[EPUB] Automated Security Management Ehab Al Shaer

Recognizing the artifice ways to get this ebook **automated security management ehab al shaer** is additionally useful. You have remained in right site to start getting this info. get the automated security management ehab al shaer colleague that we have the funds for here and check out the link.

You could buy lead automated security management ehab al shaer or get it as soon as feasible. You could quickly download this automated security management ehab al shaer after getting deal. So, taking into account you require the books swiftly, you can straight get it. Its therefore very easy and appropriately fats, isnt it? You have to favor to in this look

Automated Security Management-Ehab Al-Shaer 2013-10-12 In this contributed volume, leading international researchers explore configuration modeling and checking, vulnerability and risk assessment, configuration analysis, and diagnostics and discovery. The authors equip readers to understand automated security management systems and techniques that increase overall network assurability and usability. These constantly changing networks defend against cyber attacks by integrating hundreds of security devices such as firewalls, IPSec gateways, IDS/IPS, authentication servers, authorization/RBAC servers, and crypto systems. Automated Security Management presents a number of topics in the area of configuration automation. Early in the book, the chapter authors introduce modeling and validation of configurations based on high-level requirements and discuss how to manage the security risk as a result of configuration settings of network systems. Later chapters delve into the concept of configuration analysis and why it is important in ensuring the security and functionality of a properly configured system. The book concludes with ways to identify problems when things go wrong and more. A wide range of theoretical and practical content make this volume valuable for researchers and professionals who work with network systems.

Automated Firewall Analytics-Ehab Al-Shaer 2014-09-23 This book provides a comprehensive and in-depth study of automated firewall policy analysis for designing, configuring and managing distributed firewalls in large-scale enterpriser networks. It presents methodologies, techniques and tools for researchers as well as professionals to understand the challenges and improve the state-of-the-art of managing firewalls systematically in both research and application domains. Chapters explore set-theory, managing firewall configuration globally and consistently, access control list with encryption, and authentication such as IPSec policies. The author also reveals a high-level service-oriented firewall configuration language (called FLIP) and a methodology and framework for designing optimal distributed firewall architecture. The chapters illustrate the concepts, algorithms, implementations and case studies for each technique. Automated Firewall Analytics: Design, Configuration and Optimization is appropriate for researchers and professionals working with firewalls. Advanced-level students in computer science will find this material suitable as a secondary textbook or reference.

Advances in Cyber Security-D. Frank Hsu 2013-04-03 As you read this, your computer is in jeopardy of being hacked and your identity being stolen. Read this book to protect yourselves from this threat. The world’s foremost cyber security experts, from Ruby Lee, Ph.D., the Forrest G. Hamrick professor of engineering and Director of the Princeton Architecture Laboratory for Multimedia and Security (PALMS) at Princeton University; to Nick Mankovich, Chief Information Security Officer of Royal Philips Electronics; to FBI Director Robert S. Mueller III; to Special Assistant to the President Howard A. Schmidt, share critical practical knowledge on how the cyberspace ecosystem is structured, how it functions, and what we can do to protect it and ourselves from attack and exploitation. The proliferation of social networking and advancement of information technology provide endless benefits in our living and working environments. However, these benefits also bring horrors in various forms of cyber threats and exploitations. Advances in Cyber Security collects the wisdom of cyber security professionals and practitioners from government, academia, and industry across national and international boundaries to provide ways and means to secure and sustain the cyberspace ecosystem. Readers are given a first-hand look at critical intelligence on cybercrime and security—including details of real-life operations. The vast, useful knowledge and experience shared in this essential new volume enables cyber citizens and cyber professionals alike to conceive novel ideas and construct feasible and practical solutions for defending against all kinds of adversaries and attacks. Among the many important topics covered in this collection are building a secure cyberspace ecosystem; public–private partnership to secure cyberspace; operation and law enforcement to protect our cyber citizens and to safeguard our cyber infrastructure; and strategy and policy issues to secure and sustain our cyber ecosystem.

Autonomous Cyber Deception-Ehab Al-Shaer 2019-01-02 This textbook surveys the knowledge base in automated and resilient cyber deception. It features four major parts: cyber deception reasoning frameworks, dynamic decision-making for cyber deception, network-based deception, and malware deception. An important distinguishing characteristic of this book is its inclusion of student exercises at the end of each chapter. Exercises include technical problems, short-answer discussion questions, or hands-on lab exercises, organized at a range of difficulties from easy to advanced,. This is a useful textbook for a wide range of classes and degree levels within the security arena and other related topics. It’s also suitable for researchers and practitioners with a variety of cyber security backgrounds from novice to experienced.

Formal Aspects in Security and Trust-Theo Dimitrakos 2006-03-23 This book constitutes the thoroughly refereed post-proceedings of the Third International Workshop on Formal Aspects in Security and Trust, FAST 2005, held in Newcastle upon Tyne, UK in July 2005. The 17 revised papers presented together with the extended abstract of 1 invited paper were carefully reviewed and selected from 37 submissions. The papers focus on formal aspects in security and trust policy models, security protocol design and analysis, formal models of trust and reputation, logics for security and trust, distributed trust management systems, trust-based reasoning, digital assets protection, data protection, privacy and ID issues, information flow analysis, language-based security, security and trust aspects in ubiquitous computing, validation/analysis tools, web service security/trust/privacy, GRID security, security risk assessment, and case studies.

2003 IEEE International Conference on Communications-IEEE Communications Society 2003 Aimed at systems designers and research engineers, the subjects covered in these proceedings include: multimedia; multiple antennas and wireless networks; service portability; content delivery; MAC protocols for WLANS; energy sensitive protocols; and protection/restoration.

Moving Target Defense-Sushil Jajodia 2011-08-26 Moving Target Defense: Creating Asymmetric Uncertainty for Cyber Threats was developed by a group of leading researchers. It describes the fundamental challenges facing the research community and identifies new promising solution paths. Moving Target Defense which is motivated by the asymmetric costs borne by cyber defenders takes an advantage afforded to attackers and reverses it to advantage defenders. Moving Target Defense is enabled by technical trends in recent years, including virtualization and workload migration on commodity systems, widespread and redundant network connectivity, instruction set and address space layout randomization, just-in-time compilers, among other techniques. However, many challenging research problems remain to be solved, such as the security of virtualization infrastructures, secure and resilient techniques to move systems within a virtualized environment, automatic diversification techniques, automated ways to dynamically change and manage the configurations of systems and networks, quantification of security improvement, potential degradation and more. Moving Target Defense: Creating Asymmetric Uncertainty for Cyber Threats is designed for advanced -level students and researchers focused on computer science, and as a secondary text book or reference. Professionals working in this field will also find this book valuable.

Proceedings of ... ACM Symposium on Access Control Models and Technologies- 2007

IT Security Risk Control Management-Raymond Pompon 2016-09-14 Follow step-by-step guidance to craft a successful security program. You will identify with the paradoxes of information security and discover handy tools that hook security controls into business processes. Information security is more than configuring firewalls, removing viruses, hacking machines, or setting passwords. Creating and promoting a successful security program requires skills in organizational consulting, diplomacy, change management, risk analysis, and out-of-the-box thinking. What You Will Learn: Build a security program that will fit neatly into an organization and change dynamically to suit both the needs of the organization and survive constantly changing threats Prepare for and pass such common audits as PCI-DSS, SSAE-16, and ISO 27001 Calibrate the scope, and customize security controls to fit into an organization’s culture Implement the most challenging processes, pointing out common pitfalls and distractions Frame security and risk issues to be clear and actionable so that decision makers, technical personnel, and users will listen and value your advice Who This Book Is For: IT professionals moving into the security field; new security managers, directors, project heads, and would-be CISOs; and security specialists from other disciplines moving into information security (e.g., former military security professionals, law enforcement professionals, and physical security professionals)

Security and Resiliency Analytics for Smart Grids-Ehab Al-Shaer 2016-06-09 This book targets the key concern of protecting critical infrastructures such as smart grids. It explains various static and dynamic security analysis techniques that can automatically verify smart grid security and resiliency and identify potential attacks in a proactive manner. This book includes three main sections. The first presents the idea of formally verifying the compliance of smart grid configurations with the security and resiliency guidelines. It provides a formal framework that verifies the compliance of the advanced metering infrastructure (AMI) configurations with the security and resiliency requirements, and generates remediation plans for potential security violations. The second section covers the formal verification of the security and resiliency of smart grid control systems by using a formal model to analyze attack evasions on state estimation, a core control module of the supervisory control system in smart grids. The model identifies attack vectors that can compromise state estimation. This section also covers risk mitigation techniques that synthesize proactive security plans that make such attacks infeasible. The last part of the book discusses the dynamic security analysis for smart grids. It shows that AMI behavior can be modeled using event logs collected at smart collectors, which in turn can be verified using the specification invariants generated from the configurations of the AMI devices. Although the focus of this book is smart grid security and resiliency, the included formal analytics are generic enough to be extended to other cyber-physical systems, especially those related to industrial control systems (ICS). Therefore, industry professionals and academic researchers will find this book an exceptional resource to learn theoretical and practical aspects of applying formal methods for the protection of critical infrastructures.

Handbook of e-Business Security-João Manuel R.S. Tavares 2018-07-27 There are a lot of e-business security concerns. Knowing about e-business security issues will likely help overcome them. Keep in mind, companies that have control over their e-business are likely to prosper most. In other words, setting up and maintaining a secure e-business is essential and important to business growth. This book covers state-of-the art practices in e-business security, including privacy, trust, security of transactions, big data, cloud computing, social network, and distributed systems.

Control and Automation of Electrical Power Distribution Systems-James Northcote-Green 2017-12-19 Implementing the automation of electric distribution networks, from simple remote control to the application of software-based decision tools, requires many considerations, such as assessing costs, selecting the control infrastructure type and automation level, deciding on the ambition level, and justifying the solution through a business case. Control and Automation of Electric Power Distribution Systems addresses all of these issues to aid you in resolving automation problems and improving the management of your distribution network. Bringing together automation concepts as they apply to utility distribution systems, this volume presents the theoretical and practical details of a control and automation solution for the entire distribution system of substations and feeders. The fundamentals of this solution include depth of control, boundaries of control responsibility, stages of automation, automation intensity levels, and automated device preparedness. To meet specific performance goals, the authors discuss distribution planning, performance calculations, and protection to facilitate the selection of the primary device, associated secondary control, and fault indicators. The book also provides two case studies that illustrate the business case for distribution automation (DA) and methods for calculating benefits, including the assessment of crew time savings. As utilities strive for better economies, DA, along with other tools described in this volume, help to achieve improved management of the distribution network. Using Control and Automation of Electric Power Distribution Systems, you can embark on the automation solution best suited for your needs.

Cyber Deception-Sushil Jajodia 2016-07-15 This edited volume features a wide spectrum of the latest computer science research relating to cyber deception. Specifically, it features work from the areas of artificial intelligence, game theory, programming languages, graph theory, and more. The work presented in this book highlights the complex and multi-faceted aspects of cyber deception, identifies the new scientific problems that will emerge in the domain as a result of the complexity, and presents novel approaches to these problems. This book can be used as a text for a graduate-level survey/seminar course on cutting-edge computer science research relating to cyber-security, or as a supplemental text for a regular graduate-level course on cyber-security.

Adaptive Autonomous Secure Cyber Systems-Sushil Jajodia

Novel Algorithms and Techniques in Telecommunications and Networking-Tarek Sobh 2010-01-30 Novel Algorithms and Techniques in Telecommunications and Networking includes a set of rigorously reviewed world-class manuscripts addressing and detailing state-of-the-art research projects in the areas of Industrial Electronics, Technology and Automation, Telecommunications and Networking. Novel Algorithms and Techniques in Telecommunications and Networking includes selected papers form the conference proceedings of the International Conference on Telecommunications and Networking (TeNe 08) which was part of the International Joint Conferences on Computer, Information and Systems Sciences and Engineering (CISSE 2008).

Tribe of Hackers-Marcus J. Carey 2019-07-23 Tribe of Hackers: Cybersecurity Advice from the Best Hackers in the World (9781119643371) was previously published as Tribe of Hackers: Cybersecurity Advice from the Best Hackers in the World (9781793464187). While this version features a new cover design and introduction, the remaining content is the same as the prior release and should not be considered a new or updated product. Looking for real-world advice from leading cybersecurity experts? You’ve found your tribe. Tribe of Hackers: Cybersecurity Advice from the Best Hackers in the World is your guide to joining the ranks of hundreds of thousands of cybersecurity professionals around the world. Whether you’re just joining the industry, climbing the corporate ladder, or considering consulting, Tribe of Hackers offers the practical know-how, industry perspectives, and technical insight you need to succeed in the rapidly growing information security market. This unique guide includes inspiring interviews from 70 security experts, including Lesley Carhart, Ming Chow, Bruce Potter, Robert M. Lee, and Jayson E. Street. Get the scoop on the biggest cybersecurity myths and misconceptions about security Learn what qualities and credentials you need to advance in the cybersecurity field Uncover which life hacks are worth your while Understand how social media and the Internet of Things has changed cybersecurity Discover what it takes to make the move from the corporate world to your own cybersecurity venture Find your favorite hackers online and continue the conversation Tribe of Hackers is a must-have resource for security professionals who are looking to advance their careers, gain a fresh perspective, and get serious about cybersecurity with thought-provoking insights from the world’s most noteworthy hackers and influential security specialists.

Smart Infrastructure and Applications-Rashid Mehmood 2019-06-20 This book provides a multidisciplinary view of smart infrastructure through a range of diverse introductory and advanced topics. The book features an array of subjects that include: smart cities and infrastructure, e-healthcare, emergency and disaster management, Internet of Vehicles, supply chain management, eGovernance, and high performance computing. The book is divided into five parts: Smart Transportation, Smart Healthcare, Miscellaneous Applications, Big Data and High Performance Computing, and Internet of Things (IoT). Contributions are from academics, researchers, and industry professionals around the world. Features a broad mix of topics related to smart infrastructure and smart applications, particularly high performance computing, big data, and artificial intelligence; Includes a strong emphasis on methodological aspects of infrastructure, technology and application development; Presents a substantial overview of research and development on key economic sectors including healthcare and transportation.

Computer Vision: Concepts, Methodologies, Tools, and Applications-Management Association, Information Resources 2018-02-02 The fields of computer vision and image processing are constantly evolving as new research and applications in these areas emerge. Staying abreast of the most up-to-date developments in this field is necessary in order to promote further research and apply these developments in real-world settings. Computer Vision: Concepts, Methodologies, Tools, and Applications is an innovative reference source for the latest academic material on development of computers for gaining understanding about videos and digital images. Highlighting a range of topics, such as computational models, machine learning, and image processing, this multi-volume book is ideally designed for academicians, technology professionals, students, and researchers interested in uncovering the latest innovations in the field.

Innovative Technologies and Learning-Lisbet Rønningsbakk 2020-01-15 This book constitutes the refereed proceedings of the Second International Conference on Innovative Technologies and Learning, ICITL 2019, held in Tromsø, Norway, in December 2019. The 85 full papers presented together with 4 short papers were carefully reviewed and selected from 189 submissions. The papers are organized in the following topical sections: application and design of innovative learning software; artificial intelligence and data mining in education; augmented and virtual reality in education; computational thinking in education; design and framework of learning systems; educational data analytics techniques and adaptive learning applications; evaluation, assessment and test; innovative learning in education; mobile learning; new perspectives in education; online course and web-based environment; pedagogies to innovative technologies; social media learning; technologies enhanced language learning; and technology and engineering education.

Network Security Metrics-Lingyu Wang 2017-11-15 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.

Cyber Warfare-Sushil Jajodia 2015-04-09 This book features a wide spectrum of the latest computer science research relating to cyber warfare, including military and policy dimensions. It is the first book to explore the scientific foundation of cyber warfare and features research from the areas of artificial intelligence, game theory, programming languages, graph theory and more. The high-level approach and emphasis on scientific rigor provides insights on ways to improve cyber warfare defense worldwide. Cyber Warfare: Building the Scientific Foundation targets researchers and practitioners working in cyber security, especially government employees or contractors. Advanced-level students in computer science and electrical engineering with an interest in security will also find this content valuable as a secondary textbook or reference.

Construction des systemes d'exploitation repartis-Erhard Rahm 1990

Micro-Electronics and Telecommunication Engineering-Devendra Kumar Sharma 2020-04-02 This book presents selected papers from the 3rd International Conference on Micro-Electronics and Telecommunication Engineering, held at SRM Institute of Science and Technology, Ghaziabad, India, on 30-31 August 2019. It covers a wide variety of topics in micro-electronics and telecommunication engineering, including micro-electronic engineering, computational remote sensing, computer science and intelligent systems, signal and image processing, and information and communication technology.

Advances in Intelligent Information Hiding and Multimedia Signal Processing-Jeng-Shyang Pan 2016-11-21 This volume of Smart Innovation, Systems and Technologies contains accepted papers presented in IIH-MSP-2016, the 12th International Conference on Intelligent Information Hiding and Multimedia Signal Processing. The conference this year was technically co-sponsored by Tainan Chapter of IEEE Signal Processing Society, Fujian University of Technology, Chaoyang University of Technology, Taiwan Association for Web Intelligence Consortium, Fujian Provincial Key Laboratory of Big Data Mining and Applications (Fujian University of Technology), and Harbin Institute of Technology Shenzhen Graduate School. IIH-MSP 2016 is held in 21-23, November, 2016 in Kaohsiung, Taiwan. The conference is an international forum for the researchers and professionals in all areas of information hiding and multimedia signal processing.

Software Abstractions-Daniel Jackson 2016-02-12 Previously published in hardcover: 2012.

International Conference on Innovative Computing and Communications-Ashish Khanna 2019 This book includes high-quality research papers presented at the Third International Conference on Innovative Computing and Communication (ICICC 2020), which is held at the Shaheed Sukhdev College of Business Studies, University of Delhi, Delhi, India, on 21-23 February, 2020. Introducing the innovative works of scientists, professors, research scholars, students and industrial experts in the field of computing and communication, the book promotes the transformation of fundamental research into institutional and industrialized research and the conversion of applied exploration into real-time applications.

Advances in Security of Information and Communication Networks-Ali Ismail Awad 2013-08-15 This book constitutes the refereed proceedings of the International Conference on Advances in Security of Information and Communication Networks, Sec Net 2013, held in Cairo, Egypt, in September 2013. The 21 revised full papers presented were carefully reviewed and selected from 62 submissions. The papers are organized in topical sections on networking security; data and information security; authentication and privacy; security applications.

Proceedings of the International Conference on Advanced Intelligent Systems and Informatics 2019-Aboul Ella Hassanien 2019-10-02 This book presents the proceedings of the 5th International Conference on Advanced Intelligent Systems and Informatics 2019 (AISI2019), which took place in Cairo, Egypt, from October 26 to 28, 2019. This international and interdisciplinary conference, which highlighted essential research and developments in the fields of informatics and intelligent systems, was organized by the Scientific Research Group in Egypt (SRGE). The book is divided into several sections, covering the following topics: machine learning and applications, swarm optimization and applications, robotic and control systems, sentiment analysis, e-learning and social media education, machine and deep learning algorithms, recognition and image processing, intelligent systems and applications, mobile computing and networking, cyber-physical systems and security, smart grids and renewable energy, and micro-grid and power systems.

Information Security Analytics-Mark Talabis 2014-11-25 Information Security Analytics gives you insights into the practice of analytics and, more importantly, how you can utilize analytic techniques to identify trends and outliers that may not be possible to identify using traditional security analysis techniques. Information Security Analytics dispels the myth that analytics within the information security domain is limited to just security incident and event management systems and basic network analysis. Analytic techniques can help you mine data and identify patterns and relationships in any form of security data. Using the techniques covered in this book, you will be able to gain security insights into unstructured big data of any type. The authors of Information Security Analytics bring a wealth of analytics experience to demonstrate practical, hands-on techniques through case studies and using freely-available tools that will allow you to find anomalies and outliers by combining disparate data sets. They also teach you everything you need to know about threat simulation techniques and how to use analytics as a powerful decision-making tool to assess security control and process requirements within your organization. Ultimately, you will learn how to use these simulation techniques to help predict and profile potential risks to your organization. Written by security practitioners, for security practitioners Real-world case studies and scenarios are provided for each analytics technique Learn about open-source analytics and statistical packages, tools, and applications Step-by-step guidance on how to use analytics tools and how they map to the techniques and scenarios provided Learn how to design and utilize simulations for "what-if" scenarios to simulate security events and processes Learn how to utilize big data techniques to assist in incident response and intrusion analysis

Guidelines on Firewalls and Firewall Policy- 2002 This document provides guidelines for Federal organizations acquisition and use of security-related Information Technology (IT) products. These guidelines provide advice to agencies for sensitive (i.e., non-national security) unclassified systems. NIST's advice is given in the context of larger recommendations regarding computer systems security.

Toward Social Internet of Things (SIoT): Enabling Technologies, Architectures and Applications-Aboul Ella Hassanien 2019-07-23 This unique book discusses a selection of highly relevant topics in the Social Internet of Things (SIoT), including blockchain, fog computing and data fusion. It also presents numerous SIoT-related applications in fields such as agriculture, health care, education and security, allowing researchers and industry practitioners to gain a better understanding of the Social Internet of Things

Building Internet Firewalls-Elizabeth D. Zwicky 2000-06-26 In the five years since the first edition of this classic book was published, Internet use has exploded. The commercial world has rushed headlong into doing business on the Web, often without integrating sound security technologies and policies into their products and methods. The security risks--and the need to protect both business and personal data--have never been greater. We've updated Building Internet Firewalls to address these newer risks. What kinds of security threats does the Internet pose? Some, like password attacks and the exploiting of known security holes, have been around since the early days of networking. And others, like the distributed denial of service attacks that crippled Yahoo, E-Bay, and other major e-commerce sites in early 2000, are in current headlines. Firewalls, critical components of today's computer networks, effectively protect a system from most Internet security threats. They keep damage on one part of the network--such as eavesdropping, a worm program, or file damage--from spreading to the rest of the network. Without firewalls, network security problems can rage out of control, dragging more and more systems down. Like the bestselling and highly respected first edition, Building Internet Firewalls, 2nd Edition, is a practical and detailed step-by-step guide to designing and installing firewalls and configuring Internet services to work with a firewall. Much expanded to include Linux and Windows coverage, the second edition describes: Firewall technologies: packet filtering, proxying, network address translation, virtual private networks Architectures such as screening routers, dual-homed hosts, screened hosts, screened subnets, perimeter networks, internal firewalls Issues involved in a variety of new Internet services and protocols through a firewall Email and News Web services and scripting languages (e.g., HTTP, Java, JavaScript, ActiveX, RealAudio, RealVideo) File transfer and sharing services such as NFS, Samba Remote access services such as Telnet, the BSD "r" commands, SSH, BackOrifice 2000 Real-time conferencing services such as ICQ and talk Naming and directory services (e.g., DNS, NetBT, the Windows Browser) Authentication and auditing services (e.g., PAM, Kerberos, RADIUS); Administrative services (e.g., syslog, SNMP, SMS, RIP and other routing protocols, and ping and other network diagnostics) Intermediary protocols (e.g., RPC, SMB, CORBA, IIOP) Database protocols (e.g., ODBC, JDBC, and protocols for Oracle, Sybase, and Microsoft SQL Server) The book's complete list of resources includes the location of many publicly available firewall construction tools.

Physical Metallurgy-David E. Laughlin 2014-07-24 This fifth edition of the highly regarded family of titles that first published in 1965 is now a three-volume set and over 3,000 pages. All chapters have been revised and expanded, either by the fourth edition authors alone or jointly with new co-authors. Chapters have been added on the physical metallurgy of light alloys, the physical metallurgy of titanium alloys, atom probe field ion microscopy, computational metallurgy, and orientational imaging microscopy. The books incorporate the latest experimental research results and theoretical insights. Several thousand citations to the research and review literature are included. Exhaustively synthesizes the pertinent, contemporary developments within physical metallurgy so scientists have authoritative information at their fingertips Replaces existing articles and monographs with a single, complete solution Enables metallurgists to predict changes and create novel alloys and processes

Handbook of Multimedia Information Security: Techniques and Applications-Amit Kumar Singh 2019-07-19 This handbook is organized under three major parts. The first part of this handbook deals with multimedia security for emerging applications. The chapters include basic concepts of multimedia tools and applications, biological and behavioral biometrics, effective multimedia encryption and secure watermarking techniques for emerging applications, an adaptive face identification approach for android mobile devices, and multimedia using chaotic and perceptual hashing function. The second part of this handbook focuses on multimedia processing for various potential applications. The chapter includes a detail survey of image processing based automated glaucoma detection techniques and role of de-noising, recent study of dictionary learning based image reconstruction techniques for analyzing the big medical data, brief introduction of quantum image processing and it applications, a segmentation-less efficient Alzheimer detection approach, object recognition, image enhancements and de-noising techniques for emerging applications, improved performance of image compression approach, and automated detection of eye related diseases using digital image processing. The third part of this handbook introduces multimedia applications. The chapter includes the extensive survey on the role of multimedia in medicine and multimedia forensics classification, a finger based authentication system for e-health security, analysis of recently developed deep learning techniques for emotion and activity recognition. Further, the book introduce a case study on change of ECG according to time for user identification, role of multimedia in big data, cloud computing, the Internet of things (IoT) and blockchain environment in detail for real life applications. This handbook targets researchers, policy makers, programmers and industry professionals in creating new knowledge for developing efficient techniques/framework for multimedia applications. Advanced level students studying computer science, specifically security and multimedia will find this book useful as a reference.

Face Recognition in Adverse Conditions-De Marsico, Maria 2014-04-30 Facial recognition software has improved by leaps and bounds over the past few decades, with error rates decreasing significantly within the past ten years. Though this is true, conditions such as poor lighting, obstructions, and profile-only angles have continued to persist in preventing wholly accurate readings. Face Recognition in Adverse Conditions examines how the field of facial recognition takes these adverse conditions into account when designing more effective applications by discussing facial recognition under real world PIE variations, current applications, and the future of the field of facial recognition research. The work is intended for academics, engineers, and researchers specializing in the field of facial recognition.

Industrial Network Security-Eric D. Knapp 2014-12-09 As the sophistication of cyber-attacks increases, understanding how to defend critical infrastructure systems—energy production, water, gas, and other vital systems—becomes more important, and heavily mandated. Industrial Network Security, Second Edition arms you with the knowledge you need to understand the vulnerabilities of these distributed supervisory and control systems. The book examines the unique protocols and applications that are the foundation of industrial control systems, and provides clear guidelines for their protection. This how-to guide gives you thorough understanding of the unique challenges facing critical infrastructures, new guidelines and security measures for critical infrastructure protection, knowledge of new and evolving security tools, and pointers on SCADA protocols and security implementation. All-new real-world examples of attacks against control systems, and more diagrams of systems Expanded coverage of protocols such as 61850, Ethernet/IP, CIP, ISA-99, and the evolution to IEC62443 Expanded coverage of Smart Grid security New coverage of signature-based detection, exploit-based vs. vulnerability-based detection, and signature reverse engineering

Guide to Reliable Internet Services and Applications-Charles R. Kalmanek 2010-06-09 An oft-repeated adage among telecommunication providers goes, “There are ve things that matter: reliability, reliability, reliability, time to market, and cost. If you can’t do all ve, at least do the rst three. ” Yet, designing and operating reliable networks and services is a Herculean task. Building truly reliable components is unacceptably expensive, forcing us to c- struct reliable systems out of unreliable components. The resulting systems are inherently complex, consisting of many different kinds of components running a variety of different protocols that interact in subtle ways. Inter-networkssuch as the Internet span multiple regions of administrative control, from campus and cor- rate networks to Internet Service Providers, making good end-to-end performance a shared responsibility borne by sometimes uncooperative parties. Moreover, these networks consist not only of routers, but also lower-layer devices such as optical switches and higher-layer components such as rewalls and proxies. And, these components are highly con gurable, leaving ample room for operator error and buggy software. As if that were not dif cult enough, end users understandably care about the performance of their higher-level applications, which has a complicated relationship with the behavior of the underlying network. Despite these challenges, researchers and practitioners alike have made trem- dous strides in improving the reliability of modern networks and services.

CUCKOO'S EGG-Clifford Stoll 2012-05-23 Before the Internet became widely known as a global tool for terrorists, one perceptive U.S. citizen recognized its ominous potential. Armed with clear evidence of computer espionage, he began a highly personal quest to expose a hidden network of spies that threatened national security. But would the authorities back him up? Cliff Stoll's dramatic firsthand account is "a computer-age detective story, instantly fascinating [and] astonishingly gripping" (Smithsonian). Cliff Stoll was an astronomer turned systems manager at Lawrence Berkeley Lab when a 75-cent accounting error alerted him to the presence of an unauthorized user on his system. The hacker's code name was "Hunter"—a mysterious invader who managed to break into U.S. computer systems and steal sensitive military and security information. Stoll began a one-man hunt of his own: spying on the spy. It was a dangerous game of deception, broken codes, satellites, and missile bases—a one-man sting operation that finally gained the attention of the CIA . . . and ultimately trapped an international spy ring fueled by cash, cocaine, and the KGB.

Information Systems Design and Intelligent Applications-Vikrant Bhateja 2018-03-01 The book is a collection of high-quality peer-reviewed research papers presented at International Conference on Information System Design and Intelligent Applications (INDIA 2017) held at Duy Tan University, Da Nang, Vietnam during 15-17 June 2017. The book covers a wide range of topics of computer science and information technology discipline ranging from image processing, database application, data mining, grid and cloud computing, bioinformatics and many others. The various intelligent tools like swarm intelligence, artificial intelligence, evolutionary algorithms, bio-inspired algorithms have been well applied in different domains for solving various challenging problems.

Smart Grid Security-Sanjay Goel 2015-04-28 This book on smart grid security is meant for a broad audience from managers to technical experts. It highlights security challenges that are faced in the smart grid as we widely deploy it across the landscape. It starts with a brief overview of the smart grid and then discusses some of the reported attacks on the grid. It covers network threats, cyber physical threats, smart metering threats, as well as privacy issues in the smart grid. Along with the threats the book discusses the means to improve smart grid security and the standards that are emerging in the field. The second part of the book discusses the legal issues in smart grid implementations, particularly from a privacy (EU data protection) point of view.