

Identity Management A Primer

Identity Management A Primer Mc Press Llc

The discipline of Knowledge Management (KM) is rapidly becoming established as an essential course or module in both information systems and management programs around the world. Many KM texts pitch theoretical issues at too technical or high a level, or presenting a only a theoretical prescriptive treatment of knowledge or KM modeling problems. The Knowledge Management Primer provides students with an essential understanding of KM approaches by examining the purpose and nature of its key components. The book demystifies the KM field by explaining in a precise, accessible manner the key concepts of KM tools, strategies, and techniques, and their benefits to contemporary organizations. Readers will find this book filled with approaches to managing and developing KM that are underpinned by theory and research, are integrative in nature, and address softer approaches in manifesting and recognizing knowledge.

"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.

Every enterprise architect faces similar problems when designing and governing the enterprise architecture of a medium to large enterprise. Design patterns are a well-established concept in software engineering, used to define universally applicable solution schemes. By applying this approach to enterprise architectures, recurring problems in the design and implementation of enterprise architectures can be solved over all layers, from the business layer to the application and data layer down to the technology layer. Inversini and Perroud describe patterns at the level of enterprise architecture, which they refer to as Enterprise Architecture Patterns. These patterns are motivated by recurring problems originating from both the business and the underlying application, or from data and technology architectures of an enterprise such as identity and access management or integration needs. The Enterprise Architecture Patterns help in planning the technological and organizational landscape of an enterprise and its information technology, and are easily embedded into frameworks such as TOGAF, Zachman or FEA. This book is aimed at enterprise architects, software architects, project leaders, business consultants and everyone concerned with questions of IT and enterprise architecture and provides them with a comprehensive catalogue of ready-to-use patterns as well as an extensive theoretical framework to define their own new patterns.

Experts explore current theory and practice in the application of digitally enabled open networked social models to international development. The emergence of open

networked models made possible by digital technology has the potential to transform international development. Open network structures allow people to come together to share information, organize, and collaborate. Open development harnesses this power, to create new organizational forms and improve people's lives; it is not only an agenda for research and practice but also a statement about how to approach international development. In this volume, experts explore a variety of applications of openness, addressing challenges as well as opportunities. Open development requires new theoretical tools that focus on real world problems, consider a variety of solutions, and recognize the complexity of local contexts. After exploring the new theoretical terrain, the book describes a range of cases in which open models address such specific development issues as biotechnology research, improving education, and access to scholarly publications. Contributors then examine tensions between open models and existing structures, including struggles over privacy, intellectual property, and implementation. Finally, contributors offer broader conceptual perspectives, considering processes of social construction, knowledge management, and the role of individual intent in the development and outcomes of social models. Contributors Carla Bonina, Ineke Buskens, Leslie Chan, Abdallah Daar, Jeremy de Beer, Mark Graham, Eve Gray, Anita Gurumurthy, Havard Haarstad, Blane Harvey, Myra Khan, Melissa Loudon, Aaron K. Martin, Hassan Masum, Chidi Oguamanam, Katherine M. A. Reilly, Ulrike Rivett, Karl Schroeder, Parminder Jeet Singh, Matthew L. Smith, Marshall S.

Smith Copublished with the International Development Research Centre of Canada (IDRC)

This book contains selected papers presented at the 13th IFIP WG 9.2, 9.6/11.7, 11.6/SIG 9.2.2 International Summer School on Privacy and Identity Management, held in Vienna, Austria, in August 2018. The 10 full papers included in this volume were carefully reviewed and selected from 27 submissions. Also included are reviewed papers summarizing the results of workshops and tutorials that were held at the Summer School as well as papers contributed by several of the invited speakers. The papers combine interdisciplinary approaches to bring together a host of perspectives: technical, legal, regulatory, socio-economic, social, societal, political, ethical, anthropological, philosophical, historical, and psychological.

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.

With the increasing availability of electronic services, security and a reliable means by which identity is verified is essential. Written by Norberto Andrade the first chapter of this book provides an overview of the main legal and regulatory aspects regarding electronic identity in Europe and assesses the importance of electronic identity for

administration (public), business (private) and, above all, citizens. It also highlights the role of eID as a key enabler of the economy. In the second chapter Lisha Chen-Wilson, David Argles, Michele Schiano di Zenise and Gary Wills discuss the user-centric eCertificate system aimed at supporting the eID system. Electronic Identity is essential reading for researchers, lawyers, policy makers, technologists and anyone wishing to understand the challenges of a pan-European eID.

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.

The goals of this book are to examine the functional components that take basic identity systems and turn them into identity management operations and to highlight some of the implications of those operations for identity management schemes.

The preservation of private data is a main concern of governments, organizations, and individuals alike. For individuals, a breach in personal information can mean dire consequences for an individual's finances, medical information, and personal property. Identity Theft: Breakthroughs in Research and Practice highlights emerging perspectives and critical insights into the preservation of personal data and the complications that can arise when one's identity is compromised. This critical volume features key research on methods and technologies for protection, the problems associated with identity theft, and outlooks for the future. This publication is an essential resource for information security professionals, researchers, and graduate-level students in the fields of criminal science, business, and computer science.

This book contains a range of keynote papers and submitted papers presented at the 7th IFIP WG 9.2, 9.5, 9.6/11.7, 11.4, 11.6 International Summer School, held in Nijmegen, The Netherlands, in June 2013. The 13 revised full papers and 6 keynote papers included in this volume were carefully selected from a total of 30 presentations and 11 keynote talks and were subject to a two-step review process. The keynote papers cover the dramatic global changes, including legislative developments that society is facing today. Privacy and identity management are explored in specific settings, such as the corporate context, civic society, and education and using particular technologies such as cloud computing. The regular papers examine the challenges to privacy, security and

identity; ways of preserving privacy; identity and identity management and the particular challenges presented by social media.

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.

"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.

Identity authentication and authorization are integral tasks in today's digital world. As businesses become more technologically integrated and consumers use more web services, the questions of identity security and accessibility are becoming more prevalent. Federated identity links user credentials across multiple systems and services, altering both the utility and security landscape of both. In *Federated Identity Primer*, Derrick Rountree. Learn about Internet authentication Learn about federated authentication Learn about ADFS 2.0

This book contains a range of invited and submitted papers presented at the 11th IFIP WG 9.2, 9.5, 9.6/11.7, 11.4, 11.6/SIG 9.2.2 International Summer School, held in Karlstad, Sweden, in August 2016. The 17 revised full papers and one short paper included in this volume were carefully selected from a total of 42 submissions and were subject to a two-step 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. The paper 'Big Data Privacy

one safeguard can completely protect your assets from a highly motivated threat. It's a combination of safeguards working together that creates an environment secure enough to deter attempts to compromise the confidentiality, integrity, or availability of your information assets. To introduce the various layers in the model, this book is divided into three parts. Annotation New edition of a study of the law of electronic commerce, which requires the simultaneous management of business, technology and legal issues. Winn (law, Southern Methodist U.) and Wright (a business lawyer in Dallas) present 21 chapters that discuss introductory material such as business and technologies of e-commerce, getting online, jurisdiction and choice of law issues, and electronic commerce and law practice; contracting; electronic payments and lending; intellectual property rights and rights in data; regulation of e-business markets; and business administration. Presented in a three-ring binder. Annotation c. Book News, Inc., Portland, OR (booknews.com)

Summary: Chapters in "Critical Insights From A Practitioner Mindset" have been grouped into four categories: (1) the New digital economy; (2) e-government practices; (3) identity and access management; and (4) identity systems implementation. These areas are considered to be crucial subsets that will shape the upcoming future and influence successful governance models. "Critical Insights From A Practitioner Mindset" is eminently readable and covers management practices in the government field and the efforts of the Gulf Cooperation Council (GCC) countries and the United Arab Emirates government. The book is key reading for both practitioners and decision-making authorities. Key Features: Is highly practical and easy to read. Comprehensive, detailed and through theoretical and practical analysis. Covers issues, and sources rarely accessed, on books on this topic. The Author: Dr Al-Khoury is the Director General (Under Secretary) of the Emirates Identity Authority: a federal government organisation established in 2004 to rollout and manage the national identity management infrastructure program in the United Arab Emirates. He has been involved in the UAE national identity card program since its early conceptual phases during his work with the Ministry of Interior. He has also been involved in many other strategic government initiatives in the past 22 years of his experience in the government sector. Contents: The new digital economy: Emerging markets and digital economy: building trust in the virtual world Biometrics technology and the new economy: a review of the field and the case of the United Arab Emirates E-government practices: PKI in government digital identity management systems An innovative approach for e-government transformation PKI in government identity management systems PKI technology: a government experience The role of digital certificates in contemporary government systems Identity and access management: Optimizing identity and access management (IAM) frameworks Towards federated identity management across GCC: a solution's framework Contemporary identity systems implementation: Re-thinking enrolment in identity schemes Targeting results: lessons learned from UAE National ID Program"

This book contains the refereed proceedings of the Third International Conference on Exploring Services Science (IESS) which was held in Geneva, Switzerland, in February 2012. At the conference, researchers from all over the world presented innovative ideas, research, and applications in the design, management, and evaluation of services. This year, the main theme was the interdisciplinary aspect of services. The 22 full papers accepted for IESS were selected from 46 submissions and presented ideas and results related to innovation, services discovery, services engineering, and services management as well as the application of services in information technology, business, e-learning and public administration.

Organizations, worldwide, have adopted practical and applied approaches for mitigating risks and managing information security program. Considering complexities of a large-scale, distributed IT environments, security should be proactively planned for and prepared ahead, rather than as used as reactions to

changes in the landscape. Strategic and Practical Approaches for Information Security Governance: Technologies and Applied Solutions presents high-quality research papers and practice articles on management and governance issues in the field of information security. The main focus of the book is to provide an organization with insights into practical and applied solutions, frameworks, technologies and practices on technological and organizational factors. The book aims to be a collection of knowledge for professionals, scholars, researchers and academicians working in this field that is fast evolving and growing as an area of information assurance.

Although Europe has a significant legal data protection framework, built up around EU Directive 95/46/EC and the Charter of Fundamental Rights, the question of whether data protection and its legal framework are ‘in good health’ is increasingly being posed. Advanced technologies raise fundamental issues regarding key concepts of data protection. Falling storage prices, increasing chips performance, the fact that technology is becoming increasingly embedded and ubiquitous, the convergence of technologies and other technological developments are broadening the scope and possibilities of applications rapidly. Society however, is also changing, affecting the privacy and data protection landscape. The ‘demand’ for free services, security, convenience, governance, etc, changes the mindsets of all the stakeholders involved. Privacy is being proclaimed dead or at least worthy of dying by the captains of industry; governments and policy makers are having to manoeuvre between competing and incompatible aims; and citizens and customers are considered to be indifferent. In the year in which the plans for the revision of the Data Protection Directive will be revealed, the current volume brings together a number of chapters highlighting issues, describing and discussing practices, and offering conceptual analysis of core concepts within the domain of privacy and data protection. The book’s first part focuses on surveillance, profiling and prediction; the second on regulation, enforcement, and security; and the third on some of the fundamental concepts in the area of privacy and data protection. Reading the various chapters it appears that the ‘patient’ needs to be cured of quite some weak spots, illnesses and malformations. European data protection is at a turning point and the new challenges are not only accentuating the existing flaws and the anticipated difficulties, but also, more positively, the merits and the need for strong and accurate data protection practices and rules in Europe, and elsewhere.

?????1%??????????37?? ??????1%??????????????0? ?????????????????????????????
??
?Amazon??Fast
Company???2018?7??
??????The Muse??
??
??
??

This book constitutes the refereed proceedings of the International Conference on Recent Trends in Computer Networks and Distributed Systems Security, held in Trivandrum, India, in October 2012. The 34 revised full papers and 8 poster presentations were carefully reviewed and selected from 112 submissions. The papers cover various topics in Computer Networks and Distributed Systems. The implementation of Enterprise Networks or e-Networking is of paramount importance for organisations. Enterprise-wide networking would warrant that the components of information architecture are organised to harness more out of the organisation's computing power on the desktop. This would also involve establishment of networks that link the various but important subsystems of the enterprise. Our firm belief is that in order to gain a competitive edge the organisations need knowledge and sound strategy. This conviction is particularly true today, considering the pressures from international competition, environmental concerns and complicated ethical issues. This book, entitled A Manager's Primer on e-Networking, negotiates the hyper dimensions of the Internet through stories from myriad of Web sites with its fluent presentation and simple but chronological organisation of topics highlighting numerous opportunities and providing a solid starting point not only for inexperienced entrepreneurs and managers but anyone interested in applying information technology in the business. I sincerely hope the book will help as well many small and medium size companies and organisations to launch corporate networking successfully in order to attain their strategic objectives. Rajiv Jayashankar, Ph. D. The aim of the book is to provide latest research findings, innovative research results, methods and development techniques from both theoretical and practical perspectives related to the emerging areas of information networking and applications. Networks of today are going through a rapid evolution and there are many emerging areas of information networking and their applications. Heterogeneous networking supported by recent technological advances in low power wireless communications along with silicon integration of various functionalities such as sensing, communications, intelligence and actuations are emerging as a critically important disruptive computer class based on a new platform, networking structure and interface that enable novel, low cost and high volume applications. Several of such applications have been difficult to realize because of many interconnections problems. To fulfill their large range of applications different kinds of networks need to collaborate and wired and next generation wireless systems should be integrated in order to develop high performance computing solutions to problems arising from the complexities of these networks. This book covers the theory, design and applications of computer networks, distributed computing and information systems. Discusses important concepts of Unix system administration, covering such topics as the design of a system, user communication, and disaster recovery. This two-volume-set (CCIS 293 and CCIS 294) constitutes the refereed proceedings of the International Conference on Networked Digital Technologies, NDT 2012, held in

Dubai, UAE, in April 2012. The 96 papers presented in the two volumes were carefully reviewed and selected from 228 submissions. The papers are organized in topical sections on collaborative systems for e-sciences; context-aware processing and ubiquitous systems; data and network mining; grid and cloud computing; information and data management; intelligent agent-based systems; internet modeling and design; mobile, ad hoc and sensor network management; peer-to-peer social networks; quality of service for networked systems; semantic Web and ontologies; security and access control; signal processing and computer vision for networked systems; social networks; Web services.

Skillfully navigate through the complex realm of implementing scalable, trustworthy industrial systems and architectures in a hyper-connected business world. Key Features Gain practical insight into security concepts in the Industrial Internet of Things (IIoT) architecture Demystify complex topics such as cryptography and blockchain Comprehensive references to industry standards and security frameworks when developing IIoT blueprints Book Description Securing connected industries and autonomous systems is a top concern for the Industrial Internet of Things (IIoT) community. Unlike cybersecurity, cyber-physical security is an intricate discipline that directly ties to system reliability as well as human and environmental safety. Practical Industrial Internet of Things Security enables you to develop a comprehensive understanding of the entire spectrum of securing connected industries, from the edge to the cloud. This book establishes the foundational concepts and tenets of IIoT security by presenting real-world case studies, threat models, and reference architectures. You'll work with practical tools to design risk-based security controls for industrial use cases and gain practical know-how on the multi-layered defense techniques including Identity and Access Management (IAM), endpoint security, and communication infrastructure. Stakeholders, including developers, architects, and business leaders, can gain practical insights in securing IIoT lifecycle processes, standardization, governance and assess the applicability of emerging technologies, such as blockchain, Artificial Intelligence, and Machine Learning, to design and implement resilient connected systems and harness significant industrial opportunities. What you will learn Understand the crucial concepts of a multi-layered IIoT security framework Gain insight on securing identity, access, and configuration management for large-scale IIoT deployments Secure your machine-to-machine (M2M) and machine-to-cloud (M2C) connectivity Build a concrete security program for your IIoT deployment Explore techniques from case studies on industrial IoT threat modeling and mitigation approaches Learn risk management and mitigation planning Who this book is for Practical Industrial Internet of Things Security is for the IIoT community, which includes IIoT researchers, security professionals, architects, developers, and business stakeholders. Anyone who needs to have a comprehensive understanding of the unique safety and security challenges of connected industries and practical methodologies to secure industrial assets will find this book immensely helpful. This book is uniquely designed to benefit professionals from both IT and industrial operations backgrounds.

This book constitutes the thoroughly refereed post-conference proceedings of the 8th European Workshop on Public Key Infrastructures, Services and Applications, EuroPKI 2011, held in Leuven, Belgium in September 2011 - co-located with the 16th European

Symposium on Research in Computer Security, ESORICS 2011. The 10 revised full papers presented together with 3 invited talks were carefully reviewed and selected from 27 submissions. The papers are organized in topical sections on authentication mechanisms, privacy preserving techniques, PKI and secure applications.

[Copyright: 7b93148734221e325832807fc387272b](#)