Chapter III
Secure Web Service Composition: Issues and Architectures

Barbara Carminati
University of Insubria, Italy

Elena Ferrari
University of Insubria, Italy

Patrick C. K. Hung
University of Ontario Institute of Technology (UOIT), Canada

ABSTRACT

Web service security is today receiving growing attention, and enterprises are realizing that effective security management is essential for earning and maintaining trust in their services. One of the major benefits of Web services is that it is possible to dynamically combine different services together to form a more complex service. Also, in this case, security issues are a primary concern. In this chapter, we focus on security issues that arise when composing Web services. We first provide an overview of the main security requirements that must be taken into account when composing Web services. Then, we survey literature and standards related to Web services composition. Finally, we present a proposal for a brokered architecture on support of the secure composition of Web services.

INTRODUCTION

Current trends in information and communication technology are accelerating widespread use of Web services in supporting a service-oriented architecture consisting of services, their compositions, interactions, and management (Papazoglou, & Georgakopoulos, 2003). A Web service is a
secure web service composition
software system designed to support interoperable application-to-application interactions over the Internet. Using a standardized XML messaging system and with the essential characteristic of not being committed to a specific platform or programming language, Web services have achieved, among others, easy communication through the Internet and reduction of cost and time in the framework of enterprise applications. Web services rely on a set of XML standards, such as Universal Description, Discovery, and Integration (UDDI) (OASIS, 2002), Web Services Description Language (WSDL) (World Wide Web Consortium (W3C), 2002b), and Simple Object Access Protocol (SOAP) (World Wide Web Consortium (W3C), 2003). Each service makes its functionalities available through well-defined or standardized interfaces.

One of the major benefits of Web services is that it is possible to dynamically combine different services together to form a more complex service. The result of this approach is a service-oriented architecture (SOA), in which services are fundamental elements that can be independently developed and evolved over time. A SOA consists of services, their compositions, and interactions. Each service is a self-describing, composable, and open software component. In SOA, we typically deal with layers of services, each with a well-defined goal and functionalities. Sometimes a service can be composed as a workflow of other services. In particular, Grid technologies and infrastructures increase the need for sharing and coordinating the use of Web services for different business processes in a loosely coupled execution environment. A business process contains a set of activities that represent both business tasks and interactions between Web services. This feature is very relevant because in the real-world, business processes are often integrated in both intra- and inter-corporate environments. To this purpose, many emerging languages (e.g., BPEL4WS (IBM Corporation, 2002), WSBPEL (OASIS. Web Services Business Process Execution Language) and BPML (Arkin, 2002)) have been proposed for coordinating Web services into a workflow. Additionally, some proposals exist (Kagal, Finin, & Joshi, 2003; Maamar, Mostefaoui, & Yahyaoui, 2005; Milanovic & Malek, 2004) to deal with the composition of Web services, that we survey in the third section. However, security concerns arising during Web service composition have yet to be widely investigated, despite their relevance. In fact, enterprises are realizing that effective security management is essential for earning and maintaining trust in their services. Thus, many enterprises are still having security concerns around adapting and implementing Web services to support their businesses. For this reason, in this chapter, we focus on the security requirements that both Web service requestors and providers may have and that must be taken into account when composing Web services. For instance, a Web service provider may not want to accept requests issued by a specific IP address, or a Web service may require the use of a particular authentication mechanism to participate to the composition. Such constraints must be carefully considered when composing Web services. Constraints are used to specify configurations of the composition that violate specific security requirements of both Web services and Web services requestors.

More precisely, we first discuss security requirements that must be taken into account when composing Web services. Then, we survey related work on Web Service composition, and provide an overview of standards related to Web service composition. Then, the last part of the chapter presents a proposal of a brokered architecture to compose Web services according to the specified security requirements.

SECURITY REQUIREMENTS OF WEB SERVICE COMPOSITION

SOA is built on an insecure, unmonitored, and shared environment, which is open to events such