File Type PDF Web Services Security

If you ally craving such a referred **Web Services Security** book that will present you worth, get the unconditionally best seller from us currently from several preferred authors. If you desire to hilarious books, lots of novels, tale, jokes, and more fictions collections are in addition to launched, from best seller to one of the most current released.

You may not be perplexed to enjoy all books collections Web Services Security that we will entirely offer. It is not approximately the costs. Its practically what you need currently. This Web Services Security, as one of the most keen sellers here will categorically be among the best options to review.

GYPYFT - LONG GABRIELLE

There are a considerable number of options available to architects and developers when it comes to Web service security. The WEB SERVICE SECURITY guide helps developers and architects make the most appropriate security decisions in the context of the solution's requirements. This asset contains reliable, accurate guidance on how to design and implement secure Web services.

This book is a collection of selected papers presented at the First Congress on Intelligent Systems (CIS 2020), held in New Delhi, India during September 5 – 6, 2020. It includes novel and innovative work from experts, practitioners, scientists and decision-makers from academia and industry. It covers topics such as Internet of Things, information security, embedded systems, real-time systems, cloud computing, big data analysis, quantum computing, automation systems, bio-inspired intelligence, cognitive systems, cyber physical systems, data analytics, data/web mining, data science, intelligence for security, intelligent decision making systems, intelligent information processing, intelligent transportation, artificial intelligence for machine vision, imaging sensors technology, image segmentation, convolutional neural network, image/video classification, soft computing for machine vision, pattern recognition, human computer interaction, robotic devices and systems, autonomous vehicles, intelligent control systems, human motor control, game playing, evolutionary algorithms, swarm optimization, neural network, deep learning, supervised learning, unsupervised learning, fuzzy logic, rough sets, computational optimization, and neuro fuzzy systems.

This publication of the NIST seeks to assist organizations in understanding the challenges in integrating information security practices into SOA design and development based on Web services. This publication also provides practical, real-world guidance on current and emerging standards applicable to Web services, as well as background information on the most common security threats to SOAs based on Web services. This document presents information that is largely independent of particular hardware platforms, operating systems, and applications. Supplementary security mechanisms (i.e., perimeter security appliances) are considered outside the scope of this publication. Interfaces between Web services components and supplementary controls are noted as such throughout this document on a case-by-case basis. The document, while technical in nature, provides the background information to help readers understand the topics that are discussed. The intended audience for this document includes the following: System and software architects and engineers trained in designing, implementing, testing, or evaluating Web services; Software developers experienced in XML, C#, Visual Basic for .NET (VB.NET), C, or Java for Web services; Security architects, engineers, analysts, and secure software developers/integrators; Researchers who are furthering and extending service interfaces and conceptual designs. This document assumes that readers have some minimal Web services expertise. Because of the constantly changing nature of Web services threats and vulnerabilities, readers are expected to take advantage of other resources (including those listed in this document) for more current and detailed information. The practices recommended in this document are designed to help mitigate the risks associated with Web services. They build on and assume the implementation of practices described in other NIST guidelines listed in Appendix F. The remainder of this document is organized into five major sections. Section 2 provides background to Web services and portals and their relationship to security. Section 3 discusses the many relevant Web service security functions and related technology. Section 4 discusses Web portals, the human user's entry point into the SOA based on Web services. Section 5 discusses the challenges associated with secure Web service-enabling of legacy applications. Finally, Section 6 discusses secure implementation tools and technologies. The document also contains several appendices. Appendix A offers discussion of several attacks commonly leveraged against Web services and SOAs. Appendix B provides an overview of Electronic Business eXtensible Markup Language (ebXML), a Web services protocol suite developed by the United Nations Centre for Trade Facilitation and Electronic Business (UN/CEFACT). Appendices C and D contain a glossary and acronym list, respectively. Appendices E and F list print resources and online tools and resources that may be useful references for gaining a better understanding of Web services and SOAs, security concepts and methodologies, and the general relationship between them. Security Division, Information Technology Laboratory, National Institute of Standards and Technology.

"This book's main objective is to present some of the key approaches, research lines, and challenges that exist in the field of security in SOA systems"--Provided by publisher.

This volume illustrates the continuous arms race between attackers and defenders of the Web ecosystem by discussing a wide variety of attacks. In the first part of the book, the foundation of the Web ecosystem is briefly recapped and discussed. Based on this model, the assets of the Web ecosystem are identified, and the set of capabilities an attacker may have are enumerated. In the second part, an overview of the web security vulnerability landscape is constructed. Included are selections of the most representative attack techniques reported in great detail. In addition to descriptions of the most common mitigation techniques, this primer also surveys the research and standardization activities related to each of the attack techniques, and gives insights into the prevalence of those very attacks. Moreover, the book provides practitioners a set of best practices to gradually improve the security of their web-enabled services. Primer on Client-Side Web Security expresses insights into the future of web application security. It points out the challenges of securing the Web platform, opportunities for future research, and trends toward improving Web security.

As more companies are implementing XML based information exchange technologies - so-called web services, security has become a critical issue. This is especially true in the ares of e-commerce. Varions XML based standards have evolved to cater to the security needs of web services, such as XML Encryption (XML ENC), XML Digital Signatures (XML DSIG), and the XML Key Management Specification (XKMS). This book presents detailed information on these and other XML security standards. It goes a step further by demonstrating the practical use of XML security standards, using both the J2EE and the. NET platforms. Alter reading this book, developers will understand what secure web services are and how to implement them.

- Explains security concepts in simple terms and relates these to standards, Java APIs, software products and day-to-day job activities of programmers. - Written by a practitioner who participated in the development of a J2EE App Server and Web Services Platform at HP. - Applied security measures demonstrated on Java APIs - a unique feature of the book.

"Web Security, Privacy & Commerce" cuts through the hype and the front page stories. It tells readers what the real risks are and explains how to minimize them. Whether a casual (but concerned) Web surfer or a system administrator responsible for the security of a critical Web server, this book will tells users what they need to know.

Many techniques, algorithms, protocols and tools have been developed in the different aspects of cyber-security, namely, authentication, access control, availability, integrity, privacy, confidentiality and non-repudiation as they apply to both networks and systems. Web Services Security and E-Business focuses on architectures and protocols, while bringing together the understanding of security problems related to the protocols and applications of the Internet, and the contemporary solutions to these problems. Web Services Security and E-Business provides insight into uncovering the security risks of dynamically-created content, and how proper content management can greatly improve the overall security. It also studies the security lifecycle and how to respond to an attack, as well as the problems of site hijacking and phishing.

This book constitutes the refereed proceedings of the Second International Semantic Web Conference, ISWC 2003, held at Sanibel Island, Florida, USA in October 2003. The 58 revised full papers presented were carefully reviewed and selected from numerous submissions. The papers are organized in topical sections on foundations; ontological reasoning; semantic Web services; security, trust, and privacy; agents and the semantic Web; information retrieval; multimedia; tools and methodologies; applications; and industrial perspectives.

Gain a solid foundation for designing, building, and configuring security-enhanced, hack-resistant Microsoft® ASP.NET Web applications. This expert guide describes a systematic, task-based approach to security that can be applied to both new and existing applications. It addresses security considerations at the network, host, and application layers for each physical tier—Web server, remote application server, and database server—detailing the security configurations and countermeasures that can help mitigate risks. The information is organized into sections that correspond to both the product life cycle and the roles involved, making it easy for architects, designers, and developers to find the answers they need. All PATTERNS & PRACTICES guides are reviewed and approved by Microsoft engineering teams, consultants, partners, and customers—delivering accurate, real-world information that's been technically validated and tested.

* Only up to date book for the latest version of .NET * Concentrates on Web services not general .NET security * Describes the key aspects of Windows Operating System security, Internet Information Services security, and ASP.NET Security, laying the foundation for a complete discussion of Web Services security in the .NET Platform. * Shows how to use the WS-Security W3C specifications for industry – standard authentication, encryption, authorization, Xml signature, attachments and routing with Web Services. * Teaches the reader how to use the new WSE (Web Services Software Development Kit) from Microsoft. * Shows how to integrate Web Services security into the applications developers write with specific working code examples and explanations.

This book constitutes the refereed proceedings of the 22nd Annual IFIP WG 11.3 Working Conference on Data and Applications Security held in London, UK, in July 2008. The 22 revised full papers presented together with 1 keynote lecture and 1 invited talk were carefully reviewed and selected from 56 submissions. The papers are organized in topical sections on access control, audit and logging, privacy, systems security, certificate management, trusted computing platforms, security policies and metrics, as well as Web and pervasive systems.

Mobile Web services offer new possibilities and extraordinary rewards for the mobile telecommunications market. Service-oriented architectures (SOAs) implemented with Web services are fundamentally changing business processes supported by distributed computing. These technologies bring forward the promise of services available at any time, in any place, and on any platform. Through mobile Web services, operators can offer new value-added services for their users, explore new business opportunities and increase revenue and customer retention.This expands the commercial opportunities for developers to promote their applications and enables solutions that work seamlessly across computer and mobile environments. Mobile Web Services is a comprehensive, up-to-date and practical guide to adapting mobile Web services-based applications. The expert author team from Nokia explain in depth the software architecture and application development interfaces needed to develop solutions for these technologies. Mobile Web Services: Architecture and Implementation: Provides a complete and authoritative text on implementing mobile Web services. Describes the mobile Service-Oriented Architecture (SOA) concept. Covers the discovery, description and security of Web services. Explains how to use Simple Object Access Protocol (SOAP) in Web service messaging. Discusses the challenges and possibilities of mobile Web services, and gives case studies to illustrate the application of the technology. Presents the Nokia Mobile Web Services platform. Offers material on developing mobile Web service clients using C++ and Java. This text is essential reading for wireless Web architects, mobile application developers and programmers, software developers, technical officers and consultants, as well as advanced students in Computer Science and Electrical Engineering.

Web services technologies are advancing fast and being extensively deployed in many di?erent application environments. Web services based on the eXt- sible Markup Language (XML), the Simple Object Access Protocol (SOAP), andrelatedstandards,anddeployedinService-OrientedArchitectures(-SOAs) are the key to Web-based interoperability for applications within and across organizations. Furthermore, they are making it possible to deploy appli- tions that can be directly used by people, and thus making the Web a rich and powerful social interaction medium. The term Web 2.0 has

been coined to embrace all those new collaborative applications and to indicate a new, “social” approach to generating and distributing Web content, characterized by open communication, decentralization of authority, and freedom to share and reuse. For Web services technologies to hold their promise, it is crucial that - curity of services and their interactions with users be assured. Con?dentiality, integrity,availability,anddigitalidentitymanagementareallrequired.People need to be assured that their interactions with services over the Web are kept con?dential and the privacy of their personal information is preserved. People need to be sure that information they use for looking up and selecting s- vicesiscorrectanditsintegrityisassured.Peoplewantservicestobeavailable when needed. They also require interactions to be convenient and person- ized, in addition to being private. Addressing these requirements, especially when dealing with open distributed applications, is a formidable challenge.

With the rapid advancement in technology, myriad new threats have emerged in online environments. The broad spectrum of these digital risks requires new and innovative methods for protection against cybercrimes. The Handbook of Research on Network Forensics and Analysis Techniques is a current research publication that examines the advancements and growth of forensic research from a relatively obscure tradecraft to an important part of many investigations. Featuring coverage on a broad range of topics including cryptocurrency, hand-based biometrics, and cyberterrorism, this publication is geared toward professionals, computer forensics practitioners, engineers, researchers, and academics seeking relevant research on the development of forensic tools.

Uncovers the steps software architects and developers will need to take in order to plan and build a real-world, secure Web services system Authors are leading security experts involved in developing the standards for XML and Web services security Focuses on XML-based security and presents code examples based on popular EJB and .NET application servers Explains how to handle difficult--to-solve problems such as passing user credentials and controlling delegation of those credentials across multiple applications Companion Web site includes the source code from the book as well as additional examples and product information

Formal methods have been applied successfully to the verification of medium-sized programs in protocol and hardware design. However, their application to more complex systems, resulting from the object-oriented and the more recent component-based software engineering paradigms, requires further development of specification and verification techniques supporting the concepts of reusability and modifiability. This book presents revised tutorial lectures given by invited speakers at the Second International Symposium on Formal Methods for Components and Objects, FMCO 2003, held in Leiden, The Netherlands, in November 2003. The 17 revised lectures by leading researchers present a comprehensive account of the potential of formal methods applied to large and complex software systems such as component-based systems and object systems. The book makes a unique contribution to bridging the gap between theory and practice in software engineering.

"This book addresses various aspects of building secure E-Government architectures and services; it presents views of experts from academia, policy and the industry to conclude that secure E-Government web services can be deployed in an application-centric, interoperable way. It addresses the narrow yet promising area of web services and sheds new light on this innovative area of applications"--Provided by publisher.

Security Smarts for the Self-Guided IT Professional “Get to know the hackers—or plan on getting hacked. Sullivan and Liu have created a savvy, essentials-based approach to web app security packed with immediately applicable tools for any information security practitioner sharpening his or her tools or just starting out.” —Ryan McGeehan, Security Manager, Facebook, Inc. Secure web applications from today's most devious hackers. Web Application Security: A Beginner's Guide helps you stock your security toolkit, prevent common hacks, and defend quickly against malicious attacks. This practical resource includes chapters on authentication, authorization, and session management, along with browser, database, and file security--all supported by true stories from industry. You'll also get best practices for vulnerability detection and secure development, as well as a chapter that covers essential security fundamentals. This book's templates, checklists, and examples are designed to help you get started right away. Web Application Security: A Beginner's Guide features: Lingo--Common security terms defined so that you're in the know on the job IMHO--Frank and relevant opinions based on the authors' years of industry experience Budget Note--Tips for getting security technologies and processes into your organization's budget In Actual Practice--Exceptions to the rules of security explained in real-world contexts Your Plan--Customizable checklists you can use on the job now Into Action--Tips on how, why, and when to apply new skills and techniques at work

Web services (WS) provide a simple, standardized way to connect applications over the Internet, however they require management of security and other run-time operations to work effectively. Oracle Web Services Manager is a software solution for managing the operations of web services and the interactions between these services. This book explains the business reasons why web services security is required and gives an architectural overview of WS Security for an enterprise. It then provides details about the Oracle Web Service Manager product and how it can be leveraged to address the key security issues of Confidentiality, Integrity, Authentication, and Authorization. Whilst addressing these key issues, the book describes them fully with examples. It ends with a couple of unique features: one is the various options available for a successful deployment and the other is an explanation, in depth, of how the security components work.

"This book collects a complete set of studies addressing the security and dependability challenges of Web services and the development of protocols to meet them. Encompassing a complete range of topics including specifications for message level security, transactions, and identity management, it enables libraries to provide researchers an authoritative guide to a most challenging technological topic"--Provided by publisher.

Praise for Core Security Patterns Java provides the application developer with essential security mechanisms and support in avoiding critical security bugs common in other languages. A language, however, can only go so far. The developer must understand the security requirements of the application and how to use the features Java provides in order to meet those requirements. Core Security Patterns addresses both aspects of security and will be a guide to developers everywhere in creating more secure applications. --Whitfield Diffie, inventor of Public-Key Cryptography A comprehensive book on Security Patterns, which are critical for secure programming. --Li Gong, former Chief Java Security Architect, Sun Microsystems, and coauthor of Inside Java 2 Platform Security As developers of existing applications, or future innovators that will drive the next generation of highly distributed applications, the patterns and best practices outlined in this book will be an important asset to your development efforts. --Joe Uniejewski, Chief Technology Officer and Senior Vice President, RSA Security, Inc. This book makes an important case for taking a proactive approach to security rather than relying on the reactive security approach common in the software industry. --Judy Lin, Executive Vice President, VeriSign, Inc. Core Security Patterns provides a comprehensive patterns-driven approach and methodology for effectively incorporating security into your applications. I recommend that every application developer keep a copy of this indispensable security reference by their side. --Bill Hamilton, author of ADO.NET Cookbook, ADO.NET in a Nutshell, and NUnit Pocket Reference As a trusted advisor, this book will serve as a Java developers security handbook, providing applied patterns and design strategies for securing Java applications. --Shaheen Nasirudheen, CISSP,Senior Technology Officer, JPMorgan Chase Like Core J2EE Patterns, this book delivers a proactive and patterns-driven approach for designing end-to-end security in your applications. Leveraging the authors strong security experience, they created a must-have book for any designer/developer looking to create secure applications. --John Crupi, Distinguished Engineer, Sun Microsystems, coauthor of Core J2EE Patterns Core Security Patterns is the hands-on practitioners guide to building robust end-to-end security into J2EE(tm) enterprise applications, Web services, identity management, service provisioning, and personal identification solutions. Written by three leading Java security architects, the patterns-driven approach fully reflects todays best practices for security in large-scale, industrial-strength applications. The authors explain the fundamentals of Java application security from the ground up, then introduce a powerful, structured security methodology; a vendor-independent security framework; a detailed assessment checklist; and twenty-three proven security architectural patterns. They walk through several realistic scenarios, covering architecture and implementation and presenting detailed sample code. They demonstrate how to apply cryptographic techniques; obfuscate code; establish secure communication; secure J2ME(tm) applications; authenticate and authorize users; and fortify Web services, enabling single sign-on, effective identity management, and personal identification using Smart Cards and Biometrics. Core Security Patterns covers all of the following, and more: What works and what doesnt: J2EE application-security best practices, and common pitfalls to avoid Implementing key Java platform security features in real-world applications Establishing Web Services security using XML Signature, XML Encryption, WS-Security, XKMS, and WS-I Basic security profile Designing identity management and service provisioning systems using SAML, Liberty, XACML, and SPML Designing secure personal identification solutions using Smart Cards and Biometrics Security design methodology, patterns, best practices, reality checks, defensive strategies, and evaluation checklists End-to-end security architecture case study: architecting, designing, and implementing an end-to-end security solution for large-scale applications

A sequential and easy-to-follow guide which allows you to understand the concepts related to securing web apps/services quickly and efficiently, since each topic is explained and described with the help of an example and in a step-by-step manner, helping you to easily implement the examples in your own projects. This book is intended for web application developers who use RESTful web services to power their websites. Prior knowledge of RESTful is not mandatory, but would be advisable.

Rigorously test and improve the security of all your Web software! It’s as certain as death and taxes: hackers will mercilessly attack your Web sites, applications, and services. If you’re vulnerable, you’d better discover these attacks yourself, before the black hats do. Now, there’s a definitive, hands-on guide to security-testing any Web-based software: How to Break Web Software. In this book, two renowned experts address every category of Web software exploit: attacks on clients, servers, state, user inputs, and more. You’ll master powerful attack tools and techniques as you uncover dozens of crucial, widely exploited flaws in Web architecture and coding. The authors reveal where to look for potential threats and attack vectors, how to rigorously test for each of them, and how to mitigate the problems you find. Coverage includes · Client vulnerabilities, including attacks on client-side validation · State-based attacks: hidden fields, CGI parameters, cookie poisoning, URL jumping, and session hijacking · Attacks on user-supplied inputs: cross-site scripting, SQL injection, and directory traversal · Language- and technology-based attacks: buffer overflows, canonicalization, and NULL string attacks · Server attacks: SQL Injection with stored procedures, command injection, and server fingerprinting · Cryptography, privacy, and attacks on Web services Your Web software is mission-critical–it can’t be compromised. Whether you’re a developer, tester, QA specialist, or IT manager, this book will help you protect that software–systematically.

"The largest and most mature of the cloud platforms, AWS offers over 100 prebuilt services, practically limitless compute resources, bottomless secure storage, as well as top-notch automation capabilities. This book shows you how to develop, host, and manage applications on AWS. Amazon Web Services in Action, Second Edition is a comprehensive introduction to deploying web applications in the AWS cloud. You'll find clear, relevant coverage of all essential AWS services, with a focus on automation, security, high availability, and scalability. This thoroughly revised edition covers the latest additions to AWS, including serverless infrastructure with AWS Lambda, sharing data with EFS, and in-memory storage with ElastiCache."--Back cover.

This book constitutes the refereed proceedings of the International Conference on Web Services, ICWS-Europe 2003, held in Erfurt, Germany, in September 2003. The 16 revised full papers included in the book were carefully reviewed and selected for presentation. The papers are organized in topical sections on constructing and running service-oriented architectures, Web service security, configuration and communication, confluence with agent technology and semantic Web enabled Web services, and current and future issues.

This book focuses on web service specification, search, composition, validation, resiliency, security and engineering, and discusses various service specification standards like WSDL, SAWSDL, WSMO and OWLS. The theory and associated algorithms for service specification verification are detailed using formal models like Petrinet, FSM and UML. The book also explores various approaches proposed for web service search and composition, highlighting input/output, parameter-based search, and selection of services based on both functional and non-functional parameters. In turn, it examines various types of composite web services and presents an overview of popular fault handling strategies for each of these types. Lastly, it discusses the standards used for implementing web service security on the basis of a case study, and introduces the Web Service Development Life Cycle (WSDLC), which defines co-operation between several industry partners to develop web services in a more structured way.

Explains how to implement secure Web services and includes coverage of trust, confidentiality, cryptography, authentication, authorization, and Kerberos. You’ll also find details on Security Assertion Markup Language (SAML), XML Key Management Specification (XKMS), XML Encryption, Hypertext Transfer Protocol-Reliability (HTTP-R) and more.

ASP.NET Web API is a key part of ASP.NET MVC 4 and the platform of choice for building RESTful services that can be accessed by a wide range of devices. Everything from JavaScript libraries to RIA plugins, RFID readers to smart phones can consume your services using platform-agnostic HTTP. With such wide accessibility, securing your code effectively needs to be a top priority. You

will quickly find that the WCF security protocols you're familiar with from .NET are less suitable than they once were in this new environment, proving themselves cumbersome and limited in terms of the standards they can work with. Fortunately, ASP.NET Web API provides a simple, robust security solution of its own that fits neatly within the ASP.NET MVC programming model and secures your code without the need for SOAP, meaning that there is no limit to the range of devices that it can work with – if it can understand HTTP, then it can be secured by Web API. These SOAP--less security techniques are the focus of this book.

You know how to build Web service applications using XML, SOAP, and WSDL, but can you ensure that those applications are secure? Standards development groups such as OASIS and W3C have released several specifications designed to provide security -- but how do you combine them in working applications?

Learn to combine security theory and code to produce secure systems Security is clearly a crucial issue to consider during the design and implementation of any distributed software architecture. Security patterns are increasingly being used by developers who take security into serious consideration from the creation of their work. Written by the authority on security patterns, this unique book examines the structure and purpose of security patterns, illustrating their use with the help of detailed implementation advice, numerous code samples, and descriptions in UML. Provides an extensive, up-to-date catalog of security patterns Shares real-world case studies so you can see when and how to use security patterns in practice Details how to incorporate security from the conceptual stage Highlights tips on authentication, authorization, role-based access control, firewalls, wireless networks, middleware, VoIP, web services security, and more Author is well known and highly respected in the field of security and an expert on security patterns Security Patterns in Practice shows you how to confidently develop a secure system step by step.

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.

Learn how to make your .NET applications secure! Security and cryptography, while always an essential part of the computing industry, have seen their importance increase greatly in the last several years. Microsoft's .NET Framework provides developers with a powerful new set of tools to make their applications secure. .NET Security and Cryptography is a practical and comprehensive guide to implementing both the security and the cryptography features found in the .NET platform. The authors provide numerous clear and focused examples in both C# and Visual Basic .NET, as well as detailed commentary on how the code works. They cover topics in a logical sequence and context, where they are most relevant and most easily understood. All of the sample code is available online at . This book will allow developers to: Develop a solid basis in the theory of cryptography, so they can understand how the security tools in the .NET Framework function Learn to use symmetric algorithms, asymmetric algorithms, and digital signatures Master both traditional encryption programming as well as the new techniques of XML encryption and XML signatures Learn how these tools apply to ASP.NET and Web Services security

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

One of the first books to cover Sun Microsystem's new Java Web Services Developer Pack Written by top Sun consultants with hands-on experience in creating Web services, with a foreword from Simon Phipps, Chief Evangelist at Sun Case studies demonstrate how to create Web services with the tools most used by Java developers, including BEA WebLogic, Apache Axis, Systinet WASP, and Verisign