Chapter 21
Mitigating Security Risks in Web Service Invocations:
Contract-Based Approaches

Gabriele Costa
University of Genova, Italy

Fabio Martinelli
Institute of Informatics and Telematics of CNR, Italy

Roberto Mandati
Institute of Informatics and Telematics of CNR, Italy

Ilaria Matteucci
Institute of Informatics and Telematics of CNR, Italy

Artsiom Yautsiukhin
Institute of Informatics and Telematics of CNR, Italy

ABSTRACT

The pervasiveness of Web services increases the necessity for consumers to access and use them in a secure way. Besides secure communications, consumer security also involves providing strong guarantees that a requested security policy is satisfied. Needless to say, remote services are adverse to most techniques of analysis and control that usually require direct access to either the implementation or the execution. In this chapter, the authors classify service execution paradigms and provide a characterization of the security threats that may affect a Web service infrastructure depending on the elements composing it. In particular, the authors provide a discussion of the threat models for several different Web service paradigms involving service consumers, providers, and platforms, and illustrate how and when contract-based security approaches and its variants can be applied for mitigating risks in service integrations in the identified paradigms.

DOI: 10.4018/978-1-4666-6178-3.ch021

INTRODUCTION

Web services offer various functionalities to its consumers, including data storage, information retrieval, social interaction, and more. A service and its clients interact through specific interfaces defining the syntax and semantics of the exchanged messages (and their parameters). Papazoglou (2007) defines some key roles for Service Oriented Computing; among them, the *service consumer* and the *service provider* are the two most important ones. The two entities share knowledge only about the service interface, i.e., the protocols that they use to communicate. Existing protocols can guarantee security properties, e.g., authenticity and secrecy, on these communications. However, messages can carry complex data or even executable instructions, for example, mobile code, which makes the computation distributed over the involved systems. Needless to say, mobile systems exacerbate the problem of providing security guarantees for both service consumer and provider.

Recently, some proposals highlighted the advantages of including a third entity in services architectures, that is, the *service platform*. In general, a service platform offers support to both consumers and providers. For instance, consumers may ask the platform for information about a service, e.g., its cost and its provider identity. Similarly, providers may obtain support for the orchestration with other services. Clearly, each feature of the platform must be implemented by appropriate components. When consumers and providers interact with a service platform, they implicitly accept it as a trusted entity and they expect it to provide protection against possible misbehaviors. According to its designated purpose, the platform may include support for service publication and discovery, service composition, mobile code signature, and even execution.

In this chapter, we provide a characterization of the security threats which may affect a Web service infrastructure, according to the elements composing it. In particular, we provide a classification of the threat models for different Web service paradigms involving service consumers, providers, and platforms. We consider the consumer point of view and examine three main *resources* in each paradigm: the service *code*, the service *contract*, and the consumer *policy*. Furthermore, we survey techniques that have been proposed for assessing security issues. Then, according to the availability and reliability of the resources, we show how contract-based approaches, such as *Security-by-Contract* and its variants can be applied to guarantee the security of Web services. The result is a precise characterization of the necessary conditions for the application of the security assessment methods for the Web services.

The chapter is organized as follows. The next section provides background information on protection techniques for assessing security aspects in a service-driven environment and presents related work in the area. Next, service composition paradigms considered in this work are discussed followed by an illustration of how and when Security-by-Contract and its extensions can be applied for guaranteeing security. Finally, a discussion about future work and some concluding remarks are presented.

BACKGROUND

Several techniques have been proposed to tackle specific security aspects. These approaches may be combined in security frameworks or used to guarantee the reliability of third-party provided resources. In our context, resources are the service code, the service contract, and the consumer policy.

We assume that each consumer specifies its security requirements, herein referred to as *policies*. A *policy* is a security requirement that a consumer wants to apply to a service execution. In general, consumers want to be sure that their policies will be respected during service execution. A violation happens when a service S behaves in a way that