

The Conceptual Design and Implementing Web Services Security Framework for Ministry of Information and Communication Technology in Thailand

Pakpoom Prechapanich *, Prasong Praneetpolgrang **, Nutsapun Paopun+

* Master of Business Administration

(Electronic Commerce) Graduate School, Sripatum University

61 Phaholyothin Rd., Jatujak 10900 Bangkok, Thailand

Email : prechapanich@gmail.com

** Master of Science

(Information Technology) Graduate School, Sripatum University

61 Phaholyothin Rd., Jatujak 10900 Bangkok, Thailand

Email : prasong@spu.ac.th

+ Master of Business Administration

(Electronic Commerce) Graduate School, Sripatum University

61 Phaholyothin Rd., Jatujak 10900 Bangkok, Thailand

Email : nutsapun@spu.ac.th

Abstract: This research aims to present a Web Services Security Framework for Ministry of Information and Communication Technology (MICT) in Thailand as referred to international standard BS7799 on information security management. With a pilot development of web services which based on e-government, the researcher used Ministry of Information and Communication Technology as a case study. In order to understand the developmental pilot, it's crucial to realize particularly in web services security and to determine proposed or existing system. Finally, it can be as standard guideline for Thai public organization for developing web services security framework.

Keywords: Web Services, Security, BS7799, ISMS.

I. Introduction

Today, Internet and information technology have played important role widely overall fields. It's obvious that related security system has been increasingly interested by public. Progressively, public affair service has been developed into e-government where major technology applied is Web Services. A medium for inter-exchanging data and services which security system is needed inevitably to protect valued data of user account. In this research, web service security framework has been devised by researchers utilizing Ministry of Information and Communication Technology in Thailand as a case study. The purpose of study is to examine and establish Web Services Security Framework for Ministry of Information and Communication Technology, and to assess security system of existing Web Services in Ministry of Information and Communication Technology under developed security framework.

The applied research as a government institution case study is based on BS7799 [8], an universally acceptable standard; data management standard for security, where its requirement covers overall performance procedures in both

data access and storage in organization. This aims to develop security framework applicable to reality performance and applied to other divisions in the same direction usefully.

Since the study is focused on management practices other than technical support. The deliverable results are technical and administrative web services security framework. The appropriation of security framework has been inspected by auditing expertises and referred to research literature in framework for web services security [4,5,6], web services security theory [1,2,3,13,14], web services standard [9,10,15] and information framework [12]. The study is designed to determine if existing and potential web services are somewhat to be have security maintained. In addition to continue development to acquire future integral information.

II. Review of Related Standard and Framework

II.1 BS7799 [8]

This British Standard has been prepared for business managers and their staff to provide a model for setting up and managing and effective Information Security Management System (ISMS). The adoption of and ISMS should be strategic decision for an organization. The design and implementation of an organization's ISMS is influenced by business needs and objectives, resulting security requirements, the processes employed and the size and structure of the organization. These and their supporting systems are expected to change over time. It is expected that simple situations require simple ISMS solutions.

This British Standard can be used by internal and external parties including certification bodies, to assess an organization's ability to meet its own requirements, as well as any customer or regulatory demands.

II.2 Associated Web Services Standards [1]

Various techniques were developed to solve the problems faced in web services regarding how to make it interoperable,

distributable, integratable, and so on. Some of these techniques were proposed by industry giants and became standards over time. We will look at a few of these standards.

XML

One of the emerging concerns of web-based programmers was how to transmit data across HTTP networks in an interoperable manner. XML emerged as an interoperable format. XML typically is stored as easily as readable text files. XML documents have a structure that can be parsed to quickly turn data into other formats, for example for database storage. Many vendors of storage products, such as database storage products, have enhanced their products to easily handle the XML formats. Standards have been developed for the structure of XML for messaging use. XML has enjoyed widespread adoption and adaptation, which quickly has made it the messaging standard.

RPC, XML-RPC, and SOAP

Remote object accessing technology began with the standard RPC calls, in which method could be invoked from one application to another remote one. The limitation of the RPC was that it work on connection-oriented, communication protocols, which cannot be used with the connectionless protocols used in the Internet.

Firewalls were another fundamental problem in the RPC systems. To use the RPC system on required protocol-specific filters with additional software, configuration, and additional management. The XML-RPC evolved in the process of solving these problems.

Another standard that emerged immediately after the XML-RPC was the SOAP. This defines the structure of message to be communicated across the Internet between a web service client and a host. SOAP emerged due to the problem of firewalls being primarily configured to access objects via HTTP. SOAP does not replace RPC, as it includes the SOAP-RPC and SOAP document styles, which is why it is the preferred HTTP-based message protocol.

WSDL

A web services is published for other to discover it and then use it. To be able to use it one needs to describe it, provide details for using it, and place it under the right category, similar to the Yellow Pages. The WSDL standards were developed to fulfill this requirement by creating a standard way of capturing the service description. In this, a service is described in terms of the operations (that is, input/output messages) and a set of interactions between a service provider and a service requestor. It describes the interface of how to interact with the service. The name of the service and a list of operations and their bindings make up the XML-based WSDL file.

From a security point of view, one should keep in mind that this is a plaintext file in ASCII, UTF-8, or some base64-encoded format.

UDDI

Web services needed a way to present a company's information in a manner that compared their features equally. Using search engines for this purpose was not the most efficient means of allowing business to interoperate with each other at a web services level, and as a result the UDDI directory of web services emerged.

The UDDI is a registry service project that provides a means for business hosting a web services to register with the worldwide registries. The project is focused on assisting business in finding each other by allowing the registration of a web services and the searching of registries to locate specific web services based on a number of criteria. The UDDI is not linked directly to any other standards initiatives or standards groups. However, it does take advantage of groups that provide standards and initiatives within the web services industry.

COBIT framework [12]

COBIT has been developed as a generally applicable and accepted standard for good Information Technology (IT) security and control practices that provides a reference framework for management, users, and IS audit, control and security practitioners.

COBIT, issued by the IT Governance Institute and now in its third edition, is increasingly internationally accepted as good practice for control over information, IT and related risks. Its guidance enables an enterprise to implement effective governance over the IT that is pervasive and intrinsic throughout the enterprise. In particular, COBIT's Management Guidelines component contains a framework responding to management's need for control and measurability of IT by providing tools to assess and measure the enterprise's IT capability for the 34 COBIT IT processes.

III. Research Design

This research has developed web services security framework. Ministry of Information and Communication Technology in Thailand was selected as sample, for its core matter for conducting e-government which major goals and responsibility of Ministry of Information Technology and Communication are maintained and achieved.

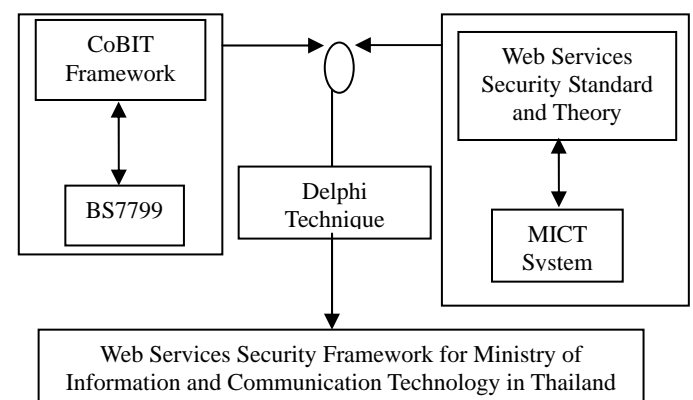


Figure 1: Conceptual design

As illustrated in Figure 1, on the left box is to determine jointing point between COBIT framework and BS7799. When they are applied to Ministry of Information and Communication Technology Web Services, the illustration as shown at the right box. Linkage of left and right box is to determine Web Services Security framework for Ministry of Information and Communication Technology in Thailand.

IV. Research Methodology

This research was applied research with referred to acceptably international standard for creating actually applied framework, or furthered development applied to other related fields in similar way.

Collected data is adopted from secondary data source; research literature, and a wide range of related technical articles and textbooks.

Another data collecting method used was Delphi Technique, which relevant expertise's opinions have been gathered to complement framework.

V. Preliminary Results

According to survey and collect data, we found that web services-related major responsibility of Ministry of Information and Communication Technology is to be navigator in e-government development through web services means, accountable for XML, SOAP, UDDI and WSDL web services creation in preparing process. Thus, the framework outcome is followed as;

1. Interchange or table of connection between requirement of BS7799 and security according to XML, SOAP, UDDI and WSDL.
2. Create ISMS document as specified in table of connection referred to BS7799
3. Add ISMS further information according to COBIT framework
4. Requirement based on BS7799 such as
 - 4.1 Security policy
 - 4.2 Organizational security
 - 4.3 Asset classification and control
 - 4.4 Personnel security
 - 4.5 Physical and environmental security
 - 4.6 Communications and Operations management
 - 4.7 Access control
 - 4.8 Systems development and maintenance
 - 4.9 Business continuity management
 - 4.10 Compliance

In addition, ISMS document used "Plan-Do-Check-Act" (PDCA) model, Plan (establish the ISMS) Do (implement and operate the ISMS) Check (monitor and review the ISMS) Act (maintain and improve the ISMS) and follows as;

- 1 Scope
- 2 Normative reference

- 3 Terms and definitions
- 4 Information security management system
- 5 Management responsibility
- 6 Management review of the ISMS
- 7 ISMS improvement

VI. Conclusion

The result indicated merely piloting development for actual application. Since BS779 requirement is considerably detailed, its connection to web service standard is impossible for all BS7799 detailed requirement. In addition, web service technology has been developed continuously and technically, along with increasingly additional new versions, specialized expertise is needed. Concerning to management and web service security, technical and managerial collaboration is necessary to allow effective regulation.

Framework created has been covered only web service on basic standard and operation by Information and Communication Technology, and not covered overall web service technology and system security modality.

BS7799 has been developed more strictly and progressed to new version of standard ISO27001, including to web service technology as significant element in future information technology. Additional standard prototypes should be given further attention to be researched and created so that they can be applied or established to web service standard particularly.

References

- [1] Galbraith, Ben., Hankison, Whitney., Hiotis, Andre., Janakiraman, Murali., Prasad, D.V., Traivedi, Ravi., Whitney, David., & Motukuru, Vamsi. (2002). *Professional Web Services Security*. United States: Wrox Press.
- [2] O'Neill, Mark., Baker, Phillip H., Cann, Sean M., Shema, Mike., Simon, Ed., Watters, Paul A., & White, Andrew. (2003). *Web Services Security*. Berkeley, California: McGraw-Hill.
- [3] Bret Hartman, Donald J. Flinn, Konstantin Beznosov & Shirley Kawamoto. (2003). *Mastering Web Services Security*. United States: Wiley Publishing.
- [4] J.Thelin & P.J.Murray. 2002. "A Public Web Services Security Framework Based on Current and Future Usage Scenarios" Proceedings of the International Conference on Internet Computing : Paper 1039IC.
- [5] Hristo Koshutanski. 2003. "An Access Control Framework for Business Process for Web Services" Proceeding of the 2003 ACM workshop on XML security. p15-24
- [6] Chen Li & Claus Pahl. 2003. "Security in the Web Services Framework" Proceeding of the 1st international symposium on Information and Communication Technology, ISICT'03. p481-486.
- [7] Daniel W K Tse. 2004. "Security in Modern Business Security Assessment Model for Information Security Practices". Proceeding of the Pacific Asia Conference of Information Systems, p.1506-1519.
- [8] British Standards. BS7799-2:2002. Information security management systems-Specification with guidance for use.
- [9] World Wide Web Consortium. *Web Services Framework*.<http://www.w3.org/2002/ws>.
- [10] OASIS Security Services TC. *Security Assertion Markup Language (SAML)*. OASIS, November 2002. <http://www.oasis-open.org/committees/security/>.
- [11] John Wallhoff. 2004. "Combining ITIL with COBIT and ISO/IEC 17799:2000" Scillani Information AB. <http://www.scillani.com>.

- [12] Information System Audit and Control Association. COBIT, <http://www.isaca.org/>.
- [13] Bob Atkinson, ET AL. Web Services Security (WS-Security). IBM, Microsoft, Verisign, April 2002. <http://www.106.ibm.com/developer/works/webservices/library/ws-secure/>.
- [14] Kreger, H.. Web Services conceptual Architecture (WSCA 1.0), May 2001. <http://www-3.ibm.com/software/solutions/webservices/pdf/WSCA.pdf>.
- [15] OASIS Advancing e-Business standards since 1993. Web Services Security (WSS) TC. <http://www.oasis-open.org/committees> .