New Threats And Countermeasures In Digital Crime And Cyber Terrorism Advances In Digital Crime Forensics And Cyber Terrorism

This book constitutes the proceedings of the 8th International Conference on Applied Cryptography and Network Security, ACNS 2010, held in Beijing, China, in June 2010. The 32 papers presented in this volume were carefully reviewed and selected from 178 submissions. The papers are divided in topical sections on public key encryption, digital signature, block ciphers and hash functions, side-channel attacks, zero knowledge and multi-party protocols, key management, authentication and identification, privacy and anonymity, RFID security and privacy, and internet security.
Algorithms for Automating Open Source Intelligence (OSINT) presents information on the gathering of information and extraction of actionable intelligence from openly available sources, including news broadcasts, public repositories, and more recently, social media. As OSINT has applications in crime fighting, state-based intelligence, and social research, this book provides recent advances in text mining, web crawling, and other algorithms that have led to advances in methods that can largely automate this process. The book is beneficial to both practitioners and academic researchers, with discussions of the latest advances in applications, a coherent set of methods and processes for automating OSINT, and interdisciplinary perspectives on the key problems identified within each discipline. Drawing upon years of practical experience and using numerous examples, editors Robert Layton, Paul Watters, and a distinguished list of contributors discuss Evidence Accumulation Strategies for OSINT, Named Entity Resolution in Social Media, Analyzing Social Media Campaigns for Group Size Estimation, Surveys and qualitative techniques in OSINT, and Geospatial reasoning of open data. Presents a coherent set of methods and processes for automating OSINT Focuses on algorithms and applications allowing the practitioner to get up and running quickly Includes fully developed case studies on the digital underground and predicting crime through OSINT Discusses the ethical considerations when using publicly available online data
In the modern world, natural disasters are becoming more commonplace, unmanned systems are becoming the norm, and terrorism and espionage are increasingly taking place online. All of these threats have made it necessary for governments and organizations to steel themselves against these threats in innovative ways. Developing Next-Generation Countermeasures for Homeland Security Threat Prevention provides relevant theoretical frameworks and empirical research outlining potential threats while exploring their appropriate countermeasures. This relevant publication takes a broad perspective, from network security, surveillance, reconnaissance, and physical security, all topics are considered with equal weight. Ideal for policy makers, IT professionals, engineers, NGO operators, and graduate students, this book provides an in-depth look into the threats facing modern society and the methods to avoid them.
Cyber Attacks, Student Edition, offers a technical, architectural, and management approach to solving the problems of protecting national infrastructure. This approach includes controversial themes such as the deliberate use of deception to trap intruders. This volume thus serves as an attractive framework for a new national strategy for cyber security. A specific set of criteria requirements allows any organization, such as a government agency, to integrate the principles into their local environment. In this edition, each principle is presented as a separate security strategy and illustrated with compelling examples. The book adds 50-75 pages of new material aimed specifically at enhancing the student experience and making it more attractive for instructors teaching courses such as cyber security, information security, digital security, national security, intelligence studies, technology and infrastructure protection. It now also features case studies illustrating actual implementation scenarios of the principles and requirements discussed in the text, along with a host of new pedagogical elements, including chapter outlines, chapter summaries, learning checklists, and a 2-color interior. Furthermore, a new and complete ancillary package includes test bank, lesson plans, PowerPoint slides, case study questions, and more. This text is intended for security practitioners and military personnel as well as for students wishing to become security engineers, network operators, software designers, technology managers, application developers, etc. Provides case studies focusing on cyber security challenges and solutions to display how theory, research, and methods, apply to real-life challenges Utilizes, end-of-chapter case problems that take chapter content and relate it to real security situations and issues Includes instructor slides for each chapter as well as an instructor’s manual with sample syllabi and test bank
Deploying an appropriate collection of information security countermeasures in an organization should result in high-level blocking power against existing threats. In this chapter, a new knapsack-based approach is proposed for finding out which subset of countermeasures is the best at preventing probable security attacks. In this regard, an effectiveness score is defined for each countermeasure based on its mitigation level against all threats. Organizations are always looking for more effective low-cost solutions, so another consideration is that the implementation cost of the selected countermeasure portfolio should not exceed the allocated budget. Following the knapsack idea, the implementation cost of each countermeasure and its effectiveness, defined as inputs and the best subset, are chosen with respect to budget limits. Our results are compared with similar research and recommend the same countermeasure portfolio.
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.

The current structure of the chapters reflects the key aspects discussed in the papers but the papers themselves contain more additional interesting information: examples of a practical application and results obtained for existing networks as well as results of experiments confirming efficacy of a synergistic analysis of anomaly detection and signature detection, and application of interesting solutions, such as an analysis of the anomalies of user behaviors and many others.

This report reviews past NRC studies that have examined various dimensions of computer and network security and vulnerability and brings the results forward into the context of the current environment of security and vulnerability. The review includes work done since 1991, such as Computers at Risk (1991), Cryptographyâ€™s Role in Securing the Information Society (1996), For the Record: Protecting Electronic Health Information (1997), Trust in Cyberspace (1999), Continued Review of the Tax Systems Modernization of the Internal Revenue Service (1996), Realizing the Potential of C4I (1999), and Embedded, Everywhere (2001).

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.

Synthetic biology is a field of biotechnology that is rapidly growing in various applications, such as in medicine, environmental sustainability, and energy production. However these technologies also have unforeseen risks and applications to humans and the environment. This open access book presents discussions on risks and mitigation strategies for these technologies including biosecurity, or the potential of synthetic biology technologies and processes to be deliberately misused for nefarious purposes. The book presents strategies to prevent, mitigate, and recover from 'dual-use concern' biosecurity challenges that may be raised by individuals, rogue states, or non-state actors. Several key topics are explored including opportunities to develop more coherent and scalable approaches to govern biosecurity from a laboratory perspective up to the international scale and strategies to prevent potential health and environmental hazards posed by deliberate misuse of synthetic biology without stifling innovation. The book brings together the expertise of top scholars in synthetic biology and biotechnology risk assessment, management, and communication to discuss potential biosecurity governing strategies and offer perspectives for collaboration in oversight and future regulatory guidance.

New Threats and Countermeasures in Digital Crime and Cyber TerrorismIGI Global

Provides research on the social and human aspects of information security. Presents the latest trends, issues, and findings in the field.

The internet is established in most households worldwide and used for entertainment purposes, shopping, social networking, business activities, banking, telemedicine, and more. As more individuals and businesses use this essential tool to connect with each other and consumers, more private data is exposed to criminals ready to exploit it for their gain. Thus, it is essential to continue discussions involving policies that regulate and monitor these activities, and anticipate new laws that should be implemented in order to protect users. Cyber Law, Privacy, and Security: Concepts, Methodologies, Tools, and Applications examines current internet and data protection laws and their impact on user experience and cybercrime, and explores the need for further policies that protect user identities, data, and privacy. It also offers the latest methodologies and applications in the areas of digital security and threats. Highlighting a range of topics such as online privacy and security, hacking, and online threat protection, this multi-volume book is ideally designed for IT specialists, administrators, policymakers, researchers, academicians, and upper-level students.

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 Vulnerabilites 5 Signaling Protection Mechanisms 6 Media Protection

Mechanisms 7 Key Management Mechanisms 8 VoIP and Network Security Controls 9 A Security Framework for Enterprise VoIP Networks 10 Provider Architectures and Security 11 Enterprise Architectures and Security

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.

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, instrusion detection systems (IDS), virtual private networks (VPNs) and strong authentication are also discussed.

"This book addresses the fact that managing information security program while effectively managing risks has never been so critical, discussing issues such as emerging threats and countermeasures for effective management of information security in organizations"--Provided by publisher.

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.

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 this introductory volume, readers will learn about the vital role that the various Critical Infrastructure (CI) sectors play in America, in the context of homeland security. The protection, maintenance, and monitoring of these interdependent CI assets is a shared responsibility of governments, private sector owner/operators, first responders, and all those involved in homeland security and emergency management. As this foundational learning resource demonstrates, rapidly advancing technologies combined with exponential growth in demand on the aging infrastructure of America’s power grid is setting the stage for a potentially catastrophic collapse that would paralyze each and every facet of civilian life and military operations. This meticulously researched primer will guide readers through the known world of power failures and cyber-attacks to the emerging threat from a High-altitude Electromagnetic Pulse (HEMP). A HEMP would cause cascading failures in the power grid, communications, water treatment facilities, oil refineries, pipelines, banking, supply chain management, food production, air traffic control, and all forms of transportation. Each chapter in America’s Greatest Existential Threat (Vol. 1) begins with learning objectives and ends with a series of review questions to assess take-up of the chapter material. Similarly, subsequent volumes will explore HEMP and emerging issues in closer detail with current research and analysis now in development.

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.

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.

The mobile threat landscape is evolving bringing about new forms of data loss. No longer can organizations rely on security policies designed during the PC era. Mobile is different and therefore requires a revised approach to countermeasures to mitigate data loss. Understanding these differences is fundamental to creating a new defense-in-depth strategy designed for mobile. Mobile Data Loss: Threats & Countermeasures reviews the mobile threat landscape using a hacker mind-set to outline risks and attack vectors that include malware, risky apps, operating system compromises, network attacks, and user behaviours. This provides the basis for then outlining countermeasures for defining a holistic mobile security methodology that encompasses proactive protections, response mechanisms, live monitoring, and incident response. Designing a comprehensive mobile security strategy is key. Mobile Data Loss: Threats & Countermeasures outlines the threats and strategies for protecting devices from a plethora of data loss vectors. Outlines differences in mobile devices versus PCs Reviews mobile threat landscape using a hacker mind-set to outline risks and attack vectors Summarizes the tools and techniques for implementing enterprise countermeasures Maps mobile to common security compliances including PCI, HIPAA, and CJIS Provides a defense-in-depth methodology and strategy for enterprises to minimize data loss

Cyber security has become a topic of concern over the past decade as private industry, public administration, commerce, and communication have gained a greater online presence. As many individual and organizational activities continue to evolve in the digital sphere, new vulnerabilities arise. Cyber Security and Threats: Concepts, Methodologies, Tools, and Applications contains a compendium of the latest academic material on new methodologies and applications in the areas of digital security and threats. Including innovative studies on cloud security, online threat protection, and cryptography, this multi-volume book is an ideal source for IT specialists, administrators, researchers, and students interested in uncovering new ways to thwart cyber breaches and protect sensitive digital information.

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!

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.

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.

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.

Reliable positioning and navigation is becoming imperative in more and more applications for public services, consumer products, and safety-critical purposes. Research for finding pervasive and robust positioning methodologies is critical for a growing amount of societal areas while making sure that navigation is trustworthy and the risks and threats of especially satellite navigation are accounted for. This book provides a comprehensive survey of the effect of radio-frequency interference (RFI) on the Global Navigation Satellite Systems (GNSS) as well as of the spoofing threats. Through case studies and practical implementation/applications, this resource presents engineers and scientists with a better understanding of interference and spoofing threats, ultimately helping them to design and implement robust systems.

Business Espionage: Risk, Threats, and Countermeasures 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

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.

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.

"This thesis examined the three core themes: the role of education in cyber security, the role of technology in cyber security, and the role of policy in cyber security, the areas in which the papers are published. The associated works are published in referred journals, peer reviewed book chapters, and conference proceedings. Research can be found in the following outlets: 1. Security Solutions for Hyperconnectivity and the Internet of Things; 2. Developing Next-Generation Countermeasures for Homeland Security Threat Prevention; 3. New Threats and Countermeasures in Digital Crime and Cyber Terrorism; 4. International Journal of Business Continuity and Risk Management; 5. Handbook of Research on 3-D Virtual Environments and Hypermedia for Ubiquitous Learning; 6. Information Security in Diverse Computing Environments; 7. Technology, Innovation, and Enterprise Transformation; 8. Journal of Information Systems Technology and Planning; 9. Encyclopedia of Information Science and Technology. The shortcomings and gaps in cyber security research is the research focus on hyperconnectivity of people and technology to include the policies that provide the standards for security hardened systems. Prior research on cyber and homeland security reviewed the three core themes separately rather than jointly. This study examined the research gaps within cyber security as it relates to core themes in an effort to develop stronger policies, education programs, and hardened technologies for cyber security use. This work illustrates how cyber security can be broken into these three core areas and used together to address issues such as developing training environments for teaching real cyber security events. It will further show the correlations between technologies and policies for system Certification & Accreditation (C&A). Finally, it will offer insights on how cyber security can be used to maintain security for international and national security. The overall results of the study provide guidance on how to create an ubiquitous learning (U-Learning) environment to teach cyber security concepts, craft polices that affect secure computing, and examines the effects on national and international security. The overall research has been improving the role of cyber security in education, technology, and policy." -- Abstract.