Identity Management A Primer

"For technology and business readers. No prior SSI, cryptography, or blockchain experience required"--Back cover.
This is Cisco's official, comprehensive self-study resource for Cisco's SISE 300-715 exam (Implementing and Configuring Cisco Identity Services Engine), one of the most popular concentration exams required for the Cisco Certified Network Professional (CCNP) Security certification. It will thoroughly prepare network professionals to deploy and use Cisco ISE to simplify delivery of consistent, highly secure access control across wired, wireless, and VPN connections. Designed for all CCNP Security candidates, CCNP Security Identity Management SISE 300-715 Official Cert Guide covers every SISE #300-715 objective concisely and logically, with extensive teaching features designed to promote retention and understanding. You'll find: Pre-chapter quizzes to assess knowledge upfront and focus your study more efficiently Foundation topics sections that explain concepts and configurations, and link theory to practice Key topics sections calling attention to every figure, table, and list you must know Exam Preparation sections with additional chapter review features Final preparation chapter providing tools and a complete final study plan A customizable practice test library CCNP Security Identity Management SISE 300-715 Official Cert Guide offers comprehensive, up-to-date coverage of all SISE #300-715 Cisco Identity Services Engine topics related to: Architecture and deployment Policy enforcement Web Auth and guest services Profiler BYOD Endpoint compliance Network access device administration
Every so called, Black man, woman, child wants to believe that slavery is over.The reason being for this belief is because times have changed.But thats not true, times may have change, and the institution of slavery has changed with it, in how its introduced. Slavery has taken on a new form, and its through words, words that would imprison our minds
This book constitutes the thoroughly refereed proceedings of the Fourth International Conference on Data Technologies and Applications, DATA 2015, held in Colmar, France, in July 2015. The 9 revised full papers were carefully reviewed and selected from 70 submissions. The papers deal with the following topics: databases, data warehousing, data mining, data management, data security, knowledge and information systems and technologies; advanced application of data.
Why Some Companies Make the Leap...And Others Don't
A Preteen Primer to the Facts of Life
Strategic and Practical Approaches for Information Security Governance: Technologies and Applied Solutions
Digital Identity
Dispelling Common Leadership Myths
Logic Primer, second edition

Quality care of patients requires evaluating large amounts of data at the right time and place and in the correct context. With the advent of electronic health records, data warehouses now provide information at the point of care and facilitate a continuous learning environment in which lessons learned can provide updates to clinical, administrative, and financial processes. Given the advancement of the information tools and techniques of today's knowledge economy, utilizing these resources are imperative for effective healthcare. Thus, the principles of Knowledge Management (KM) are now essential for quality healthcare management. The Healthcare Knowledge Management Primer explores and explains essential KM principles in healthcare settings in an introductory and easy to understand fashion. This concise book is ideal for both students and professionals who need to learn more about key aspects of the KM field as it pertains to effecting superior healthcare delivery. It provides readers with an understanding of approaches to KM by examining the purpose and nature of its key components and demystifies the KM field by explaining in an accessible manner the key concepts of KM tools, strategies and techniques, and their benefits to contemporary healthcare organizations.
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).
A Primer on Reptiles and Amphibians is an innovative educational resource designed to forge a connection between the reader and the creeping critters of the world. Turtles, frogs, lizards, salamanders, snakes, and crocodiles¿ these animals evoke fear and fascination. This primer dispels myths and unlocks mysteries surrounding these diverse survivors which have mastered virtually every habitat on Earth. Tragically, these animals now face pressures of unprecedented severity, but there is still time to make a difference if more of us work together.Micha Petty is an international award-winning Master Naturalist and wildlife rehabilitator. This critically-acclaimed debut volume is a collection of Micha's interpretive writings, carefully crafted to make learning easy for everyone. These bulletins display his passion for Conservation Through Education while covering topics such as living harmoniously with wildlife, physiology, natural history, observation, and conservation. Flip to any page to be instantly introduced to new facets of reptiles, amphibians, the perils they face, and how you can join the fight to save them.
The Cybersecurity Body of Knowledge explains the content, purpose, and use of eight knowledge areas that define the boundaries of the discipline of cybersecurity. The discussion focuses on, and is driven by, the essential concepts of each knowledge area that collectively capture the cybersecurity body of knowledge to provide a complete picture of the field. This book is based on a brand-new and up to this point unique, global initiative, known as CSEC2017, which was created and endorsed by ACM, IEEE-CS, AIS SIGSEC, and IFIP WG 11.8. This has practical relevance to every educator in the discipline of cybersecurity. Because the specifics of this body of knowledge cannot be imparted in a single text, the authors provide the necessary comprehensive overview. In essence, this is the entry-level survey of the comprehensive field of cybersecurity. It will serve as the roadmap for individuals to later drill down into a specific area of interest. This presentation is also explicitly designed to aid faculty members, administrators, CISOs, policy makers, and stakeholders involved with cybersecurity workforce development initiatives. The book is oriented toward practical application of a computing-based foundation, crosscutting concepts, and essential knowledge and skills of the cybersecurity discipline to meet workforce demands. Dan Shoemaker, PhD, is full professor, senior research scientist, and program director at the University of Detroit Mercy's Center for Cyber Security and Intelligence Studies. Dan is a former chair of the Cybersecurity &

Information Systems Department and has authored numerous books and journal articles focused on cybersecurity. Anne Kohnke, PhD, is an associate professor of cybersecurity and the principle investigator of the Center for Academic Excellence in Cyber Defence at the University of Detroit Mercy. Anne's research is focused in cybersecurity, risk management, threat modeling, and mitigating attack vectors. Ken Sigler, MS, is a faculty member of the Computer Information Systems (CIS) program at the Auburn Hills campus of Oakland Community College in Michigan. Ken's research is in the areas of software management, software assurance, and cybersecurity.

Second Edition

Medical Informatics: An Executive Primer

Healthcare Knowledge Management Primer

The Duh! Book of Management and Supervision

97 Things Every Cloud Engineer Should Know

Access Control, Authentication, and Public Key Infrastructure

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.

The perimeter defenses guarding your network perhaps are not as secure as you think. Hosts behind the firewall have no defenses of their own, so when a host in the "trusted" zone is breached, access to your data center is not far behind. That's an all-too-familiar scenario today. With this practical book, you'll learn the principles behind zero trust architecture, along with details necessary to implement it. The Zero Trust Model treats all hosts as if they're internet-facing, and considers the entire network to be compromised and hostile. By taking this approach, you'll focus on building strong authentication, authorization, and encryption throughout, while providing compartmentalized access and better operational agility. Understand how perimeter-based defenses have evolved to become the broken model we use today Explore two case studies of zero trust in production networks on the client side (Google) and on the server side (PagerDuty) Get example configuration for open source tools that you can use to build a zero trust network Learn how to migrate from a perimeter-based network to a zero trust network in production

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.

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.

Emerging Research and Opportunities

The Nature of Risk

Digital Identity Management

A Primer of Conservation Behavior

Practical Industrial Internet of Things Security

Digital Identity and Access Management: Technologies and Frameworks

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 ent identity lifecycle.

CULTURAL COMPETENCE: A PRIMER FOR EDUCATORS, 2nd Edition, covers the basics of multicultural education, making it easy for instructors to assign as a main text or use in conjunction with other books. The author gives special attention to the psycho-social dimensions of teaching culturally diverse populations. Important Notice: Media content referenced within the product description or t product text may not be available in the ebook version.

This Primer nurtures the development of biologists interested in using animal behavior concepts and tools to solve conservation and wildlife management problems. This is the first practical guide foste integration and showing how to apply these methodologies to issues that would benefit from an animal behavior perspective.

"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 fa with major organizational, economic and market changes"--Provided by publisher.

The Role of Digital Identity Management in the Internet Economy [electronic Resource]

A Collection of Educational Nature Bulletins
Identity Management
Cultural Competence: A Primer for Educators
Technologies and Applied Solutions
The ACM/IEEE/AIS/IFIP Recommendations for a Complete Curriculum in Cybersecurity

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

Logic Primer presents a rigorous introduction to natural deduction systems of sentential and first-order logic. Logic Primer presents a rigorous introduction to natural deduction systems of sentential and first-order logic. The text is designed to foster the student-instructor relationship. The key concepts are laid out in concise definitions and comments, with the expectation that the instructor will elaborate upon them. New to the second edition is the addition of material on the logic of identity in chapters 3 and 4. An innovative interactive Web site, consisting of a "Logic Daemon" and a "Quizmaster," encourages students to formulate their own proofs and links them to appropriate explanations in the book.

Learn to 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, and cryptographic and persistence services. Deploying Identity and Access Management with Free Open Source Software 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 Why to deploy a centralized authentication and policy management infrastructure Use: SAML for single sign-on, OpenID Connect for web and mobile single sign-on, and OAuth2 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

For almost every organization in the future, both public and private sector, identity management presents both significant opportunities and risks. Successfully managed, it will allow everyone to access products and services that are tailored to their needs and their behaviours. But successful management implies that organizations will have overcome the significant obstacles of security, individual human rights and social concern that could cause the whole process to become mired. Digital Identity Management, based on the work of the annual Digital Identity Forum in London, provides a wide perspective on the subject and explores the current technology available for identity management, its applications within business, and its significance in wider debates about identity, society and the law. This is an essential introduction for organizations seeking to use identity to get closer to customers; for those in government at all levels wrestling with online delivery of targeted services; as well as those concerned with the wider issues of identity, rights, the law, and the potential risks.

Federated Identity Primer
A Primer on Reptiles and Amphibians
Your Special Gift
Enterprise Architecture Patterns
Data Management Technologies and Applications
Deploying Identity and Access Management with Free Open Source Software

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.

Today's economy is fueled by knowledge. Every leader knows this to be true, yet few have systematic methods for converting organizational knowledge into economic value. This book argues that communities of practice--groups of individuals formed around common interests and expertise--provide the ideal vehicle for driving knowledge-management strategies and building lasting competitive

advantage. Written by leading experts in the field, Cultivating Communities of Practice is the first book to outline models and methods for systematically developing these essential groups. Through compelling research and company examples, including DaimlerChrysler, McKinsey & Company, Shell, and the World Bank, authors Etienne Wenger, Richard McDermott, and William M. Snyder show how world-class organizations have leveraged communities of practice to drive strategy, generate new business opportunities, solve problems, transfer best practices, develop employees' professional skills, and recruit and retain top talent. Underscoring the new central role communities of practice are playing in today's knowledge economy, Cultivating Communities of Practice is the definitive guide to fostering, designing, and developing these powerful groups within and across organizations.

Business information systems and business information technology are integral aspects of modern business, and managers in these areas are now expected to have knowledge of human and managerial issues, as well as technical ones. This concise and readable book is a level-by-level primer that addresses the core subjects in business information systems and business information technology to enhance students ' understanding of the key areas. Each chapter begins with a case study and features at the end: a summary of major points, glossary of terms, suggested further reading and student activities. Some areas covered include: Different functional areas of business, including accounting, HRM and marketing Development and implementation of information systems Methods to support the analysis and design of policy and practice Strategic management to align information technology with organizational needs Covering the subject matter in a highly accessible manner, this is an ideal text for both undergraduate and masters students on business information systems, business information technology and business information management courses. This text is supplemented with over 900 detailed powerpoint slides for instructors, accessible via the Routledge Instructor Resource page at http://cw.routledge.com/textbooks/instructordownload/

The Challenge Built to Last, the defining management study of the nineties, showed how great companies triumph over time and how long-term sustained performance can be engineered into the DNA of an enterprise from the verybeginning. But what about the company that is not born with great DNA? How can good companies, mediocre companies, even bad companies achieve enduring greatness? The Study For years, this question preyed on the mind of Jim Collins. Are there companies that defy gravity and convert long-term mediocrity or worse into long-term superiority? And if so, what are the universal distinguishing characteristics that cause a company to go from good to great? The Standards Using tough benchmarks, Collins and his research team identified a set of elite companies that made the leap to great results and sustained those results for at least fifteen years. How great? After the leap, the good-to-great companies generated cumulative stock returns that beat the general stock market by an average of seven times in fifteen years, better than twice the results delivered by a composite index of the world's greatest companies, including Coca-Cola, Intel, General Electric, and Merck. The Comparisons The research team contrasted the good-to-great companies with a carefully selected set of comparison companies that failed to make the leap from good to great. What was different? Why did one set of companies become truly great performers while the other set remained only good? Over five years, the team analyzed the histories of all twenty-eight companies in the study. After sifting through mountains of data and thousands of pages of interviews, Collins and his crew discovered the key determinants of greatness -- why some companies make the leap and others don't. The Findings The findings of the Good to Great study will surprise many readers and shed light on virtually every area of management strategy and practice. The findings include: Level 5 Leaders: The research team was shocked to discover the type of leadership required to achieve greatness. The Hedgehog Concept (Simplicity within the Three Circles): To go from good to great requires transcending the curse of competence. A Culture of Discipline: When you combine a culture of discipline with an ethic of entrepreneurship, you get the magical alchemy of great results. Technology Accelerators: Good-to-great companies think differently about the role of technology. The Flywheel and the Doom Loop: Those who launch radical change programs and wrenching restructurings will almost certainly fail to make the leap. " Some of the key concepts discerned in the study, " comments Jim Collins, "fly in the face of our modern business culture and will, quite frankly, upset some people. " Perhaps, but who can afford to ignore these findings?

A practitioner's guide to securing connected industries

The Cybersecurity Body of Knowledge

Proceedings of the 33rd International Conference on Advanced Information Networking and Applications (AINA-2019)

The Role of Digital Identity Management in the Internet Economy

NEW BUSINESS MODELS AND SUSTAINABLE COMPETITIVENESS

Good to Great

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.

If you create, manage, operate, or configure systems running in the cloud, you're a cloud engineer--even if you work as a system administrator, software developer, data scientist, or site reliability engineer. With this book, professionals from around the world provide valuable insight into today's cloud engineering role. These concise articles explore the entire cloud computing experience, including fundamentals, architecture, and migration. You'll delve into security and compliance, operations and reliability, and software development. And examine networking, organizational culture, and more. You're sure to find 1, 2, or 97 things that inspire you to dig deeper and expand your own career. "Three Keys to Making the Right Multicloud Decisions," Brendan O'Leary "Serverless Bad Practices," Manases Jesus Galindo Bello "Failing a Cloud Migration," Lee Atchison "Treat Your Cloud Environment as If It Were On Premises," Iyana Garry "What Is Toil, and Why Are SREs Obsessed with It?", Zachary Nickens "Lean QA: The QA Evolving in the DevOps World," Theresa Neate "How Economies of Scale Work in the Cloud," Jon Moore "The Cloud Is Not About the Cloud," Ken Corless "Data Gravity: The Importance of Data Management in the Cloud," Geoff Hughes "Even in the Cloud, the Network Is the Foundation," David Murray "Cloud Engineering Is About Culture, Not Containers," Holly Cummins

Having “the talk” can sometimes be an awkward experience for both parent and child. Even so, I didn’t want to wait until my children’s hormones kicked in, and I didn’t want to be caught off guard when they had questions, but most of all, I didn’t want them growing up with misconceptions concerning sex. I wanted my children to be informed about the facts of life, yet without being too sexually explicit in the process, because some of the facts weren’t good such as pornography, diseases, and predators, but these subjects needed to be addressed as well. As a result, I told them what I have written in Your Special Gift, by using the analogy of a gift, a lock, and a key to define commonly used sexual terms, and to caution them about possible consequences, and to warn them of potential predators. I also used Scripture as the basis of defining true love. The simplicity of the gift analogy opens the door of communication between parent and child in an effective straightforward, and yet sensitive way, so that any question concerning sex can be answered by using this method. Your Special

Gift is well-suited for children in the 8-to-12 year-old range.
Managerial styles are influenced by habit, familiarity, and workplace culture. It's no wonder that well-intentioned professionals doing their best to be good organizational leaders often repeat unhelpful supervisory practices experienced in their early careers, even if they disliked them at the time. In the DUH! Book of Management and Supervision, the author disagrees with many accepted leadership principles (unabashedly referring to them as myths) and makes new and different approaches easier to imagine. Her challenging and controversial concepts illustrated with poignant stories suggest common-sense and immediately applicable alternatives more suitable in today's workplace.
Y They Call Me Black
A Primer
A Primer for Policy Makers
Practical Solutions for Recurring IT-Architecture Problems
CCNP Security Identity Management Sise 300-715 Official Cert Guide
Concepts, Technologies, and Systems
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
This primer aims to provide policy makers a broad-brush understanding of the various dimensions of digital identity management (IdM). Consistent with the Seoul Ministerial Declaration, it also aims to support efforts to address public policy issues for securely managing and protecting digital identities, with a view to strengthening confidence in the online activities crucial to the growth of the Internet Economy.
"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.
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.
A Guide to Managing Knowledge
Public Key Infrastructures, Services and Applications
Cultivating Communities of Practice
4th International Conference, DATA 2015, Colmar, France, July 20-22, 2015, Revised Selected Papers
Advanced Information Networking and Applications
Technologies and Frameworks
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-Khouri 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"

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.

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.

The Nature of Risk is a short, beautifully illustrated and easy-to-understand book written to help readers face one of modern life's most important and difficult tasks—confronting risk. Free of complicated theories or formulas, The Nature of Risk relies instead on a simple story featuring a cast of familiar, forest-dwelling animals, each of which embodies a different approach to risk management. At least one of these approaches will seem familiar to every reader—whether they knew they had an approach to risk management or not. Then, as the story unfolds, the strengths and weaknesses of each approach will be revealed through a series of "natural" tests. Finally, at the conclusion of the story, readers will come to a short review section designed to help them frame their first attempts at managing risk—with or without professional help.

Contemporary Identity and Access Management Architectures: Emerging Research and Opportunities

Self-Sovereign Identity

Knowledge Management Primer

Building Secure Systems in Untrusted Networks

Service Quality Management

Zero Trust Networks