Chapter 7.16
An Approach for Intentional Modeling of Web Services Security Risk Assessment

Subhas C. Misra
Carleton University, Canada

Vinod Kumar
Carleton University, Canada

Uma Kumar
Carleton University, Canada

ABSTRACT

In this chapter, we provide a conceptual modeling approach for Web services security risk assessment that is based on the identification and analysis of stakeholder intentions. There are no similar approaches for modeling Web services security risk assessment in the existing pieces of literature. The approach is, thus, novel in this domain. The approach is helpful for performing means-end analysis, thereby, uncovering the structural origin of security risks in WS, and how the root-causes of such risks can be controlled from the early stages of the projects. The approach addresses "why" the process is the way it is by exploring the strategic dependencies between the actors of a security system, and analyzing the motivations, intents, and rationales behind the different entities and activities in constituting the system.

INTRODUCTION

The area of *Web services* (WS) has currently emerged as an approach for integrating Web-based applications. To facilitate this, several standards have been proposed, for example, simple object access protocol (SOAP) for data transfer, Web service definition language (WSDL) for providing a description of different available services, and extensible markup language (XML) for tagging data in such a way that users can create their customized applications. In the WS world, information can be transmitted between two service end points using SOAP messages. Security in WS has, therefore, gained importance, as the WS-based systems are susceptible to attacks by malicious users. For example, malicious users have the potential to intrude into the integrity and confidentiality of messages transmitted us-

ing SOAP. Several mechanisms are commonly available to address these security issues. An example is the use of secure socket layer (SSL), and transport layer security (TLS) to provide authentication, integrity, and confidentiality of information. Transport layer security can be provided using IPSec. Several pieces of literature are available in the area of architecting secured WS-based systems. A recent example is the work done by Gutierreze et al. (Gutierrez, Fernandez-Medina, & Piattini, 2005), who proposed an architecture-based process for the development of WS security. This process helps in identifying, defining, and analyzing the security requirements of a WS-based system using an architecture approach. Recently, different researchers have explored model-based assessment of security risk. (Alghathbar, Wijesekera, & Farkas, 2005; Dimitrakos, Ritchie, Raptis, & Stolen, 2002; Fernandez, Sorgente, & Larrondo-Petrie, 2005; Lodderstedt, Bastin, & Doser, 2002; Lund, Hogganvik, Seehusen, & Stolen, 2003; Swiderski & Snyder, 2004; Villarroel, Fernandez, Trujillo, & Piattini, 2005).

Fletcher et. al. (1995), Labuschangne (1999), and Martel (2002) have advocated that the field of security risk analysis has evolved through three generations. The *first generation* of risk analysis techniques date back to those associated with the advent of centralized mainframes. A brief overview of them can be had from Martel's thesis (Martel, 2002), and Labuschagne's paper (Labuschagne, 1999). Most of these approaches are checklist based, ad hoc, and assume that the risk scenarios are static and they do not change. There are different commercial tools available that support these ad hoc approaches (e.g., @RISK, and RiskPAC (Labuschagne, 1999)).

The *second generation* of risk analysis tools and techniques emerged with the growth of LANs, and distributed computing. COBRA Risk Consultant (COBRA, 2005) and Tivoli Secure Way Risk Manager (TSRM) (Tivoli, 2005) are two examples. While the former supports ISO 17799 compliant risk analysis, the later supports enterprise-wide risk management, whereby organizations are able to correlate security information from different sources in an enterprise. The second generation of the risk analysis techniques and tools are concerned more with the combined effects of threats rather than individual elements of threat. These techniques and tools attempt to view security from a holistic viewpoint of equipment, software, and data.

The *third generation* is what we have currently. Today security is no longer limited to local area networks, and individual standalone networks and data. Current security needs are cross-organizational because of interorganizational communication via the Internet, and extranets for organization-to-organization communication. Today data of one enterprise is transmitted over several third-party networks. Additionally, there are new types of attacks that emerge everyday. Martel (2002) provides an approach for risk analysis of current day security issues. She proposed a model wherein a global risk value is dynamically determined for a specific asset/exposure pair with the changes in the environment. Discussions of other such third-generation risk analysis approaches can be found in Swiderski and Snyder (2004) Dimitrakos et al. (2002), Lund et al. (2003), Lodderstedt et al. (2002), Fernandez et al. (2005), Villarroel et al. (2005), and Alghathbar et al. (2005). They are not individually elaborated over here, but most of them work based on dataflow diagramming and UML profiling approaches. These approaches help to address "what" the requirements are, and not "why" those requirements are needed. A critical comparative analysis has been done by rigorous review of the different existing pieces of literature, the summary of which is listed in Table 1.

In this chapter, we present a new approach for modeling information systems security risk assessment. The approach is based on the analysis of the strategic dependencies between the actors of a system. The purpose of this chapter is to