

Computer Network Security Literature Review Papers

Right here, we have countless book Computer Network Security Literature Review Papers and collections to check out. We additionally have the funds for variant types and after that type of the books to browse. The all right book, fiction, history, novel, scientific research, as without difficulty as various other sorts of books are readily open here.

As this Computer Network Security Literature Review Papers, it ends taking place innate one of the favored ebook Computer Network Security Literature Review Papers collections that we have. This is why you remain in the best website to look the incredible book to have.



Case Studies in Secure Computing John Wiley & Sons

This book presents the proceedings of The 2020 International Conference on Machine Learning and Big Data Analytics for IoT Security and Privacy (SPIoT-2020), held in Shanghai, China, on November 6, 2020. Due to the COVID-19 outbreak problem, SPIoT-2020 conference was held online by Tencent Meeting. It provides comprehensive coverage of the latest advances and trends in information technology, science and engineering, addressing a number of broad themes, including novel machine learning and big data analytics methods for IoT security, data mining and statistical modelling for the secure IoT and machine learning-based security detecting protocols, which inspire the development of IoT security and privacy technologies. The contributions cover a wide range of topics: analytics and machine learning applications to IoT security; data-based metrics and risk assessment approaches for IoT; data confidentiality and privacy in IoT; and authentication and access control for data usage in IoT. Outlining promising future research directions, the book is a valuable resource for students, researchers and professionals and provides a useful reference guide for newcomers to the IoT security and privacy field.

Introduction to Network Security Springer

Computers at Risk presents a comprehensive agenda for developing nationwide policies and practices for computer security. Specific recommendations are provided for industry and for government agencies engaged in computer security activities. The volume also outlines problems and opportunities in computer security research, recommends ways to improve the research infrastructure, and suggests topics for investigators. The book explores the diversity of the field, the need to engineer countermeasures based on speculation of what experts think computer attackers may do next, why the technology community has failed to

respond to the need for enhanced security systems, how innovators could be encouraged to bring more options to the marketplace, and balancing the importance of security against the right of privacy.

Holistic Approach to Quantum Cryptography in Cyber Security
IGI Global

Bluetooth technology has enjoyed tremendous success, and it's now employed in billions of devices for short-range wireless data and real-time audio or video transfer. In this book the authors provide an overview of Bluetooth security. They examine network vulnerabilities and provide a literature-review comparative analysis of recent security attacks. They analyze and explain related countermeasures, including one based on secure simple pairing, and they also propose a novel attack that works against all existing Bluetooth versions. They conclude with a discussion on future research directions. The book is appropriate for practitioners and researchers in information security, in particular those engaged in the design of networked and mobile devices.

Computer and Network Security CRC Press

A comprehensive survey of computer network security concepts, methods, and practices. This authoritative volume provides an optimal description of the principles and applications of computer network security in particular, and cyberspace security in general. The book is thematically divided into three segments: Part I describes the operation and security conditions surrounding computer networks; Part II builds from there and exposes readers to the prevailing security situation based on a constant security threat; and Part III - the core - presents readers with most of the best practices and solutions currently in use. It is intended as both a teaching tool and reference. This broad-ranging text/reference

comprehensively surveys computer network security concepts, methods, and practices and covers network security tools, policies, and administrative goals in an integrated manner. It is an essential security resource for undergraduate or graduate study, practitioners in networks, and professionals who develop and maintain secure computer network systems.

Network Security 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.

Modern Theories and Practices for Cyber Ethics and Security Compliance Springer Nature Computer System and Network Security provides the reader with a basic understanding of the issues involved in the security of computer systems and networks. Introductory in nature, this important new book covers all aspects related to the growing field of computer security. Such complete coverage in a single text has previously been unavailable, and college professors and students, as well as professionals responsible for system security, will find this unique book a valuable source of information, either as a textbook or as a general reference. Computer System and Network Security discusses existing and potential threats to computer systems and networks and outlines the basic actions that are generally taken to protect them. The first two chapters of the text introduce the reader to the field of computer security, covering fundamental issues and objectives. The next several chapters describe security models, authentication issues, access control, intrusion detection, and damage control. Later chapters address network and database security and systems/networks connected to wide-area networks and internetworks. Other topics include firewalls, cryptography, malicious software, and security standards. The book includes case studies with information about incidents involving computer security, illustrating the problems and potential damage that can be caused when security fails. This unique reference/textbook covers all aspects of computer and network security, filling an obvious gap in the existing literature.

Security, Privacy and Reliability in Computer Communications and Networks Syngress

Introductory textbook in the important area of network security for undergraduate and graduate students. Comprehensively covers fundamental concepts with newer topics such as electronic cash, bit-coin, P2P, SHA-3, E-voting, and Zigbee security. Fully updated to reflect new developments in network security. Introduces a chapter on Cloud

security, a very popular and essential topic. Uses everyday examples that most computer users experience to illustrate important principles and mechanisms. Features a companion website with Powerpoint slides for lectures and solution manuals to selected exercise problems, available at <http://www.cs.uml.edu/~wang/NetSec>

Handbook of Research on Intrusion Detection Systems Syngress

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.

Artificial Intelligence and Bioinspired Computational Methods 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.

Advances in Cyber Security Analytics and Decision Systems Springer Nature

This updated guide presents expert information on analyzing, designing, and implementing all aspects of computer network security. Based on the authors' earlier work, Computer System and Network Security, this new book addresses important concerns regarding network security. It contains new chapters on World Wide Web security issues, secure electronic commerce, incident response, as well as two new appendices on PGP and UNIX security fundamentals.

Handbook Of Security And Networks Springer Nature

This volume contains papers presented at the 3rd International Workshop on Mathematical Methods, Models and Architectures for Computer Network Security (MMM-ACNS 2005) held in St. Petersburg, Russia, during September 25-27, 2005. The workshop was organized by the St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences (SPIIRAS) in cooperation with Binghamton University (SUNY, USA). The 1st and the 2nd International Workshops on Mathematical Methods, Models and Architectures for Computer Network Security (MMM-ACNS 2001 and MMM-ACNS 2003), hosted by the St. Petersburg Institute for Informatics and Automation, demonstrated the keen interest of the international research community in the subject area. It was recognized that conducting a biannual series of such workshops in St. Petersburg stimulates fruitful exchanges between the different schools of thought, facilitates the dissemination of new ideas and promotes the spirit of cooperation between researchers on the international scale. MMM-ACNS 2005 provided an international forum for sharing original search results and application experiences among specialists in fundamental and applied problems of computer network security. An important distinction of the workshop was its focus on mathematical aspects of information and computer

network security addressing the ever-increasing demands for secure computing and highly dependable computer networks.

Guide to Computer Network Security Springer Nature

This book provides a reference tool for the increasing number of scientists whose research is more or less involved in network security. Coverage includes network design and modeling, network management, data management, security and applications.

Advances in Malware and Data-Driven Network Security CRC Press

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.

Information Assurance in Computer Networks: Methods, Models and Architectures for Network Security Springer Science & Business Media

An Interdisciplinary Approach to Modern Network Security presents the latest methodologies and trends in detecting and

preventing network threats. Investigating the potential of current and emerging security technologies, this publication is an all-inclusive reference source for academicians, researchers, students, professionals, practitioners, network analysts and technology specialists interested in the simulation and application of computer network protection. It presents theoretical frameworks and the latest research findings in network security technologies, while analyzing malicious threats which can compromise network integrity. It discusses the security and optimization of computer networks for use in a variety of disciplines and fields. Touching on such matters as mobile and VPN security, IP spoofing and intrusion detection, this edited collection emboldens the efforts of researchers, academics and network administrators working in both the public and private sectors. This edited compilation includes chapters covering topics such as attacks and countermeasures, mobile wireless networking, intrusion detection systems, next-generation firewalls, web security and much more. Information and communication systems are an essential component of our society, forcing us to become dependent on these infrastructures. At the same time, these systems are undergoing a convergence and interconnection process that has its benefits, but also raises specific threats to user interests. Citizens and organizations must feel safe when using cyberspace facilities in order to benefit from its advantages. This book is interdisciplinary in the sense that it covers a wide range of topics like network security threats, attacks, tools and

procedures to mitigate the effects of malware and common network attacks, network security architecture and deep learning methods of intrusion detection.

Fundamentals of Network Security National Academies Press

In today's age of wireless and mobile computing, network and computer security is paramount. Case Studies in Secure Computing: Achievements and Trends gathers the latest research from researchers who share their insights and best practices through illustrative case studies. This book examines the growing security attacks and countermeasures in the stand-alone and networking worlds, along with other pertinent security issues. The many case studies capture a truly wide range of secure computing applications. Surveying the common elements in computer security attacks and defenses, the book: Describes the use of feature selection and fuzzy logic in a decision tree model for intrusion detection Introduces a set of common fuzzy-logic-based security risk estimation techniques with examples Proposes a secure authenticated multiple-key establishment protocol for wireless sensor networks Investigates various malicious activities associated with cloud computing and proposes some countermeasures Examines current and emerging security threats in long-term evolution backhaul and core networks Supplies a brief introduction to application-layer denial-of-service (DoS) attacks Illustrating the security challenges currently facing practitioners, this book presents powerful security solutions proposed by leading researchers in the field. The examination of the various case studies will help to develop the practical understanding required to stay one step ahead of the security threats on the horizon. This book will help those new to the field understand how to mitigate security threats. It will also help established practitioners fine-tune their approach to establishing robust and resilient security for next-generation computing systems.

Computers at Risk Springer Science & Business Media

This new book discusses the concepts while also highlighting the challenges in the field of quantum cryptography and also covering

cryptographic techniques and cyber security techniques, in a single volume. It comprehensively covers important topics in the field of quantum cryptography with applications, including quantum key distribution, position-based quantum cryptography, quantum teleportation, quantum e-commerce, quantum cloning, cyber security techniques' architectures and design, cyber security techniques management, software-defined networks, and cyber security techniques for 5G communication. The text also discusses the security of practical quantum key distribution systems, applications and algorithms developed for quantum cryptography, as well as cyber security through quantum computing and quantum cryptography. The text will be beneficial for graduate students, academic researchers, and professionals working in the fields of electrical engineering, electronics and communications engineering, computer science, and information technology.

Introduction to Network & Cybersecurity Springer Science & Business Media

This authoritative guide explores computer network infrastructures and protocol design security flaws, as well as discussing current security solutions and best practices, in both fixed and mobile computer networks. It broadly surveys thought-provoking security issues and discusses and raises questions about the impact of these new technologies and protocols, with particular emphasis on the rapid growth and skyrocketing interests and use in mobile technologies. It explores the security threats and vulnerabilities in the current network infrastructure and protocols and outlines current security efforts. It provides support materials for lecturers and students such as PowerPoint slides, syllabus suggestions, solutions, instructor manual and student laboratory materials. This text/reference is an invaluable instructional and research tool for undergraduates in computer and information security - it will also be a rich resource for practitioners, and professionals.

Computer Network Security Springer

This book comprises the proceedings of the 2nd International Conference on Computer Vision, High-Performance Computing, Smart Devices, and Networks (CHSN 2021). This book highlights the high-quality research articles in machine learning, computer vision, and networks. The content of this volume gives the reader an up-to-date picture of the state-of-the-art connection between computational intelligence, machine learning, and IoT. The papers included in this volume are peer-reviewed by experts in the related areas. The book will serve as a valuable reference resource for academics and researchers across the globe.

Simulation in Computer Network Design and Modeling: Use and Analysis IGI Global

This book examines different aspects of network security metrics and their application to enterprise networks. One of the most pertinent issues in securing mission-critical computing networks is the lack of effective security metrics which this book discusses in detail. Since "you cannot improve what you cannot measure", a network security metric is essential to evaluating the relative effectiveness of potential network security solutions. The authors start by examining the limitations of existing solutions and standards on security metrics, such as CVSS and attack surface, which typically focus on known vulnerabilities in individual software products or systems. The first few chapters of this book describe different approaches to fusing individual metric values obtained from CVSS scores into an overall measure of network security using attack graphs. Since CVSS scores are only available for previously known vulnerabilities, such approaches do not consider the threat of unknown attacks exploiting the so-called zero day vulnerabilities. Therefore, several chapters of this book are dedicated

to develop network security metrics especially designed for dealing with zero day attacks where the challenge is that little or no prior knowledge is available about the exploited vulnerabilities, and thus most existing methodologies for designing security metrics are no longer effective. Finally, the authors examine several issues on the application of network security metrics at the enterprise level. Specifically, a chapter presents a suite of security metrics organized along several dimensions for measuring and visualizing different aspects of the enterprise cyber security risk, and the last chapter presents a novel metric for measuring the operational effectiveness of the cyber security operations center (CSOC). Security researchers who work on network security or security analytics related areas seeking new research topics, as well as security practitioners including network administrators and security architects who are looking for state of the art approaches to hardening their networks, will find this book helpful as a reference. Advanced-level students studying computer science and engineering will find this book useful as a secondary text.

Best Practices in Computer Network Defense:

Incident Detection and Response IGI Global
"This book reviews methodologies in computer network simulation and modeling, illustrates the benefits of simulation in computer networks design, modeling, and analysis, and identifies the main issues that face efficient and effective computer network simulation"--Provided by publisher.