Preface

The flow of today’s market conditions is continuously changing. Competitive demands from traditional and non-traditional businesses, the rapid appearance and growth of new channels, the rising trend to outsource certain business processes, and the demand to comply with an ever-growing amount of new regulatory and legal requirements, are all creating an increasing demand for change. The effective and efficient management of organizational changes has traditionally been a real challenge. In order to withstand this and to show a profit in the future, organizations will need to develop their capability to sustain a constant state of change and evolution. The capability of an organization’s IT systems to handle this level of change will be a major factor in its success when it comes to adapting to increasingly more dynamic marketplace environments.

Service-Oriented Architecture (SOA) is the main architectural style that IT departments are currently adopting to support the aforementioned business requirements owing to its capacity to enable the loose-coupling and dynamic integration of business services and applications, and their possible operations across trust limits.

Just as organizations’ timely response to changes in the business environment is critical to their survival, so is the appropriate protection of their assets. In the field of IT systems, the main assets are information and IT services, which support the implementation of the business services and must, therefore, handle this information in a secure manner. Securing access to information is thus a critical factor for any business, and security is even more critical for IT deployments based on SOA principles.

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.

It is a valuable resource for senior undergraduate or graduate courses in information security which have a special focus on SOA security. It might also be useful for technologists, managers, and developers who are interested in discovering more about this topic. Its authors are noted researchers in the field of IT security engineering, methodologies, Semantic Web, Web services and SOA.

We shall first provide a general picture of security in Web services and then discuss the contents of the book.

GENERAL PICTURE OF SECURITY IN WEB SERVICES: CHALLENGES AND OBJECTIVES

As was previously mentioned, the SOA paradigm enables organizations to actually fall into line with the current changing business environment requirements. There has consequently been an increasing
adoption of SOA, both in industry and academia, and as a consequence of its main implementation technology: Web services technology.

The security challenges presented by the Web services approach are highly complex and technologically advanced. On the one hand, the security challenges arising from this technology are:

- Risks that appear as a result of the publication on the Internet of a complete and well-documented interface to back office data and company’s business logic. One of the main security problems associated with the adoption of WS is derived from the Internet publication of business interfaces through HTTP or HTTPS ports.
- Protecting the semantic Web by ensuring that security is preserved at the semantic level.
- Context-aware and context-based protection at the document level. Documents usually have information with different “degrees of sensitivity” which it is necessary to protect at different levels of security. Access control policies that govern access to the different security parts of the documents, and an architecture enforcing these policies, currently constitute an extremely important research area in the context of WS security.
- Service trustworthiness. Dynamic discovery and the composition of services imply that a Web service consumer may not know whether the services, either individually or as a whole, will behave as expected. How to select trustworthy Web services consequently remains a challenge.
- The unstructured and overwhelming number of WS security related literature and approaches make the developers’ task of attaining a complete knowledge of all the potential WS security issues, and the standard means to address them, extremely difficult.

On the other hand, some of the main security objectives are:

- Management of security policies in a large and distributed WS environment.
- Application-level, end-to-end and just-one-context-security communications. Network topologies require that end-to-end security be maintained in all the intermediaries in the path of the message. When data is received and forwarded on by an intermediary beyond the transport layer, both the data integrity and any security information that flows with it may be lost.
- Interoperability of the requirements and on-line security elements.
- Ability to federate the full information concerning the subjects, thus permitting single sign-on environments and facilitating across-enterprise interoperability.
- Maintaining sensitive users’ attributes and identity private in trust domains.

**AIMS OF THIS BOOK**

This book aims to provide a theoretical and academic description of Web services security issues, and practical and useful guidelines, models and techniques for implementing secure Web services-based systems in organizations.

The book covers the following topics:

- Security goals, features and requirements specification of Web services-based systems: reviews of approaches toward modelling, analyzing, validating, verifying and documenting security require-
ments for Web services-based systems from both theoretical and practical perspectives will be presented.

- Web services-based security architectures: theoretical and industrial approaches through which to define Web services-security architectures will be covered, and we shall also attempt to cover all potential types of threats, attacks and security requirements.

- Web services-based security standards: an in-depth review of the major international standards related to Web services security will be carried out.

**ORGANIZATION OF THIS BOOK**

This book is divided into four sections, each addressing a state-of-the-art topic in Web services security, and then a fifth containing selected readings. These are as follows: *Web Services Security Engineering, Web Services Security Architectures, Web Services Security Standards* and *Web Services Security Threats and Policies*.

**Section 1: Web Services Security Engineering**

Security engineering integrated into software development is one the major security topics developed during the last few years. Applying security engineering throughout the different steps devised by the different software development methodologies has been a major topic in both scientific and industrial literature.

This section of the book deals with this subject in Chapters 1 and 2.

The first chapter, “Identification of Vulnerability in Web Services Using Model-Based Security” by Sebastian Höhn, Lutz Lowis, Jan Jürjens, and Rafael Accorsi, presents an approach that integrates model-based engineering and vulnerability analysis in order to cope with the security challenges of a service-oriented architecture.

The second chapter, “Security Analysis of Service Oriented Systems: A Methodical Approach and Case Study” by Frank Innerhofer-Oberperfler, Markus Mitterer, Michael Hafnera and Ruth Breu, presents the ProSecO process which is aimed at defining a security model process for security requirement elicitation, security risk evaluation and security control specification, thus providing security analysts with system security state information in both design and production-time.

**Section 2: Web Services Security Architectures**

Web services security architectures should define the highest level organization of the IT security infrastructure necessary to meet the security requirements specified for the systems to be built by articulating the necessary security mechanisms in such a way that reusability, manageability and (internal/external) interoperability is guaranteed.

Section 2 of the book shows different architectural approaches to different security requirements, and consists of five chapters.

Chapter 3, “Ontology-Based Authorization Model for XML Data in Distributed Systems”, by Amit Jain and Csilla Farkas, proposes a framework that preserves authorization permissions on XML data even when its structure changes during transactions. In order for this to occur, the authors define an
authorization framework that permits the specification of authorization requirements from the semantic perspective rather than on the syntactic representation of that information.

Chapter 4, “Secure Service Rating in Federated Software Systems Based on SOA”, by Nico Brehm and Jorge Marx Gómez, deals with the establishment of reputation in federated software systems in which trust evaluation management is de-centralized.

Chapter 5, “Forensics over Web Services: The FWS” by Murat Gunestas, Duminda Wijesekera and Anoop Singhal describes a security Web service whose objective is to store and preserve the evidences yielded from Web services interactions thereby enabling the capability to recreate the composed Web service invocations independent of those parties with a vested interest. This forensic service would facilitate and base later forensic investigations on a reliable infrastructure that could be used in a court of law.

Chapter 6, “Policy-Based Security Engineering of Service Oriented Systems”, by Antonio Maña, Gimena Pujol and Antonio Muñoz, presents a policy-based security engineering process for service oriented applications based on security and dependability patterns. This chapter focuses on the verification of the compliance with security policies, based on the formal specification of security and dependability properties.

Chapter 7, “Security Policies in Web Services”, by Deepti Parachuri and Sudeep Mallick, discusses the different approaches developed in the field of security policies in Web services systems giving a brief overview for each one.

Section 3: Web Services Security Standards

Undoubtedly, the earliest and greatest effort on the subject of Web services security has been that of the definition of the security standards that accomplish all the security aspects that this type of systems must deal with. The main motivation behind this effort is the particular feature that Web services (and their security) should provide: interoperability. This quality aspect is being achieved thanks to the definition of an overwhelming number of standards generated from a diverse set of standardization bodies, consortiums, organizations, etc.

This aspect is covered by Chapters 8 and 9. Chapter 8, entitled “Web Services Security: Standards and Industrial Practice” by Eduardo B. Fernandez, Keiko Hashizume, Ingrid Buckley, Maria M. Larrondo-Petrie, and Michael VanHilst provides an in-depth state-of-the-art review of the existing Web services security standards and their practical implementations.

Chapter 9, entitled “Security in Service Oriented Architectures: Standards and Challenges” by Anne V.D.M. Kayem, reviews current Web services security standards and how they cope with the dynamic nature of the scenarios enabled by Web services technologies.

Section 4: Web Services Security Threats and Countermeasures

This last section of the book covers specific threats and policies inherent to Web services technologies. The main security threats and attacks are exemplified and the countermeasures to, fully or partially, mitigate them are shown.

Chapter 10, “A Survey of Attacks in the Web Services World” by Meiko Jensen and Nils Gruschka, reviews the main types of security attacks on Web services enabled infrastructures and explains the main countermeasures to allow their mitigation at an acceptable level of risk.

Section 5 includes four selected readings.

Carlos A. Gutierrez, Correos Telecom, Spain
Eduardo Fernandez-Medina, University of Castilla – La Mancha, Spain
Mario Piattini, University of Castilla – La Mancha, Spain
June 2009