Asian Journal of Information Technology 7 (5): 226-231, 2008
ISSN: 1682-3915

Integrated Security Architecture for Web Services and this Challenging

Marzouk S. Mokbel and Le Jiajin
School of Computer Science and Technology, Donghua University, China

Abstract: Web Services has emerged as a dominant paradigm for constructing and composing distributed business collaborations over the web. The focus of this study is propose the main challenges for securing Web Services and summarizes emerging standards of web services security mechanisms. Security is one of the major concerns when developing mission critical business applications and this concern motivated the Web Services Security specifications. This study puts forward a kind of Current Security Mechanisms for Web Services and Security in a Web Services World Proposed Architecture and Roadmap, which includes secure communication protocol, authentication, Signature, Encryption, Authorization and Transport Security etc. It provides Strong ways to protect information for Browser/Server applications.

Key words: Web Services, XML, XKMS, SAML, XACML, WS-Security, kerberos

INTRODUCTION

Web services are a widely touted technology that aims to provide tangible benefits to both business and IT. Their increasing use in the enterprise sector for the integration of distributed systems and business critical functions dictates the need for security assurance yet there is currently no security testing methodology specifically adapted to applications that implement web services.

The potential risks of deploying this technology should concern every security professional that might have to deal with them. Network defenses require new protection layers to block the numerous security holes that Web Services usually leave open.

There are many security challenges, among them are Security pertaining to Web service requestors, Web services security should be independent of the underlying communication protocols. Authentication mechanisms This is needed in order to allow the mutual authentication of service provider and a service invoker to verify their identities. End-to-end message content security and not just transport-level security… etc. These security challenges are an expression of real world Web services security requirements that need to be addressed by any Web service security model that is to be considered as being a comprehensive security solution.

WS-Security is flexible and is designed to be used as the basis for the construction of a wide variety of security models including PKI, Kerberos and SSL. Specifically WS-Security provides support for multiple security token formats, multiple trust domains, multiple signature formats and multiple encryption technologies. On the other hand WS-Security provides mechanisms for securing a single envelope.

In this study we will present some Security mechanisms for web services these mechanisms can be used independently to pass a security token or in a tightly coupled manner for example signing and encrypting a message or part of a message and providing a security token or token path associated with the keys used for signing and encryption.

In addition, this study will depict a Standard methodology for web services security and outline a process that can be adopted to appraise web services security throughout the development lifecycle.

The Core security mechanisms like XKMS, SAML, WS-Security and (XML Signature and XML Encryption) are directly integrated into XML, thus making fine-grained integrity protection, data origin authentication and selective field confidentiality available to all applications which use XML for data storage and exchange.

The Web Services Security (WS-Security) Architecture and Roadmap describes Microsoft's strategy for addressing security within a Web service environment. It defines a comprehensive Web service security model that supports, integrates and unifies several popular security models, mechanisms and technologies (including both symmetric and public key technologies) in a way that enables a variety of systems to securely interoperate in a platform and language-neutral manner. It describes scenarios that show how the following specifications might be used together. This family of specifications delivers on this roadmap.

Corresponding Author: Marzouk S. Mokbel, School of Computer Science and Technology, Donghua University, China

This study gives a brief overview of the key technologies in the arena of Web services and the relevant security technologies. In the body of the article description the Web services and his benefits ease of use make the adoption of Web Services a foregone conclusion.

SECURITY CHALLENGES SPECIFIC TO WEB SERVICES

The security challenges presented by the Web services approach are formidable and unavoidable. Many of the features (GSWS, 2006) that make Web services attractive, including greater accessibility of data, dynamic application-to-application connections and relative autonomy (lack of human intervention) are at odds with traditional security models and controls .

Web service security presents many more challenges than securing a typical enterprise application, there are a number of challenges that standards organizations are currently addressing-particularly in the area of Web services discovery and reliability. In the following, we address some of these challenges in order:

- End-to-end message content security and not just transport-level security.
- Authorization policies are more difficult to write as environments become more loosely coupled.
- Methodologies for Secure Web Services.
- Clients and services do not have a way to negotiate their mutual constraints and capabilities before interacting.
- Securing Web services infrastructure needs XML's granularity.
- Candidate technology: Technology solutions that can be used to address security threats and risks associated with this challenge.
- Multiple security token formats.

CURRENT SECURITY MECHANISMS FOR WEB SERVICES

Web Services Security is a message-level standard that is based on securing SOAP messages through XML digital signature, confidentiality through XML encryption and credential propagation through security tokens. The Web services security specification defines the core facilities for protecting the integrity and confidentiality of a message and provides mechanisms for associating security-related claims with the message. In this part we will discuss some Security mechanisms of web services.

XKMS: The XML Key Management Specification (XKMS) (SWSC, 2003) initiative was jointly developed by VeriSign, Microsoft and WebMethods as an open standard to simplify the securing of XML-based Internet transactions using PKI and digital certificates. The ability to secure all Web Services communications and transactions is critical for the success of Web Services in the enterprise. XKMS describes protocols for distributing and registering public keys, suitable for use in conjunction with the standards for XML Signature and XML Encryption. XKMS helps overcome PKI complexity by allowing Web services to become clients of a key management service. A key objective of the XKMS protocol design is to minimize the complexity of client application implementations by shielding them from the complexity and syntax of the underlying PKI used to establish trust relationships. The XKMS comprises two parts, the XML Key Information Service Specification (X-KISS) and the XML Key Registration Service Specification (X-KRSS).

The XML Key Management Specification (XKMS) (XACML, 2003) offers a simplified approach to integrating public key management capabilities with applications. However, enterprises and vendors must still create the infrastructure necessary to manage keys and secure data within the enterprise for the long term.

SAML: The Security Assertion Markup Language (SAML) (FIM, 2005) is an open message standard that encodes security assertions and corresponding protocol messages in XML format. SAML currently defines authentication, authorization and attribute assertions; furthermore, SAML specifies a request-response-protocol which can be used by the service provider to request assertions from the identity provider. A binding defines how SAML protocol messages are to be transmitted using SOAP over HTTP and profiles determine how SAML can be used by standard web browsers. SAML also provides flexible extension mechanisms; e.g., it can be used with the eXtensible Access Control Markup Language (XACML) to achieve fine-grained access control as it has been done in the area of Grid Computing.

In addition, the SAML standard includes descriptions of the use of SAML assertions in communication protocols and frameworks. These so-called profiles contain protocol flows and security constraints for applications of SAML.

SAML defines three kinds of statements that can be carried within an assertion:

- Authentication-confirms that the holder of this claim was authenticated in some way at a defined time.

- Attribute-the subject is associated with the given attributes and values.
- AuthorizationDecision-response to an access request, whether the access has been granted or denied.

XACML: The OASIS eXtensible Access Control Markup Language [XACML] is a powerful, standard language that specifies schemas for authorization policies and for authorization decision requests and responses. It also specifies how to evaluate policies against requests to compute a response (SAML, 2005). XACML defines three top-level policy elements: <Rule>, <Policy> and <PolicySet>.

XACML provides a necessary component for complex, interactive Web services, enterprise wide security management and DRM. Using XACML, an enterprise can define platform-independent rules for how its resources are used by those inside and outside the enterprise. Enterprises can work together without having to align their computing platforms (whether based on Java. NET or another technology); they just have to align their access policies. By allowing each to examine the access control policies of the other, XACML can foster a certain level of trust between enterprises even without prior contact (XACML, 2003).

XML signature and XML encryption: XML (eXtensible Markup Language) provides a standard for structuring information and data in a standard form. The World Wide Web Consortium (W3C) XML Signature and XML Encryption standards provide mechanisms for harnessing the strengths of XML in applications with cryptographic requirements. These XML security standards developed by W3C allow XML content to be signed and encrypted. Because all SOAP messages are written in XML, Web service developers can sign or encrypt any portion of the SOAP message.

WS-Security: WS-Security (WSS, 2002) was developed as an extension of the SOAP standard, describing a mechanism for using XML Encryption and XML Digital Signature to secure SOAP messages. Each secure messaging option has its own strengths and weaknesses.

WS-Security supports, integrates and unifies several popular security models, mechanisms and technologies. WS-Security aims at enabling applications to construct secure SOAP message exchanges. This specification provides a flexible set of mechanisms that can be used to construct a range of security protocols.

In addition, WS-Security provides mechanisms for encrypting and signing elements of a SOAP message including any WS-Security tokens. WS-Security explains how to use the XML Signature (XML DSig) and XML

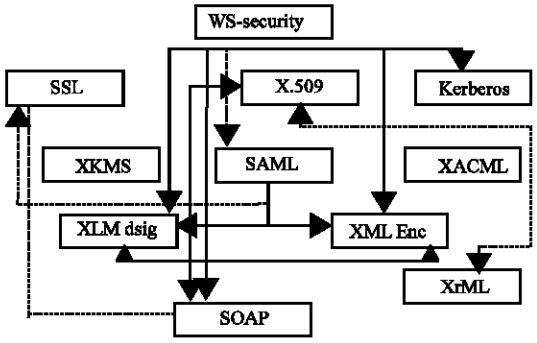

Fig. 1: View The WS-Security specification model

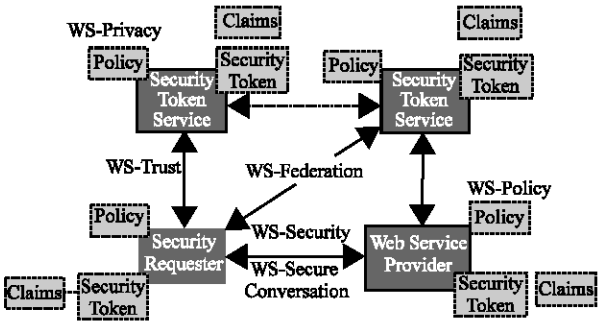

Fig. 2: Relationship between the Web Service Provider and Security Requester

Encryption (XML Enc) specifications within SOAP messages and what headers and elements are necessary to correctly process the ciphertext (GSWS, 2006).

In Fig. 1 view The WS-Security specification defines new SOAP extensions (message headers) to provide per-message authentication and describes how to attach signature and encryption headers to SOAP messages. Also, it describes how to attach security tokens, including binary security tokens such as X.509 certificates and Kerberos tickets, to messages.

The model in Fig. 1, has been chosen to facilitate combining of end-point, the following consequences flow from the model. The first we can show WS-Security is Refer to Composite standard, the WS-Security defines a set of SOAP header extensions for end-to-end SOAP messaging security. It supports message integrity and confidentiality by allowing communicating partners to exchange signed encrypted messages in a Web services environment, XKMS is the Public-key infrastructure -An XML protocol that allows a simple client to obtain key information (value, certificate, management, or trust data) from a Web service. It also describes protocols for distributing and registering public keys, suitable for use in conjunction with the standards for XML Signature and XML encryption. XrML and XACML Access control of

the process which Appearing in the plan. The Task of the Technologies for securing representation on the SAML, Kerberos and X.509 is Security tokens (authentication assertions). Assignment of the XML Enc, XML Dsig and SSL is Confidentiality and integrity information, finally the SOAP Working Role is transport message.

SECURITY IN A WEB SERVICES WORLD PROPOSED ARCHITECTURE AND ROADMAP

The security strategy expressed here and the WS-Security specification introduced below provide the strategic goals and cornerstone for this proposed Web services security model (SWSW, 2002). Figure 2 shows the relationship between the Web Service Provider and Security Requester, the basic security elements are illustrated in the Fig. 2.

WS-Security: WS-Security describes enhancements to SOAP messaging to provide quality of protection through message integrity and message confidentiality. As well, this specification defines how to attach and include security tokens within SOAP messages.

WS-Security provides profiles that specify how to insert different types of security tokens in WS-Security headers: Username token profile, X.509 certificate token profile, Kerberos token profile, SAML token profile, REL token profile, XCBF token profile.

WS-Secure conversation: WS-Secure Conversation will describe how a Web service can authenticate requester messages, how requesters can authenticate services and how to establish mutually authenticated security contexts.

WS-Policy: Describes the capabilities and constraints of the security (and other business) policies on intermediaries and endpoints (e.g. required security tokens, supported encryption algorithms, privacy rules).

WS-Trust: WS-Trust defines means for establishing trust relationships between entities. These trust relationships can either be established directly or brokered, in which case a trust proxy is used in order to request security tokens based on WS-Policy information.

WS-Privacy: WS-Privacy can be used to communicate privacy policies created by organizations for their Web services also it Will describe a model for how Web services and requesters state privacy preferences and organizational privacy practice statements.

WS-Authorization: WS-Authorization is a standard for authorization data and policy management for Web Services on another hound it describe how to manage authorization data and authorization policies.

WS-Federation: Finally, WS-Federation defines how trust relationships are managed in a heterogeneous security environment.

RELATING WEB SERVICES SECURITY TO TODAY'S SECURITY

This Web services security model is compatible with the existing security models for authentication, data integrity and data confidentiality in common use today. As a consequence, it is possible to integrate Web services-based solutions with other existing security models:

Transport security: Existing technologies such as secure sockets (SSL/TLS) can provide simple point-to-point integrity and confidentiality for a message. The Web Services security model supports using these existing secure transport mechanisms in conjunction with WS-Security (and other specifications) to provide end-to-end integrity and confidentially in particular across multiple transports, intermediaries and transmission protocols.

PKI: The primary function of a PKI is to allow the distribution and use of public keys and certificates with security and integrity. A PKI is a foundation on which other applications and network security components are built.

A PKI enables the basic security services for such varied systems as:

- SSL, IPsec and HTTPS for communication and transactional security
- S/MIME and PGP for email security
- SET for value exchange
- Identrus for B2B

PKI does not serve a particular business function; that some benefits of PKI and its use of public key cryptography offers for e-commerce and other organizations are as follows:

- Reduces transactional processing expenses.
- Reduces and compartmentalizes risk.
- Enhances efficiency and performance of systems and networks.
- Reduces the (Sun- PSSM, 2001) complexity of security systems with binary symmetrical methods.

Kerberos: Kerberos (KTH-KRB, 1999) is a system for authenticating users and services on a network. It is built upon the assumption that the network is unsafe. For example, data sent over the network can be eavesdropped and altered and addresses can also be faked. Therefore they cannot be used for authentication purposes.

The Kerberos V5 protocol is now on a standards track with the IETF. The implementation of the protocol in Windows Server, 2003 closely follows the specification defined in Internet RFC 1510. In addition, the mechanism and format for passing security tokens in Kerberos messages (Kerberos, 2003).

In a Kerberos system, there is a designated site on each network, called the Kerberos server, which performs centralized key management and administrative functions. The server maintains a database containing the secret keys of all users, authenticates the identities of users and distributes session keys to users and servers who wish to authenticate one another. Kerberos requires trust in a third party. If the server is compromised, the integrity of the whole system is lost. Public-key cryptography was designed precisely to avoid the necessity to trust third parties with secrets. Kerberos is generally considered adequate within an administrative domain; however across domains the more robust functions and properties of public-key systems are often preferred.

INTEGRATED SECURITY ARCHITECTURE

Most security professionals would agree on the fact that a layered security solution is the most appropriate means to protect the network and that the firewall is the cornerstone of a layered security solution. Layered security, also call defense in depth, leverages multiple security technologies to protect the network-if one fails to stop the attack; it should be caught by one of the supporting layers. Layered security can be deployed in one of 2 ways (ISG, 2005).

Many system architectures fail to adequately design-in and/or implement security functionality. Too often architectures only consider functional capabilities during initial development. Critical operational capabilities such as security, performance and management are often retrofitted into the original operation as the system approaches production readiness. This approach leads to disjointed and inconsistent security capabilities that negatively impact other functional and operational characteristics.

Physical security: The primary objective in developing a security program is to render industrial espionage ineffective by implementing appropriate security measures. Realistically, it's extremely difficult to reach a level of security that is 100% foolproof. However, proper steps should be taken to reduce every possible security breach. This involves an approach incorporating extensive protective measures-from personnel screening and training to electronic systems applications.

Essentially, security efforts will be a state of mind as much as the application of countermeasures. Every member of the organization has an important role to play in safeguarding company assets-especially those processes that are particularly sensitive and critical.

A well-planned security program will encompass a number of efforts, with special attention paid to many of the following aspects: Screening and background checks for personnel; training security professionals and in-house staff; preventing unauthorized entry and controlling access; classifying sensitive and critical materials and information; safeguarding and protecting sensitive materials actively and effectively; inspecting security controls and audits periodically; establishing levels of accountability, enforcement and authorization; controlling disposal efforts; developing access restrictions and controlling movement in the facility; evaluating and monitoring personnel continuously in sensitive areas; developing education programs in information security and applying security techniques, devices, procedures and policies.

Network security: Network Security encompasses measures to protect all elements of the network infrastructure from unauthorized access. Most organizations, for example, have firewalls and so-called demilitarized zones (DMZs) in place to protect their networks' connections to other networks. In addition to having these devices in place, however, an effective network security plan will prescribe measures to harden these devices themselves against intrusion.

Other elements of the network infrastructure require protection, as well. Most vendors, for instance, deliver routers and switches with passwords required for network management (SNMP community strings) set to well-known defaults. Organizations must have policies, processes and procedures in place to insure that these community strings are changed before placing the devices in service. In addition, organizations should develop and implement policies, processes and procedures to insure that they configure routers, switches and other network devices appropriately to address security concerns before placing them in service. Organizations may wish to negotiate an arrangement with the vendors from whom

they purchase these devices whereby the vendors deliver these network devices arrive pre-hardened.

System security: Security is one of the major concerns when developing mission critical business applications and this concern motivated the Web Services Security specifications. These specifications are very flexible so as to cover various security requirements.

Application security: Developing secure requirements and modeling security as part of analysis and design provides direction for the developer when it comes time to code the application. However, if BWAS (2005) an application is not built securely, it doesn't matter how well the requirements were defined or the system was modeled. Ensuring an application is built securely involves developing and enforcing secure coding practices. It is important to note that secure coding practices include not just the application code, but also other aspects of development such as User Interface (UI) development and prototyping.

CONCLUSION AND FUTURE DEVELOPMENTS

Securing Web Services is a major concern when implementing mission critical business transactions with Web Services. In this study we have presented several points of the main pivots of the web services security architecture, security challenges and described a number of important emerging standards in field. We have already shown in part three some interesting for web services securing mechanisms (XKMS, SAML, XACML and WS-Security) these mechanisms can be used to provide a wide variety of web services security models and encryption technologies. The goal of the Web services security architecture is to summary out the details of message-level security from the mainstream business logic.

REFERENCES

Building Web Application Security into, 2005. Your Development Process, By Kevin Heineman.

Federated Identity Management, 2005. Shortcomings of Existing Standards. In: Clemm, A., O. Festor and A. Pras (Eds.). 9th IFIP/IEEE International ymposium on Integrated Network Management (IM, 2005)-Managing New Networked Worlds; IEEE, Nice, France, Wolfgang Hommel Helmut Reiser.

Guide to Secure Web Services (DRAFT), 2006. Recommendations of the National Institute of Standards and Technology Computer Security Division Information Technology Laboratory National Institute of Standards and Technology Gaithersburg, MD., 20899-8930.

Integrated Security Gateway (ISG), 2005. Series Architecture. Juniper Networks, Inc.

KTH-KRB, 1999. Kerberos 4 from KTH For release 0.10.1999. Johan Danielsson Assar Westerlund, http://www.pdc.kth.se/kth-krb/doc/kth-krb_toc.html.

PSSM, 2001. Public Key Infrastructure Overview by JoelWeise-Sun. Global Security Practice Sun Blue Prints™ OnLine.

SAML, 2005. 2.0 profile of XACML v2.0 OASIS Standard.

Securing Web Services-Concepts, 2003. Standards and Requirements, 3 Securing Web Services-Concepts, Standards and Requirements.

Security in a Web Services World, 2002. A Proposed Architecture and Roadmap A joint whitepaper from IBM Corporation and Microsoft Corporation Version 1.0.

Web Services Security for Web Services, 2002. Wednesday Kapil Apshankar. http://www.web servicesarchitect.com/content/articles/apshankar04 print.asp.

What Is Kerberos Authentication? Updated, 2003. http://technet2.microsoft.com/WindowsServer/en/library/b748fb3f-dbf0-4b01-9b22-be14a8b4ae101033.mspx?mfr=true

XACML, 2003. Will Help Enterprises in Three Areas. Ray Wagner Publication.