Chapter 14

Behavioral Attestation for Web Services Based Business Processes

Masoom Alam  
Institute of Management Sciences, Pakistan

Mohammad Nauman  
Institute of Management Sciences, Pakistan

Xinwen Zhang  
Samsung Information Systems America, USA

Tamleek Ali  
Institute of Management Sciences, Pakistan

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

Quratulain Alam  
Institute of Management Sciences, Pakistan

ABSTRACT

Service Oriented Architecture (SOA) is an architectural paradigm that enables dynamic composition of heterogeneous, independent, multi-vendor business services. A prerequisite for such inter-organizational workflows is the establishment of trustworthiness, which is mostly achieved through non-technical measures, such as legislation, and/or social consent that businesses or organizations pledge themselves to adhere. A business process can only be trustworthy if the behavior of all services in it is trustworthy. Trusted Computing Group (TCG) has defined an open set of specifications for the establishment of trustworthiness through a hardware root-of-trust. This paper has three objectives: firstly, the behavior of individual services in a business process is formally specified. Secondly, to overcome the inherent weaknesses of trust management through software alone, a hardware root of-trust devised by the TCG, is used for the measurement of the behavior of individual services in a business process. Finally, a verification mechanism is detailed through which the trustworthiness of a business process can be verified.
1. INTRODUCTION

Service Oriented Architecture (SOA) with underlying technologies like web services and web service orchestration facilitates smooth interaction among independent, multivendor data sources and legacy applications running on heterogeneous platforms across distributed information networks. Such interactions require intelligently interfaced application software and dynamic integration with other connected cooperative environments. As a result, more applications and services have been deployed which bring new businesses and pervasive information sharing.

With these trends, the paradigm of SOA opens new vistas for businesses in the form of dynamic collaborations, where services comprise unassociated, loosely coupled units of functionality and call to other services are not embedded in them. This means that there are no hardcore calls to each other in their source code. Instead a number of protocols are defined that describe how these services can pass and parse messages. These protocols e.g., Business Process Execution Language (BPEL) (Weerawarana, 2005) define the patterns based on which these service calls are composed to form a business process.

Services provide interface to the individual components of a software. However, abstracting the internals behind a single interface makes SOA more prone to security vulnerabilities. For example, it is extremely difficult to verify that an electronic health record or credit card number input into a service is updated or used in a trustworthy way. A prerequisite for the realization of SOA based inter-organizational workflows is the establishment of trustworthiness. However, according to current best practices, trustworthiness is mostly achieved through nontechnical measures such as legislation, or social consent that businesses, or organizations simply pledge themselves to adhere. All existing approaches for secure composition of business processes are focused on the issues of authentication and authorization only. Authentication and authorization are primarily concerned with the verification of service identity and checking permissions for calling a specific service.

Existing approaches for secure composition of business processes (Bertino, 2001), (Gudes, 1999), (Huang, 1999), (Wainer, 2003), (Anderson, 2002) do not take the behavior of individual services into account while composing business processes. Behavioral attestation of a service is concerned with the question that whether a service is consuming the input in a trusted way and as a result producing the trusted output or not. It is a third dimension that goes well beyond the traditional view of authentication and authorization.

We have laid down the following three requirements for the behavioral attestation of business processes. Firstly, a framework is needed that can explicitly specify the behavior of individual services in a business process. A formal means of specification helps to abstract the complex details of the underlying hardware and software.

Secondly, a mechanism is needed that can measure the dynamic behavior of services in a trustworthy way. Existing approaches for platform protection through software alone – by their very principle – are uncompromising and have inherent weaknesses (Pearson, 2002), (Grawrock, 2006), (Alam, 2007). Trusted Computing Group (TCG) has taken a quantum leap in security, “a hardware root of trust”, which provides secure storage for data and cryptographic keys. Remote attestation is an essential characteristic of Trusted Computing that provides a hardware supported evidence in enciphered form that a trusted environment actually exists on a remote platform (Pearson, 2002), (Grawrock, 2006). This feature can be used in reporting the behavior of a service to a remote authority. However, existing approaches for the realization of remote attestation measure