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

EDWARDS RUSH

Intrusion Detection Systems CRC Press
Introduces the concept of intrusion detection, discusses various approaches for intrusion detection systems (IDS), and presents the architecture and implementation of IDS. This title also includes the performance comparison of various IDS via simulation.
The State of the Art in Intrusion Prevention and Detection World Scientific
On computer security
Challenges for Next Generation Network Operations and Service Management Springer
The definitive guide to understanding, selecting, and deploying intrusion detection in the enterprise! Product selection, planning, and operations Filled with real-life cases and stories of intrusion detection systems in action Covers host-based and network-based intrusion detection Foreword by Dorothy Denning, author of "Cryptography and Data Security" and "Information Warfare and Security" Technical Edit by Ira Winkler, author of "Corporate Espionage" In "The Practical Intrusion Detection Handbook," one of the field's leading experts shows exactly how to detect, deter, and respond to security threats using intrusion detection systems. Using real-world case studies and practical checklists, Paul E. Proctor shows what intrusion detection software can achieve, and how to integrate it into a comprehensive strategy for protecting information and e-commerce assets. No other guide to intrusion detection offers all this: Practical coverage of host-based, network-based, and hybrid solutions Detailed selection criteria and sample RFPs Key factors associated with successful deployment Intrusion detection in action: response, surveillance, damage assessment, data forensics, and beyond Six myths of intrusion detection and the realities Whether you're a senior IT decision-maker, system administrator, or infosecurity specialist, intrusion detection is a key weapon in your security arsenal. Now, there's a start-to-finish guide to making the most of it: "The Practical Intrusion Detection Handbook" by Paul E. Proctor. "Intrusion detection has gone from a theoretical concept to a practical solution, from a research dream to a major product area, from an idea worthy of study to a key element of the national plan for cyber defense. . . Nobody brought that about more than Paul Proctor. . . Paul brings his considerable knowledge and experience with commercial intrusion detection products to this first-of-a-kind book."
Network Security Bible John Wiley & Sons
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.

Network Anomaly Detection Springer Science & Business Media
“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
Practical Intrusion Detection Handbook CRC Press
"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.
Network Intrusion Alert Springer
With the rapid rise in the ubiquity and sophistication of Internet technology and the accompanying growth in the number of network attacks, network intrusion detection has become increasingly important. Anomaly-based network intrusion detection refers to finding exceptional or nonconforming patterns in network traffic data compared to normal behavior. Finding these anomalies has extensive applications in areas such as cyber security, credit card and insurance fraud detection, and military surveillance for enemy activities. Network Anomaly Detection: A Machine Learning Perspective presents machine learning techniques in depth to help you more effectively detect and counter network intrusion. In this book, you’ll learn about: Network anomalies and vulnerabilities at various layers The pros and cons of various machine learning techniques and algorithms A taxonomy of attacks based on their characteristics and behavior Feature selection algorithms How to assess the accuracy, performance, completeness, timeliness, stability, interoperability, reliability, and other dynamic aspects of a network anomaly detection system Practical tools for launching attacks, capturing packet or flow traffic, extracting features, detecting attacks, and evaluating detection performance Important unresolved issues and research challenges that need to be overcome to provide better protection for networks Examining numerous attacks in detail, the authors look at the tools that intruders use and show how to use this knowledge to protect networks. The book also provides material for hands-on development, so that you can code on a testbed to implement detection methods toward the development of your own intrusion detection system. It offers a thorough introduction to the state of the art in network anomaly detection using machine learning approaches and systems.
Recent Advances in Intrusion Detection Course Technology
Network Intrusion Detection and Prevention: Concepts and Techniques provides detailed and concise information on different types of attacks, theoretical foundation of attack detection approaches, implementation, data collection, evaluation, and intrusion response. Additionally, it provides an overview of some of the commercially/publicly available intrusion detection and response systems. On the topic of intrusion detection system it is impossible to include everything there is to say on all subjects. However, we have tried to cover the most important and common ones. Network Intrusion Detection and Prevention: Concepts and Techniques is designed for researchers and practitioners in industry. This book is suitable for advanced-level students in computer science as a reference book as well.
Advances in Network Security and Applications CRC Press
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
Intrusion Detection in Distributed Systems Springer Science & Business Media
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
Guide to Firewalls and Network Security Pearson Education
Intrusion Detection In Distributed Systems: An Abstraction-Based Approach presents research contributions in three areas with respect to intrusion detection in distributed systems. The first contribution is an abstraction-based approach to addressing heterogeneity and autonomy of distributed environments. The second contribution is a formal framework for modeling requests among cooperative IDSs and its application to Common Intrusion Detection Framework (CIDF). The third contribution is a novel approach to coordinating different IDSs for distributed event correlation.
Introduction to Security and Network Forensics Computer Intrusion Detection and Network Monitoring
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.
Handbook of Research on Intrusion Detection Systems Sams Publishing
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.
Intrusion Detection and Correlation IGI Global
In the era of Internet of Things (IoT), and with the explosive worldwide growth of electronic data volume and the associated needs of processing, analyzing, and storing this data, several new challenges have emerged. Particularly, there is a need for novel schemes of secure authentication, integrity protection, encryption, and non-repudiation to protect the privacy of sensitive data and to secure systems. Lightweight symmetric key cryptography and adaptive network security algorithms are in demand for mitigating these challenges. This book presents state-of-the-art research in the fields of cryptography and security in computing and communications. It covers a wide range of topics such as machine learning, intrusion detection, steganography, multi-factor authentication, and more. It is a valuable reference for researchers, engineers, practitioners, and graduate and doctoral students working in the fields of cryptography, network security, IoT, and machine learning.
The Tao of Network Security Monitoring CRC Press
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 Springer Science & Business Media
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.
An Interdisciplinary Approach to Modern Network Security Springer Science & Business Media

This monograph comprises work on network-based Intrusion Detection (ID) that is grounded in visualisation and hybrid Artificial Intelligence (AI). It has led to the design of MOVICAB-IDS (MObile VIsualisation Connectionist Agent-Based IDS), a novel Intrusion Detection System (IDS), which is comprehensively described in this book. This novel IDS combines different AI paradigms to visualise network traffic for ID at packet level. It is based on a dynamic Multiagent System (MAS), which integrates an unsupervised neural projection model and the Case-Based Reasoning (CBR) paradigm through the use of deliberative agents that are capable of learning and evolving with the environment. The proposed novel hybrid IDS provides security personnel with a synthetic, intuitive snapshot of network traffic and protocol interactions. This visualisation interface supports the straightforward detection of anomalous situations and their subsequent identification. The performance of MOVICAB-IDS was tested through a novel mutation-based testing method in different real domains which entailed several attacks and anomalous situations.

Network Security Technologies: Design and Applications Springer Science & Business Media

Network Science and Cybersecurity introduces new research and development efforts for cybersecurity solutions and applications taking place within various U.S. Government Departments of Defense, industry and academic laboratories. This book examines new algorithms and tools, technology platforms and reconfigurable technologies for cybersecurity systems. Anomaly-based intrusion detection systems (IDS) are explored as a key component of any general network intrusion detection service, complementing signature-based IDS components by attempting to identify novel attacks. These attacks may not yet be known or have well-developed signatures. Methods are also suggested to simplify the construction of metrics in such a manner that they retain their ability to effectively cluster data, while simultaneously easing human interpretation of outliers. This is a professional book for practitioners or government employees working in cybersecurity, and can also be used as a reference. Advanced-level students in computer science or electrical engineering studying security will also find this book useful .

Network Intrusion Detection and Prevention "O'Reilly Media, Inc."

Intrusion detection is one of the hottest growing areas of network security. As the number of corporate, government, and educational networks grow and as they become more and more interconnected through the Internet, there is a correlating increase in the types and numbers of attacks to penetrate those networks. Intrusion Detection, Second Edition is a training aid and reference for intrusion detection analysts. This book is meant to be practical. The authors are literally the most recognized names in this specialized field, with unparalleled experience in defending our country s government and military computer networks. People travel from all over the world to hear them speak, and this book will be a distillation of that experience. The book's approach is to introduce and ground topics through actual traffic patterns. The authors have been through the trenches and give you access to unusual and unique data.

Intrusion Detection McGraw Hill Professional

This indispensable text/reference presents a comprehensive overview on the detection and prevention of anomalies in computer network traffic, from coverage of the fundamental theoretical concepts to in-depth analysis of systems and methods. Readers will benefit from invaluable practical guidance on how to design an intrusion detection technique and incorporate it into a system, as well as on how to analyze and correlate alerts without prior information. Topics and features: introduces the essentials of traffic management in high speed networks, detailing types of anomalies, network vulnerabilities, and a taxonomy of network attacks; describes a systematic approach to generating large network intrusion datasets, and reviews existing synthetic, benchmark, and real-life datasets; provides a detailed study of network anomaly detection techniques and systems under six different categories: statistical, classification, knowledge-base, cluster and outlier detection, soft computing, and combination learners; examines alert management and anomaly prevention techniques, including alert preprocessing, alert correlation, and alert post-processing; presents a hands-on approach to developing network traffic monitoring and analysis tools, together with a survey of existing tools; discusses various evaluation criteria and metrics, covering issues of accuracy, performance, completeness, timeliness, reliability, and quality; reviews open issues and challenges in network traffic anomaly detection and prevention. This informative work is ideal for graduate and advanced undergraduate students interested in network security and privacy, intrusion detection systems, and data mining in security. Researchers and practitioners specializing in network security will also find the book to be a useful reference.