OMB No. 1565364972741

Access Control Authentication And Public Key Infrastructure Information Systems Security Assurance

What is Two-Factor Authentication For Access Control Access and Authentication Intro to Access Control: Prox \u0026 Smart Cards Logical Access Controls: Authentication \u0026 Authorization. Information Systems and Controls. CPA Exam Access Control, Authentication and Authorization Benefits of Access Control Authorization and Access Control - CompTIA Security+ SY0-401: 5.2 Authentication and Access Control 101: How to Protect Your Data and Identity What is Access Control? Fundamentals of Access Control : The Only Access Control Guide You'll Ever Need Role Based Access Control Access Controls - CompTIA Security+ SY0-701 - 4.6 Explain Access Control Types| Administrative, Logical, Physical| Preventive, Detective, Compensating Cybersecurity Expert Demonstrates How Hackers Easily Gain Access To Sensitive Information Rethinking Access Control and Authentication for the Home IoT Authentication Based Access Control Issues Asymmetric Encryption - Simply explained Lecture 3 Unit A – Access Control and Authentication NIST CSF PR AC Lesson 7 Access Control

Getting Started with RACF
Encyclopedia of Cryptography and Security
NiSTIR 7316
The InfoSec Handbook
IFIP WG 11.4 International Workshop, INetSec 2010, Sofia, Bulgaria, March 5-6, 2010, Revised Selected Papers
An Enterprise Perspective on Risks and Compliance
Attribute-Based Access Control
Role-based Access Control
Making Passwords Secure
A Guide to Claims-Based Identity and Access Control
Access Control, Security, and Trust
Laboratory Manual to Accompany Access Control, Authentication, and Public Key Infrastructure
Guide to Computer Network Security
Zero Trust Networks
Practical Cryptography Methods and Tools
Access Control, Authentication, and Public Key Infrastructure
Access Control, Authentication, and Public Key Infrastructure + Virtual Lab Access

Access Control Authentication And Public Key Infrastructure Information Systems Security Assurance ***OMB No. 1565364972741 edited by***

RIVERA GOOD

Getting Started with RACF Elsevier
Leverage Your Security Expertise in IBM® System z™ Mainframe Environments For over 40 years, the IBM mainframe has been the backbone of the world’s largest enterprises. If you’re coming to the IBM System z mainframe platform from UNIX ® , Linux ® , or Windows ® , you need practical guidance on leveraging its unique security capabilities. Now, IBM experts have written the first authoritative book on mainframe security specifically designed to build on your experience in other environments. Even if you’ve never logged onto a mainframe before, this book will teach you how to run today’s z/OS ® operating system command line and ISPF toolset and use them to efficiently perform every significant security administration task. Don’t have a mainframe available for practice? The book contains step-by-step videos walking you through dozens of key techniques. Simply log in and register your book at www.ibmpressbooks.com/register to gain access to these videos. The authors illuminate the mainframe’s security model and call special attention to z/OS security techniques that differ from UNIX, Linux, and Windows. They thoroughly introduce IBM’s powerful Resource Access Control Facility (RACF) security subsystem and demonstrate how mainframe security integrates into your enterprise-wide IT security infrastructure. If you’re an experienced system administrator or security professional, there’s no faster way to extend your expertise into “big iron” environments. Coverage includes Mainframe basics: logging on, allocating and editing data sets, running JCL jobs, using UNIX System Services, and accessing documentation Creating, modifying, and deleting users and groups Protecting data sets, UNIX file system files, databases, transactions, and other resources Manipulating profiles and managing permissions Configuring the mainframe to log security events, filter them appropriately, and create usable reports Using auditing tools to capture static configuration data and dynamic events, identify weaknesses, and remedy them Creating limited-authority administrators: how, when, and why

Encyclopedia of Cryptography and Security Springer Science & Business Media
Your expert guide to information security As businesses and consumers become more dependent on complexmultinational information systems, the need to understand anddevise sound information security systems has never been greater.This title takes a practical approach to information security byfocusing on real-world examples. While not sidestepping the theory,the emphasis is on developing the skills and knowledge thatsecurity and information technology students and professionals needto face their challenges. The book is organized around four majorthemes: * Cryptography: classic cryptosystems, symmetric key cryptography,public key cryptography, hash functions, random numbers,information hiding, and cryptanalysis * Access control: authentication and authorization, password-basedsecurity, ACLs and capabilities, multilevel and multilateralsecurity, covert channels and inference control, BLP and Biba'smodels, firewalls, and intrusion detection systems * Protocols: simple authentication protocols, session keys, perfectforward secrecy, timestamps, SSL, IPSec, Kerberos, and GSM * Software: flaws and malware, buffer overflows, viruses and worms,software reverse engineering, digital rights management, securesoftware development, and operating systems security Additional features include numerous figures and tables toillustrate and clarify complex topics, as well as problems-rangingfrom basic to challenging-to help readers apply their newlydeveloped skills. A solutions manual and a set of classroom-testedPowerPoint(r) slides will assist instructors in their coursedevelopment. Students and professors in information technology,computer science, and engineering, and professionals working in thefield will find this reference most useful to solve theirinformation security issues. An Instructor's Manual presenting detailed solutions to all theproblems in the book is available from the Wiley editorialdepartment. An Instructor Support FTP site is also available.

NiSTIR 7316 Springer Nature
The authors explain role based access control (RBAC), its administrative and cost advantages, implementation issues and imigration from conventional access control methods to RBAC.

The InfoSec Handbook Artech House
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.

IFIP WG 11.4 International Workshop, INetSec 2010, Sofia, Bulgaria, March 5-6, 2010, Revised Selected Papers Createspace Independent Publishing Platform
Provides research on security issues in various wireless communications, recent advances in wireless security, the wireless security model, and future directions in wireless security.

An Enterprise Perspective on Risks and Compliance Springer Science & Business Media
PART OF THE JONES & BARTLETT LEARNING INFORMATION SYSTEMS SECURITY & ASSURANCE SERIESSeries meets all standards put forth by CNSS 4011 & 4013A!Access control protects resources against unauthorized viewing, tampering, or destruction. They serve as a primary means of ensuring privacy, confidentiality, and prevention of unauthorized disclosure. Revised and updated with the latest data from this fast paced field, Access Control, Authentication, and Public Key Infrastructure defines the components of access control, provides a business framework for implementation, and discusses legal requirements that impact access control programs. It looks at the risks, threats, and vulnerabilities prevalent in information systems and IT infrastructures and how to handle them. It provides a student and professional resource that details how to put access control systems to work as well as testing and managing them. New to the Second Edition: Updated references to Windows 8 and Outlook 2011 A new discussion of recent Chinese hacking incidence Examples depicting the risks associated with a missing unencrypted laptop containing private data. New sections on the Communications Assistance for Law Enforcement Act (CALEA) and granting Windows folder permissions are added. New information on the Identity Theft Enforcement and Restitution Act and the Digital Millennium Copyright Act (DMCA).

Attribute-Based Access Control Access Control, Authentication, and Public Key Infrastructure
This book constitutes the refereed post-proceedings of the Joint International Conference on Pervasive Computing and the Networked World, ICPCA-SWS 2012, held in Istanbul, Turkey, in November 2012. This conference is a merger of the 7th International Conference on Pervasive Computing and Applications (ICPCA) and the 4th Symposium on Web Society (SWS). The 53 revised full papers and 26 short papers presented were carefully reviewed and selected from 143 submissions. The papers cover a wide range of topics from different research communities such as computer science, sociology and psychology and explore both theoretical and practical issues in and around the emerging computing paradigms, e.g., pervasive collaboration, collaborative business, and networked societies. They highlight the unique characteristics of the "everywhere" computing paradigm and promote the awareness of its potential social and psychological consequences.

Role-based Access Control Addison-Wesley Professional
PART OF THE NEW JONES & BARTLETT LEARNING INFORMATION SYSTEMS SECURITY & ASSURANCE SERIES! Access control protects resources against unauthorized viewing, tampering, or destruction. They serve as a primary means of ensuring privacy, confidentiality, and prevention of unauthorized disclosure. The first part of Access Control, Authentication, and Public Key Infrastructure defines the components of access control, provides a business framework for implementation, and discusses legal requirements that impact access contol programs. It then looks at the risks, threats, and vulnerabilities prevalent in information systems and IT infrastructures and how to handle them. The final part is a resource for students and professionals which disucsses putting access control systems to work as well as testing and managing them.

Making Passwords Secure

Jones & Bartlett Publishers
PART OF THE JONES & BARTLETT LEARNING INFORMATION SYSTEMS SECURITY & ASSURANCE SERIES Revised and updated with the latest information from this fast-paced field, Fundamentals of Information System Security, Second Edition provides a comprehensive overview of the essential concepts readers must know as they pursue careers in information systems security. The text opens with a discussion of the new risks, threats, and vulnerabilities associated with the transformation to a digital world, including a look at how business, government, and individuals operate today. Part 2 is adapted from the Official (ISC)2 SSCP Certified Body of Knowledge and presents a high-level overview of each of the seven domains within the System Security Certified Practitioner certification. The book closes with a resource for readers who desire additional material on information security standards, education, professional certifications, and compliance laws. With its practical, conversational writing style and step-by-step examples, this text is a must-have resource for those entering the world of information systems security. New to the Second Edition: - New material on cloud computing, risk analysis, IP mobility, OMNIBus,

and Agile Software Development. - Includes the most recent updates in Information Systems Security laws, certificates, standards, amendments, and the proposed Federal Information Security Amendments Act of 2013 and HITECH Act. - Provides new cases and examples pulled from real-world scenarios. - Updated data, tables, and sidebars provide the most current information in the field.

A Guide to Claims-Based Identity and Access Control Jones & Bartlett Learning

This book constitutes the refereed proceedings of the 13th International Conference on Provable Security, ProvSec 2019, held in Cairns, QLD, Australia, in October 2019. The 18 full and 6 short papers presented were carefully reviewed and selected from 51 submissions. The papers focus on provable security as an essential tool for analyzing security of modern cryptographic primitives, including a special theme on “Practical Security.”

Access Control, Security, and Trust

Pearson Education

An up-to-date guide to an overview of authentication in the Internet of Things (IoT) The Internet of things (IoT) is the network of the countless physical devices that have the possibility to connect and exchange data. Among the various security requirements, authentication to the IoT is the first step to prevent the impact of attackers. IoT Security offers an important guide into the development of the many authentication mechanisms that provide IoT authentication at various levels such as user level, device level and network level. The book covers a wide range of topics including an overview of IoT and addresses in detail the security challenges at every layer by considering both the technologies and the architecture used. The authors—noted experts on the topic—provide solutions for remediation of compromised security, as well as methods for risk mitigation, and offer suggestions for prevention and improvement. In addition, IoT Security offers a variety of illustrative use cases. This important book: Offers an authoritative reference designed for use by all IoT stakeholders Includes information for securing devices at the user, device, and network levels Contains a classification of existing vulnerabilities Written by an international group of experts on the topic Provides a guide to the most current information available on IoT security Written for network operators, cloud operators, IoT device manufacturers, IoT device users, wireless users, IoT standardization organizations, and security solution developers, IoT Security is an essential guide that contains information on security features, including underlying networks, architectures, and security requirements.

Laboratory Manual to Accompany Access Control, Authentication, and Public Key Infrastructure "O'Reilly Media, Inc."

This volume features the refereed proceedings from the 4th European Public Key Infrastructure Workshop: Theory and Practice, held in Palma de Mallorca, Spain in June 2007. Twenty-one full papers and eight short papers, contributed by experts in the field, are included. The papers address all current issues in public key infrastructure, ranging from theoretical and foundational topics to applications and regulatory issues.

Guide to Computer Network Security Apress

Take advantage of JavaScript’s power to build robust web-scale or enterprise applications that are easy to extend and maintain. By applying the design patterns outlined in this practical book, experienced JavaScript developers will learn how to write flexible and resilient code that’s easier—yes, easier—to work with as your code base grows. JavaScript may be the most essential web programming language, but in the real world, JavaScript applications often break when you make changes. With this book, author Eric Elliott shows you how to add client- and server-side features to a large JavaScript application without negatively affecting the rest of your code. Examine the anatomy of a large-scale JavaScript application Build modern web apps with the capabilities of desktop applications Learn best practices for code organization, modularity, and reuse Separate your application into different layers of responsibility Build efficient, self-describing hypermedia APIs with Node.js Test, integrate, and deploy software updates in rapid cycles Control resource access with user authentication and authorization Expand your application’s reach through internationalization

Zero Trust Networks CRC Press

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.

Practical Cryptography Methods and Tools National Academies Press

With their rapidly changing architecture and API-driven automation, cloud platforms come with unique security challenges and opportunities. This hands-on book guides you through security best practices for multivendor cloud environments, whether your company plans to move legacy on-premises projects to the cloud or build a new infrastructure from the ground up. Developers, IT architects, and security professionals will learn cloud-specific techniques for securing popular cloud platforms such as Amazon Web Services, Microsoft Azure, and IBM Cloud. Chris Dotson—an IBM senior technical staff member—shows you how to establish data asset management, identity and access management, vulnerability management, network security, and incident response in your cloud environment.

Access Control, Authentication, and Public Key Infrastructure Springer Nature

You may regard cloud computing as an ideal way for your company to control IT costs, but do you know how private and secure this service really is? Not many people do. With Cloud Security and Privacy, you'll learn what's at stake when you trust your data to the cloud, and what you can do to keep your virtual infrastructure and web applications secure. Ideal for IT staffers, information security and privacy practitioners, business managers, service providers, and investors alike, this book offers you sound advice from three well-known authorities in the tech security world. You'll learn detailed information on cloud computing security that-until now-has been sorely lacking. Review the current state of data security and storage in the cloud, including confidentiality, integrity, and availability Learn about the identity and access management (IAM) practice for authentication, authorization, and auditing of the users accessing cloud services Discover which security management frameworks and standards are relevant for the cloud Understand the privacy aspects you need to consider in the cloud, including how they compare with traditional computing models Learn the importance of audit and compliance functions within the cloud, and the various standards and frameworks to consider Examine security delivered as a service-a different facet of cloud security

Access Control, Authentication, and Public Key Infrastructure + Virtual Lab Access Jones & Bartlett Publishers

As systems have become interconnected and more complicated, programmers needed ways to identify parties across multiple computers. One way to do this was for the parties that used applications on one computer to authenticate to the applications (and/or operating systems) that ran on the other computers. This mechanism is still widely used-for example, when logging on to a great number of Web sites. However, this approach becomes unmanageable when you have many co-operating systems (as is the case, for example, in the enterprise). Therefore, specialized services were invented that would register and authenticate users, and subsequently provide claims about them to interested applications. Some well-known examples are NTLM, Kerberos, Public Key Infrastructure (PKI), and the Security Assertion Markup Language (SAML). Most enterprise applications need some basic user security features. At a minimum, they need to authenticate their users, and many also need to authorize access to certain features so that only privileged users can get to them. Some apps must go further and audit what the user does. On Windows®, these features are built into the operating system and are usually quite easy to integrate into an application. By taking advantage of Windows integrated authentication, you don't have to invent your own authentication protocol or manage a user database. By using access control lists (ACLs), impersonation, and features such as groups, you can implement authorization with very little code. Indeed, this advice applies no matter which OS you are using. It's almost always a better idea to integrate closely with the security features in your OS rather than reinventing those features yourself. But what happens when you want to extend reach to users who don't happen to have Windows accounts? What about users who aren't running Windows at all? More and more applications need this type of reach, which seems to fly in the face of traditional advice. This book gives you enough information to evaluate claims-based identity as a possible option when you're planning a new application or making changes to an existing one. It is intended for any architect, developer, or information technology (IT) professional who designs, builds, or operates Web applications and services that require identity information about their users.

Advances in Authentication Apress

User identification and authentication are essential parts of information security. Users must authenticate as they access their computer systems at work or at home every day. Yet do users understand how and why they are actually being authenticated, the security level of the authentication mechanism that they are using, and the potential impacts o

For the Record John Wiley & Sons

Adequate security of information and information systems is a fundamental management responsibility. Nearly all applications that deal with financial, privacy, safety, or defense include some form of access control. Access control is concerned with determining the allowed activities of legitimate users, mediating every attempt by a user to access a resource in the system. In some systems, complete access is granted after successful authentication of the user, but most systems require more sophisticated and complex control. In addition to the authentication mechanism (such as a password), access control is concerned with how authorizations are structured. Why buy a book you can download for free? We print this book so you don't have to. First you gotta find a good clean (legible) copy and make sure it's the latest version (not always easy). Some documents found on the web are missing some pages or the image quality is so poor, they are difficult to read. We look over each document carefully and replace poor quality images by going back to the original source document. We proof each document to make sure it's all there - including all changes. If you find a good copy, you could print it using a network printer you share with 100 other people (typically its either out of paper or toner). If it's just a 10-page document, no problem, but if it's 250-pages, you will need to punch 3 holes in all those pages and put it in a 3-ring binder. Takes at least an hour. It's much more cost-effective to just order the latest version from Amazon.com This book is published by 4th Watch Books and includes copyright material. We publish compact, tightly-bound, full-size books (8 1⁄2 by 11 inches), with large text and glossy covers. 4th Watch Books is a Service Disabled Veteran-Owned Small Business (SDVOSB). If you like the service we provide, please leave positive review on Amazon.com. Without positive feedback from the community, we may discontinue the service and y'all can go back to printing these books manually yourselves. For more titles published by 4th Watch Publishing Co., please visit: www.usgovpub.com

Mechanics of User Identification and Authentication Springer

The InfoSec Handbook offers the reader an organized layout of information that is easily read and understood. Allowing beginners to enter the field and understand the key concepts and ideas, while still keeping the experienced readers updated on topics and concepts. It is intended mainly for beginners to the field of information security, written in a way that makes it easy for them to understand the detailed content of the book. The book offers a practical and simple view of the security practices while still offering somewhat technical and detailed information relating to security. It helps the reader build a strong foundation of information, allowing them to move forward from the book with a larger knowledge base. Security is a constantly growing concern that everyone must deal with. Whether it’s an average computer user or a highly skilled computer user, they are always confronted with different security risks. These risks range in danger and should always be dealt with accordingly. Unfortunately, not everyone is aware of the dangers or how to prevent them and this is where most of the issues arise in information technology (IT). When computer users do not take security into account many issues can arise from that like system compromises or loss of data and information. This is an obvious issue that is present with all computer users. This book is intended to educate the average and experienced user of what kinds of different security practices and standards exist. It will also cover how to manage security software and updates in order to be as protected as possible from all of the threats that they face.