Administration In Role Based Access Control

"This book offers insightful articles on the most salient contemporary issues of managing social and human aspects of information security"--Provided by publisher.

Control Engineering and Information Systems contains the papers presented at the 2014 International Conference on Control Engineering and Information Systems (ICCEIS 2014, Yueyang, Hunan, China, 20-22 June 2014). All major aspects of the theory and applications of control engineering and information systems are addressed, including: Intelligent s

Role Mining In Business: Taming Role-based Access Control AdministrationWorld Scientific

This comprehensive new resource provides an introduction to fundamental Attribute Based Access Control (ABAC) models. This book provides valuable information for developing ABAC to improve information sharing within organizations while taking into consideration the planning, design, implementation, and operation. It explains the history and model of ABAC, related standards, verification and assurance, applications, as well as deployment challenges. Readers find authoritative insight into specialized topics including formal ABAC history, ABAC's relationship with other access control models, ABAC model validation and analysis, verification and testing, and deployment frameworks such as XACML. Next Generation Access Model (NGAC) is explained, along with attribute considerations in implementation. The book explores ABAC applications in SOA/workflow domains, ABAC architectures, and includes details on feature sets in commercial and open source products. This insightful resource presents a combination of technical and administrative information for models, standards, and products that will benefit researchers as well as implementers of ABAC systems in the field.

This book constitutes the refereed proceedings of the 9th International Conference on Information Systems Security, ICISS 2013, held in Kolkata, India, in December 2013. The 20 revised full papers and 6 short papers presented together with 3 invited papers were carefully reviewed and selected from 82 submissions. The papers address theoretical and practical problems in information and systems security and related areas.

Microsoft Exchange Server 2010 Administrator's Pocket Consultant

Security, Privacy and Trust in Cloud Systems

Model, Processes, and Management

27th Annual IFIP WG 11.3 Conference, DBSec 2013, Newark, NJ, USA, July 15-17, 2013, Proceedings

Tools and Algorithms for the Construction and Analysis of Systems

Handbook of Research on Social and Organizational Liabilities in Information Security

Solaris 10 System Administration Exam Prep

Administration of access control was and still is a crucial, critical and complex aspect of Security Administration. Many models were developed and used to effect this administration such as Mandatory access Control (MAC), Discretionary Access Control (DAC) and Role Base access Control. the latter, RBAC which is a flexible and policy-independent access control, represents a natural structure of an orginization where functions are grouped into roles and users are permitted to one or more of these roles. In large organizations with relatively large systems, with hundreds of roles and users and thousands and more of permission(s), managing all the roles, users, and permission(s) is not an easy task that can be centralized in a small team of security administrators. While it is not a new concept, Role Based Access Control continues to gain wider commercial acceptance as it simplifies and enhances definition, auditing and administration of security access rights. Moreover,it has been implemented in different areas, such as ORACLE and solaris. In this thesis RBAC is applied to Windows 2000 in order to simplify the management of security, through using a simulation of ARBAC administration capabilities on Windows 2000 implementing groups hierarchies and the decentralization of group assignments.

This book constitutes the refereed proceedings of the 6th International Conference on Mathematical Methods, Models, and Architectures for Computer Network Security, MMM-ACNS 2012, held in St. Petersburg, Russia in October 2012. The 14 revised full papers and 8 revised short presentations were carefully reviewed and selected from a total of 44 submissions. The papers are organized in topical sections on applied cryptography and security protocols, access control and information protection, security policies, security event and information management, instrusion prevention, detection and response, anti-malware techniques, security modeling and cloud security.

Identity and Access Management: Business Performance Through Connected Intelligence provides you with a practical, in-depth walkthrough of how to plan, assess, design, and deploy IAM solutions. This book breaks down IAM into manageable components to ease systemwide implementation. The hands-on, end-to-end approach includes a proven step-by-step method for deploying IAM that has been used successfully in over 200 deployments. The book also provides reusable templates and source code examples in Java, XML, and SPML. Focuses on real-word implementations Provides end-to-end coverage of IAM from business drivers, requirements, design, and development to implementation Presents a proven, step-by-step method for deploying IAM that has been successfully used in over 200 cases Includes companion website with source code examples in Java, XML, and SPML as well as reusable templates

Security and privacy are paramount concerns in information processing systems, which are vital to business, government and military operations and, indeed, society itself. Meanwhile, the expansion of the Internet and its convergence with telecommunication networks are providing incredible connectivity, myriad applications and, of course, new threats. Data and Applications Security XVII: Status and Prospects describes original research results, practical experiences and innovative ideas, all focused on maintaining security and privacy in information processing systems and applications that pervade cyberspace. The areas of coverage include: -Information Warfare, -Information Assurance, -Security and Privacy, -Authorization and Access Control in Distributed Systems, -Security Technologies for the Internet, -Access Control Models and Technologies, -Digital Forensics. This book is the seventeenth volume in the series produced by the International Federation for Information Processing (IFIP) Working Group 11.3 on Data and Applications Security. It presents a selection of twenty-six updated and edited papers from the Seventeenth Annual IFIP TC11 / WG11.3 Working Conference on Data and Applications Security held at Estes Park, Colorado, USA in August 2003, together with a report on the conference keynote speech and a summary of the conference panel. The contents demonstrate the richness and vitality of the discipline, and other directions for future research in data and applications security. Data and Applications Security XVII: Status and Prospects is an invaluable resource for information assurance researchers, faculty members and graduate students, as well as for individuals engaged in research and development in the information technology sector.

This book constitutes the refereed proceedings of the 7th International Symposium on Engineering Secure Software and Systems, ESSoS 2015, held in Milan, Italy, in March 2015. The 11 full papers presented together with 5 short papers were carefully reviewed and selected from 41 submissions. The symposium features the following topics: formal methods; cloud passwords; machine learning; measurements ontologies; and access control.

Computer Aided Verification

Mastering FreeBSD and OpenBSD Security

Engineering Secure Software and Systems

Access Control in Data Management Systems

26th International Conference, CAV 2014, Held as Part of the Vienna Summer of Logic, VSL 2014, Vienna, Austria, July 18-22, 2014, Proceedings

Proceedings of the IFIP TC-11 21st International Information Security Conference (SEC 2006), 22-24 May 2006, Karlstad, Sweden

On The Move to Meaningful Internet Systems 2003: OTM 2003 Workshops

This textbook introduces new business concepts on cloud environments such as secure, scalable anonymity and practical payment protocols for the Internet of things and Blockchain technology. The protocol uses electronic cash for payment transactions. In this new protocol, from the viewpoint of banks, consumers can improve anonymity if they are worried about disclosure of their identities in the cloud. Currently, there is not a book available that has reported the techniques covering the protocols with anonymizations and Blockchain technology. Thus this will be a useful book for universities to purchase. This textbook provides new direction for access control management and online business, with new challenges within Blockchain technology that may arise in cloud environments. One is related to the authorization granting process. For example, when a role is granted to a user, this role may conflict with other roles of the user or together with this role; the user may have or derive a high level of authority. Another is related to authorization revocation. For instance, when a role is revoked from a user, the user may still have the role. Experts will get benefits from these challenges through the developed methodology for authorization granting algorithm, and weak revocation and strong revocation algorithms.

This book constitutes the refereed proceedings of the 27th IFIP WG 11.3 International Conference on Data and Applications Security and Privacy, DBSec 2013, held in Newark, NJ, USA in July 2013. The 16 revised full and 6 short papers presented were carefully reviewed and selected from 45 submissions. The papers are organized in topical sections on privacy, access control, cloud computing, data outsourcing, and mobile computing.

Struts 2 Black Book brings to you a detailed discussion on Web application development by using Struts 2 Framework. Targeting beginner to advance level readers, this book begins with an introduction to Struts 2 and describes its evolutions as a new Web Application Framework. It covers various concepts supported by Struts 2, such as Interceptors, Results, Validators, Generic and UI Tags and Plugins. The book also describes the benefits of these concepts and different ways of implementing them. In addition, the book discusses various components created and configured in Struts 2 Framework based web application. The book also covers the architecture and implementation changed in Struts 2 from Struts 1. The book describes the process of migrating a Struts 1 application to a Struts 2 based application, and a lot more.

This book constitutes the proceedings of the 19th International Conference on Tools and Algorithms for the Construction and Analysis of Systems, TACAS 2013, held in Rome, Italy, in March 2013. The 42 papers presented in this volume were carefully reviewed and selected from 172 submissions. They are organized in topical sections named: Markov chains; termination; SAT/SMT; games and synthesis; process algebra; pushdown; runtime verification and model checking; concurrency; learning and abduction; timed automata; security and access control; frontiers (graphics and quantum); functional programs and types; tool demonstrations; explicit-state model checking; B ü chi automata; and competition on software verification.

This book is perfect for IT administrators who are looking to enhance their skills on system and asset management. A fair understanding of the core elements and applications related to SCCM would be helpful.

Third VLDB Workshop, SDM 2006, Seoul, Korea, September 10-11, 2006, Proceedings

Data and Applications Security XVII

5th International Conference, WAIM 2004, Dalian, China, July 15-17, 2004, Proceedings

15th European Symposium on Research in Computer Security, Athens, Greece, September 20-22, 2010. Proceedings

Role Mining In Business: Taming Role-based Access Control Administration

OTM Confederated International Workshops, HCI-SWWA, IPW, JTRES, WORM, WMS, and WRSM 2003, Catania, Sicily, Italy, November 3-7, 2003, Proceedings

Role Base Access Control and Its Administrative Implementation with Windows 2000

Learn the art of leveraging PowerShell to automate Office 365 repetitive tasks About This Book Master the fundamentals of PowerShell to automate Office 365 tasks. Easily administer scenarios such as user management, reporting, cloud services, and many more. A fast-paced guide that leverages PowerShell commands to increase your productivity. Who This Book Is For The book is aimed at sys admins who are administering office 365 tasks and looking forward to automate the manual tasks. They have no knowledge about PowerShell however basic understanding of PowerShell would be advantageous. What You Will Learn Understand the benefits of scripting and automation and get started using Powershell with Office 365 Explore various PowerShell packages and permissions required to manage Office 365 through PowerShell Create, manage, and remove Office 365 accounts and licenses using PowerShell and the Azure AD Learn about using powershell on other platforms and how to use Office 365 APIs through remoting Work with Exchange Online and SharePoint Online using PowerShell Automate your tasks and build easy-to-read reports using PowerShell In Detail While most common administrative tasks are available via the Office 365 admin center, many IT professionals are unaware of the real power that is available to them below the surface. This book aims to educate readers on how learning PowerShell for Office 365 can simplify repetitive and complex administrative tasks, and enable greater control than is available on the surface. The book starts by teaching readers how to access Office 365 through PowerShell and then explains the PowerShell fundamentals required for automating Office 365 tasks. You will then walk through common administrative cmdlets to manage accounts, licensing, and other scenarios such as automating the importing of multiple users,assigning licenses in Office 365, distribution groups, passwords, and so on. Using practical examples, you will learn to enhance your current functionality by working with Exchange Online, and SharePoint Online using PowerShell. Finally, the book will help you effectively manage complex and repetitive tasks (such as license and account management) and build productive reports. By the end of the book, you will have automated major repetitive tasks in Office 365 using PowerShell. Style and approach This step by step guide focuses on teaching the fundamentals of working with PowerShell for Office 365. It covers practical usage examples such as managing user accounts, licensing, and administering common Office 365 services. You will be able to leverage the processes laid out in the book so that you can move forward and explore other less common administrative tasks or functions.

Totally updated for 2011, here's the ultimate study guide for the CISSP exam Considered the most desired certification for IT security professionals, the Certified Information Systems Security Professional designation is also a career-booster. This comprehensive study guide covers every aspect of the 2011 exam and the latest revision of the CISSP body of knowledge. It offers advice on how to pass each section of the exam and features expanded coverage of biometrics, auditing and accountability, software security testing, and other key topics. Included is a CD with two full-length, 250-question sample exams to test your progress. CISSP certification identifies the ultimate IT security professional; this complete study guide is fully updated to cover all the objectives of the 2011 CISSP exam Provides in-depth knowledge of access control, application development security, business continuity and disaster recovery planning, cryptography, Information Security governance and risk management, operations security, physical (environmental) security, security architecture and design, and telecommunications and network security Also covers legal and regulatory investigation and compliance Includes two practice exams and challenging review questions on the CD Professionals seeking the CISSP certification will boost their chances of success with CISSP: Certified Information Systems Security Professional Study Guide, 5th Edition.

Role-based access control (RBAC) has been widely accepted within computer security communities over the last decade. Thus, many formalized and practical approaches attempted to leverage roles for access control, primarily aiming at easing complex security administration within closed domain environments. However, roles can be a convenient construct for expressing the degree of trust between entities, based upon which further specification of responsibility and capability is made, and thus they can be efficiently used for access control in open domain environments. This aspect of roles is especially beneficial to trust management, which is an approach to access control for unknown entities through the use of capability delegation. The primary goal of this dissertation work is to provide an integrated mechanism for facilitating role-based authorization in open and distributed environments. For the purpose, we first propose a role-based access control model for trust management called TRUSTr. TRUSTr introduces a new component called trust assignment (TA) to traditional RBAC models, thereby associating roles in a local domain with roles from trusted domains. Central to understanding TA is that capability delegation across domains can be expressed on the basis of roles associated by TA. We also discuss two operations that TA supports, entrust and distrust, with a view to managing those associated roles. In addition, we investigate how role hierarchies and constraints can be realized in TRUSTr. By extending an existing mathematical framework, we describe a feasible scheme for instantiating the model as a proof-of-concept. After discussing how roles can be used for access control in open and distributed environments by presenting a trust-enabled RBAC model, we further investigate two important issues relevant to the usage of roles: how valid roles can be defined and how defined roles can be managed systematically for access control. Role engineering (RE) is an approach to defining roles and assigning permissions to roles, whereby an organizational access control policy can be formulated on roles. We present an RE framework called SIREN for enabling process-driven role definition. The core of our framework is that informational characteristics and flows in the process of RE are analyzed, and then, system-centric information is modeled for the purpose of providing both a method of analysis and a method of communication between two authority boundaries identified in the process of RE. Unified Modeling Language (UML) extension mechanisms are exploited for modeling the information. A case study of using the information model is described to demonstrate its feasibility. Role administration (RA) is an approach to managing defined roles. We propose three methodological constituents that enable systematic role management. We also describe a role administration system called RolePartner, which is built on the top of those methodological constituents. RolePartner leverages a directory service for storing role-based authorization policies. We demonstrate that the system can be seamlessly integrated into an existing privilege-based authorization infrastructure based on trust management. As a trust-enabled role model, TRUSTr contributes to broaden RBAC's applicability into open and distributed environments. As a generic RE framework for enabling process-driven role definition, SIREN is considered to be the first RE framework in the literature that analyzes the general process of RE and leverages system-centric information for defining valid roles. We also believe that RolePartner illustrates how roles can be managed systematically so as to carry out role-based security policy administration. Finally, we believe that all of the three above are associated in the sense that they are complimentary to each other in order to build an integrated solution for facilitating role-based authorization in open and distributed environments.

The authors explain role based access control (RBAC), its administrative and cost advantages, implementation issues and imigration from conventional access control methods to RBAC.

This book constitutes the refereed proceedings of the 8th International Conference On Secure Knowledge Management In Artificial Intelligence Era, SKM 2019, held in Goa, India, in December 2019. The 12 full papers presented were carefully reviewed and selected from 34 submissions. They were organized according to the following topical sections: cyber security; security and artifcial intelligence; access control models; and social networks.

Information Security Applications

28th Annual IFIP WG 11.3 Working Conference, DBSec 2014, Vienna, Austria, July 14-16, 2014, Proceedings

Computational Science and Its Applications - ICCSA 2010

19th International Conference, TACAS 2013, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2013, Rome, Italy, March 16-24, 2013, Proceedings

Secure Data Management

Secure Knowledge Management In Artificial Intelligence Era

In role based access control systems (RBAC) permissions are associated with roles, and users are made members of appropriate roles thereby acquiring the roles' permissions. This greatly simplifies management of permissions. Roles are created for the various job functions in an organization and users are assigned roles based on their responsibilities and qualifications. Users can be easily reassigned from one role to another. Roles can be granted new permissions as new applications and systems are incorporated, and permissions can be revoked from roles as needed. Role-role relationships can be established to lay out broad policy objectives. The principal motivation of RBAC is to simplify administration. In large organizations the number of roles can be in the hundreds or thousands, and users can be in the tens or hundreds of thousands, maybe even millions. To be

effective, management and administration of RBAC in such systems need some form of decentralization and automation without loosing central control over broad policy. An appealing possibility is to use RBAC to manage itself. Our work looks at proposing models that would allow for decentralization and automation of user-role assignment. In this dissertation we identify architectures and models for decentralized administration of user-role assignment. Our work is performed in context of the OM-AM layered models framework. OM-AM stands for objectives, models, architectures and mechanisms. OM layer addresses security requirements and trade offs, essentially it represents "what" needs to be achieved. AM layer articulates "how" to meet the specified requirements. In this dissertation we use the terms architecture and models as they relate to OM-AM framework. Initially we focus our work on user-role assignment in a centralized system. Then we concentrate our work on user-role relationship as it pertains to distributed systems. Finally we look at how self-service and automation can be achieved in user-role assignment. We propose a model called URA97 for user-role assignment. This model provides the semantics for granting and revoking roles from users in a centralized system. URA97 achieves assignment and revocation of users to and from roles by means of simple and intuitive relations named can-assign and can-revoke. In URA97 grant and revoke operations are performed by administrators assigned to administrative roles. We explore some of the possible architectures in a distributed environment. These depend on how the resources, data and users are distributed and how they interact in a distributed environment. We then develop a push-based model for user-role assignment, which deals with two operations assignment of users to roles and revocation of roles from users. URA97 was developed in context of the RBAC96 model. URA97 was developed during early stages of RBAC96 when it was still an academic discipline, since then RBAC96 has received strong support from the research and practitioner communities and today is widely practiced as preferred form of access control. It is becoming clear that relying on manual intervention in all aspects of RBAC administration is cumbersome. Concurrently access control has started adopting emerging concepts like usage control, rate limits and accountability etc. To this effect we propose five founding principles for next-generation RBAC, summarized as ASCAA for Abstraction, Separation, Containment, Automation and Accountability. Finally we develop a framework for self service based RBAC called SSRBAC08 based on ASCAA principles. The SSRBAC08 is a modified version of RBAC96 model. The primary goal of SSRBAC08 as it pertains to our dissertation work is to show how automation, containment and accountability aspects can be achieved in user-role assignment.

Portable and precise, this pocket-sized guide delivers immediate answers for the day-to-day administration of Exchange Server 2010. Zero in on core support and maintenance tasks using quick-reference tables, instructions, and lists. You'll get the focused information you need to solve problems and get the job done—whether you're at your desk or in the field! Get fast facts to: Configure and manage Exchange clients Set up users, contacts, distribution lists, and address books Administer permissions, rules, policies, and security settings Manage databases and storage groups Optimize message processing, logging, and anti-spam filtering Administer at the command line using Exchange Management Shell Configure SMTP, connectors, links, and Edge subscriptions Manage mobile device features and client access Back up and restore systems

This book contains the Proceedings of the 21st IFIP TC-11 International Information Security Conference (IFIP/SEC 2006) on "Security and Privacy in Dynamic Environments". The papers presented here place a special emphasis on Privacy and Privacy Enhancing Technologies. Further topics addressed include security in mobile and ad hoc networks, access control for dynamic environments, new forms of attacks, security awareness, intrusion detection, and network forensics.

Access control is one of the fundamental services that any Data Management System should provide. Its main goal is to protect data from unauthorized read and write operations. This is particularly crucial in today's open and interconnected world, where each kind of information can be easily made available to a huge user population, and where a damage or misuse of data may have unpredictable consequences that go beyond the boundaries where data reside or have been generated. This book provides an overview of the various developments in access control for data management systems. Discretionary, mandatory, and role-based access control will be discussed, by surveying the most relevant proposals and analyzing the benefits and drawbacks of each paradigm in view of the requirements of different application domains. Access control mechanisms provided by commercial Data Management Systems are presented and discussed. Finally, the last part of the book is devoted to discussion of some of the most challenging and innovative research trends in the area of access control, such as those related to the Web 2.0 revolution or to the Database as a Service paradigm. This book is a valuable reference for an heterogeneous audience. It can be used as either an extended survey for people who are interested in access control or as a reference book for senior undergraduate or graduate courses in data security with a special focus on access control. It is also useful for technologists, researchers, managers, and developers who want to know more about access control and related emerging trends. Table of Contents: Access Control: Basic Concepts / Discretionary Access Control for Relational Data Management Systems / Discretionary Access Control for Advanced Data Models / Mandatory Access Control / Role-based Access Control / Emerging Trends in Access Control

This book constitutes the refereed proceedings of the 28th IFIP WG 11.3 International Working Conference on Data and Applications Security and Privacy, DBSec 2014, held in Vienna, Austria, in July 2014. The 22 revised full papers and 4 short papers presented were carefully reviewed and selected from 63 submissions. The papers are organized in topical sections on access control, privacy, networked and mobile environments, data access, cloud databases, and private retrieval.

Computer Security - ESORICS 2010

Information Systems Security

Access Control Management in Cloud Environments

Security and Privacy in Dynamic Environments

7th International Symposium, ESSoS 2015, Milan, Italy, March 4-6, 2015, Proceedings

Advances in Web-Age Information Management

International Conference, Fukuoka, Japan, March 23-26, 2010, Proceedings, Part IV

This four-volume set synthesizes the International Conference on Computational Science and Its Applications, ICCSA 2010. Topics include computational methods, algorithms and scientific application, high performance computing and networks, and more.

This book constitutes the proceedings of the 15th European Symposium on Computer Security held in Athens, Greece in September 2010. The 42 papers included in the book were carefully reviewed and selected from 201 papers. The articles are organized in topical sections on RFID and Privacy, Software Security, Cryptographic Protocols, Traffic Analysis, End-User Security, Formal Analysis, E-voting and Broadcast, Authentication, Access Control, Authorization and Attestation, Anonymity and Unlinkability, Network Security and Economics, as well as Secure Update, DOS and Intrustion Detection.

Solaris 10 System Administration Part II Exam CX-310-202 Bill Calkins In this book you ' ll learn Advanced Topics in Solaris 10 System Administration for SPARC and x86-based systems including: Administering the network environment in Solaris 10 Setting up RAID metadevices using SVM Configuring ZFS storage pools and file systems Configuring and administering Solaris zones and containers Administering virtual file systems and swap space Creating and administering user and Role-Based access accounts (RBAC) Using advanced installation tools to install, clone, and upgrade the operating system Bill ' s original Cert Prep guides were used throughout Sun ' s service organization as the SEs studied for Certification. This was not mandated by Sun management but happened through word-of-mouth by those software engineers who had successfully passed the exam. In this new edition, Bill adds a chapter for ZFS. It includes Live Upgrade conversion to a ZFS root filesystem and Zone/ZFS inter-operation. Plus, all chapters have been updated to reflect the Solaris 10 10/08 enhancements. This new guide remains the best source of preparation for the Solaris 10 Cert exam. –Brian Howard, Systems Engineer / Solaris Ambassador WRITTEN BY A LEADING SOLARIS EXPERT! Bill Calkins is owner and president of Pyramid Consulting, a computer training and consulting firm specializing in the implementation and administration of open systems. He works as a consultant with Sun Microsystems and has contributed extensively to the Solaris certification program and simulation technology. He also owns www.unixed.com, a website that provides online UNIX training materials. Bill has more than 20 years of experience in UNIX system administration, consulting, and training at more than 250 different companies and government agencies and has authored several books on Solaris. informit.com/examcram ISBN-13: 978-0-7897-3817-2 ISBN-10: 0-7897-3817-1

This book constitutes the refereed proceedings of the 5th International Conference on Web-Age Information Management, WAIM 2004, held in Dalian, China in July 2004. The 57 revised full papers and 23 revised short and industrial papers presented together with 3 invited contributions were carefully reviewed and selected from 291 submissions. The papers are organized in topical sections on data stream processing, time series data processing, security, mobile computing, cache management, query evaluation, Web search engines, XML, Web services, classification, and data mining.

The book compiles technologies for enhancing and provisioning security, privacy and trust in cloud systems based on Quality of Service requirements. It is a timely contribution to a field that is gaining considerable research interest, momentum, and provides a comprehensive coverage of technologies related to cloud security, privacy and trust. In particular, the book includes - Cloud security fundamentals and related technologies to-date, with a comprehensive coverage of evolution, current landscape, and future roadmap. - A smooth organization with introductory, advanced and specialist content, i.e. from basics of security, privacy and trust in cloud systems, to advanced cartographic techniques, case studies covering both social and technological aspects, and advanced platforms. - Case studies written by professionals and/or industrial researchers. - Inclusion of a section on Cloud security and eGovernance tutorial that can be used for knowledge transfer and teaching purpose. - Identification of open research issues to help practitioners and researchers. The book is a timely topic for readers, including practicing engineers and academics, in the domains related to the engineering, science, and art of building networks and networked applications. Specifically, upon reading this book, audiences will perceive the following benefits: 1. Learn the state-of-the-art in research and development on cloud security, privacy and trust. 2. Obtain a future roadmap by learning open research issues. 3. Gather the background knowledge to tackle key problems, whose solutions will enhance the evolution of next-generation secure cloud systems.

Computer Security - ESORICS 2000

19th International Conference, ISC 2016, Honolulu, HI, USA, September 3-6, 2016. Proceedings

9th International Conference, ICISS 2013, Kolkata, India, December 16-20, 2013. Proceedings

Attribute-Based Access Control

6th International Workshop, WISA 2005, Jeju Island, Korea, August 22-24, 2005, Revised Selected Papers

Data and Applications Security and Privacy XXVII

Struts 2 Black Book, 2Nd Ed (With Cd)

FreeBSD and OpenBSD are increasingly gaining traction in educational institutions, non-profits, and corporations worldwide because they provide significant security advantages over Linux. Although a lot can be said for the robustness, clean organization, and stability of the BSD operating systems, security is one of the main reasons system administrators use these two platforms. There are plenty of books to help you get a FreeBSD or OpenBSD system off the ground, and all of them touch on security to some extent, usually dedicating a chapter to the subject. But, as security is commonly named as the key concern for today's system administrators, a single chapter on the subject can't provide the depth of information you need to keep your systems secure. FreeBSD and OpenBSD are rife with security "building blocks" that you can put to use, and Mastering FreeBSD and OpenBSD Security shows you how. Both operating systems have kernel options and filesystem features that go well beyond traditional Unix permissions and controls. This power and flexibility is valuable, but the colossal range of possibilities need to be tackled one step at a time. This book walks you through the installation of a hardened operating system, the installation and configuration of critical services, and ongoing maintenance of your FreeBSD and OpenBSD systems. Using an application-specific approach that builds on your existing knowledge, the book provides sound technical information on FreeBSD and Open-BSD security with plenty of real-world examples to help you configure and deploy a secure system. By imparting a solid technical foundation as well as practical know-how, it enables administrators to push their server's security to the next level. Even administrators in other environments--like Linux and Solaris--can find useful paradigms to emulate. Written by security professionals with two decades of operating system experience, Mastering FreeBSD and OpenBSD Security features broad and deep explanations of how how to secure your most critical systems. Where other books on BSD systems help you achieve functionality, this book will help you more thoroughly secure your deployments.

This book constitutes the refereed proceedings of the 19th International Conference on Information Security, ISC 2016, held in Honolulu, HI, USA, in September 2016. The 19 revised full papers presented together with 7 short papers were carefully reviewed and selected from 76 submissions. The conference focuses on following subjects technical aspects of information security, cryptanalysis, cryptographic protocols, network and systems security and access control, privacy and watermarking, software security, encryption, signatures and fundamentals.

his book presents the refereed proceedings of the 6th European Symposium on Research in Computer Security, ESORICS 2000, held in Toulouse, France in October 2000. The 19 revised full papers presented were carefully reviewed and selected from a total of 75 submissions. The papers are organized in sections on personal devices and smart cards, electronic commerce protocols, access control, protocol verification, Internet security, security property analysis, and mobile agents.

This book constitutes the refereed proceedings of the Third VLDB 2006 International Workshop on Secure Data Management, SDM 2006, held in Seoul, Korea in September 2006 in conjunction with VLDB 2006. The book presents 13 revised full papers, organized in topical sections on privacy protection, privacy preserving data management, access control, and database security.

This book constitutes the refereed proceedings of the 6th International Workshop on Information Security Applications, WISA 2005, held in Jeju Island, Korea, in August 2005. The 29 revised full papers presented were carefully selected during two rounds of reviewing and improvement from 168 submissions. The papers are organized in topical sections on security analysis and attacks, systems security, network security, DRM/software security, efficient HW implementation, side-channel attacks, privacy/anonymity, and efficient implementation.

Data and Applications Security and Privacy XXVIII

4th International Conference, FDSE 2017, Ho Chi Minh City, Vietnam, November 29 – December 1, 2017, Proceedings

Future Data and Security Engineering

PowerShell for Office 365

Proceedings of the 2014 International Conference on Control Engineering and Information Systems (ICCEIS 2014, Yueyang, Hunan, China, 20-22 June 2014).

Role-based Access Control for Trust Management

7th International Conference, WAIM 2006, Hong Kong, China, June 17-19, 2006, Proceedings

This book constitutes the proceedings of the 26th International Conference on Computer Aided Verification, CAV 2014, held as part of the Vienna Summer of Logic, VSL 2014, in Vienna, Austria, in July 2014. The 46 regular papers and 11 short papers presented in this volume were carefully reviewed and selected from a total of 175 regular and 54 short paper submissions. The contributions are organized in topical sections named: software verification; automata; model checking and testing; biology and hybrid systems; games and synthesis; concurrency; SMT and theorem proving; bounds and termination; and abstraction.

This book constitutes the refereed proceedings of the Third International Conference on Future Data and Security Engineering, FDSE 2016, held in Can Tho City, Vietnam, in November 2016. The 28 revised full papers and 7 short papers presented were carefully reviewed and selected from 128 submissions. The accepted papers were grouped into the following sessions: Advances in query processing and optimization Big data analytics and applications Blockchains and emerging authentication techniques Data engineering tools in software development Data protection, data hiding, and access control Internet of Things and applications Security and privacy engineering Social network data analytics and recommendation systems

This book constitutes the thoroughly refereed post-conference proceedings of the 6th International Workshop on Security and Trust Management, STM 2010, held in Athens, Greece, in September 2010. The 17 revised full papers presented were carefully reviewed and selected from 40 submissions. Focusing on high-quality original unpublished research, case studies, and implementation experiences, STM 2010 encouraged submissions discussing the application and deployment of security technologies in practice.

With continuous growth in the number of information objects and the users that can access these objects, ensuring that access is compliant with company policies has become a big challenge. Role-based Access Control (RBAC) — a policy-neutral access control model that serves as a bridge between academia and industry — is probably the most suitable security model for commercial applications.Interestingly, role design determines RBAC's cost. When there are hundreds or thousands of users within an organization, with individual functions and responsibilities to be accurately reflected in terms of access permissions, only a well-defined role engineering process allows for significant savings of time and money while protecting data and systems.Among role engineering approaches, searching through access control systems to find de facto roles embedded in existing permissions is attracting increasing interest. The focus falls on role mining, which is applied data mining techniques to automate — to the extent possible — the role design task.This book explores existing role mining algorithms and offers insights into the automated role design approaches proposed in the literature. Alongside theory, this book acts as a practical guide for using role mining tools when implementing RBAC. Besides a comprehensive survey of role mining techniques deeply rooted in academic research, this book also provides a summary of the role-based approach, access control concepts and describes a typical role engineering process.Among the pioneering works on role mining, this book blends business elements with data mining theory, and thus further extends the applications of role mining into business practice. This makes it a useful guide for all academics, IT and business professionals.

missions in fact also treat an envisaged mutual impact among them. As for the 2002 edition in Irvine, the organizers wanted to stimulate this cross-pollination with a program of shared famous keynote speakers (this year we got Sycara, - ble, Soley and Mylopoulos!), and encouraged multiple attendance by providing authors with free access to another conference or workshop of their choice. We received an even larger number of submissions than last year for the three conferences (360 in total) and the workshops (170 in total). Not only can we therefore again claim a measurable success in attracting a representative volume of scienti?c papers, but such a harvest allowed the program committees of course to compose a high-quality cross-section of worldwide research in the areas covered. In spite of the increased number of submissions, the Program Chairs of the three main conferences decided to accept only approximately the same number of papers for presentation and publication as in 2002 (i. e. , around 1 paper out of every 4 – 5 submitted). For the workshops, the acceptance rate was about 1 in 2. Also for this reason, we decided to separate the proceedings into two volumes with their own titles, and we are grateful to Springer-Verlag for their collaboration in producing these two books. The reviewing process by the respective program committees was very professional and each paper in the main conferences was reviewed by at least three referees.

6th International Conference on Mathematical Methods, Models and Architectures for Com ü uter Network Security, MMM-ACNS 2012, St. Petersburg, Russia, October 17-19, 2012, Proceedings

6th International Workshop, STM 2010, Athens, Greece, September 23-24, 2010, Revised Selected Papers

Information Security

Control Engineering and Information Systems

Mastering System Center Configuration Manager

CISSP: Certified Information Systems Security Professional Study Guide

Business Performance Through Connected Intelligence

Contains the proceedings of the 7th International Conference on Web-Age Information Management, WAIM 2006. The papers are organized in topical sections on, indexing, XML query processing, information retrieval, sensor networks and grid computing, peer-to-peer systems, Web services, Web searching, caching and moving objects, clustering, and more. This book constitutes the refereed proceedings of the 7th International Conference on Web-Age Information Management, WAIM 2006, held in Hong Kong, China in June 2006. The 50 revised full papers presented were carefully reviewed and selected from 290 submissions. The papers are organized in topical sections on, indexing, XML query processing, information retrieval, sensor networks and grid computing, peer-to-peer systems, Web services, Web searching, caching and moving objects, temporal database, clustering, clustering and classification, data mining, data stream processing, XML and semistructured data, data distribution and query processing, and advanced applications

6th European Symposium on Research in Computer Security Toulouse, France, October 4-6, 2000 Proceedings

Security and Trust Management

Role-based Access Control

8th International Conference, SKM 2019, Goa, India, December 21 – 22, 2019, Proceedings

Identity and Access Management

Architectures and Models for Administration of User-role Assignment in Role Based Access Control

Computer Network Security