Computer Intrusion Detection And Network Monitoring A Statistical Viewpoint Information Science And Statistics

Network Anomaly Detection
Network Intrusion Detection
Trends in Intelligent Robotics, Automation, and Manufacturing
NIST SP 800-94 - Guide to Intrusion Detection and Prevention Systems (IDPS)
How to Cheat at VoIP Security
Intrusion Detection
Guide to Intrusion Detection and Prevention Systems
Intrusion Detection in Wireless Ad-Hoc Networks
Game Theory and Machine Learning for Cyber Security
Computer and Network Security Essentials
Intrusion Detection
Contemporary Computing
Intrusion Detection
Intrusion Detection Systems
Deep Learning Applications for Cyber-Physical Systems
Intrusion Detection Systems with Snort
Intrusion Detection and Correlation
Cisco Secure Intrusion Detection System
Network Intrusion Detection
Handbook of Information and Communication Security
Advances in Network Security and Applications
Intrusion Detection
Computational Methodologies for Electrical and Electronics Engineers
Network Intrusion Detection and Prevention
Statistical Techniques for Network Security: Modern Statistically-Based Intrusion Detection and Protection
Computer Intrusion Detection and Network Monitoring
Network Intrusion Detection using Deep Learning
Managing Cyber Threats
Industrial Internet of Things and Cyber-physical Systems
Machine Learning Techniques and Analytics for Cloud Security
The Tao of Network Security Monitoring
Computer Intrusion Detection and Network Monitoring
Recent Advances in Intrusion Detection
Cisco Security Professional's Guide to Secure Intrusion Detection Systems
Intrusion Prevention and Active Response

Applied Network Security Monitoring
Handbook of Research on Intrusion Detection Systems
Intrusion Detection Networks
Advances in Malware and Data-Driven Network Security
Design and Analysis of Security Protocol for Communication

CAMERON ROJAS

Network Anomaly Detection Springer Science & Business Media
Presenting cutting-edge research, Intrusion Detection in Wireless Ad-Hoc Networks explores the security aspects of the basic categories of wireless ad-hoc networks and related application areas. Focusing on intrusion detection systems (IDSs), it explains how to establish security solutions for the range of wireless networks, including mobile ad-hoc
Network Intrusion Detection Springer
This book is a training aid and reference for intrusion detection analysts. While the authors refer to research and theory, they focus their attention on providing practical information. New to this edition is coverage of packet dissection, IP datagram fields, forensics, and snort filters.
Trends in Intelligent Robotics, Automation, and Manufacturing Elsevier
"This book explores recent advances in the development, implementation, and business impact of IoT technologies on sustainable societal development and improved life quality"--
NIST SP 800-94 - Guide to Intrusion Detection and Prevention Systems (IDPS) World Scientific
Artificial intelligence has been applied to many areas of science and technology, including the power and energy sector. Renewable energy in particular has experienced the tremendous positive impact of these developments. With the recent evolution of smart energy technologies, engineers and scientists working in this sector need an exhaustive source of current knowledge to effectively cater to the energy needs of citizens of developing countries. Computational Methodologies for Electrical and Electronics Engineers is a collection of innovative research that provides a complete insight and overview of the application of intelligent computational techniques in power and energy. Featuring research on a wide range of topics such as artificial neural networks, smart grids, and soft computing, this book is ideally designed for programmers, engineers, technicians, ecologists, entrepreneurs, researchers, academicians, and students.
How to Cheat at VoIP Security Sams Publishing
This book constitutes the proceedings of the First International Conference on Intelligent Robotics and Manufacturing, IRAM 2012, held in Kuala Lumpur, Malaysia, in November 2012. The 64 revised full papers included in this volume were carefully reviewed and selected from 102 initial submissions. The papers are organized in topical sections named: mobile robots, intelligent autonomous systems, robot vision and robust, autonomous agents, micro, meso and nano-scale automation and assembly, flexible manufacturing systems, CIM and micro-machining, and fabrication techniques.
Intrusion Detection IGI Global
Cisco Systems, Inc. is the worldwide leader in networking for the Internet, and its Intrusion Detection Systems line of products is making in roads in the IDS market segment, with major upgrades having happened in February of 2003. Cisco Security Professional's Guide to Secure Intrusion Detection Systems is a comprehensive, up-to-date guide to the hardware and software that comprise the Cisco IDS. Cisco Security Professional's Guide to Secure Intrusion Detection Systems does more than show network engineers how to set up and manage this line of best selling products ... it walks them step by step through all the objectives of the Cisco Secure Intrusion Detection System course (and corresponding exam) that network engineers must pass on their way to achieving sought-after CCSP certification. - Offers complete coverage of the Cisco Secure Intrusion Detection Systems Exam (CSIDS 9E0-100) for CCSPs
Guide to Intrusion Detection and Prevention Systems Springer
Modern society depends critically on computers that control and manage the systems on which we depend in many aspects of our daily lives. While this provides conveniences of a level unimaginable just a few years ago, it also leaves us vulnerable to attacks on the computers managing these systems. In recent times the explosion in cyber attacks, including viruses, worms, and intrusions, has turned this vulnerability into a clear and visible threat. Due to the escalating number and increased sophistication of cyber attacks, it has become important to develop a broad range of techniques, which can ensure that the information infrastructure continues to operate smoothly, even in the presence of dire and continuous threats. This book brings together the latest techniques for managing cyber threats, developed by some of the world’s leading experts in the area. The book includes broad surveys on a number of topics, as well as specific techniques. It provides an excellent reference point for researchers and practitioners in the government, academic, and industrial communities who want to understand the issues and challenges in this area of growing worldwide importance.
Intrusion Detection in Wireless Ad-Hoc Networks IGI Global
This book introduces readers to the tools needed to protect IT resources and communicate with security specialists when there is a security problem. The book covers a wide range of security topics including Cryptographic Technologies, Network Security, Security Management, Information Assurance, Security Applications, Computer Security, Hardware Security, and Biometrics and Forensics. It introduces the concepts, techniques, methods, approaches, and trends needed by security specialists to improve their security skills and capabilities. Further, it provides a glimpse into future directions where security techniques, policies, applications, and theories are headed. The book represents a collection of carefully selected and reviewed chapters written by diverse security experts in the listed fields and edited by prominent security researchers. Complementary slides are available for download on the book’s website at Springer.com.

Game Theory and Machine Learning for Cyber Security IGI Global
Intrusion detection is the process of monitoring the events occurring in a computer system or network & analyzing them for signs of possible incidents, which are viol. or imminent threats of viol. of computer security policies, acceptable use policies, or standard security practices. Intrusion prevention is the process of performing intrusion detection to stop detected possible incidents. Intrusion detection & prevention systems (IDPS) record info. related to observed events, notify security admin. of important events, & produce reports. This pub. provides recommend. for designing, implementing, configuring, securing, monitoring, & maintaining IDPS¿s. Discusses 4 types of IDPS¿s: Network-Based; Wireless; Network Behavior Analysis; & Host-Based.

Computer and Network Security Essentials Elsevier
Applied Network Security Monitoring is the essential guide to becoming an NSM analyst from the ground up. This book takes a fundamental approach to NSM, complete with dozens of real-world examples that teach you the key concepts of NSM. Network security monitoring is based on the principle that prevention eventually fails. In the current threat landscape, no matter how much you try, motivated attackers will eventually find their way into your network. At that point, it is your ability to detect and respond to that intrusion that can be the difference between a small incident and a major disaster. The book follows the three stages of the NSM cycle: collection, detection, and analysis. As you progress through each section, you will have access to insights from seasoned NSM professionals while being introduced to relevant, practical scenarios complete with sample data. If you've never performed NSM analysis, Applied Network Security Monitoring will give you an adequate grasp on the core concepts needed to become an effective analyst. If you are already a practicing analyst, this book will allow you to grow your analytic technique to make you more effective at your job. - Discusses the proper methods for data collection, and teaches you how to become a skilled NSM analyst - Provides thorough hands-on coverage of Snort, Suricata, Bro-IDS, SiLK, and Argus - Loaded with practical examples containing real PCAP files you can replay, and uses Security Onion for all its lab examples - Companion website includes up-to-date blogs from the authors about the latest developments in NSM

Intrusion Detection Springer
"The book you are about to read will arm you with the knowledge you need to defend your network from attackers—both the obvious and the not so obvious.... If you are new to network security, don't put this book back on the shelf! This is a great book for beginners and I wish I had access to it many years ago. If you've learned the basics of TCP/IP protocols and run an open source or commercial IDS, you may be asking 'What's next?' If so, this book is for you." —Ron Gula, founder and CTO, Tenable Network Security, from the Foreword "Richard Bejtlich has a good perspective on Internet security—one that is orderly and practical at the same time. He keeps readers grounded and addresses the fundamentals in an accessible way." —Marcus Ranum, TruSecure "This book is not about security or network monitoring: It's about both, and in reality these are two aspects of the same problem. You can easily find people who are security experts or network monitors, but this book explains how to master both topics." —Luca Deri, ntop.org "This book will enable security professionals of all skill sets to improve their understanding of what it takes to set up, maintain, and utilize a successful network intrusion detection strategy." —Kirby Kuehl, Cisco Systems Every network can be compromised. There are too many systems, offering too many services, running too many flawed applications. No amount of careful coding, patch management, or access control can keep out every attacker. If prevention eventually fails, how do you prepare for the intrusions that will eventually happen? Network security monitoring (NSM) equips security staff to deal with the inevitable consequences of too few resources and too many responsibilities. NSM collects the data needed to generate better assessment, detection, and response processes—resulting in decreased impact from unauthorized activities. In The Tao of Network Security Monitoring , Richard Bejtlich explores the products, people, and processes that implement the NSM model. By focusing on case studies and the application of open source tools, he helps you gain hands-on knowledge of how to better defend networks and how to mitigate damage from security incidents. Inside, you will find in-depth information on the following areas. The NSM operational framework and deployment considerations. How to use a variety of open-source tools—including Sguil, Argus, and Ethereal—to mine network traffic for full content, session, statistical, and alert data. Best practices for conducting emergency NSM in an incident response scenario, evaluating monitoring vendors, and deploying an NSM architecture. Developing and applying knowledge of weapons, tactics, telecommunications, system administration, scripting, and programming for NSM. The best tools for generating arbitrary packets, exploiting flaws, manipulating traffic, and conducting reconnaissance. Whether you are new to network intrusion detection and incident response, or a computer-security veteran, this book will enable you to quickly develop and apply the skills needed to detect, prevent, and respond to new and emerging threats.

Contemporary Computing CRC Press
Big data generates around us constantly from daily business, custom use, engineering, and science activities. Sensory data is collected from the internet of things (IoT) and cyber-physical systems (CPS). Merely storing such a massive amount of data is meaningless, as the key point is to identify, locate, and extract valuable knowledge from big data to forecast and support services. Such extracted valuable knowledge is usually referred to as smart data. It is vital to providing suitable decisions in business, science, and engineering applications. Deep Learning Applications for Cyber-Physical Systems provides researchers a platform to present state-of-the-art innovations, research, and designs while implementing methodological and algorithmic solutions to data processing problems and designing and analyzing evolving trends in health informatics and computer-aided diagnosis in deep learning techniques in context with cyber physical systems. Covering topics such as smart medical systems, intrusion detection systems, and predictive analytics, this text is essential for computer scientists, engineers, practitioners, researchers, students, and academicians, especially those interested in the areas of internet of things, machine learning, deep learning, and cyber-physical systems.

Intrusion Detection IGI Global
Details how intrusion detection works in network security with comparisons to traditional methods such as firewalls and cryptography Analyzes the challenges in interpreting and correlating Intrusion Detection alerts

Intrusion Detection Systems Syngress
Businesses in today’s world are adopting technology-enabled operating models that aim to improve growth, revenue, and

identify emerging markets. However, most of these businesses are not suited to defend themselves from the cyber risks that come with these data-driven practices. To further prevent these threats, they need to have a complete understanding of modern network security solutions and the ability to manage, address, and respond to security breaches. The Handbook of Research on Intrusion Detection Systems provides emerging research exploring the theoretical and practical aspects of prominent and effective techniques used to detect and contain breaches within the fields of data science and cybersecurity. Featuring coverage on a broad range of topics such as botnet detection, cryptography, and access control models, this book is ideally designed for security analysts, scientists, researchers, programmers, developers, IT professionals, scholars, students, administrators, and faculty members seeking research on current advancements in network security technology.

Deep Learning Applications for Cyber-Physical Systems Springer Science & Business Media

MACHINE LEARNING TECHNIQUES AND ANALYTICS FOR CLOUD SECURITY This book covers new methods, surveys, case studies, and policy with almost all machine learning techniques and analytics for cloud security solutions The aim of Machine Learning Techniques and Analytics for Cloud Security is to integrate machine learning approaches to meet various analytical issues in cloud security. Cloud security with ML has long-standing challenges that require methodological and theoretical handling. The conventional cryptography approach is less applied in resource-constrained devices. To solve these issues, the machine learning approach may be effectively used in providing security to the vast growing cloud environment. Machine learning algorithms can also be used to meet various cloud security issues, such as effective intrusion detection systems, zero-knowledge authentication systems, measures for passive attacks, protocols design, privacy system designs, applications, and many more. The book also contains case studies/projects outlining how to implement various security features using machine learning algorithms and analytics on existing cloud-based products in public, private and hybrid cloud respectively. Audience Research scholars and industry engineers in computer sciences, electrical and electronics engineering, machine learning, computer security, information technology, and cryptography.

Intrusion Detection Systems with Snort Springer

To defend against computer and network attacks, multiple, complementary security devices such as intrusion detection systems (IDSs), and firewalls are widely deployed to monitor networks and hosts. These various IDSs will flag alerts when suspicious events are observed. This book is an edited volume by world class leaders within computer network and information security presented in an easy-to-follow style. It introduces defense alert systems against computer and network attacks. It also covers integrating intrusion alerts within security policy framework for intrusion response, related case studies and much more.

Intrusion Detection and Correlation Springer Science & Business Media

Provides statistical modeling and simulating approaches to address the needs for intrusion detection and protection. Covers topics such as network traffic data, anomaly intrusion detection, and prediction events.

Cisco Secure Intrusion Detection System Springer Science & Business Media

A complete nuts-and-bolts guide to improving network security using today's best intrusion detection products Firewalls cannot catch all of the hacks coming into your network. To properly safeguard your valuable information resources against attack, you need a full-time watchdog, ever on the alert, to sniff out suspicious behavior on your network. This book gives you the additional ammo you need. Terry Escamilla shows you how to combine and properly deploy today's best intrusion detection products in order to arm your network with a virtually impenetrable line of defense. He provides: * Assessments of commercially available intrusion detection products: what each can and cannot do to fill the gaps in your network security * Recommendations for dramatically improving network security using the right combination of intrusion detection products * The lowdown on identification and authentication, firewalls, and access control * Detailed comparisons between today's leading intrusion detection product categories * A practical perspective on how different security products fit together to provide protection for your network The companion Web site at www.wiley.com/compbooks/escamilla features: White papers * Industry news * Product information

Network Intrusion Detection Sams Publishing

At its core, information security deals with the secure and accurate transfer of information. While information security has long been important, it was, perhaps, brought more clearly into mainstream focus with the so-called “Y2K” issue. Te Y2K scare was the fear that c- puter networks and the systems that are controlled or operated by sofware would fail with the turn of the millennium, since their clocks could lose synchronization by not recognizing a number (instruction) with three zeros. A positive outcome of this scare was the creation of several Computer Emergency Response Teams (CERTs) around the world that now work - operatively to exchange expertise and information, and to coordinate in case major problems should arise in the modern IT environment. Te terrorist attacks of 11 September 2001 raised security concerns to a new level. Te - ternational community responded on at least two fronts; one front being the transfer of reliable information via secure networks and the other being the collection of information about - tential terrorists. As a sign of this new emphasis on security, since 2001, all major academic publishers have started technical journals focused on security, and every major communi- tions conference (for example, Globecom and ICC) has organized workshops and sessions on security issues. In addition, the IEEE has created a technical committee on Communication and Information Security. Te ?rst editor was intimately involved with security for the Athens Olympic Games of 2004.

Handbook of Information and Communication Security IGI Global

This book covers the basic statistical and analytical techniques of computer intrusion detection. It is the first to present a data-centered approach to these problems. It begins with a description of the basics of TCP/IP, followed by chapters dealing with network traffic analysis, network monitoring for intrusion detection, host based intrusion detection, and computer viruses and other malicious code.