Attack Prevention Detection And Response Tum Info Viii

MATA BALDWIN

Intelligent Communication Technologies and Virtual Mobile Networks Springer Science & Business Media
Stories of massive data breaches litter the 24-hour newsday headlines. Hackers and cybercrime syndicates are hitting a who's who of banks, retailers, law firms, and healthcare organizations: companies with sophisticated security systems designed to stop crime before it starts. They're also hitting companies that thought they were too small to matter. So how do cybercriminals continue to breach the defenses of the big companies--and why do they go after the small ones? And, most importantly, how can companies of all sizes protect themselves? Cybersecurity expert Mark Sangster deftly weaves together real-life cases in a thrilling narrative that illustrates the human complexities behind the scenes that can lead to companies throwing their digital front doors open to criminals. Within a security context, deep social engineering is the newest and biggest means of breaching our systems. Sangster shows readers that cybersecurity is not an IT problem to solve--it is a business risk to manage. Organizations need to shift the security discussion away from technology gates alone toward a focus on leadership, team behaviors, and mutual support. Sangster punctuates his eye-opening narratives with sets of questions businesspeople at all levels need to ask themselves, facts they need to know, and principles they need to follow to keep their companies secure.
Intrusion Prevention and Active Response IGI Global
"This book provides a valuable resource by addressing the most pressing issues facing cyber-security from both a national and global perspective"--Provided by publisher.
Cybersecurity for Hospitals and Healthcare Facilities Springer
Annotation. This book constitutes the refereed proceedings of the International Workshops on Service-Oriented Computing, ICSOC/ServiceWave 2009, held in Stockholm, Sweden, in November 2009. The book includes papers of workshops on trends in enterprise architecture research (TEAR 2009), SOA, globalization, people, and work (SG-PAW), service oriented computing in logistics (SOC-LOG), non-functional properties and service level agreements management in service oriented computing (NFPSLAM-SOC 09), service monitoring, adaptation and beyond (MONA+), engineering service-oriented applications (WESOA09), and user-generated services (UGS2009). The papers are organized in topical sections on business models and architecture; service quality and service level agreements track; and service engineering track.
Security in Computing and Communications John Wiley & Sons
“Practical Intrusion Analysis provides a solid fundamental overview of the art and science of intrusion analysis.” –Nate Miller, Cofounder, Stratum Security The Only Definitive Guide to New State-of-the-Art Techniques in Intrusion Detection and Prevention Recently, powerful innovations in intrusion detection and prevention have evolved in response to emerging threats and changing business environments. However, security practitioners have found little reliable, usable information about these new IDS/IPS technologies. In Practical Intrusion Analysis, one of the field’s leading experts brings together these innovations for the first time and demonstrates how they can be used to analyze attacks, mitigate damage, and

track attackers. Ryan Trost reviews the fundamental techniques and business drivers of intrusion detection and prevention by analyzing today's new vulnerabilities and attack vectors. Next, he presents complete explanations of powerful new IDS/IPS methodologies based on Network Behavioral Analysis (NBA), data visualization, geospatial analysis, and more. Writing for security practitioners and managers at all experience levels, Trost introduces new solutions for virtually every environment. Coverage includes Assessing the strengths and limitations of mainstream monitoring tools and IDS technologies Using Attack Graphs to map paths of network vulnerability and becoming more proactive about preventing intrusions Analyzing network behavior to immediately detect polymorphic worms, zero-day exploits, and botnet DoS attacks Understanding the theory, advantages, and disadvantages of the latest Web Application Firewalls Implementing IDS/IPS systems that protect wireless data traffic Enhancing your intrusion detection efforts by converging with physical security defenses Identifying attackers' "geographical fingerprints" and using that information to respond more effectively Visualizing data traffic to identify suspicious patterns more quickly Revisiting intrusion detection ROI in light of new threats, compliance risks, and technical alternatives Includes contributions from these leading network security experts: Jeff Forristal, a.k.a. Rain Forest Puppy, senior security professional and creator of libwhisker Seth Fogie, CEO, Airscanner USA; leading-edge mobile security researcher; coauthor of Security Warrior Dr. Sushil Jajodia, Director, Center for Secure Information Systems; founding Editor-in-Chief, Journal of Computer Security Dr. Steven Noel, Associate Director and Senior Research Scientist, Center for Secure Information Systems, George Mason University Alex Kirk, Member, Sourcefire Vulnerability Research Team

Cybersecurity Attacks – Red Team Strategies Springer

The Complete Guide to Understanding the Structure of Homeland Security Law New topics featuring leading authors cover topics on Security Threats of Separatism, Secession and Rightwing Extremism; Aviation Industry's 'Crew Resource Management' Principles'; and Ethics, Legal, and Social Issues in Homeland Security Legal, and Social Issues in Homeland Security. In addition, the chapter devoted to the Trans-Pacific Partnership is a description of economic statecraft, what we really gain from the TPP, and what we stand to lose. The Power of Pop Culture in the Hands of ISIS describes how ISIS communicates and how pop culture is used expertly as a recruiting tool Text organized by subject with the portions of all the laws related to that particular subject in one chapter, making it easier to reference a specific statute by topic Allows the reader to recognize that homeland security involves many specialties and to view homeland security expansively and in the long-term Includes many references as a resource for professionals in various fields including: military, government, first responders, lawyers, and students Includes an Instructor Manual providing teaching suggestions, discussion questions, true/false questions, and essay questions along with the answers to all of these

Critical Infrastructure Security Apress

Computer and network systems have given us unlimited opportunities of reducing cost, improving efficiency, and increasing revenues, as demonstrated by an increasing number of computer and network applications. Yet, our dependence on computer and network systems has also exposed us to new risks, which threaten the security of, and present new challenges for protecting our assets and information on computer and network systems. The reliability of computer and network systems ultimately depends on security and quality of service (QoS) performance. This book presents quantitative modeling and analysis techniques to address these numerous challenges in cyber attack prevention and detection for security and QoS, including: the latest research on computer and network behavior under attack and normal use conditions; new design principles and algorithms, which can be used by engineers and practitioners to build secure computer and network systems, enhance security practice and move to providing QoS assurance on the Internet; mathematical and statistical methods for achieving the accuracy and timeliness of cyber attack detection with the lowest computational overhead; guidance on managing admission control, scheduling, reservation and service of computer and network jobs to assure the service stability and end-to-end delay of those jobs even under Denial of Service attacks or abrupt demands. Secure Computer and Network Systems: Modeling, Analysis and Design is an up-to-date resource for practising engineers and researchers involved in security, reliability and quality management of computer and network systems. It is also a must-read for postgraduate students developing advanced technologies for improving computer network dependability.

Service-Oriented Computing. ICSOC/ServiceWave 2009 Workshops Greenwood Publishing Group

Heterogeneous Computing Architectures: Challenges and Vision provides an updated vision of the state-of-the-art of heterogeneous computing systems, covering all the aspects related to their design: from the architecture and programming models to hardware/software integration and orchestration to real-time and security requirements. The transitions from multicore processors, GPU computing, and Cloud computing are not separate trends, but aspects of a single trend-mainstream; computers from desktop to smartphones are being permanently transformed into heterogeneous supercomputer clusters. The reader will get an organic perspective of modern heterogeneous systems and their future evolution.

Network Intrusion Detection and Prevention Packt Publishing Ltd

These proceedings contain the papers of IFIP/SEC 2010. It was a special honour and privilege to chair the Program Committee and prepare the proceedings for this conf- ence, which is the 25th in a series of well-established international conferences on security and privacy organized annually by Technical Committee 11 (TC-11) of IFIP. Moreover, in 2010 it is part of the IFIP World Computer Congress 2010 celebrating both the Golden Jubilee of IFIP (founded in 1960) and the Silver Jubilee of the SEC conference in the exciting city of Brisbane, Australia, during September 20–23. The call for papers went out with the challenging motto of "Security & Privacy Silver Linings in the Cloud" building a bridge between the long standing issues of security and privacy and the most recent developments in information and commu- cation technology. It attracted 102 submissions. All of them were evaluated on the basis of their significance, novelty, and technical quality by at least five member of the Program Committee. The Program Committee meeting was held electronically over a period of a week. Of the papers submitted, 25 were selected for presentation at the conference; the acceptance rate was therefore as low as 24. 5% making SEC 2010 a highly competitive forum. One of those 25 submissions could unfortunately not be included in the proceedings, as none of its authors registered in time to present the paper at the conference.

Information Systems Security Page Two

This book constitutes the refereed proceedings of the 7th International Symposium on Security in Computing and Communications, SSCC 2019, held in Trivandrum, India, in December 2019. The 22 revised full papers and 7 revised short papers presented were carefully reviewed and selected from 61 submissions. The papers cover wide research fields including cryptography, database and storage security, human and societal aspects of security and privacy.

Cyber Security Innovation for the Digital Economy Springer

Presents theories and models associated with information privacy and safeguard practices to help anchor and guide the development of technologies, standards, and best practices. Provides recent, comprehensive coverage of all issues related to information security and ethics, as well as the opportunities, future challenges, and emerging trends related to this subject.

Information Security and Ethics: Concepts, Methodologies, Tools, and Applications Springer Science & Business Media

Our world is increasingly driven by sophisticated networks of advanced computing technology, and the basic operation of everyday society is becoming increasingly vulnerable to these 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. Research Anthology on Combating Denial-of-Service Attacks examines the latest research on the development of intrusion detection systems and best practices for preventing and combatting cyber-attacks intended to disrupt business and user experience. Highlighting a range of topics such as network administration, application-layer protocols, and malware detection, this publication is an ideal reference source for cybersecurity professionals, IT specialists, policymakers, forensic analysts, technology developers, security administrators, academicians, researchers, and students.

Cyber Security and Global Information Assurance: Threat Analysis and Response Solutions Springer

This book provides a comprehensive survey of state-of-the-art techniques for the security of critical infrastructures, addressing both logical and physical aspects from an engineering point of view. Recently developed methodologies and tools for CI analysis as well as strategies and technologies for CI protection are investigated in the following strongly interrelated and multidisciplinary main fields: - Vulnerability analysis and risk assessment - Threat prevention, detection and response - Emergency planning and management Each of the aforementioned topics is addressed considering both theoretical aspects and practical applications. Emphasis is given to model-based holistic evaluation approaches as well as to emerging protection technologies, including smart surveillance through networks of intelligent sensing devices. Critical Infrastructure Security can be used as a self-contained reference handbook for both practitioners and researchers or even as a textbook for master/doctoral degree students in engineering or related disciplines.More specifically, the topic coverage of the book includes: - Historical background on threats to critical infrastructures - Model-based risk evaluation and management approaches - Security surveys and game-theoretic vulnerability assessment - Federated simulation for interdependency analysis - Security operator training and emergency preparedness - Intelligent multimedia (audio-video) surveillance - Terahertz body scanners for weapon and explosive detection - Security system design (intrusion detection / access control) - Dependability and resilience of computer networks (SCADA / cyber-security) - Wireless smart-sensor networks and structural health monitoring - Information systems for crisis response and emergency management - Early warning, situation awareness and decision support software

Quantum Cryptography and the Future of Cyber Security McGraw Hill Professional

Many professionals and students in engineering, science, business, and other application fields need to develop Windows-based and web-enabled information systems to store and use data for decision support, without help from professional programmers. However, few books are available to train professionals and students who are not professional programmers to develop these information systems. Developing Windows-Based and Web-Enabled Information Systems fills this gap, providing a self-contained, easy-to-understand, and well-illustrated text that explores current concepts, methods, and software tools for developing Windows-based and web-enabled information systems. Written in an easily accessible style, the book details current concepts, methods, and software tools for Windows-based and web-enabled information systems that store and use data. It is self-contained with easy-to-understand small examples to walk through concepts and implementation details along with large-scale case studies. The book describes data modeling methods including entity–relationship modeling, relational modeling and normalization, and object-oriented data modeling, to develop data models of a database. The author covers how to use software tools in the Microsoft application development environment, including Microsoft Access, MySQL, SQL, Visual Studio, Visual Basic, VBA, HTML, and XML, to implement databases and develop Windows-based and web-enabled applications with the database, graphical user interface, and program components. The book takes you through the entire process of developing a computer and network application for an information system, highlighting concepts and operation details. In each chapter, small data examples are used to manually walk through concepts and operational details. These features and more give you the conceptual understanding and practical skill required, even if you don't have a computer science background, to develop Windows-based or web-enabled applications for your specialized information system.

Heterogeneous Computing Architectures CRC Press

This book presents the outcomes of the Intelligent Communication Technologies and Virtual Mobile Networks Conference (ICICV 2019) held in Tirunelveli, India, on February 14–15, 2019. It presents the state of the art in the field, identifying emerging research topics and communication technologies and defining the future of intelligent communication approaches and virtual computing. In light of the tremendous growth ICT, it examines the rapid developments in virtual reality in communication technology and high-quality services in mobile networks, including the integration of virtual mobile computing and communication technologies, which permits new technologies based on the resources and services of computational intelligence, big data analytics, Internet of Things (IoT), 5G technology, automation systems, sensor networks, augmented reality, data mining, and vehicular ad hoc networks with massive cloud-based backend. These services have a significant impact on all areas of daily life, like transportation, e-commerce, health care, secure communication, location detection, smart home, smart city, social networks and many more.

Machine Learning in Intrusion Detection John Wiley & Sons

Get to grips with security operations through incident response, the ATT&CK framework, active defense, and agile threat intelligence Key FeaturesExplore robust and predictable security operations based on measurable service performanceLearn how to improve the security posture and work on security auditsDiscover ways to integrate agile security operations into development and operationsBook Description Agile security operations allow organizations to survive cybersecurity incidents, deliver key insights into the security posture of an organization, and operate

security as an integral part of development and operations. It is, deep down, how security has always operated at its best. Agile Security Operations will teach you how to implement and operate an agile security operations model in your organization. The book focuses on the culture, staffing, technology, strategy, and tactical aspects of security operations. You'll learn how to establish and build a team and transform your existing team into one that can execute agile security operations. As you progress through the chapters, you'll be able to improve your understanding of some of the key concepts of security, align operations with the rest of the business, streamline your operations, learn how to report to senior levels in the organization, and acquire funding. By the end of this Agile book, you'll be ready to start implementing agile security operations, using the book as a handy reference. What you will learnGet acquainted with the changing landscape of security operationsUnderstand how to sense an attacker's motives and capabilitiesGrasp key concepts of the kill chain, the ATT&CK framework, and the Cynefin frameworkGet to grips with designing and developing a defensible security architectureExplore detection and response engineeringOvercome challenges in measuring the security postureDerive and communicate business values through security operationsDiscover ways to implement security as part of development and business operationsWho this book is for This book is for new and established CSOC managers as well as CISO, CDO, and CIO-level decision-makers. If you work as a cybersecurity engineer or analyst, you'll find this book useful. Intermediate-level knowledge of incident response, cybersecurity, and threat intelligence is necessary to get started with the book.

Visualization for Computer Security CRC Press

System administrators need to stay ahead of new security vulnerabilities that leave their networks exposed every day. A firewall and an intrusion detection systems (IDS) are two important weapons in that fight, enabling you to proactively deny access and monitor network traffic for signs of an attack. Linux Firewalls discusses the technical details of the iptables firewall and the Netfilter framework that are built into the Linux kernel, and it explains how they provide strong filtering, Network Address Translation (NAT), state tracking, and application layer inspection capabilities that rival many commercial tools. You'll learn how to deploy iptables as an IDS with psad and fwsnort and how to build a strong, passive authentication layer around iptables with fwknop. Concrete examples illustrate concepts such as firewall log analysis and policies, passive network authentication and authorization, exploit packet traces, Snort ruleset emulation, and more with coverage of these topics: –Passive network authentication and OS fingerprinting –iptables log analysis and policies –Application layer attack detection with the iptables string match extension –Building an iptables ruleset that emulates a Snort ruleset –Port knocking vs. Single Packet Authorization (SPA) –Tools for visualizing iptables logs Perl and C code snippets offer practical examples that will help you to maximize your deployment of Linux firewalls. If you're responsible for keeping a network secure, you'll find Linux Firewalls invaluable in your attempt to understand attacks and use iptables—along with psad and fwsnort—to detect and even prevent compromises.

Intrusion Detection & Prevention No Starch Press

This volume contains articles written by leading researchers in the fields of algorithms, architectures, and information systems security. The first five chapters address several challenging geometric problems and related algorithms. These topics have major applications in pattern recognition, image analysis, digital geometry, surface reconstruction, computer vision and in robotics. The next five chapters focus on various optimization issues in VLSI design and test architectures, and in wireless networks. The last six chapters comprise scholarly articles on information systems security covering privacy issues, access control, enterprise and network security, and digital image forensics.

Information Systems Security IGI Global

Learn how to detect and prevent the hacking of medical equipment at hospitals and healthcare facilities. A cyber-physical attack on building equipment pales in comparison to the damage a determined hacker can do if he/she gains access to a medical-grade network as a medical-grade network controls the diagnostic, treatment, and life support equipment on which lives depend. News reports inform us how hackers strike hospitals with ransomware that prevents staff from accessing patient records or scheduling appointments. Unfortunately, medical equipment also can be hacked and shut down remotely as a form of extortion. Criminal hackers will not ask for a $500 payment to unlock an MRI, PET or CT scan, or X-ray machine—they will ask for much more. Litigation is bound to follow and the resulting punitive awards will drive up hospital insurance costs and healthcare costs in general. This will undoubtedly result in increased regulations for hospitals and higher costs for compliance. Unless hospitals and other healthcare facilities take the steps necessary to secure their medical-grade networks, they will be targeted for cyber-physical attack, possibly with life-threatening consequences. Cybersecurity for Hospitals and Healthcare Facilities is a wake-up call explaining what hackers can do, why hackers would target a hospital, the way hackers research a target, ways hackers can gain access to a medical-grade network (cyber-attack vectors), and ways hackers hope to monetize their cyber-attack. By understanding and detecting the threats, you can take action now—before your hospital becomes the next victim. What You Will Learn: Determine how vulnerable hospital and healthcare building equipment is to cyber-physical attack Identify possible ways hackers can hack hospital and healthcare facility equipment Recognize the cyber-attack vectors—or paths by which a hacker or cracker can gain access to a computer, a medical-grade network server, or expensive medical equipment in order to deliver a payload or malicious outcome Detect and prevent man-in-the-middle or denial-of-service cyber-attacks Find and prevent hacking of the hospital database and hospital web application Who This Book Is For: Hospital administrators, healthcare professionals, hospital & healthcare facility engineers and building managers, hospital & healthcare facility IT professionals, and HIPAA professionals

Algorithms, Architectures and Information Systems Security WIT Press

DDoS Attacks: Evolution, Detection, Prevention, Reaction, and Tolerance discusses the evolution of distributed denial-of-service (DDoS) attacks, how to detect a DDoS attack when one is mounted, how to prevent such attacks from taking place, and how to react when a DDoS attack is in progress, with the goal of tolerating the attack. It introduces types and characteristics of DDoS attacks, reasons why such attacks are often successful, what aspects of the network infrastructure are usual targets, and methods used to launch attacks. The book elaborates upon the emerging botnet technology, current trends in the evolution and use of botnet technology, its role in facilitating the launching of DDoS attacks, and challenges in countering the role of botnets in the proliferation of DDoS attacks. It introduces statistical and machine learning methods applied in the detection and prevention of DDoS attacks in order to provide a clear understanding of the state of the art. It presents DDoS reaction and tolerance mechanisms with a view to studying their effectiveness in protecting network resources without compromising the quality of services. To practically understand how attackers plan and mount DDoS attacks, the authors discuss the development of a testbed that can be used to perform experiments such as attack launching, monitoring of network traffic, and detection of attacks, as well as for testing strategies for prevention, reaction, and mitigation. Finally, the authors address current issues and challenges that need to be overcome to provide even better defense against DDoS attacks.

Foundations of Homeland Security Pearson Education

Intrusion Prevention and Active Response provides an introduction to the field of Intrusion Prevention and provides detailed information on various IPS methods and technologies. Specific methods are covered in depth, including both network and host IPS and response technologies such as port deactivation, firewall/router network layer ACL modification, session sniping, outright application layer data modification, system call interception, and application shims. Corporate spending for Intrusion Prevention systems increased dramatically by 11% in the last quarter of 2004 alone Lead author, Michael Rash, is well respected in the IPS Community, having authored FWSnort, which greatly enhances the intrusion prevention capabilities of the market-leading Snort IDS