Association for Information Systems
AIS Electronic Library (AISeL)

PACIS 2007 Proceedings

Pacific Asia Conference on Information Systems (PACIS)

2007

Selecting Web Services with Security Compliances: A Managerial Perspective

Khaled Md Khan
Qatar University, k.khan@qu.edu.qa

74. Selecting Web Services with Security Compliances: A Managerial Perspective

Khaled Md Khan
Department of Computer Science and Engineering
Qatar University
k.khan@qu.edu.qa

Abstract

This paper proposes a framework of a decision support system (DSS) for the assessment process of selecting Web services with security compliances consistent with the enterprise business goal. The proposed DSS framework is a systematic assessment model which could aid IS managers in making decision on which Web services would most likely meet the security requirements of their information systems. The proposed process is based on the standard ISO/IEC 15408, the Common Criteria for Information Technology Security Evaluation. The framework consists of five components: (i) Identification of security objectives; (ii) Formulation of criteria; (iii) Selection of candidate Web services; (iv) Security profiling of Web services; and (v) Variance analysis engine. The framework is presented with a running example to demonstrate the applicability of the approach.

Keywords: Decision support systems, Web services, security properties, security assurances, security properties.

Introduction

With the rapid development of Web services, security has become an important issue for information systems (IS) managers in distinguishing the successful and secure integration of Web services with their enterprise systems. Security is one of the determining factors that could contribute to the effectiveness of Web services. The dynamic integration of enterprise systems with third-party Web services calls for security assurances consistent with the enterprise business goal. Ensuring security of Web services is beyond the control of IS managers, however, they can determine the selection of Web services which could likely satisfy their security requirements. Selecting third-party Web services arbitrarily over the Internet is a critical and challenging task because of their dynamic and unpredictable nature. Transactions with Web services are very important for enterprise systems to ensure that a set of security properties is satisfied. Web services with unknown security assurances can cause critical transactional problems to the enterprise information systems. The information systems can suffer unacceptable levels of performance degradation if the system is not integrated with the right Web services. Secure and effective integration of third-part Web services into enterprise systems is a major research challenge.

The increasing recognition of security problems involved with third-party Web services, there is a need for at least a semi-automatic decision support system (DSS) for the selection of Web services with required security assurances. The IS managers could use such a DSS to select appropriate Web services consistent with the required security attributes of their enterprise information systems. The complex nature of the selection process of secure Web services might not be envisioned without a DSS support. With the rapid evolving nature of security contexts in the field of enterprise systems, decision support systems for selecting secure Web services can play an increasingly important role.

This paper proposes an architecture of an easy-to-use decision support system (DSS) for selecting Web services with security compliance consistent with the enterprise business goal. The architecture consists of five components: (i) *Identification of security objective*; (ii) *Formulation of criteria*; (iii) *Selection of candidate Web services*; (iv) *Security profiling of Web services*; and (v) *Variance analysis engine*. The proposed architecture makes an attempt to aid the IS managers as a tool in making their decisions for selecting appropriate Web services which could deliver the required security services for their enterprises. It would also help the IS managers to include security features to their business systems if they find that a Web service does not offer all required security services. Enterprises can deploy such DSS on the top of their application for selecting the Web services.

The paper is organized as follows. Next section briefly describes the background and the context of the topic including a quick summary of the key existing work related to this area. Section 3 presents the architecture of the proposed DSS framework with running examples. Section 4 closes the paper with a conclusion.

Background

During the process of using Web services for the enterprises, IS managers engage in decision making - the act of selecting from alternative Web services available in the market. It is not enough that managers only assess the business functionalities that Web services provide for their organizational needs, rather, they have to actively consider the security implications of using third-party Web services. It is unrealistic to expect by the IS managers that a Web service addresses all security requirements of all enterprises in all execution environments. It is not realistic either to expect such universal capability of a Web service. It is, therefore, necessary for the IS managers to select and decide suitable Web services which could likely meet their specific enterprise-wide security requirements. This definitely demands a systematic approach in the decision making process. A decision support system could assist managers such systematic approach of selecting suitable Web services.

In the current practice, IS managers have little choice but to use Web services without properly evaluating the security properties of third-party services. This may lead to potential compromise to the enterprise-wide security requirements. Consequently, this risky practice often results to degradation of system security. This practice virtually forces IS managers to take undue risks in order to achieve services. Generally speaking, most IS managers have neither the time nor resources to examine the security properties of candidate Web services. The best alternative for the IS managers is to use decision support systems which could significantly improve the selection process of secure Web services.

The security requirements that a business system requires may not comply with the available security profiles provided by a candidate Web services. In the assessment process if a critical security feature appears to be weak, additional security functions could be designed and applied to the enterprise system. Without a well defined process, the selection of best Web services along with required security properties is not always accomplished by a straight forward analysis.

A thorough browse of related literature suggests that a very few research works on this area have been reported in the public forum. Most works tend to focus on how to make secure Web services or how to make the enterprise systems more secure. Some notable papers propose various models (Berinto 2005, Payne 2002, Swanson *et al.* 2003, Foundstone 2003) for security metrics. A scheme for assessing security properties of software components has been reported in (Khan *et al.* 2006). The paper claims that the assessment scheme provides a

numeric score indicating a relative strength of the security properties of the candidate component. The FoundScore (2003) is a security metric that can be used as a guide to measure the risk and the business value of expenditures to information security. FoundScore is a security rating system that compares security aspects of an organization against best practices in order to quantify the security risk. The approach assesses vulnerabilities and risk of an organization, and calculates the cost for the security measures taken to address the identified vulnerabilities and risks.

A seven-step methodology has been proposed in (Payne, 2001) to guide the process of defining security metrics. The approach basically yields an understanding of the purpose of the security metrics program, its deliverables, and how, by whom and when these deliverables will be provided. Berinto (2005) has recently reported on five security metrics. It argues that a constant measure of security incidents is a great indicator of the security posture, and it could be used to quantify the efficiency of the deployed security functions.

National Institute of Standards and Technology (Swanson, 2003) defines security metrics guide for information technology systems. The document provides guidance on how an enterprise through the use of metrics identifies the security needs, security controls, policies and procedures. The approach guides management of an organization in deciding where to invest in security.

The architecture

To address the issues highlighted in the previous sections and to aid the IS managers in their decision making process, we propose an architecture of a security decision support system consisting of five components as depicted in Figure 1. This section elaborates each of these five components and the associated tasks related to the Web service selection process in the following sub sections.

Identification of security objective

Before using a Web service, an enterprise first decides the functionality that it needs from the Web service. After determining the required *functionality* based on the need of the enterprise business, this component captures enterprise-wide security requirements and assurances. An example of a business functionality could be: *analyzes patients' pathological data* in a health care system. The security requirements related to this functionality may be determined based on the threats, vulnerabilities and risk associated with this functionality. Information processed (input, output) by the identified functionality needs to be analyzed from a business point of view in order to identify the threats, risks and/or vulnerability. The threats could be disclosure of patients' data to unauthorized entity, illegal modification of patients' data etc. The selection of candidate web services is based on the security threats identified in this component.

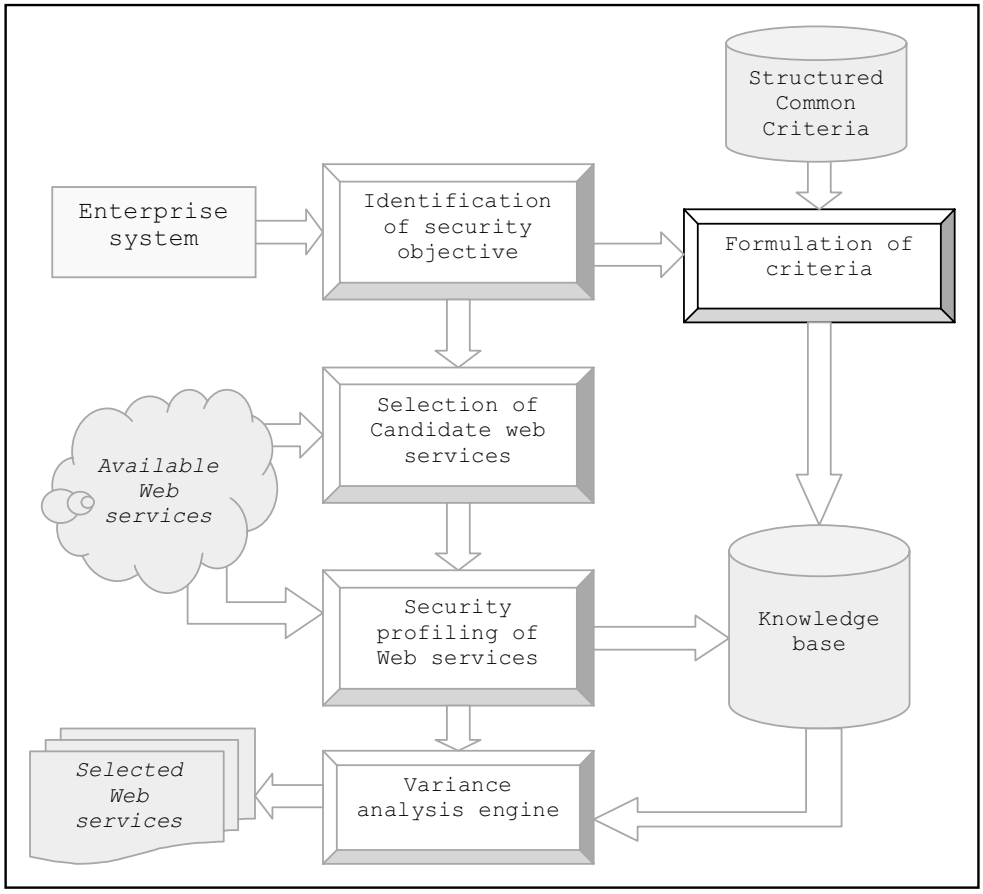

Figure 1. A Decision Support System for Selecting Secure Web Services

The high level security requirements are defined to withstand the identified risks and threats. A high level security requirement does not spell out the actual implemented security functions. In our example, a high level security requirement could be *confidentiality of patient data.* Based on this discussion, three associated tasks are defined in the process:

- Identify *business functionality* needed by the enterprise system
- Analyze *threat*, risk, vulnerability
- Define *high level security objective* of the system.

These tasks are the part of the Web service selection process. The IS manager initiates these tasks, and the outcomes are fed to this component. To clarify these three tasks further, let us consider the following scenario. Assume that a system running at a general medical practitioner's (we refer it a GP system) office needs a service of analyzing its patients' pathological data. The GP system sends the patients' pathological data to the Web service. The Web service analyzes the data and provides a diagnosis report to the GP system. Several independent Web services can provide this service to the GP system. We also assume that a hostile entity (a person, or a software) makes constant attempts to intercept the messages exchanged between the GP system and the Web service which analyzes the pathological data. The hostile entity makes sense out of the data exchanged between the Web service and the GP system. It also attempts to modify the intercepted patient data, and re-transmits the altered data to GP system. The threats in this case can be defined as: attempting to *steal* and *alter* patients' data with malicious intent. Based on this scenario, we can develop a template to capture the output of the three tasks as follows:

Business functionality:
- *Analyzes patients' pathological data*

Threat:
- *Patients' data can be disclosed to the unauthorized entity* and modified illegally

High level security objective:
- *Confidentiality and integrity of patients' data.*

The template is populated with data by the IS manager based on the identified functionality, threats, and the high-level security objectives. This component loads the template in an internal database for later processing.

Formulation of criteria

This component spells out the high level security objective into more measurable terms. It defines the criteria for the security objective in a structured form. In our example, several key issues need to be addressed if we want to check the conformity of *confidentiality and integrity of patient data*. For instance, if the confidentiality is achieved by means of *encryption*, then next issues are what would be the suitable *length of the key*, which *key generation algorithm* would be used and so on. These could be the specific criteria to check whether a Web service could provide the required functionality with the desired level of confidentiality of patient data.

The structure and the elements of security criteria can be defined based on ISO/IEC Standard 15408, the Common Criteria for Information Technology Security Evaluation (CC) (Common Criteria 1999). The Common Criteria (CC) provides evaluation measures of security by means of a common set of requirements of the security functions of a system, and a set of evaluation measures. The entire approach is quantitative, and it describes the security behavior of functions expected of an information system. CC gives a comprehensive catalogue of high level security requirements and assurances for information systems products. CC consists of eleven 'classes' for generic grouping of similar types of security requirements: security audit, communication, cryptographic support, user data protection, identification and authentication, security management, privacy, protection of system security functions, resource utilization, system access, and trusted path and channels. Following tasks are required to provide input data to this component:

- Identify the appropriate security class consistent with the security objective, its associated security functions and properties from the structured Common Criteria
- Formulate the criteria.

We analyze our example and define the criteria as follows.

Identify the security class:
User data protection.
Encryption, digital signature(patient data)

In this example, the high level security objective is related to the class *user data protection* defined in CC. *Encryption* and digital signature are the security functions used to ensure data confidentiality and integrity.

Formulate Criteria:
Encryption, digital signature(patient data, 128-bit, RSA)

This criteria specifies that the patient data needs to be encrypted with a 128 bit key using

RSA algorithm to ensure the confidentiality of data. It also specifies that the digital signature must be used in order to preserve the integrity of patient data. The knowledge base is populated with the defined criteria.

Selection of candidate Web services

This component identifies the candidate Web services that would likely meet the required functionality as well as the security requirements of the enterprises. At this stage we do not check the conformity of the criteria defined in the previous component. We select only those Web services which can provide the desired functionality and support the identified security objectives. In our example, we identify only those Web services which could: (i) *analyze the patients*' data; and (ii) support *confidentiality and integrity of patient data*. Assume we identify three independent Web services; WS1, WS2, and WS3 which could likely provide the same business functionality *analyze the patients'* data.

Security profiling of Web services

This component gathers information regarding the security properties of the candidate Web services, we call it *security profiling.* In this component, security properties of each candidate Web service are collected from the published security claim, available user's guide, and from enquiries. This profiling process enlists all security properties supporting the claimed security function of each Web service. The security functions and the associated security properties supported by each candidate Web service are structured and mapped into same format as security criteria have been formulated earlier. The security profiles are stored in the knowledge base. Assume, we have characterized the security properties of the three candidate Web services as follows:

WS1: encrypted(patient data, 256-bit, RSA)
WS2: (patient data)
WS3: encryption, digital signature(patient data, 256-bit, RSA)

WS1 does encrypt the patient data, and the key length is 256, greater than the required length, using RSA, but it does not provide digital signature.
WS2 does not provide any security functions.
WS3 provides encryption with 256 bit key using RSA encryption algorithm. It also offers digital signature with the patient data.
The next component of this framework variance analysis engine compares the profiles of these three candidate Web services with the defined security criteria stored in the knowledge base.

Variance analysis engine

This component compares the enterprise-wide security criteria with the extracted security properties of the candidate Web services collected in the previous component. Inference rules are applied to compute the deviation between the security criteria and the security profiles of the candidate Web services. In our example, the variance engine will find WS3 consistent with the security requirements of the GP system.
In a security decision support system, a rule based approach is applied with the data such as name of the functionality, related high level security objectives, security criteria, and the collected security properties of candidate Web services. Inference engine can identify the right Web service which could most likely satisfy the set security requirements. Security properties can be reasoned about with the use of inference rules of the logic programming. Rules make inference with the security criteria associated with each Web service and the required security of the enterprise system. The criteria are analyzed from the point of view of

the enterprise system that participates in a composition with a Web service. The inference rules are applied to prove whether security criteria for a Web service are satisfied or not. Logic programming is used as a formal reasoning tool to check the conformity between the security criteria and the security profiles. The simple structure of logic program allows us to represent complicated form of security knowledge and their properties.

The components of the proposed DSS need input from the IS managers. Some of the information required by the tool is based on subjective assessment of various data such as the security profiles of a Web service. It also requires some investigation by the IS managers to gather security information of candidate Web services. The formulation of criteria is a semi-automatic process because it requires significant intervention from the managers in order to reflect the desired conditions to test a security function. The variance analysis engine could be implemented as an automatic process provided that the inference rules and the axioms are well defined to reason about a security profile against a set of security criteria.

Future directions and conclusion

This paper has presented a framework for a decision support system for selecting Web services with appropriate security assurances. The paper argues that the selection process of appropriate Web services for the enterprise application needs an automatic tool support such as DSS. The approach could be automated to aid enterprise decision support systems. This can be used in strategic planning of information systems as well.

We plan to implement the proposed approach as a prototype in order to test its applicability. We are currently evaluating some existing tools such as *smodels* and *lparse* (Syrjanen 2000) which could be utilized as the supporting components of the DSS in order to facilitate the inference mechanisms. The approach can be further expanded to select Web services with other non-functional properties such as usability, maintainability, reusability etc.

References

Berinto, S. "A Few Food Metrics", CIO-Asia Magazine, September, 2005.

Common Criteria (1999). ISO/IEC 15408. Common Criteria for Information Technology Security Evaluation. NIST, USA, http://csrc.nist.gov/cc/, June.

Foundstone. "Information Security Metrics", White paper, Foundstone Strategic Security, April 2003.

Khan, K., Han, J. "Assessing Security Properties of Software Components: A Software Engineer's Perspective", In proceedings of the Australian Software Engineering Conference, April, IEEE Computer Society, 2006.

Payne, S. "A Guide to Security Metrics", SANS Institute, 2002.

Swanson, M., Bartol, N., Sabato, J., Hash, J., Graffo, L. "Security Metrics Guide for Information Technology Systems", National Institute of Standard and Technology (NIST), Special Publication 800-55, July 2003.

Syrjanen, T. Lparse 1.0 User's Manual. University of Helsinki, 2000.