Security Threats And Countermeasures In Cloud Computing

This timely book offers you a solid understanding of the critical facets of homeland security, including threats, countermeasures, and privacy. You find important discussions on how to overcome challenges in today's information systems and how to analyze emerging phenomena in large complex systems. The book offers detailed guidance on the model-based design of trustworthy health information systems. Moreover, you get an in-depth overview of the detection, identification, and track of dangerous materials. This comprehensive resource also explores urban defense using mobile sensor platforms, focusing on both surveillance and protection. Supported with nearly 100 illustrations, Homeland Security Facets includes detailed case studies and real-world examples.

This is the must-have book for a must-know field. Today, general security knowledge is mandatory, and, if you who need to understand the fundamentals, Computer Security Basics 2nd Edition is the book to consult. The new edition builds on the well-established principles developed in the original edition and thoroughly updates that core knowledge. For anyone involved with computer security, including security administrators, system administrators, developers, and IT managers, Computer Security Basics 2nd Edition offers a clear overview of the security concepts you need to know, including access controls, malicious software, security policy, cryptography, biometrics, as well as government regulations and standards. This handbook describes complicated concepts such as trusted systems, encryption, and
mandatory access control in simple terms. It tells you what you need to know to understand the basics of computer security, and it will help you persuade your employees to practice safe computing. Topics include: Computer security concepts Security breaches, such as viruses and other malicious programs Access controls Security policy Web attacks Communications and network security Encryption Physical security and biometrics Wireless network security Computer security and requirements of the Orange Book OSI Model and TEMPEST Securing the Internet of Things provides network and cybersecurity researchers and practitioners with both the theoretical and practical knowledge they need to know regarding security in the Internet of Things (IoT). This booming field, moving from strictly research to the marketplace, is advancing rapidly, yet security issues abound. This book explains the fundamental concepts of IoT security, describing practical solutions that account for resource limitations at IoT end-node, hybrid network architecture, communication protocols, and application characteristics. Highlighting the most important potential IoT security risks and threats, the book covers both the general theory and practical implications for people working in security in the Internet of Things. Helps researchers and practitioners understand the security architecture in IoT and the state-of-the-art in IoT security countermeasures Explores how the threats in IoT are different from traditional ad hoc or infrastructural networks Provides a comprehensive discussion on the security challenges and solutions in RFID, WSNs, and IoT Contributed material by Dr. Imed Romdhani 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.

Computers at Risk presents a comprehensive agenda for developing nationwide policies and practices for computer security. Specific recommendations are provided for industry and for government agencies engaged in computer security activities. The volume also outlines problems and opportunities in computer security research, recommends ways to improve the research infrastructure, and suggests topics for investigators. The book explores the diversity of the field, the need to engineer countermeasures based on speculation of what experts think computer attackers may do next, why the technology community has failed to respond to the need for enhanced security systems, how innovators could be encouraged to bring more options to the marketplace, and balancing the importance of security against the right of privacy.

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.

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.

This book presents a new threat modelling approach that specifically targets the hardware supply chain, covering security risks throughout the lifecycle of an electronic system. The authors present a case study on a new type of security attack, which
combines two forms of attack mechanisms from two different stages of the IC supply chain. More specifically, this attack targets the newly developed, light cipher (Ascon) and demonstrates how it can be broken easily, when its implementation is compromised with a hardware Trojan. This book also discusses emerging countermeasures, including anti-counterfeit design techniques for resources constrained devices and anomaly detection methods for embedded systems.

In today’s modern age of information, new technologies are quickly emerging and being deployed into the field of information technology. Cloud computing is a tool that has proven to be a versatile piece of software within IT. Unfortunately, the high usage of Cloud has raised many concerns related to privacy, security, and data protection that have prevented cloud computing solutions from becoming the prevalent alternative for mission critical systems. Up-to-date research and current techniques are needed to help solve these vulnerabilities in cloud computing. Modern Principles, Practices, and Algorithms for Cloud Security is a pivotal reference source that provides vital research on the application of privacy and security in cloud computing. While highlighting topics such as chaos theory, soft computing, and cloud forensics, this publication explores present techniques and methodologies, as well as current trends in cloud protection. This book is ideally designed for IT specialists, scientists, software developers, security analysts, computer engineers, academicians, researchers, and students seeking current research on the defense of cloud services.
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.

"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--

A guide to the current technologies related to the delivery process for both live and on-demand services within IPTV delivery networks

IPTV Delivery Networks is an important resource that offers an in-depth discussion to the IPTV (Internet Protocol Television) delivery networks for both live and on-demand IPTV services. This important book also includes a review of the issues and challenges surrounding the delivery of IPTV over various emerging networking and communications technologies. The authors — an international team of experts — introduce a framework for delivery network applicable for live and video-on-demand services. They review the fundamental issues of IPTV delivery networks and explore the QoS (Quality of Service) issue for IPTV delivery networks that highlights the questions of security and anomaly detection as related to quality. IPTV Delivery Networks also contains a discussion of the mobility issues and next-generation delivery networks. This guide captures the latest available and usable technologies in the field and: Explores the technologies related to delivery process for both live (real time) and on-demand services in highly accessible terms.

Includes
information on the history, current state and future of IPTV delivery. Reviews all the aspects of delivery networks including storage management, resource allocation, broadcasting, video compression, QoS and QoE. Contains information on current applications including Netflix (video on demand), BBC iPlayer (time-shifted IPTV) and live (real time) streaming. Written for both researchers and industrial experts in the field of IPTV delivery networks. IPTV Delivery Networks is a groundbreaking book that includes the most current information available on live and on demand IPTV services. This new CTR report addresses the multifaceted threats facing organizations conducting business over the Internet and suggests countermeasures to them. The increased use of automated attack tools, the growing threat from viruses and the threat from competitors are detailed. The effective use of countermeasures such as firewalls, intrusion detection systems (IDS), virtual private networks (VPNs) and strong authentication are also discussed. Bluetooth is a technology for short range wireless communication. It can be used to connect almost any device to another device. Bluetooth-enabled devices, such as mobile phones, headsets, PCs, laptops, printers, mice, and keyboards, are widely used all over the world. Therefore, it is very important to keep Bluetooth security issues up-to-date. The aim of this book is to evaluate security threats in Bluetooth-enabled systems. The book concentrates on practical aspects of Bluetooth security: weaknesses of Bluetooth security are studied, new attacks are proposed, new Bluetooth security...
analysis tools are implemented, practical experiments are carried out in our research laboratory, vulnerability evaluation is performed, countermeasures against discovered attacks are proposed, a comparative analysis of the Man-In-The-Middle attacks on Bluetooth is presented, a novel system for detecting and preventing intrusions in Bluetooth networks is proposed, and a further classification of Bluetooth-enabled networks is provided. This book helps all kinds of Bluetooth users, from home users to IT enterprise experts, to make sure that the security of their Bluetooth networks is strong enough!

The book covers a decade of work with some of the largest commercial and government agencies around the world in addressing cyber security related to malicious insiders (trusted employees, contractors, and partners). It explores organized crime, terrorist threats, and hackers. It addresses the steps organizations must take to address insider threats at a people, process, and technology level. Today’s headlines are littered with news of identity thieves, organized cyber criminals, corporate espionage, nation-state threats, and terrorists. They represent the next wave of security threats but still possess nowhere near the devastating potential of the most insidious threat: the insider. This is not the bored 16-year-old hacker. We are talking about insiders like you and me, trusted employees with access to information - consultants, contractors, partners, visitors, vendors, and cleaning crews. Anyone in an organization’s building or networks that possesses some level of trust. * Full coverage of this hot topic for virtually every global 5000 organization, government agency, and individual interested in security. * Brian Contos is the Chief Security Officer for one of the most well
known, profitable and respected security software companies in the U.S.—ArcSight. 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

This fully-updated, integrated self-study system offers complete coverage of the revised 2015 Systems Security Certified Practitioner (SSCP) exam domains. Thoroughly revised for the April 2015 exam update, SSCP Systems Security Certified Practitioner All-in-One Exam Guide, Second Edition enables you to take the exam with complete confidence. To aid in self-study, each chapter includes Exam Tips that highlight key exam information, chapter summaries that reinforce salient points, and end-of-chapter questions that are an accurate reflection of the content and question format of the real exam. Beyond exam prep, the practical examples and real-world insights offered in this guide make it an ideal on-the-job reference for IT security professionals. You will learn the security concepts, tools, and procedures needed to employ and enforce solid security policies and effectively react to security incidents. Features 100% coverage of the revised SSCP Common Body of Knowledge (CBK), effective April 2015 CD-ROM contains two full-length, customizable practice exams in the Total Tester exam engine and a searchable PDF copy of the book. Written by a bestselling IT security certification and training expert

This book looks at network security in a new and refreshing way. It guides readers step-by-step through the "stack" -- the seven layers of a network. Each chapter focuses on one layer of the stack along with the attacks, vulnerabilities, and exploits that can be found at that layer.
The book even includes a chapter on the mythical eighth layer: The people layer. This book is designed to offer readers a deeper understanding of many common vulnerabilities and the ways in which attacker’s exploit, manipulate, misuse, and abuse protocols and applications. The authors guide the readers through this process by using tools such as Ethereal (sniffer) and Snort (IDS). The sniffer is used to help readers understand how the protocols should work and what the various attacks are doing to break them. IDS is used to demonstrate the format of specific signatures and provide the reader with the skills needed to recognize and detect attacks when they occur. What makes this book unique is that it presents the material in a layer by layer approach which offers the readers a way to learn about exploits in a manner similar to which they most likely originally learned networking. This methodology makes this book a useful tool to not only security professionals but also for networking professionals, application programmers, and others. All of the primary protocols such as IP, ICMP, TCP are discussed but each from a security perspective. The authors convey the mindset of the attacker by examining how seemingly small flaws are often the catalyst of potential threats. The book considers the general kinds of things that may be monitored that would have alerted users of an attack. * Remember being a child and wanting to take something apart, like a phone, to see how it worked? This book is for you then as it details how specific hacker tools and techniques accomplish the things they do. * This book will not only give you knowledge of security tools but will provide you the ability to design more robust security solutions * Anyone can tell you what a tool does but this book shows you how the tool works

Our world is increasingly driven by sophisticated networks of advanced computing technology, and the basic operation of everyday society is becoming increasingly vulnerable to those
networks’ shortcomings. The implementation and upkeep of a strong network defense is a substantial challenge, beset not only by economic disincentives, but also by an inherent logistical bias that grants advantage to attackers. Network Security Attacks and Countermeasures discusses the security and optimization of computer networks for use in a variety of disciplines and fields. Touching on such matters as mobile and VPN security, IP spoofing, and intrusion detection, this edited collection emboldens the efforts of researchers, academics, and network administrators working in both the public and private sectors. This edited compilation includes chapters covering topics such as attacks and countermeasures, mobile wireless networking, intrusion detection systems, next-generation firewalls, and more. In Securing VoIP Networks, two leading experts systematically review the security risks and vulnerabilities associated with VoIP networks and offer proven, detailed recommendations for securing them. Drawing on case studies from their own fieldwork, the authors address VoIP security from the perspective of real-world network implementers, managers, and security specialists. The authors identify key threats to VoIP networks, including eavesdropping, unauthorized access, denial of service, masquerading, and fraud; and review vulnerabilities in protocol design, network architecture, software, and system configuration that place networks at risk. They discuss the advantages and tradeoffs associated with protection mechanisms built into SIP, SRTP, and other VoIP protocols; and review key management solutions such as MIKEY and ZRTP. Next, they present a complete security framework for enterprise VoIP networks, and provide detailed architectural guidance for both service providers and enterprise users. 1 Introduction 2 VoIP Architectures and Protocols 3 Threats and Attacks 4 VoIP Vulnerabilities 5 Signaling Protection Mechanisms 6 Media Protection Mechanisms 7 Key
Cyber security has become a topic of concern over the past decade. As many individual and organizational activities continue to evolve digitally, it is important to examine the psychological and behavioral aspects of cyber security. Psychological and Behavioral Examinations in Cyber Security is a critical scholarly resource that examines the relationship between human behavior and interaction and cyber security. Featuring coverage on a broad range of topics, such as behavioral analysis, cyberpsychology, and online privacy, this book is geared towards IT specialists, administrators, business managers, researchers, and students interested in online decision making in cybersecurity.

Cyber attacks are rapidly becoming one of the most prevalent issues in the world. As cyber crime continues to escalate, it is imperative to explore new approaches and technologies that help ensure the security of the online community. The Handbook of Research on Threat Detection and Countermeasures in Network Security presents the latest methodologies and trends in detecting and preventing network threats. Investigating the potential of current and emerging security technologies, this publication is an all-inclusive reference source for academicians, researchers, students, professionals, practitioners, network analysts, and technology specialists interested in the simulation and application of computer network protection.

Technological advances, although beneficial and progressive, can lead to vulnerabilities in system networks and security. While researchers attempt to find solutions, negative uses of
technology continue to create new security threats to users. New Threats and Countermeasures in Digital Crime and Cyber Terrorism brings together research-based chapters and case studies on security techniques and current methods being used to identify and overcome technological vulnerabilities with an emphasis on security issues in mobile computing and online activities. This book is an essential reference source for researchers, university academics, computing professionals, and upper-level students interested in the techniques, laws, and training initiatives currently being implemented and adapted for secure computing.

New Threats and Countermeasures in Digital Crime and Cyber Terrorism provides the best practices needed to protect a company's most sensitive information. It takes a proactive approach, explaining the measures and countermeasures that can be enacted to identify both threats and weaknesses. The text fully explains the threat landscape, showing not only how spies operate, but how they can be detected. Drawn from the author's 40 years of experience, this vital resource will give readers a true understanding of the threat of business spying and what businesses can do to protect themselves. It is ideal for use as a tool to educate staff on the seriousness of the threat of business espionage. Shows how to identify a company's threats, weaknesses, and most critical assets Provides proven and practical countermeasures that any business can employ to protect their most sensitive assets from both internal and external threats Uses real-life case studies and examples to help the reader understand how to apply the tactics discussed

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. This book on computer security threats explores the computer security threats and includes a broad set of solutions to defend the computer systems from these threats. The book is triggered by the understanding that digitalization and growing dependence on the Internet poses an increased risk of computer security threats in the modern world. The chapters discuss different research frontiers in computer security with algorithms and implementation details for use in the real world. Researchers and practitioners in areas such as statistics, pattern recognition, machine learning, artificial intelligence, deep learning, data mining, data analytics and visualization are contributing to the field of computer security. The intended audience of this book will mainly consist of researchers, research students, practitioners, data analysts, and business professionals who seek information on computer security threats and
its defensive measures.

This book presents the proceedings of the International Conference on Computing Networks, Big Data and IoT [ICCBI 2019], held on December 19–20, 2019 at the Vaigai College of Engineering, Madurai, India. Recent years have witnessed the intertwining development of the Internet of Things and big data, which are increasingly deployed in computer network architecture. As society becomes smarter, it is critical to replace the traditional technologies with modern ICT architectures. In this context, the Internet of Things connects smart objects through the Internet and as a result generates big data. This has led to new computing facilities being developed to derive intelligent decisions in the big data environment. The book covers a variety of topics, including information management, mobile computing and applications, emerging IoT applications, distributed communication networks, cloud computing, and healthcare big data. It also discusses security and privacy issues, network intrusion detection, cryptography, 5G/6G networks, social network analysis, artificial intelligence, human–machine interaction, smart home and smart city applications.

This book constitutes the refereed proceedings of the First Asian Internet Engineering Conference, AINTEC 2005, held in Bangkok, Thailand in December 2005. The 18 revised full papers presented together with 3 invited papers and 1 invited position paper were carefully reviewed and selected from 52 submissions. The papers are organized in topical sections on wireless, mobility and emergency network, routing in ad-hoc network, extending manet, securing network, multi-services in IP-based networks, as well as measurement and performance.
analysis.
This book investigates the way that the molecular sciences are shaping contemporary security practices in relation to the governance of biological threats. In response to biological threats, such as pandemics and bioterrorism, governments around the world have developed a range of new security technologies, called medical countermeasures, to protect their populations. This book argues that the molecular sciences’ influence has been so great that security practices have been molecularised. Focusing on the actions of international organisations and governments in the past two decades, this book identifies two contrasting conceptions of the nature or inherent workings of molecular life as driving this turn. On the one hand, political notions of insecurity have been shaped by the contingent or random nature of molecular life. On the other, the identification of molecular life’s constant biological dynamics supports and makes possible the development and stockpiling of effective medical countermeasures. This study is one of the few to take seriously the conceptual implications that the detailed empirical workings of biotechnology have on security practices today. This book will be of much interest to students of security studies, bio-politics, life sciences, global governance, and International Relations in general.
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.

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.

Copyright: f22a69cecf655cb09509b9c3168f073f