

Intrusion Detection In Computer Network Using Genetic

Advances in Network Security and Applications
 Managing Cyber Threats
 Trends in Intelligent Robotics, Automation, and Manufacturing
 Deep Learning Applications for Cyber-Physical Systems
 Intrusion Detection
 Handbook of Research on Intrusion Detection Systems
 Intrusion Detection and Correlation
 Industrial Internet of Things and Cyber-physical Systems
 Machine Learning Techniques and Analytics for Cloud Security
 Intrusion Detection
 Design and Analysis of Security Protocol for Communication
 Network Intrusion Detection and Prevention
 Intrusion Detection in Wireless Ad-Hoc Networks
 Computational Methodologies for Electrical and Electronics Engineers
 Intrusion Detection and Prevention for Mobile Ecosystems
 Guide to Computer Network Security
 Advances in Malware and Data-Driven Network Security
 Network Intrusion Detection using Deep Learning
 Privacy-Respecting Intrusion Detection
 NIST SP 800-94 - Guide to Intrusion Detection and Prevention Systems (IDPS)
 Network Intrusion Detection
 Intrusion Detection
 Intelligent Systems and Applications
 Logging and Log Management
 Intrusion Detection Systems with Snort
 Practical Intrusion Analysis
 Cisco Security Professional's Guide to Secure Intrusion Detection Systems
 Computer Intrusion Detection and Network Monitoring
 Snort
 The Tao of Network Security Monitoring
 Intrusion Detection
 Intrusion Detection
 Handbook of Information and Communication Security
 Network Anomaly Detection
 Intrusion Detection
 Intrusion Detection Networks
 Statistical Techniques for Network Security: Modern Statistically-Based Intrusion Detection and Protection
 How to Cheat at VoIP Security
 Intrusion Detection Systems

Intrusion Detection In Computer Network Using Genetic

Downloaded from intra.itu.edu by guest

BRAYLON SASHA

Advances in Network Security and Applications CRC Press

This guide to Open Source intrusion detection tool SNORT features step-by-step instructions on how to integrate SNORT with other open source products. The book contains information and custom built scripts to make installation easy.

Managing Cyber Threats 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.

Trends in Intelligent Robotics, Automation, and Manufacturing Springer Science & Business Media

This book presents state-of-the-art contributions from both scientists and practitioners working in intrusion detection and prevention for mobile networks, services, and devices. It covers fundamental theory, techniques, applications, as well as practical experiences concerning intrusion

detection and prevention for the mobile ecosystem. It also includes surveys, simulations, practical results and case studies.

Deep Learning Applications for Cyber-Physical Systems IGI Global

This book constitutes the proceedings of the 4th International Conference on Network Security and Applications held in Chennai, India, in July 2011. The 63 revised full papers presented were carefully reviewed and selected from numerous submissions. The papers address all technical and practical aspects of security and its applications for wired and wireless networks and are organized in topical sections on network security and applications, ad hoc, sensor and ubiquitous computing, as well as peer-to-peer networks and trust management.

Intrusion Detection Springer Science & Business Media

Effective response to misuse or abusive activity in IT systems requires the capability to detect and understand improper activity. Intrusion Detection Systems observe IT activity, record these observations in audit data, and analyze the collected audit data to detect misuse. Privacy-Respecting Intrusion Detection introduces the concept of technical purpose binding, which restricts the linkability of pseudonyms in audit data to the amount necessary for misuse detection. Also, it

limits the recovery of personal data to pseudonyms involved in a detected misuse scenario. The book includes case studies demonstrating this theory, and solutions that are constructively validated by providing algorithms.

Handbook of Research on Intrusion Detection Systems Sams Publishing

The Perfect Reference for the Multitasked SysAdmin This is the perfect guide if VoIP engineering is not your specialty. It is the perfect introduction to VoIP security, covering exploit tools and how they can be used against VoIP (Voice over IP) systems. It gives the basics of attack methodologies used against the SIP and H.323 protocols as well as VoIP network infrastructure. * VoIP Isn't Just Another Data Protocol IP telephony uses the Internet architecture, similar to any other data application. However, from a security administrator's point of view, VoIP is different. Understand why. * What Functionality Is Gained, Degraded, or Enhanced on a VoIP Network? Find out the issues associated with quality of service, emergency 911 service, and the major benefits of VoIP. * The Security Considerations of Voice Messaging Learn about the types of security attacks you need to protect against within your voice messaging system. * Understand the VoIP Communication Architectures Understand what PSTN is and what it does as well as the H.323 protocol specification,

and SIP Functions and features.* The Support Protocols of VoIP Environments Learn the services, features, and security implications of DNS, TFTP, HTTP, SNMP, DHCP, RSVP, SDP, and SKINNY.* Securing the Whole VoIP Infrastructure Learn about Denial-of-Service attacks, VoIP service disruption, call hijacking and interception, H.323-specific attacks, and SIP-specific attacks.* Authorized Access Begins with Authentication Learn the methods of verifying both the user identity and the device identity in order to secure a VoIP network.* Understand Skype Security Skype does not log a history like other VoIP solutions; understand the implications of conducting business over a Skype connection.* Get the Basics of a VoIP Security Policy Use a sample VoIP Security Policy to understand the components of a complete policy. - Provides system administrators with hundreds of tips, tricks, and scripts to complete administration tasks more quickly and efficiently - Short on theory, history, and technical data that ultimately is not helpful in performing their jobs - Avoid the time drains associated with securing VoIP

Intrusion Detection and Correlation 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, Aircanner 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

Industrial Internet of Things and Cyber-physical Systems IGI Global

Cisco Systems, Inc. is the worldwide leader in networking for the Internet, and its Intrusion Detection Systems line of products is making inroads 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

Machine Learning Techniques and Analytics for Cloud Security Springer Science & Business Media

The purpose of designing this book is to discuss and analyze security protocols available for communication. Objective is to discuss protocols across all layers of TCP/IP stack and also to discuss protocols independent to the stack. Authors will be aiming to identify the best set of security protocols for the similar applications and will also be identifying the drawbacks of existing

protocols. The authors will be also suggesting new protocols if any.

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

Design and Analysis of Security Protocol for Communication Syngress Press

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.

Network Intrusion Detection and Prevention Newnes

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.

Intrusion Detection in Wireless Ad-Hoc Networks CRC Press

Every day approximately three-hundred thousand to four-hundred thousand new malware are registered, many of them being adware and variants of previously known malware. Anti-virus companies and researchers cannot deal with such a deluge of malware – to analyze and build patches. The only way to scale the efforts is to build algorithms to enable machines to analyze malware and classify and cluster them to such a level of granularity that it will enable humans (or machines) to gain critical insights about them and build solutions that are specific enough to detect and thwart existing malware and generic-enough to thwart future variants. Advances in Malware and Data-Driven Network Security comprehensively covers data-driven malware security with an emphasis on using statistical, machine learning, and AI as well as the current trends in ML/statistical approaches to detecting, clustering, and classification of cyber-threats. Providing information on advances in malware and data-driven network security as well as future research directions, it is ideal for graduate students, academicians, faculty members, scientists, software developers, security analysts, computer engineers, programmers, IT specialists, and researchers who are seeking to learn and carry out research in the area of malware and data-driven network security.

Computational Methodologies for Electrical and Electronics Engineers CRC Press

Logging and Log Management: The Authoritative Guide to Understanding the Concepts Surrounding Logging and Log Management introduces information technology professionals to the basic concepts of logging and log management. It provides tools and techniques to analyze log data and detect malicious activity. The book consists of 22 chapters that cover the basics of log data; log data sources; log storage technologies; a case study on how syslog-ng is deployed in a real environment for log collection; covert logging; planning and preparing for the analysis log data; simple analysis techniques; and tools and techniques for reviewing logs for potential problems. The book also discusses statistical analysis; log data mining; visualizing log data; logging laws and logging mistakes; open source and commercial toolsets for log data collection and analysis; log management procedures; and attacks against logging systems. In addition, the book addresses logging for programmers; logging and compliance with regulations and policies; planning for log analysis system deployment; cloud logging; and the future of log standards,

logging, and log analysis. This book was written for anyone interested in learning more about logging and log management. These include systems administrators, junior security engineers, application developers, and managers. - Comprehensive coverage of log management including analysis, visualization, reporting and more - Includes information on different uses for logs -- from system operations to regulatory compliance - Features case Studies on syslog-ng and actual real-world situations where logs came in handy in incident response - Provides practical guidance in the areas of report, log analysis system selection, planning a log analysis system and log data normalization and correlation

Intrusion Detection and Prevention for Mobile Ecosystems Elsevier

This book presents state-of-the-art research on intrusion detection using reinforcement learning, fuzzy and rough set theories, and genetic algorithm. Reinforcement learning is employed to incrementally learn the computer network behavior, while rough and fuzzy sets are utilized to handle the uncertainty involved in the detection of traffic anomaly to secure data resources from possible attack. Genetic algorithms make it possible to optimally select the network traffic parameters to reduce the risk of network intrusion. The book is unique in terms of its content, organization, and writing style. Primarily intended for graduate electrical and computer engineering students, it is also useful for doctoral students pursuing research in intrusion detection and practitioners interested in network security and administration. The book covers a wide range of applications, from general computer security to server, network, and cloud security.

Guide to Computer Network Security John Wiley & Sons

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.

Advances in Malware and Data-Driven Network Security 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.

Network Intrusion Detection using Deep Learning IGI Global

This fully revised and updated new edition of the definitive text/reference on computer network and information security presents a comprehensive guide to the repertoire of security tools, algorithms and best practices mandated by the technology we depend on. Topics and features: highlights the magnitude of the vulnerabilities, weaknesses and loopholes inherent in computer networks; discusses how to develop effective security solutions, protocols, and best practices for the modern computing environment; examines the role of legislation, regulation, and enforcement in securing computing and mobile systems; describes the burning security issues brought about by the advent of the Internet of Things and the eroding boundaries between enterprise and home networks (NEW); provides both quickly workable and more thought-provoking exercises at the end of each chapter, with one chapter devoted entirely to hands-on exercises; supplies additional support materials for instructors at an associated website.

Privacy-Respecting Intrusion Detection Springer

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.

[NIST SP 800-94 - Guide to Intrusion Detection and Prevention Systems \(IDPS\)](#) Engineering Science Reference

Computer Intrusion Detection and Network Monitoring Springer Science & Business Media

Best Sellers - Books :

- [Beyond The Story: 10-year Record Of Bts](#)
- [It Starts With Us: A Novel \(2\) \(it Ends With Us\) By Colleen Hoover](#)
- [Things We Hide From The Light \(knockemout Series, 2\) By Lucy Score](#)
- [The Going To Bed Book By Sandra Boynton](#)
- [Fast Like A Girl: A Woman's Guide To Using The Healing Power Of Fasting To Burn Fat, Boost Energy, And Balance Hormones By Dr. Mindy Pelz](#)
- [Tomorrow, And Tomorrow, And Tomorrow: A Novel](#)
- [Stop Overthinking: 23 Techniques To Relieve Stress, Stop Negative Spirals, Declutter Your Mind, And Focus On The Present \(the Path To Calm\) By Nick Trenton](#)
- [The Last Thing He Told Me: A Novel](#)
- [Brown Bear, Brown Bear, What Do You See?](#)
- [The Psychology Of Money: Timeless Lessons On Wealth, Greed, And Happiness By Morgan Housel](#)