A Case Study in the Role of Trust in Web Service Securities

Pauline Ratnasingam
University of Central Missouri, USA

INTRODUCTION

The Internet, a rapidly expanding global computer and communication infrastructure, has facilitated the emergence of digitization and globalization that in turn has permitted businesses to extensively engage in foreign investments. The reasons for using the Internet include: first considerably reducing the coordination costs involved in inter-organizational transactions. Second, business partners from remote locations are able to communicate and coordinate together using Web services and finally, the widespread adoption of open standards on the Web has greatly reduced the complexities thereby providing flexibility in conducting inter-organizational transactions. According to Forrester Research, e-commerce in the U.S. will grow at 19% reaching $230 billion by 2008. Today firms are attempting to attain their value chain goals by offering and selling products and services in an increasingly competitive market environment. Given the uncertainties of online transactions, Web services encourage the creation of institutional structures for online exchange relationships. Building upon the notion of institutional structures, this chapter examines the role of technology trust that develops through governance mechanisms and provides structural assurances that in turn enhance relationship trust thereby reducing and mitigating risks in Web services.

Security has always been a concern for businesses engaged in digitization and globalization. IT managers need to ensure that their corporate computing infrastructure is able to deliver unaltered content, verify transactions, ensure privacy, maintain confidentiality, and ensure that information is used appropriately. Cavello and Merkhofer (1994) define risk as *"the possibility of an adverse outcome, and uncertainty over the occurrence, timing or magnitude of that adverse outcome."* Perceived risks have been negatively associated with transaction intentions (Jarvenpaa, Tractinsky, & Vitale, 2000), inter-organizational partnerships (Leverick & Cooper, 1998), and joint ventures. Web server security risks can occur either internally or externally and can be primarily human or non-human (technology). The risks can be accidental or intentional and are caused by the disclosure, destruction, and modification of Web transactions, or by denial of service attacks that lead to availability problems and the violation of confidential data. For example, unauthorized access can be accomplished by impersonating or masquerading someone with valid rights. Previous research in Internet-based e-commerce have pointed towards the lack of security, as there are still problems with eavesdropping, password sniffing, data modification, spoofing, repudiation, snooping, misuse, theft, and corruption of information (Bhimani, 1996; Drummond, 1995; Kaeo, 1999; Stallings, 1999; Stewart, 1998). Further, viruses that cause physical risks in Web services may be derived from adding new nodes with hubs or concentrators with either the hardware or software based on sniffing capabilities.

This chapter aims to examine the role of trust on risks in Web services. As such, the research question is: How and why can trust impact risks in Web services? In the next section, we discuss the role of the Web service architecture and its impact on technology trust, relationship trust, and risks in Web services. Then we describe the case study research method followed by background information of a firm that uses e-services for their business operations and present the findings. Finally, we conclude the chapter with lessons learned, future trends and contributions to theory and practice.

BACKGROUND

The Web Services Architecture

Web services are creating a service oriented architecture that provides technical solutions for e-collaborations among value chain partners (Chan, Kellen, & Nair, 2004; Yen, 2004). Mohan (2002) defines Web services as a new breed of Web applications as "self-contained, selfdescribing modular applications that can be published, located and invoked across the Web." Businesses use existing software components specified as services to perform business operations in a "service-oriented architecture." We define Web services as *"modular Internet-based business functions that perform specific business tasks to facilitate business interactions within and beyond the organization."* Others have defined Web services as a software system designed to support interoperable machine-to-machine interactions over the Internet. Most of these definitions imply the importance of technology. Another important element of Web services often not emphasized is the importance of maintaining trust among business partners.

Without getting too technical, the Web services architecture is made up of three layers of technology. At the foundation, (the bottom layer) is the software standards and communication protocols that provide a common language for Web services and enables applications to be connected. The service grid (the middle layer) provides a set of shared utilities from security to third-party auditing, and to billing and payment so that critical business functions and transactions over the Internet can be conducted. This layer publishes the services that serve as entry points for queries to find service descriptions. In short, the service grid plays two roles. First, it helps the Web service requestors and providers to find and connect with one another, and second, it creates a trusted environment essential for carrying out mission-critical business activities, thereby contributing to technology trust. Finally, the top layer consists of a diverse array of application services. It is in this top layer where the day-to-day operations will be most visible to employees, customers, and trading partners. The top layer performs the service binding and invocation. Similarly, previous research discusses three layers of Web services namely; basic services, composite services, and managed services. While basic services manage the publication, discovery, selection, and binding, composite services facilitate the coordination, conformance, monitoring, and quality of service. Finally, managed services provide the market certification rating and operations support.

Table 1 presents the three layers of the Web services architecture adapted from Hagel and Brown (2001).

Table 1. The Web services architecture

Top Layer: Application service Web services runs on any application platform as long as it has a web server connected to the Internet.
Middle Layer: Service Grid The service grid layer provides four types of utilities: (1) Service management utilities (including provisioning, monitoring, ensuring quality of service, synchronization, conflict resolution); (2) Resource knowledge management utilities (including directories, brokers, registries, repositories, data transformation); (3) Transport management utilities (including message queuing, filtering, metering, monitoring, routing, resource orchestration); and (4) Shared utilities (including security, auditing, and assessment of third party performance, billing and payment).
Bottom Layer: Software Standards and Communication Protocols Software standards include: (1) Web Service Description Language (WSDL) to describe the Web service; (2) Universal, Description, Discovery and Integration (UDDI) to advertise, syndicate as a central organization for registering, finding, and using Web services); (3) Web Services Flow Language (WSFL) to define work flows; (4) XML (format for data exchange and description); and (5) Communication protocols including Simple Object Access Protocol (SOAP) to communicate that are for calling Web services, HTTP, and TCP/IP).

Related Content