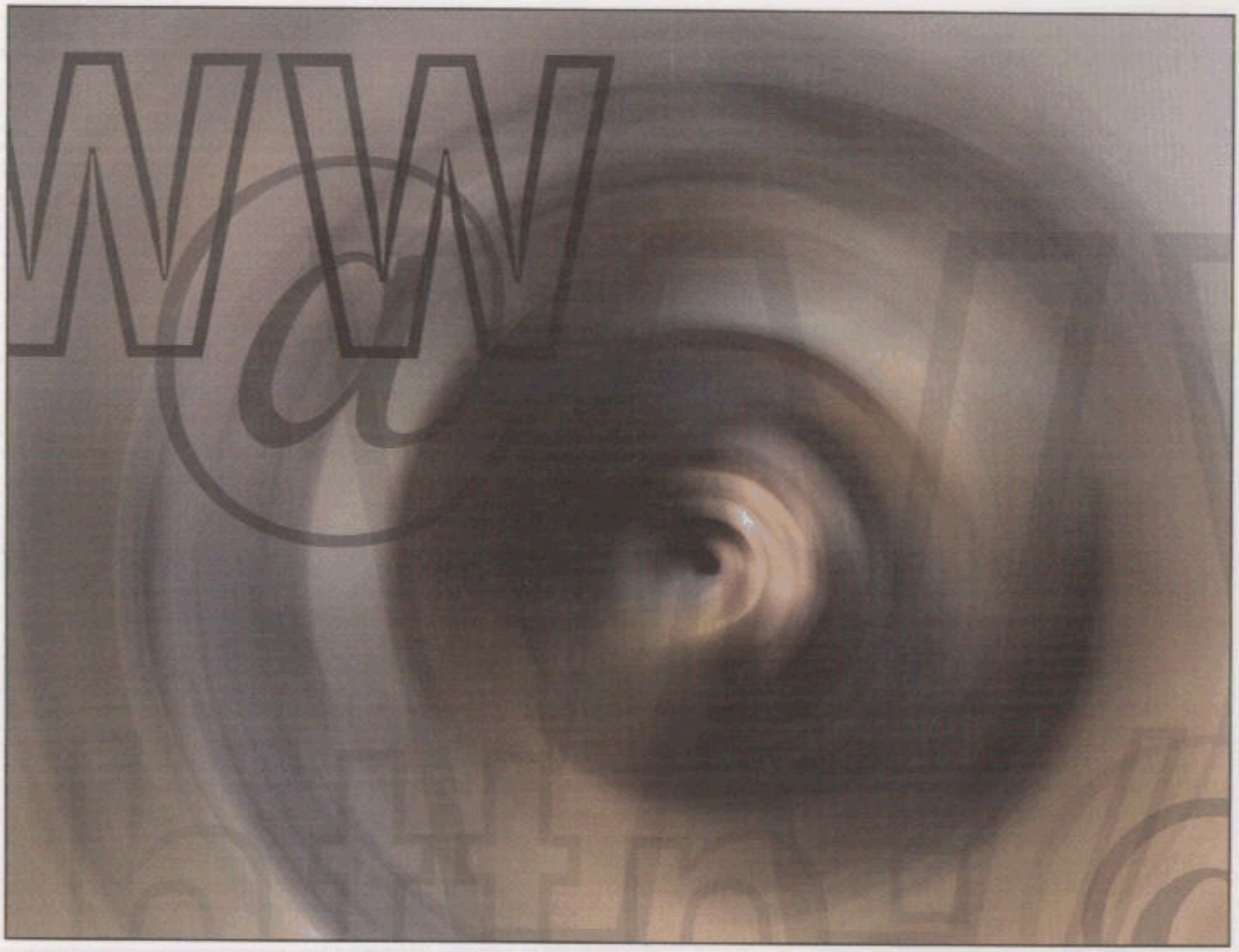
PREMIER REFERENCE SOURCE

SECURING WEB SERVICES

PRACTICAL USAGE OF STANDARDS AND SPECIFICATIONS



PANOS PERIORELLIS

Detailed Table of Contents

Nick Cook et al. tackles a specific security requirement; that of nonrepudiation, and provides 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 contribution 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.

Clemente et al. 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. concludes 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 deployes 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. discusses 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 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.