Identity And Access Management For Dummies

Leverage existing free open source software to build an identity and access management (IAM) platform that can serve your organization for the long term. With the emergence of open standards and open source software, it's now easier than ever to build and operate your own IAM stack. The most common culprit of the largest hacks has been bad personal identification. In terms of bang for your buck, effective access control is the best investment you can make. Financially, it's more valuable to prevent than to detect a security breach. That's why Identity and Access Management (IAM) is a critical component of an organization's security infrastructure. In the past, IAM software has been available only from large enterprise software vendors. Commercial IAM offerings are bundled as "suites" because IAM is not just one component. It's a number of components working together, including web, authentication, authorization, cryptographic, and persistence services. Securing the Perimeter documents a recipe to take advantage of open standards to build an enterprise-class IAM service using free open source software. This recipe can be adapted to meet the needs of both small and large organizations. While not a comprehensive guide for every application, this book provides the key concepts and patterns to help administrators and developers leverage a central security infrastructure. Cloud IAM service providers would have you believe that managing an IAM is too

hard. Anything unfamiliar is hard, but with the right road map, it can be mastered. You may find SaaS identity solutions too rigid or too expensive. Or perhaps you don't like the idea of a third party holding the credentials of your users—the keys to your kingdom. Open source IAM provides an alternative. Take control of your IAM infrastructure if digital services are key to your organization's success. What You'll Learn Understand why you should deploy a centralized authentication and policy management infrastructure Use the SAML or Open ID Standards for web or single sign-on, and OAuth for API Access Management Synchronize data from existing identity repositories such as Active Directory Deploy two-factor authentication services Who This Book Is For Security architects (CISO, CSO), system engineers/administrators, and software developers

"This book explores important and emerging advancements in digital identity and access management systems, providing innovative answers to an assortment of problems as system managers are faced with major organizational, economic and market changes"--Provided by publisher.

This book contains selected papers presented at the 12th IFIP WG 9.2, 9.5, 9.6/11.7, 11.6/SIG 9.2.2 International Summer School on Privacy and Identity Management, held in Ispra, Italy, in September 2017. The 12 revised full papers, 5 invited papers and 4 workshop papers included in this volume were carefully selected from a total of 48 submissions and were subject to a three-phase review process. The papers combine interdisciplinary approaches to bring together a host of

perspectives: technical, legal, regulatory, socio-economic, social, societal, political, ethical, anthropological, philosophical, and psychological. They are organized in the following topical sections: privacy engineering; privacy in the era of the smart revolution; improving privacy and security in the era of smart environments; safeguarding personal data and mitigating risks; assistive robots; and mobility and privacy.

This essential resource for professionals and advanced students in security programming and system design introduces the foundations of programming systems security and the theory behind access control models, and addresses emerging access control mechanisms.

Description: Consumer identity and access management (CIAM) is a critical component of any modern organisation's digital transformation initiative. If you used the Internet yesterday, you would very likely have interacted with a website that had customer identity and access management at its foundation. Making an online purchase, checking your bank balance, getting a quote for car insurance, logging into a social media site or submitting and paying your income tax return. All of those interactions require high scale, secure identity and access management services. But how are those systems designed? Synopsis: Modern organisations need to not only meet end user privacy, security and usability requirements, but also provide business enablement opportunities that are agile and can respond to market changes rapidly. The modern enterprise architect and CISO is no longer just focused upon internal employee security - they now need to address

the growing need for digital enablement across consumers and citizens too. CIAM Design Fundamentals, is CISO and architect view on designing the fundamental building blocks of a scaleable, secure and usable consumer identity and access management (CIAM) system. Covering: business objectives, drivers, requirements, CIAM life-cycle, implementer toolkit of standards, design principles and vendor selection guidance. Reviews: "Consumer identity is at the very core of many a successful digital transformation project. Simon blends first hand experience, research and analysis, to create a superbly accessible guide to designing such platforms - "Scott Forrester CISSP, Principal Consultant, UK. "This is the book that needs to be on every Identity Architect's Kindle. Simon does a great job of laying the foundation and history of Consumer Identity and Access Management and then gives you the roadmap that you need as an architect to deliver success on a project" - Brad Tumy, Founder & Principal Architect, Tumy Technology, Inc, USA. "Leveraging his strong security and industry background, Simon has created a must-have book for any Identity and Access Management professional looking to implement a CIAM solution. I strongly recommend the Consumer Identity & Access Management Design Fundamentals book!" - Robert Skoczylas, Chief Executive Officer, Indigo Consulting Canada Inc. About the Author: Simon Moffatt is a recognised expert in the field of digital identity and access management, having spent nearly 20 years working in the sector, with experience gained in consultancies, startups, global

vendors and within industry. He has contributed to identity and security standards for the likes of the National Institute of Standards and Technology and the Internet Engineering Task Force. Simon is perhaps best well known as a public speaker and industry commentator via his site The Cyber Hut.He is a CISSP, CCSP, CEH and CISA and has a collection of vendor related qualifications from the likes Microsoft, Novell and Cisco. He is an accepted full member of the Chartered Institute of Information Security (M.CIIS), a long time member of the British Computer Society and a senior member of the Information Systems Security Association. He is also a postgraduate student at Royal Holloway University, studying for a Masters of Science in Information Security.Since 2013, he has worked at ForgeRock, a leading digital identity software platform provider, where he is currently Global Technical Product Management Director.

Due to the proliferation of distributed mobile technologies and heavy usage of social media, identity and access management has become a very challenging area. Businesses are facing new demands in implementing solutions, however, there is a lack of information and direction. Contemporary Identity and Access Management Architectures: Emerging Research and Opportunities is a critical scholarly resource that explores management of an organization’s identities, credentials, and attributes which assures the identity of a user in an extensible manner set for identity and access administration. Featuring coverage on a broad range of topics, such as biometric application programming

interfaces, telecommunication security, and role-based access control, this book is geared towards academicians, practitioners, and researchers seeking current research on identity and access management. Learn to leverage the advanced capabilities of Keycloak, an open-source identity and access management solution, to enable authentication and authorization in applications Key Features Get up to speed with Keycloak, OAuth 2.0, and OpenID Connect using practical examples Configure, manage, and extend Keycloak for optimized security Leverage Keycloak features to secure different application types Book Description Implementing authentication and authorization for applications can be a daunting experience, often leaving them exposed to security vulnerabilities. Keycloak is an open-source solution for identity management and access management for modern applications. Keycloak - Identity and Access Management for Modern Applications is a comprehensive introduction to Keycloak, helping you get started with using it and securing your applications. Complete with hands-on tutorials, best practices, and self-assessment questions, this easy-to-follow guide will show you how to secure a sample application and then move on to securing different application types. As you progress, you will understand how to configure and manage Keycloak as well as how to leverage some of its more advanced capabilities. Finally, you'll gain insights into securely using Keycloak in production. By the end of this book, you will have learned how to install and manage Keycloak as well as how to secure new and

existing applications. What you will learn Understand how to install, configure, and manage Keycloak Secure your new and existing applications with Keycloak Gain a basic understanding of OAuth 2.0 and OpenID Connect Understand how to configure Keycloak to make it ready for production use Discover how to leverage additional features and how to customize Keycloak to fit your needs Get to grips with securing Keycloak servers and protecting applications Who this book is for Developers, sysadmins, security engineers, or anyone who wants to leverage Keycloak and its capabilities for application security will find this book useful. Beginner-level knowledge of app development and authentication and authorization is expected.

Start empowering users and protecting corporate data, while managing identities and access with Microsoft Azure in different environments Key Features Understand how to identify and manage business drivers during transitions Explore Microsoft Identity and Access Management as a Service (IDaaS) solution Over 40 playbooks to support your learning process with practical guidelines Book Description Microsoft Azure and its Identity and access management are at the heart of Microsoft's software as service products, including Office 365, Dynamics CRM, and Enterprise Mobility Management. It is crucial to master Microsoft Azure in order to be able to work with the Microsoft Cloud effectively. You'll begin by identifying the benefits of Microsoft Azure in the field of identity and access management. Working through the functionality of identity and access management as a service, you will

get a full overview of the Microsoft strategy. Understanding identity synchronization will help you to provide a well-managed identity. Project scenarios and examples will enable you to understand, troubleshoot, and develop on essential authentication protocols and publishing scenarios. Finally, you will acquire a thorough understanding of Microsoft Information protection technologies. What you will learn Apply technical descriptions to your business needs and deployments Manage cloud-only, simple, and complex hybrid environments Apply correct and efficient monitoring and identity protection strategies Design and deploy custom Identity and access management solutions Build a complete identity and access management life cycle Understand authentication and application publishing mechanisms Use and understand the most crucial identity synchronization scenarios Implement a suitable information protection strategy Who this book is for This book is a perfect companion for developers, cyber security specialists, system and security engineers, IT consultants/architects, and system administrators who are looking for perfectly up–to-date hybrid and cloud-only scenarios. You should have some understanding of security solutions, Active Directory, access privileges/rights, and authentication methods. Programming knowledge is not required but can be helpful for using PowerShell or working with APIs to customize your solutions.

Summary OAuth 2 in Action teaches you the practical use and deployment of this HTTP-based protocol from the perspectives of a client, authorization server, and resource

server. You'll learn how to confidently and securely build and deploy OAuth on both the client and server sides. Foreword by Ian Glazer. Purchase of the print book includes a free eBook in PDF, Kindle, and ePub formats from Manning Publications. About the Technology Think of OAuth 2 as the web version of a valet key. It is an HTTP-based security protocol that allows users of a service to enable applications to use that service on their behalf without handing over full control. And OAuth is used everywhere, from Facebook and Google, to startups and cloud services. About the Book OAuth 2 in Action teaches you practical use and deployment of OAuth 2 from the perspectives of a client, an authorization server, and a resource server. You'll begin with an overview of OAuth and its components and interactions. Next, you'll get hands-on and build an OAuth client, an authorization server, and a protected resource. Then you'll dig into tokens, dynamic client registration, and more advanced topics. By the end, you'll be able to confidently and securely build and deploy OAuth on both the client and server sides. What's Inside Covers OAuth 2 protocol and design Authorization with OAuth 2 OpenID Connect and User-Managed Access Implementation risks JOSE, introspection, revocation, and registration Protecting and accessing REST APIs About the Reader Readers need basic programming skills and knowledge of HTTP and JSON. About the Author Justin Richer is a systems architect and software engineer. Antonio Sanso is a security software engineer and a security researcher. Both authors contribute to open standards and open source. Table of Contents Part 1 - First steps What is OAuth 2.0 and why should you care? The OAuth dance Part 2 - Building an OAuth 2 environment Building a simple OAuth client Building a simple OAuth protected resource Building a simple OAuth authorization server OAuth 2.0 in the real world Part 3 - OAuth 2 implementation and vulnerabilities Common

client vulnerabilities Common protected resources vulnerabilities Common authorization server vulnerabilities Common OAuth token vulnerabilities Part 4 - Taking OAuth further OAuth tokens Dynamic client registration User authentication with OAuth 2.0 Protocols and profiles using OAuth 2.0 Beyond bearer tokens Summary and conclusions
Digital identity can be defined as the digital representation of the information known about a specific individual or organization. Digital identity management technology is an essential function in customizing and enhancing the network user experience, protecting privacy, underpinning accountability in transactions and interactions, and complying with regulatory controls. This practical resource offers you a in-depth understanding of how to design, deploy and assess identity management solutions. It provides a comprehensive overview of current trends and future directions in identity management, including best practices, the standardization landscape, and the latest research finding. Additionally, you get a clear explanation of fundamental notions and techniques that cover the entire identity lifecycle.
See how privileges, insecure passwords, administrative rights, and remote access can be combined as an attack vector to breach any organization. Cyber attacks continue to increase in volume and sophistication. It is not a matter of if, but when, your organization will be breached. Threat actors target the path of least resistance: users and their privileges. In decades past, an entire enterprise might be sufficiently managed through just a handful of credentials. Today's environmental complexity has seen an explosion of privileged credentials for many different account types such as domain and local administrators, operating systems (Windows, Unix, Linux, macOS, etc.), directory services, databases, applications, cloud instances, networking hardware, Internet of Things (IoT), social media, and so many more. When

unmanaged, these privileged credentials pose a significant threat from external hackers and insider threats. We are experiencing an expanding universe of privileged accounts almost everywhere. There is no one solution or strategy to provide the protection you need against all vectors and stages of an attack. And while some new and innovative products will help protect against or detect against a privilege attack, they are not guaranteed to stop 100% of malicious activity. The volume and frequency of privilege-based attacks continues to increase and test the limits of existing security controls and solution implementations. Privileged Attack Vectors details the risks associated with poor privilege management, the techniques that threat actors leverage, and the defensive measures that organizations should adopt to protect against an incident, protect against lateral movement, and improve the ability to detect malicious activity due to the inappropriate usage of privileged credentials. This revised and expanded second edition covers new attack vectors, has updated definitions for privileged access management (PAM), new strategies for defense, tested empirical steps for a successful implementation, and includes new disciplines for least privilege endpoint management and privileged remote access. What You Will Learn Know how identities, accounts, credentials, passwords, and exploits can be leveraged to escalate privileges during an attack Implement defensive and monitoring strategies to mitigate privilege threats and risk Understand a 10-step universal privilege management implementation plan to guide you through a successful privilege access management journey Develop a comprehensive model for documenting risk, compliance, and reporting based on privilege session activity Who This Book Is For Security management professionals, new security professionals, and auditors looking to understand and solve privilege access management problems

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).

Understand the IAM toolsets, capabilities, and paradigms of the AWS platform and learn how to apply practical identity use cases to AWS at the administrative and application level Key Features Learn administrative lifecycle management and authorization Extend workforce identity to AWS for applications deployed to Amazon Web Services (AWS) Understand how to use native AWS IAM capabilities with apps deployed to AWS Book Description AWS identity management offers a powerful yet complex array of native

capabilities and connections to existing enterprise identity systems for administrative and application identity use cases. This book breaks down the complexities involved by adopting a use-case-driven approach that helps identity and cloud engineers understand how to use the right mix of native AWS capabilities and external IAM components to achieve the business and security outcomes they want. You will begin by learning about the IAM toolsets and paradigms within AWS. This will allow you to determine how to best leverage them for administrative control, extending workforce identities to the cloud, and using IAM toolsets and paradigms on an app deployed on AWS. Next, the book demonstrates how to extend your on-premise administrative IAM capabilities to the AWS backplane, as well as how to make your workforce identities available for AWS-deployed applications. In the concluding chapters, you'll learn how to use the native identity services with applications deployed on AWS. By the end of this IAM Amazon Web Services book, you will be able to build enterprise-class solutions for administrative and application identity using AWS IAM tools and external identity systems. What you will learn Understand AWS IAM concepts, terminology, and services Explore AWS IAM, Amazon Cognito, AWS SSO, and AWS Directory Service to solve customer and workforce identity problems Apply the concepts you learn about to solve business, process, and compliance challenges when expanding into AWS Navigate the AWS CLI to unlock the programmatic administration of AWS Explore how AWS IAM, its policy objects, and notational language can be applied to solve security and access management use cases Relate concepts easily to your own environment through IAM patterns and best practices Who this book is for Identity engineers and administrators, cloud administrators, security architects, or anyone who wants to explore and manage IAM solutions in AWS will find this book useful. Basic

knowledge of AWS cloud infrastructure and services is required to understand the concepts covered in the book more effectively.

Information Security in Healthcare is an essential guide for implementing a comprehensive information security management program in the modern healthcare environment. Combining the experience and insights of top healthcare IT managers and information security professionals, this book offers detailed coverage of myriad

Develop and Implement an End-to-End IAM Solution Maintain a high-performance, fully integrated security foundation across your enterprise using the detailed information in this Oracle Press guide. Designing an IAM Framework with Oracle Identity and Access Management Suite explains how to reduce risk exposure by effectively managing your full spectrum of users. Learn how to create and provision accounts, employ strong authentication and authorization, integrate legacy applications, and handle regulatory compliance. The latest performance-testing, self-auditing, and business intelligence reporting techniques are also covered in this comprehensive resource. Establish company requirements and develop implementation plans Build and execute your identity business case Set up accounts, roles, and provisioning workflows using Oracle Identity Manager and Analysis Authenticate and authorize users with Oracle Access Manager Enact strong authorization policies using Oracle Entitlements Server Identify anomalous behavior and create proactive fraud prevention rules with Oracle Adaptive Access Manager Enforce regulatory compliance and generate audit-ready reports Learn about latest additions from the acquired Sun stack

Plan, design, and implement identity and access management solutions with Okta Key Features Learn how to use Okta for complete identity and access management in

your organization Use single sign-on, multifactor authentication, and life cycle management for enhanced security Set up, manage, and audit API access policies Book Description IAM, short for identity and access management, is a set of policies and technologies for ensuring the security of an organization through careful role and access assignment for users and devices. With this book, you'll get up and running with Okta, an identity and access management (IAM) service that you can use for both employees and customers. Once you've understood how Okta can be used as an IAM platform, you'll learn about the Universal Directory, which covers how to integrate other directories and applications and set up groups and policies. As you make progress, the book explores Okta's single sign-on (SSO) feature and multifactor authentication (MFA) solutions. Finally, you will delve into API access management and discover how you can leverage Advanced Server Access for your cloud servers and Okta Access Gateway for your on-premises applications. By the end of this Okta book, you'll have learned how to implement Okta to enhance your organization's security and be able to use this book as a reference guide for the Okta certification exam. What you will learn Understand different types of users in Okta and how to place them in groups Set up SSO and MFA rules to secure your IT environment Get to grips with the basics of end-user functionality and customization Find out how provisioning and synchronization with applications work Explore API management, Access Gateway, and Advanced Server Access Become well-versed in the terminology used by IAM professionals Who this book is for If you are an IT consultant, business decision-maker, system administrator, system and security engineer, or anyone who wishes to use Okta to plan, design, and implement identity and access management solutions, this book is for you. A basic understanding of

authentication and authorization is necessary.

This updated study guide by two security experts will help you prepare for the CompTIA CySA+ certification exam. Position yourself for success with coverage of crucial security topics! Where can you find 100% coverage of the revised CompTIA Cybersecurity Analyst+ (CySA+) exam objectives? It's all in the CompTIA CySA+ Study Guide Exam CS0-002, Second Edition! This guide provides clear and concise information on crucial security topics. You'll be able to gain insight from practical, real-world examples, plus chapter reviews and exam highlights. Turn to this comprehensive resource to gain authoritative coverage of a range of security subject areas. Review threat and vulnerability management topics Expand your knowledge of software and systems security Gain greater understanding of security operations and monitoring Study incident response information Get guidance on compliance and assessment The CompTIA CySA+ Study Guide, Second Edition connects you to useful study tools that help you prepare for the exam. Gain confidence by using its interactive online test bank with hundreds of bonus practice questions, electronic flashcards, and a searchable glossary of key cybersecurity terms. You also get access to hands-on labs and have the opportunity to create a cybersecurity toolkit. Leading security experts, Mike Chapple and David Seidl, wrote this valuable guide to help you prepare to be CompTIA Security+ certified. If you're an IT professional who has earned your CompTIA Security+ certification, success on the CySA+ (Cybersecurity

Analyst) exam stands as an impressive addition to your professional credentials. Preparing and taking the CS0-002exam can also help you plan for advanced certifications, such as the CompTIA Advanced Security Practitioner (CASP+).

In the past four decades, information technology has altered chains of value production, distribution, and information access at a significant rate. These changes, although they have shaken up numerous economic models, have so far not radically challenged the bases of our society. This book addresses our current progress and viewpoints on digital identity management in different fields (social networks, cloud computing, Internet of Things (IoT), with input from experts in computer science, law, economics and sociology. Within this multidisciplinary and scientific context, having crossed analysis on the digital ID issue, it describes the different technical and legal approaches to protect digital identities with a focus on authentication systems, identity federation techniques and privacy preservation solutions. The limitations of these solutions and research issues in this field are also discussed to further understand the changes that are taking place. Offers a state of the discussions and work places on the management of digital identities in various contexts, such as social networking, cloud computing and the Internet of Things Describes the advanced technical and legal measures to protect digital identities Contains a strong emphasis of authentication techniques, identity federation tools and technical protection of privacy

A concise guide for ophthalmologists detailing

tuberculosis, which can cause disease in multiple organs throughout the body, including the eye. Tuberculosis is an infection caused by mycobacterium tuberculosis, which can cause disease in multiple organs throughout the body, including the eye. This can also affect any part of the eye (intraocular, superficial, or surrounding the eye), with or without systemic involvement and Ocular Tuberculosis is a text devoted to in-depth coverage of this topic. Written and edited by international leaders in the field, discussing detailed and practical information on everything from clinical features, ocular imaging studies, and pathology, to investigations, treatment, and surgical management of this disease, Ocular Tuberculosis is a truly comprehensive text.

As cloud technology continues to advance and be utilized, many service providers have begun to employ multiple networks, or cloud federations; however, as the popularity of these federations increases, so does potential utilization challenges. Developing Interoperable and Federated Cloud Architecture provides valuable insight into current and emergent research occurring within the field of cloud infrastructures. Featuring barriers, recent developments, and practical applications on the interoperability issues of federated cloud architectures, this book is a focused reference for administrators, developers, and cloud users interested in energy awareness, scheduling, and federation policies and usage.

Focus on IAM (Identity and Access Management) is a very unique book addressing all the facets of IAM. It is written for all IAM and Information security professionals

in IT. This book is not focused on any specific IAM tool/ product; it will provide the deep delving information on Identity and Access Management with respect to process, technology, best practices, checklists, etc.

In this easy-to-read action guide, Corbin H. Links shares key strategies for successfully planning and organizing an Identity and Access Management (IAM) Program. Mr. Links brings something to the table that no one else does - success tips and strategies that are truly vendor neutral, and designed to work for any organization regardless of size or business type. This book is the result of over 11 years designing and implementing IAM strategies for a diverse international client base. This book has one primary purpose: save organizations time and money in their Strategic Business Initiatives, without sacrificing quality or alignment with goals. The companion website to this book is located at http://www.iamsuccesstips.com.

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.

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.

Identity and Access ManagementBusiness

Performance Through Connected IntelligenceNewnes

Looks at the standards for interoperability, their meaning, and their impact on an organization's overall identity management strategy, explaining how digital identity can be employed to create an agile digital identity infrastructure and outlining specific problems and solutions.

The book is a powerful, novel approach to the analysis and synthesis of IAM systems. It is motivated by the realization that the current practice of Information Systems in general, and Identity and Access Management in particular, is increasingly divorced from its Systems Engineering underpinnings. Even for the most innovative and resourceful practitioners, the architecture, design, implementation and support of enterprise Information Technology systems has taken a complex inferential approach, driven by algorithmic and rule based protocols and standards. This work creates a solid foundation for IAM by using established concepts from Systems Engineering, using systems representations for major IAM processes like authentication and authorization. Such systems formulations may then be used to analyze IAM systems in complicated organizations using established Systems Engineering methods. For example, the book shows that problems in IAM such as risk propagation and authentication processes

that were heretofore analyzed in terms of prescriptive, algorithmic or empirical schemes, are indeed amenable to general theoretical treatment. The book is specifically designed to be accessible to the general IT practitioner. It is with this goal in mind that it teases out the concepts in a way that anyone with some college education will be able to understand.

"Identity Management: A Primer provides a complete and comprehensive overview of the elements required for a properly planned identity environment. In it, the authors cover the entire gamut of IDM-related matters, including directories; authentication; provisioning; role-based access control; single sign-on; governance, risk, and compliance; implementation and roadmap; public key infrastructure; electronic identity smartcards; and a wealth of other important topics. As the title indicates, this book is a primer in which the key issues of identity management are identified and appropriate strategies and preventative measures are covered in an easy-to-understand format with extensive use of real-world case study examples. Students and IT professionals alike will appreciate this resource as they seek to understand and master the complexity of identity in a virtual world."--Resource description p.

Start empowering users and protecting corporate data, while managing Identities and Access with

Microsoft Azure in different environments About This Book Deep dive into the Microsoft Identity and Access Management as a Service (IDaaS) solution Design, implement and manage simple and complex hybrid identity and access management environments Learn to apply solution architectures directly to your business needs and understand how to identify and manage business drivers during transitions Who This Book Is For This book is for business decision makers, IT consultants, and system and security engineers who wish to plan, design, and implement Identity and Access Management solutions with Microsoft Azure. What You Will Learn Apply technical descriptions and solution architectures directly to your business needs and deployments Identify and manage business drivers and architecture changes to transition between different scenarios Understand and configure all relevant Identity and Access Management key features and concepts Implement simple and complex directory integration, authentication, and authorization scenarios Get to know about modern identity management, authentication, and authorization protocols and standards Implement and configure a modern information protection solution Integrate and configure future improvements in authentication and authorization functionality of Windows 10 and Windows Server 2016 In Detail Microsoft Azure and

its Identity and Access Management is at the heart of Microsoft's Software as a Service, including Office 365, Dynamics CRM, and Enterprise Mobility Management. It is an essential tool to master in order to effectively work with the Microsoft Cloud. Through practical, project based learning this book will impart that mastery. Beginning with the basics of features and licenses, this book quickly moves on to the user and group lifecycle required to design roles and administrative units for role-based access control (RBAC). Learn to design Azure AD to be an identity provider and provide flexible and secure access to SaaS applications. Get to grips with how to configure and manage users, groups, roles, and administrative units to provide a user- and group-based application and self-service access including the audit functionality. Next find out how to take advantage of managing common identities with the Microsoft Identity Manager 2016 and build cloud identities with the Azure AD Connect utility. Construct blueprints with different authentication scenarios including multi-factor authentication. Discover how to configure and manage the identity synchronization and federation environment along with multi -factor authentication, conditional access, and information protection scenarios to apply the required security functionality. Finally, get recommendations for planning and implementing a future-oriented and sustainable identity and access

management strategy. Style and approach A practical, project-based learning experience explained through hands-on examples.
Work with common biometrics such as face, fingerprint, and iris recognition for business and personal use to ensure secure identification and authentication for fintech, homes, and computer systems Key Features Explore the next iteration of identity protection and overcome real-world challenges Understand different biometric use cases to deploy a large-scale biometric system Curated by renowned security ambassador and experienced author Lisa Bock Book Description Biometric technologies provide a variety of robust and convenient methods to securely identify and authenticate an individual. Unlike a password or smart card, biometrics can identify an attribute that is not only unique to an individual, but also eliminates any possibility of duplication. Identity Management with Biometrics is a solid introduction for anyone who wants to explore biometric techniques, such as fingerprint, iris, voice, palm print, and facial recognition. Starting with an overview of biometrics, you'll learn the various uses and applications of biometrics in fintech, buildings, border control, and many other fields. You'll understand the characteristics of an optimal biometric system and then review different types of errors and discover the benefits of multi-factor authentication. You'll also get

to grips with analyzing a biometric system for usability and accuracy and understand the process of implementation, testing, and deployment, along with addressing privacy concerns. The book outlines the importance of protecting biometric data by using encryption and shows you which factors to consider and how to analyze them before investing in biometric technologies. By the end of this book, you'll be well-versed with a variety of recognition processes and be able to make the right decisions when implementing biometric technologies. What you will learn Review the advantages and disadvantages of biometric technology Understand the characteristics of an optimal biometric system Discover the uses of biometrics and where they are used Compare different types of errors and see how to tune your system Understand the benefits of multi-factor authentication Work with commonly used biometrics such as face, fingerprint, and iris Analyze a biometric system for usability and accuracy Address privacy concerns and get a glimpse of the future of biometrics Who this book is for Identity Management with Biometrics is for IT managers, security professionals, students, teachers, and anyone involved in selecting, purchasing, integrating, or securing a biometric system. This book will help you understand how to select the right biometric system for your organization and walk you through the steps for implementing identity management and

authentication. A basic understanding of biometric authentication techniques, such as fingerprint and facial recognition, and the importance of providing a secure method of authenticating an individual will help you make the most of the book.

The Internet of Things is a wide-reaching network of devices, and these devices can intercommunicate and collaborate with each other to produce variety of services at any time, any place, and in any way. Maintaining access control, authentication and managing the identity of devices while they interact with other devices, services and people is an important challenge for identity management. The identity management presents significant challenges in the current Internet communication. These challenges are exacerbated in the internet of things by the unbound number of devices and expected limitations in constrained resources. Current identity management solutions are mainly concerned with identities that are used by end users, and services to identify themselves in the networked world. However, these identity management solutions are designed by considering that significant resources are available and applicability of these identity management solutions to the resource constrained internet of things needs a thorough analysis. Technical topics discussed in the book include: Internet of Things; Identity Management; Identity models in Internet of Things; Identity management

and trust in the Internet of Things context; Authentication and access control; Identity management for Internet of Things contributes to the area of identity management for ubiquitous devices in the Internet of Things. It initially presents the motivational factors together with the identity management problems in the context of Internet of Things and proposes an identity management framework. Following this, it refers to the major challenges for Identity management and presents different identity management models. This book also presents relationship between identity and trust, different approaches for trust management, authentication and access control. Key milestones identified for Identity management are clustering with hierarchical addressing, trust management, mutual authentication and access control. Identity management for Internet of Things is ideal for personnel in computer/communication industries as well as academic staff and master/research students in wireless communication, computer science, operational research, electrical engineering and telecommunication systems Internet, and cloud computing. Content Preface; 1. Internet of Things Overview; 2. Elements of Internet of Things Security; 3: Identity Management Models; 4. Identity Management and Trust; 5. Identity Establishment; 6. Access Control; 7. Conclusions

Know how to design and use identity management to

protect your application and the data it manages. At a time when security breaches result in increasingly onerous penalties, it is paramount that application developers and owners understand identity management and the value it provides when building applications. This book takes you from account provisioning to authentication to authorization, and covers troubleshooting and common problems to avoid. The authors include predictions about why this will be even more important in the future. Application best practices with coding samples are provided. Solving Identity and Access Management in Modern Applications gives you what you need to design identity and access management for your applications and to describe it to stakeholders with confidence. You will be able to explain account creation, session and access management, account termination, and more. What You'll Learn Understand key identity management concepts Incorporate essential design principles Design authentication and access control for a modern application Know the identity management frameworks and protocols used today (OIDC/ OAuth 2.0, SAML 2.0) Review historical failures and know how to avoid them Who This Book Is For Developers, enterprise or application architects, business application or product owners, and anyone involved in an application's identity management solution

This is a practical and fast-paced guide that gives you all the information you need to start implementing secure OAuth 2.0 implementations in your web applications.OAuth 2.0 Identity and Access Management Patterns is intended for software developers, software architects, and enthusiasts working with the OAuth 2.0 framework. In order to learn and understand the OAuth 2.0 grant flow, it is assumed that you have some basic knowledge of HTTP communication. For the practical examples, basic knowledge of HTML templating, programming languages, and executing commands in the command line terminal is assumed.

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

Discover how poor identity and privilege management

can be leveraged to compromise accounts and credentials within an organization. Learn how role-based identity assignments, entitlements, and auditing strategies can be implemented to mitigate the threats leveraging accounts and identities and how to manage compliance for regulatory initiatives. As a solution, Identity Access Management (IAM) has emerged as the cornerstone of enterprise security. Managing accounts, credentials, roles, certification, and attestation reporting for all resources is now a security and compliance mandate. When identity theft and poor identity management is leveraged as an attack vector, risk and vulnerabilities increase exponentially. As cyber attacks continue to increase in volume and sophistication, it is not a matter of if, but when, your organization will have an incident. Threat actors target accounts, users, and their associated identities, to conduct their malicious activities through privileged attacks and asset vulnerabilities. Identity Attack Vectors details the risks associated with poor identity management practices, the techniques that threat actors and insiders leverage, and the operational best practices that organizations should adopt to protect against identity theft and account compromises, and to develop an effective identity governance program. What You Will Learn Understand the concepts behind an identity and how their associated credentials and accounts can be leveraged as an attack vector Implement an effective Identity Access Management (IAM) program to manage identities and roles, and provide certification for regulatory compliance See where identity management controls play a part of

the cyber kill chain and how privileges should be managed as a potential weak link Build upon industry standards to integrate key identity management technologies into a corporate ecosystem Plan for a successful deployment, implementation scope, measurable risk reduction, auditing and discovery, regulatory reporting, and oversight based on real-world strategies to prevent identity attack vectors Who This Book Is For Management and implementers in IT operations, security, and auditing looking to understand and implement an identity access management program and manage privileges in these environments

A practical, indispensable security guide that will navigate you through the complex realm of securely building and deploying systems in our IoT-connected world About This Book Learn to design and implement cyber security strategies for your organization Learn to protect cyber-physical systems and utilize forensic data analysis to beat vulnerabilities in your IoT ecosystem Learn best practices to secure your data from device to the cloud Gain insight into privacy-enhancing techniques and technologies Who This Book Is For This book targets IT Security Professionals and Security Engineers (including pentesters, security architects and ethical hackers) who would like to ensure security of their organization's data when connected through the IoT. Business analysts and managers will also find it useful. What You Will Learn Learn how to break down cross-industry barriers by adopting the best practices for IoT deployments Build a rock-solid security program for IoT that is cost-effective and easy to maintain Demystify

complex topics such as cryptography, privacy, and penetration testing to improve your security posture See how the selection of individual components can affect the security posture of the entire system Use Systems Security Engineering and Privacy-by-design principles to design a secure IoT ecosystem Get to know how to leverage the burdgening cloud-based systems that will support the IoT into the future. In Detail With the advent of Intenret of Things (IoT), businesses will be faced with defending against new types of threats. The business ecosystem now includes cloud computing infrastructure, mobile and fixed endpoints that open up new attack surfaces, a desire to share information with many stakeholders and a need to take action quickly based on large quantities of collected data. . It therefore becomes critical to ensure that cyber security threats are contained to a minimum when implementing new IoT services and solutions. . The interconnectivity of people, devices, and companies raises stakes to a new level as computing and action become even more mobile, everything becomes connected to the cloud, and infrastructure is strained to securely manage the billions of devices that will connect us all to the IoT. This book shows you how to implement cyber-security solutions, IoT design best practices and risk mitigation methodologies to address device and infrastructure threats to IoT solutions. This book will take readers on a journey that begins with understanding the IoT and how it can be applied in various industries, goes on to describe the security challenges associated with the IoT, and then provides a set of guidelines to architect and

deploy a secure IoT in your Enterprise. The book will showcase how the IoT is implemented in early-adopting industries and describe how lessons can be learned and shared across diverse industries to support a secure IoT. Style and approach This book aims to educate readers on key areas in IoT security. It walks readers through engaging with security challenges and then provides answers on how to successfully manage IoT security and build a safe infrastructure for smart devices. After reading this book, you will understand the true potential of tools and solutions in order to build real-time security intelligence on IoT networks.

Keystone—OpenStack's Identity service—provides secure controlled access to a cloud's resources. In OpenStack environments, Keystone performs many vital functions, such as authenticating users and determining what resources users are authorized to access. Whether the cloud is private, public, or dedicated, access to cloud resources and security is essential. This practical guide to using Keystone provides detailed, step-by-step guidance to creating a secure cloud environment at the Infrastructure-as-a-Service layer—as well as key practices for safeguarding your cloud's ongoing security. Learn about Keystone's fundamental capabilities for providing Identity, Authentication, and Access Management Perform basic Keystone operations, using concrete examples and the latest version (v3) of Keystone's Identity API Understand Keystone's unique support for multiple token formats, including how it has evolved over time Get an in-depth explanation of Keystone's LDAP support and how to configure

Keystone to integrate with LDAP Learn about one of Keystone's most sought-after features—support for federated identity

With The Rapid Increase the use of electronic resources in libraries, managing access to online information is an area many librarians struggle with. Managers of online information wish to implement policies about who can access the information and under what terms and conditions but often they need further guidance. Written by experts in the field, this practical book is the first to explain the principles behind access management, the available technologies and how they work. This includes an overview of federated access management technologies, such as Shibboleth, that have gained increasing international recognition in recent years. This book provides detailed case studies describing how access management is being implemented at organizational and national levels in the UK, USA and Europe, and gives a practical guide to the resources available to help plan, implement and operate access management in libraries. Key topics include: What is access management and why do libraries do it? Authorization based on user identity or affiliation Electronic resources: public and not so public Federated access: history, current position and future developments Principles and definitions of identity and access management How to choose access management and identity management products and services Current access management technologies Internet access provided by (or in) libraries Authentication technologies Library statistics Authorization based on physical location

The business case for libraries This is essential reading for all who need to understand the principles behind access management or implement a working system in their library.

Developers, designers, engineers, and creators can no longer afford to pass responsibility for identity and data security onto others. Web developers who don't understand how to obscure data in transmission, for instance, can open security flaws on a site without realizing it. With this practical guide, you'll learn how and why everyone working on a system needs to ensure that users and data are protected. Authors Jonathan LeBlanc and Tim Messerschmidt provide a deep dive into the concepts, technology, and programming methodologies necessary to build a secure interface for data and identity—without compromising usability. You'll learn how to plug holes in existing systems, protect against viable attack vectors, and work in environments that sometimes are naturally insecure. Understand the state of web and application security today Design security password encryption, and combat password attack vectors Create digital fingerprints to identify users through browser, device, and paired device detection Build secure data transmission systems through OAuth and OpenID Connect Use alternate methods of identification for a second factor of authentication Harden your web applications against attack Create a secure data transmission system using SSL/TLS, and synchronous and asynchronous cryptography