researchers who are exploring different dimensions associated with the DDoS attack, developers and security professionals who are focusing on developing defensive schemes and applications for detecting or mitigating the DDoS attacks, and faculty members across different universities. This book provides readers with a valuable reference on cyber weapons and, in particular, viruses, software and hardware Trojans. The authors discuss in detail the most dangerous computer viruses, software Trojans and spyware, models of computer Trojans affecting computers, methods of implementation and mechanisms of their interaction with an attacker — a hacker, an intruder or an intelligence agent. Coverage includes Trojans in electronic equipment such as telecommunication systems, computers, mobile communication systems, cars and even consumer electronics. The evolutionary path of development of hardware Trojans from "cabinets", "crates" and "boxes" to the microcircuits (IC) is also discussed. Readers will benefit from the detailed review of the major known types of hardware Trojans in chips, principles of their design, mechanisms of their functioning, methods of their introduction, means of camouflaging and detecting, as well as methods of protection and counteraction. It is estimated that, in the United States, around 20 percent of all Police-reported road crashes involve driver distraction as a contributing factor. This figure increases if other forms of inattention are considered. Evidence (reviewed in this volume) suggests that the situation is similar in other countries and that driver distraction and inattention are even more dangerous as contributing factors in crashes than drug and alcohol intoxication. Having a solid evidence-base from which to develop injury countermeasures is a cornerstone of road-safety management. This book adds to the accumulating evidence-base on driver distraction and inattention. With 24 chapters by 52 authors from more than 10 countries, it provides important new perspectives on the definition and meaning of driver distraction and inattention, the mechanisms that characterize them, the measurement of their effects, strategies for mitigating their effects, and recommendations for further research. The goal of this book is to inspire further research and countermeasure development to prevent and mitigate the potentially adverse effects of driver distraction and driver inattention, and, in doing so, to save lives. Examining computer security from the hacker's perspective, Practical Hacking Techniques and Countermeasures employs virtual computers to illustrate how an attack is executed, including the script, compilation, and results. It provides detailed screen shots in each lab for the reader to follow along in a step-by-step process in order to duplicate an Gain a solid foundation for designing, building, and configuring security-enhanced, hack-resistant Microsoft® ASP.NET Web applications. This expert guide describes a systematic, task-based approach to security that can be applied to both new and existing applications. It addresses security considerations at the network, host, and application layers for each physical tier—Web server, remote application server, and database server—detailing the security configurations and countermeasures that can help mitigate risks. The information is organized into sections that correspond to both the product life cycle and the roles involved, making it easy for architects, designers, and developers to find the answers they need. All PATTERNS & PRACTICES guides are reviewed and approved by Microsoft engineering teams, consultants, partners, and customers—delivering accurate, real-world information that's been technically validated and tested. Comprehensive account, treating both theoretical and applied aspects of debris flow. The text begins with a discussion of fundamental mechanical aspects, such as flow characteristics, type classification, mechanics, occurrence and development, fully-developed flow and deposition processes. The second part of the book sheds light on the application of theory in relation to computer-simulated reproductions of real disasters. Attention is paid to debris flow controlling structures, design effectiveness and performance, soft countermeasure problems, such as identification of debris flow prone ravines and the prediction of occurrence by the concept of precipitation threshold. The qualitative and fundamental character of this book makes it an excellent textbook for graduate courses in debris flow and it is recommended reading for professionals in engineering, geosciences and water resources who are concerned with mechanics and countermeasures of debris flow. Keywords: stony debris flow, viscous debris flo, landslide induced debris flow, hazard zone mapping, grid type sabo dam. GUIDE TO NETWORK DEFENSE AND COUNTERMEASURES provides a thorough guide to perimeter defense fundamentals, including intrusion detection and firewalls. This trusted text also covers more advanced topics such as security policies, network address translation (NAT), packet filtering and analysis, proxy servers, virtual private networks (VPN), and network traffic signatures. Thoroughly updated, the new third edition reflects the latest technology, trends, and techniques including virtualization, VMware, IPv6, and ICMPv6 structure, making it easier for current and aspiring professionals to stay on the cutting edge and one step ahead of potential security threats. A clear writing style and numerous screenshots and illustrations make even complex technical material easier to understand, while tips, activities, and projects throughout the text allow you to hone your skills by applying what you learn. Perfect for students and professionals alike in this high-demand, fast-growing field, GUIDE TO NETWORK DEFENSE AND COUNTERMEASURES, Third Edition, is a must-have resource for success as a network security professional. Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version. Examining computer security from the hacker's perspective, Practical Hacking Techniques and Countermeasures employs virtual computers to illustrate how an attack is executed, including the script, compilation, and results. It provides detailed screen shots in each lab for the reader to follow along in a step-by-step process in order to duplicate and understand how the attack works. It enables experimenting with hacking techniques without fear of corrupting computers or violating any laws. Written in a lab manual style, the book begins with the installation of the VMware Workstation product and guides the users through detailed hacking labs enabling them to experience what a hacker actually does during an attack. It covers social engineering techniques, footprinting techniques, and scanning tools. Later chapters examine spoofing techniques, sniffing techniques, password cracking, and attack tools. Identifying wireless attacks, the book also explores Trojans, Man-in-the-Middle (MTM) attacks, and Denial of Service (DoS) attacks. Learn how to secure your computers with this comprehensive guide on hacking techniques and countermeasures By understanding how an attack occurs the reader can better understand how to defend against it. This book shows how an attack is conceptualized, formulated, and performed. It offers valuable information for constructing a system to defend against attacks and provides a better understanding of securing your own computer or corporate network. During the launch and re-entry phases of spaceflight pilots of military fast jets, civilian aerobatic pilots and astronauts are frequently and repetitively exposed to high G forces, for which the human body is not fundamentally designed. This unique book examines the nature of the high G environment and its physiological effects on the various systems of the human body. It draws together the accumulated knowledge of human exposure to high G, resulting in a definitive volume on its physiological effects and countermeasures. Web Application Security will present timeless security concepts (from both an offensive and defensive standpoint) in a format that any software engineer can absorb. Readers will be able to write significantly more secure code by the end of this book. Additionally, for those interested in the more offensive elements of web application security, this book will provide a solid foundation from which they can rapidly move toward becoming an expert hacker. Guide to Network Defense and Countermeasures examines the practice of intrusion detection, which encompasses virtually all aspects of network security. As more businesses and organizations use the Internet for day-to-day communications, they can use intrusion-detection techniques to deter attacks, detect intrusion attempts, respond to break-ins, assess the damage of hack attacks, and locate and prosecute intruders. Guide to Network Defense and Countermeasures includes coverage of intrusion, detection design and implementation, firewalls design and implementation, virtual private networks (VPNs), packet filters, and network traffic signatures. In addition, this text prepares students to take the Network Defense and Countermeasures exam, which is the second exam for the Security Certified Professional (SCP) Certification. Describes Information Hiding in communication networks, and highlights their important issues, challenges, trends, and applications. Highlights development trends and potential future directions of Information Hiding Introduces a new classification and taxonomy for modern data hiding techniques Presents different types of network steganography mechanisms Introduces several example applications of information hiding in communication networks including some recent covert communication techniques in popular Internet services GNSS Interference Threats and Countermeasures: Modern society is highly reliant on global navigation satellite systems (GNSS) and satellite and radio navigation are evolving at an accelerating pace. This new resource provides a comprehensive survey of the effect of radio-frequency interference (RFI) on GNSS, along with a detailed presentation of spoofing threats. Through in-depth case studies and practical applications, this book ultimately helps engineers and scientists design and implement robust systems to meet the needs of their challenging projects. The techniques investigated in this book take advantage of the increased computational capabilities of GNSS receivers, allowing for the implementation of more sophisticated signal processing algorithms. Contents Overview: The Interference Threat; Classification of Interfering Sources and Analysis of the Effects on GNSS Receivers; The Spoofing Menace; Analytical Assessment of

Interference on GNSS Signals; Interference Detection Strategies; Classical Digital Signal Processing Countermeasures to Interference in GNSS; Interference Mitigation Based on Transformed Domain Techniques; Antispoofing Techniques for GNSS. Book jacket.

- Guide To Network Defense And Countermeasures
- Phishing And Countermeasures
- Improving Web Application Security
- Internet Of Things Threats Landscape And Countermeasures
- Risk Analysis And Security Countermeasure Selection
- Practical Hacking Techniques And Countermeasures
- Analyzing Computer Security
- Internet Of Things Security
- Security Privacy And Digital Forensics In The Cloud
- Practical Hacking Techniques And Countermeasures Second Edition
- Practical Hacking Techniques And Countermeasures
- Surveillance Countermeasures
- Ethical Hacking And Countermeasures Web Applications And Data Servers
- Web Application Security
- Threats Countermeasures And Advances In Applied Information Security
- High G Flight
- IoT Applications Security Threats And Countermeasures
- Guide To Network Defense And Countermeasures
- Viruses Hardware And Software Trojans
- Electromagnetic Information Leakage And Countermeasure Technique
- Security And Privacy In The Internet Of Things
- Information Hiding In Communication Networks
- Ethical Hacking And Countermeasures Secure Network Operating Systems And Infrastructures CEH
- Distributed Denial Of Service DDoS Attacks
- Ethical Hacking Techniques Tools And Countermeasures
- Ethical Hacking And Countermeasures Attack Phases
- Optimization Of Exercise Countermeasures For Human Space Flight Lessons From Terrestrial Physiology And Operational Implementation
- Ethical Hacking And Countermeasures Linux Macintosh And Mobile Systems
- Guide To Network Defense And Countermeasures
- Analysis Of Return Oriented Programming And Countermeasures
- Network Defense And Countermeasures
- Network Defense And Countermeasures
- Driver Distraction And Inattention
- Ethical Hacking And Countermeasures Threats And Defense Mechanisms
- Security Of Internet Of Things Nodes
- Social And Human Elements Of Information Security
- GNSS Interference Threats And Countermeasures
- Guide To Network Defense And Countermeasures
- Side Channel Attacks And Countermeasures
- Debris Flow