Preface

Editing this book is the outcome of several years of research and publishing in the areas of dependability and security, which are both fields of high importance that are constantly expanding. The application domain is that of Web services, and my most recent work has been targeted toward making sense of the standards and specifications available in this new arena, while at the same time providing security solutions for various distributed applications. Web services are a business-driven technology, as they have arisen out of a need for services on demand and just-in-time integration, to enable the rapid exploitation of market opportunities. The Web service ideology of late binding seems to present the ideal solution, as it enables loosely coupled organizational services to collaborate without any prior transactional history. Integration is abstracted to a new level; that of XML and dependability mechanisms that stem from such specifications are targeted at this particular level of abstraction.

This abstracted approach to integration does have drawbacks however, rooted in the trust and security issues that arise from doing business in such a manner. The security and dependability requirements themselves in the Web Services arena are not new. They have in fact been accompanying distributed computing since its beginnings. There have been more than 30 standards and specifications proposed to address security issues and provide mechanisms for authorization, authentication, confidentiality, integrity, and nonrepudiation. Each of these proposed specifications span across a number of security and dependability related issues. However, despite such a large number of specifications, there appears to be no clear consensus regarding the overall architectural framework. This book is a contribution toward this need.

I received a large number of proposals, which consequently resulted in a large number of potential chapters. I conducted a highly skilled reviewing team composed largely of fellow academics and IT professionals that helped me through the selection process and eventually to narrow it down to the 14 chapters included in the book. Let us have a quick look at the structure of the book.

The book kicks off with the chapter contribution of Padmanabhan and Adarkar. Through a set of core security requirements for Web services, they discuss and compare several mechanisms available for addressing those challenges from current standards to specifications under review. In addition, their attempt to address future trends in the domain of Web service security makes this chapter a very valuable contribution.

Shrideep Pallickara, Geoffrey Fox, et al. discuss how service-oriented architectures are envisaged using Web services. They address a number of specifications and as such provide a valuable insight into some of the core elements of this book.

Barbara Carminati et al. address the issue of Web service composition and discuss the challenges in building large applications from modular pieces of software (Web services). Focusing on dependability, the authors provide an overview of the main security requirements that must be taken into account when composing Web services. In addition, a detailed survey of the related literature and standards relevant to Web services are outlined. Finally, the authors present a proposal for a brokered architecture to support secure Web services composition.

Nick Cook et al. tackle a specific security requirement, that of nonrepudiation, and provide a thorough discussion of the problem of making high-value business-to-business (B2B) interactions nonrepudiable. The chapter presents the design and implementation details of the authors’ novel Web services-based middleware that addresses nonrepudiable interactions using existing Web service standards.
The subject of access control sets off with the contribution of David Chadwick and his chapter on dynamic delegation of access control rights. David enumerates the requirements for delegation of authority, discusses the various implementation and architectural models, and finally highlights the essential elements of such an approach. David’s authority and expertise in the field make this chapter one of the most valuable contributions of the book.

Rafae Bhatti et al., from IBM’s Almaden Research Center, describe and at the same time defend their effort at defining a new access control policy description language for Web services. They make use of some of the current Web services standards and show how their effort can be integrated with existing technologies, such as WS-Policy, to provide a robust, fine-grained mechanism for access control.

We continue our discussion on policies and see how these can potentially govern Web service interactions with the contribution by Clemente et al. Felix provides an evaluation of the ongoing efforts to use semantically rich ontological languages to represent policies for distributed systems, while at the same time highlighting the architectural considerations and implementation aspects of those efforts.

Asuman Dogac et al. conclude the access control part of the book with what is probably the most widely used of the Web service standards, namely XACML and SAML. The authors demonstrate how they can be combined to provide an overall authentication and authorization mechanism and at the same time discuss their pros and cons.

Kostantin Beznosov presents an experience report on designing and implementing an architecture for protecting enterprise-grade Web service applications hosted by ASP.NET. Kosta deploys his invaluable insight into .NET security mechanisms to discuss design patterns and best practices for constructing flexible and extensible authentication and authorization logic for .NET Web Services.

Kaliontzoglou et al. discuss a particular domain, that of e-government, and in this light the authors outline specific requirements for e-government services, interoperability, and security. Their chapter presents three innovative e-government architecture and implementation strategies based on Web service technologies, focusing on their security and interoperability aspects.

Asif Akram presents an industrial-based case study that provides a pragmatic test bed for evaluating Web service technologies against emerging GRID scenarios. The author discusses issues such as state-full interactions, interoperability, integration, and others.

Aisha Naseer and Lampros Stergoulias discuss infrastructural aspects of GRID computing and argue that Grids should be developed using the underlying Web infrastructure and GRID services should be integrated with Web Services using inheritance techniques to produce Grid-supported Web Services.

David Meredith addresses message-level reliability by providing a lot of valuable technical details on WSDL interface style, strength of data typing, and approach to data binding and validation to demonstrate how these have important implications on application security (and interoperability). David shows how these Web service styles and implementation choices must be carefully considered and applied correctly by providing implementation examples and best practice recommendations.

The book concludes with Christian Platz et al. raising quality of service-related concerns. Focusing on general Web services dependability issues while leveraging his expertise and experience in distributed computing, their chapter deals with the various ways of describing, bootstrapping, and evaluating QoS attributes. The chapter addresses a way to bootstrap the most important performance and dependability values.

My main aim is to address both sides of the spectrum; namely, developers that face security requirements in the arena of Web services on a day-to-day basis, as well as academics. As such, I worked tirelessly to maintain the balance between academic research and industrial practice. As a result, the book includes chapters with engaging technical details, as well as thought-provoking ideas from several major IT companies and world-renowned academics.