Global Information Assurance Certification Paper

Analyzing Web Services Security against FEA TRM Enterprise Security Criteria

By: Abdulrahman Hijazi

T1: GSEC SANS Security Essentials

Version: 1.4

Abstract

As the Internet has developed into an internationally accessed basis for commerce, it has seen an evolution of security practices and challenges. This accounts for the exponential growth of hackers, virus manufacturers, and other industry enemies that have accompanied the spread of the Internet. [1]

As Web services use the Web technologies, its security involves most of those security issues of the Internet. However, some enterprise security criteria are not applicable to the Web services security.

In this paper, the web services security was analyzed and checked against a subset of the Federal Enterprise Architecture FEA Technical Reference Model TRM criteria.

Table of Contents

Scope and Limitations

The scope of this paper addresses enterprise security criteria which are based on a subset of a FEA TRM criteria referenced in appendix A. Not all aspects of the referenced FEA TRM criteria have been addressed. This is because some of them may not apply to the Web services and some others are beyond the limitation intended for this paper.

Within the referenced criteria, I limit the analysis to the following subset:

1. Security architecture and placement of security into specific applications for wired Web services only.
2. Electronic Authentication common services.
3. Single sign on through the portal.
4. Authorization and access control.
5. Confidentiality excluding VPN, VLAN and virus control.
6. Logging of Intra/Inter enterprise integration messages of secure audit.
7. Disaster recovery within availability.
8. Cryptographic key management and enterprise IT security policy within security and risk management.

Web Services Security Analysis versus Enterprise Security Criteria

In this analysis, two main schools of thoughts of Web services security will be highlighted. The first one is the Liberty Alliance Project led by Sun and other industry players. That is where SAML is being applied on top of SOAP (layer 8 in the Web services new architecture stack).

The second one is the new Web services specifications (WS-Security series) led by IBM, MS and others. This is what layer 9 (in the Web services new architecture stack) is all about.

Both projects are analyzed against the subset of the enterprise security criteria defined before in scope and limitations.

1. Wired FEA Web Services Security and FEA, EA Enterprise Security Architecture:

Liberty Alliance (SAML) Security has been placed mainly in layer 8 in the new Web services security architecture stack. Whereas layer 9 is devoted for the new Web services security series WS-Security.

Part (d): Security architecture and placement of security into specific applications

Layer 8--XML Messaging supports basic Web services and Web services security standards that are required by higher Web services layers for intra-domain interoperability and secure intra-domain interoperability via the Internet.
Layer 9--Secure Messaging supports the evolving WS (Web Services)-Security standards that are necessary for secure Internet interoperability. [2] [3]
The functionality of Layer 9 (WS-Security) builds on the functionality of layer 8 (SOAP). WS-Security describes how to attach signature and encryption headers to SOAP messages. In addition, it describes how to attach security tokens, including binary security tokens such as X.509 certificates and Kerberos tickets, to messages. [4]

2. E-Authentication Common Services

Part (a): Unique and proper identification and authentication of system elements

The de facto Secure Socket Layer (SSL) along with the de jure Transport Layer Security (TLS) and the Request For Comments (RFC) are used to provide transport level security for Web services applications. SSL/TLS offers several security features including authentication, data integrity and data confidentiality. SSL/TLS enables point-to-point secure sessions.
IPSec is another network layer standard for transport security that may become important for Web services. Like SSL/TLS, IPSec also provides secure sessions with host authentication, data integrity and data confidentiality. [3]

i. Integrity

Message integrity is provided by leveraging XML Signature in conjunction with security tokens to ensure that messages are transmitted without modifications. The integrity mechanisms are designed to support multiple signatures, potentially by multiple actors, and to be extensible to support additional signature formats. [5]

ii. Non-repudiation

In general, non-repudiation depends on digital signature and appropriate safe guards. For example, one of the basic safe guards is using hardware to save digital signature. None hardware digital signature solutions cannot support non-repudiation. Unfortunately, there are some software digital signatures involved in Web security. In addition, digital signature can only support non-repudiation at layer 7 and above. (See part 2.d.i)

Part (b): Reliability – business messages

The reliable delivery of messages is seen as crucial for Web services to become the primary infrastructure for heterogeneous interconnection of business processes, systems and products. [6]
Web Services Reliability (WS-Reliability) is a SOAP-based protocol for exchanging SOAP messages with guaranteed delivery, no duplicate s, and guaranteed message ordering. WS-Reliability is defined as SOAP header extensions, and is independent of the underlying protocol. This specification contains a binding to HTTP.
This model enables a sender (i.e., a SOAP node with reliable messaging functions for sending) to send a message to a receiver (i.e., a SOAP node with reliable messaging functions for receiving) that can accept an incoming connection. Functions to accommodate a receiver that cannot accept an incoming connection (e.g., because of a firewall) are intended for further study, and are not included in this version of the specification. [7]
WS-Reliability is part of the WS-Security series which develops a generic and open model for ensuring reliable message delivery of Web services. [2]

Part (c): Authentication Protocols.

i. Protection of system through open-system integrity, network integrity and data integrity

Liberty Alliance limits open system to the federated liberty project community. Whereas, IBM and MS open the system to the whole community.

ii. Data is not altered or destroyed in an unauthorized manner

(See part 2.a)

Part (d): Access Authentication Protocols—Authorization.
i. Non-repudiation.
ii. Non-denial of origin or delivery of data, validation of source software packages and hardware.

Security tokens assert claims and signatures provide a mechanism for proving the sender's knowledge of the key. As well, the signature can be used to "bind" or "associate" the signature with the claims in the security token (assuming the token is trusted). Note that such a binding is limited to those elements covered by the signature. Note that no particular method for authentication is indicated, however, security tokens may be bound to messages. The signature is a cryptographic binding of a proof-of-possession and a digest. This covers both symmetric key-based and public key-based signatures. Consequently, non-repudiation is not always achieved. [3] Only public key-based signatures can support non-repudiation, because the private key for digital signature is not shared.

3. Single Sign On through the Portal.

Web services can be used to integrate an electronic Customer Relationship Management (eCRM) application into an existing e-Commerce marketplace application to provide a single-sign-in experience for the user. With the synchronous and asynchronous Web services, the system achieves the single-sign-in goals. [8]
SAML (Security Access Markup Language) is a promising standard that encodes authentication and authorization information in XML format. A Web Service interface can thus request and receive SAML Assertions from a SAML compliant authority to authenticate and authorize a service requestor. SAML can be used to pass credentials off to multiple systems and thus can be used for single sign-on solutions. [9]

Part (a & b): Inter-domain single sign on & Intra-domain single sign on.

The Inter-domain single sign on describes the IBM and MS work, whereas, the Intra-domain single sign on describes the liberty project.

Part (c): Access Control.

i. Token and password usage.

The extensible Access Control Markup Language or XACML is an XML-based security standard for expressing rules and policies for controlling access to information. These rules and policies are associated with a target resource in the context of an overall access control and privacy strategy. IBM has already come up with its version of XACML, which it calls XML Access Control Language, or XACL. [1]

ii. Policy engines.

WS-Policy will describe 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-Policy will describe how senders and receivers can specify their requirements and capabilities.
WS-Policy will be fully extensible and will not place limits on the types of requirements and capabilities that may be described; however, the specification will likely identify several basic service attributes including privacy attributes, encoding formats, security token requirements, and supported algorithms.
This specification will define a generic SOAP policy format, which can support more than just security policies. This specification will also define a mechanism for attaching service policies to SOAP messages. [6]

Part (d): Entities are principals with several roles and tokens.

In single sign on, you may have several roles and tokens. For example, with sing sign on you may have two roles. Role 1 with secret key token and Role 2 with public key token.
On the other hand, single sign on may be implemented differently in layer 9 as opposed to layer 8.

4. Access Control by Requestor Application and Transaction Services.

As organizations using different identity mechanisms collaborate using Web services, the security trust model provides a flexible framework within which the organizations can interconnect when configured with appropriate authorization.

Web services have complete flexibility in specifying the claims they require in order to process messages. Collectively we refer to these required claims and related information as the "Web Service Endpoint Policy". Endpoint policies may be expressed in XML and can be used to indicate requirements related to authentication (e.g. proof of user or group identity), authorization (e.g. proof of certain execution capabilities), or other custom requirements.

Part (a): Authorization.

The SAML specification defines a number of elements for making assertions and queries regarding authentication, authorization decisions and attributes. SAML defines a message exchange between a policy enforcement point (PEP) and a policy decision point (PDP) consisting of an AuthorizationDecisionQuery flowing from the PEP to the PDP, with an Assertion returned containing some number of AuthorizationDecisionStatements. [10]
WS-Authorization is one of the WS-Security eight specifications which will describe how access policies for a Web service are specified and managed. In particular it will describe how claims may be specified within security tokens and how these claims will be interpreted at the endpoint.
This specification will be designed to be flexible and extensible with respect to both authorization format and authorization language. This enables the widest range of scenarios and ensures the long-term viability of the security framework. [9]

Part (b): Access Control of unauthorized use of information-system resources.

i. RBAC (Role-Based Access Control).

SAML 1.0 is fast becoming the dominant industry standard for federating diverse security environments in support of multidomain Web single sign-on (SSO), role-based access control (RBAC) and other interoperability scenarios. [11]

ii. Policy engines.

(See Part 3.c.ii)

5. Confidentiality

Confidentiality should follow mutual authentication. For example, service end point should first mutually authenticate each other before establishing confidentiality.

WS-Security describes enhancements to SOAP messaging to provide *quality of protection* through message integrity and message confidentiality. WS-Security defines the core facilities for protecting the integrity and confidentiality of a message, as well as mechanisms for associating security-related claims with the message. While WS-Security is the cornerstone of this effort, it is only the beginning and IBM will cooperate with the industry to produce additional specifications that will deal with policy, trust and privacy issues. [6]

Part (a): Ensures that data is not made available to unauthorized individuals or computer resources.

The need of Web services can be accessed by sending SOAP messages to service endpoints identified by URIs, requesting specific actions, and receiving SOAP message responses (including fault indications). Within this context, the broad goal of securing Web services breaks into the subsidiary goals of providing facilities for securing the integrity and confidentiality of the messages and for ensuring that the service acts only on requests in messages that express the claims required by policies.
A customer can add message-level integrity or persistent confidentiality (encryption of message elements) to an existing Web service whose messages are carried through, for example, Secure Sockets Layer (SSL/TLS). The messages now have integrity (or confidentiality) that persists beyond the transport layer.

Part (b & h): E-Commerce and E-Business Cryptographic Protocols & Security Protocols.

Cryptographic protocols basis available for IBM and MS at layer 9 are potentially much more comprehensive than the ones available for layer 8. One reason, WS-Security can support much more comprehensive cryptogrphic protocols. WS-Security, WS-Trust, WS-SecureConversation. More comprehensive family.
WS-Trust: will describe a framework for trust models that enables Web services to securely interoperate.
WS-SecureConversation: will describe how to manage and authenticate message exchanges between parties including security context exchange and establishing and deriving session keys. [6]

Part (c): Encryption of network communication to the browser**.**

i. End-to-end encryption from browser to content server.

Encryption of network communication to the browser may not be available if the encryption is SSL or TSL from browser to firewall. The reason is the

firewall may be decrypting the SSL or TSL confidential message, and this may need to be decrypted behind firewalls.

Part (g): Public Key Infrastructure (PKI).

At a high level, the PKI model involves certificate authorities issuing certificates with public asymmetric keys and authorities which assert properties other than key ownership (for example, attribute authorities). Owners of such certificates may use the associated keys to express a variety of claims, including identity. The Web services security model supports security token services issuing security tokens using public asymmetric keys. PKI is used here in the broadest sense and does not assume any particular hierarchy or model. [6]
WS-Security gives more robust support to PKI than what is available in layer 8.

6. Secure Audit

The general messaging model provides an integrating abstraction allowing systems to build a bridge between different security technologies. The general model is sufficient to construct higher-level key exchange, authentication, authorization, auditing, and trust mechanisms.

Part (a): Logging of Intra/Inter Enterprise Integration messages and Legacy System database updates.

When a security-related event such as authentication or an unproven claim or a bad signature occurs, it is logged. An administrator can securely access the log to review security-related events and manage the log. [6]

7. Availability

Part (b): Disaster recovery.

As the need for companies to move toward electronic means of communicating and interacting increases, Web services become an important aspect of deploying e-business initiatives. Enterprises now consider Web services as one of their primary means of support. The necessity to ensure the availability and performance of the Web services is greatly apparent. Tivoli systems management products were produced to ensure the performance and availability of Web services and Web sites. Among these products are:

- Tivoli Web Services Manager
- Tivoli Web Component Manager
- Tivoli Web Services Analyzer [12]

The powerful development tools and Web services introduced with the .NET Framework will help drive the development of a new class of powerful, Web-based applications. These new applications will move the Windows operating systems into more business-critical environments, where the unique availability advantages of the Stratus ftServer series offers significant benefits. [13]

8. Security management—risk management.

Part (1): Enterprise IT security policy is coordinated with
i. Enterprise architecture (EA).
ii. Enterprise IT portfolio.

WS-Policy specification will describe 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-Policy will describe how senders and receivers can specify their requirements and capabilities.
WS-Policy will be fully extensible and will not place limits on the types of requirements and capabilities that may be described; however, the specification will likely identify several basic service attributes including privacy attributes, encoding formats, security token requirements, and supported algorithms.
This specification will define a generic SOAP policy format, which can support more than just security policies. This specification will also define a mechanism for attaching service policies to SOAP messages. [6]

Part (f): Cryptographic key management.

XML Key Management Specification is a protocol developed by the W3C which describes the distribution and registration of public keys. Services can access an XKMS compliant server in order to receive updated key information for encryption and authentication. [14]
WS-Federation specification will define how to construct federated trust scenarios using the WS-Security, WS-Policy, WS-Trust, and WS-SecureConversation specifications. For example, it will describe how to federate Kerberos and PKI infrastructures.
As well, a trust policy is introduced to indicate and constrain and identify the type of trust that is being brokered. This specification also will define mechanisms for managing the trust relationships. [6]

Conclusion

For most of the referenced FEA TRM criteria, Web services security is found to fit very reasonably. This is with the understanding that two main influences affect the Web services architecture. Both, the Liberty Alliance Project and the new WS-Security specifications play important role in getting Web services to adhere to the enterprise security requirements. For the most part, the new WS-Security specifications are found to give much more broader and robust coverage of security than the federated Liberty Alliance Project.

Appendix A: Enterprise Security Criteria

To facilitate efforts to transform the Federal Government to one that is citizen-centered, results-oriented, and market-based, the Office of Management and Budget (OMB) is developing the Federal Enterprise Architecture (FEA), a business-based framework for Government-wide improvement. [15]

"The TRM is a component-driven, technical framework used to identify the standards, specifications, and technologies that support and enable the delivery of service components and capabilities." [16]

The following is a list of the eight FEA TRM criteria as stated in [2]:

1. **Wired/Wireless FEA Web Services Security and FEA, EA Enterprise Security Architecture.**
    a. Security Administration for
        i. Wired/wireless network architecture
        ii. VoIP (Voice over IP (Internet Protocol)) integration with IP network infrastructure—network architecture and supporting resources.
    b. SNM.
    c. Network Security Services: Integrated firewalls, IDS (Intrusion Detection Systems), virus detection etc.
    d. Security architecture and placement of security into specific applications.
2. **E-Authentication Common Services.**
    a. Unique and proper identification and authentication of system elements.
        i. Integrity.
        ii. Nonrepudiation.
    b. Reliability – business messages.
    c. Authentication Protocols.
        i. Protection of system though open-system integrity, network integrity and data integrity.
        ii. Data is not altered or destroyed in an unauthorized manner.
    d. Access Authentication Protocols—Authorization.
        i. Nonrepudiation.
        ii. Non-denial of origin or delivery of data, validation of source software packages and hardware.
3. **Single Sign On through the Portal.**
    a. Inter-domain single sign on.
    b. Intra-domain single sign on.

c. Access Control.
    i. Token and password usage.
    ii. Policy engines.
d. Entities are principals with several roles and tokens.

4. **Access Control by Requestor Application and Transaction Services.**
    a. Authorization.
    b. Access Control of unauthorized use of information-system resources.
        i. RBAC (Role-Based Access Control).
        ii. Policy engines.
    c. Security Labeling.
        i. Accuracy and integrity of security labeling.
        ii. Software tools to manage labeled databases.
5. **Confidentiality**
    a. Ensures that data is not made available to unauthorized individuals or computer resources.
    b. E-Commerce and E-Business Cryptographic Protocols
    c. Encryption of network communication to the browser**.**
        i. End-to-end encryption from browser to content server.
    d. Virtual Private Network (VPN).
    e. VLAN (Virtual LAN (Local Area Network)).
    f. Virus Control.
    g. Public Key Infrastructure (PKI).
    h. Security Protocols.
6. **Secure Audit**
    a. Logging of Intra/Inter Enterprise Integration messages and Legacy System database updates.
    b. Access Filtering, Monitoring, and Reporting.
    c. Resistance to attack.
    d. Support
        i. Redundant database processes.
        ii. Secure disaster recovery.
7. **Availability.**
    a. Network redundancy.
        i. Assurance of timely and regular communications, graceful degradation.
        ii. Multi-node redundant network infrastructure.
        iii. Redundant ISP (Internet Service Providers), power, and communications.
    b. Disaster recovery.

8. **Security management—risk management.**
    - **a.** Enterprise IT security policy is coordinated with
        - **i.** Enterprise architecture (EA).
        - **ii.** Enterprise IT portfolio.
    - **b.** Enterprise IT security policy provides overarching guidance for
        - **i.** Enterprise security architecture.
        - **ii.** Uniform information assurance security guidelines.
        - **iii.** System protection profiles.
        - **iv.** Disaster planning criteria.
    - **c.** Two-phase certification and accreditation (C&A).
        - **i.** First phase: IT system security criteria.
        - **ii.** Second phase: Connecting the IT system to the enterprise network infrastructure should not increase enterprise residual risk.
    - **d.** Alarm reporting.
    - **e.** Audits.
    - **f.** Cryptographic key management

References

[1] Ben Galbraith et al, Professional Web Services Security, Wrox Press Ltd., December 2002, Chapter 1. Web Services.

[2] Harold Podell, *Seven Candidate Categories for Secure Interoperability*, Cyber-Security Technology for the U.S. Critical Infrastructure Protection Community, May 7, 2003.

[3] Chappell, Dave. "Web Services Reliability Specification Published by Leading IT Vendors". Jan. 13, 2003. URL: http://www.oreillynet.com/pub/wlg/2594

[4] Myerson, Judith. "A proposed synthesis of IBM's Web services architecture stack and new IBM technologies**".** June 1, 2002. URL: http://www-106.ibm.com/developerworks/webservices/library/WS-wsa/

[5] Atkinson, Bob et al. "Specification: Web Services Security (WS-Security)". April 5, 2002 . URL: http://www-106.ibm.com/developerworks/library/WS-secure/

[6] IBM & MS. "Reliable Message Delivery in a Web Services World: A Proposed Architecture and Roadmap". March 13, 2003. URL: http://msdn.microsoft.com/webservices/understanding/gxa/default.aspx?pull=/library/en-us/dnglobspec/html/WS-rm-exec-summary.asp

[7] … "Web Services Vendors Publish Royalty-Free WS-Reliability Specification". Jan. 9, 2003. URL: http://www.sonicsoftware.com/docs/ws_reliability.pdf

[8] Cohen, Frank. "Using Web services for e-Commerce single sign-in**".** Jan. 1, 2002. URL: http://www-106.ibm.com/developerworks/webservices/library/WS-single/

[9] Yang, Andrew. "XML Web Services Security Issues". April 10, 2002 http://www.xwss.org/articlesThread.jsp?forum=34&thread=648

[10] Welch, Von et al. "Use of SAML for OGSA Authorization". Feb 15, 2003. URL: http://www.cs.virginia.edu/~humphrey/ogsa-sec-wg/OGSA%20SAML%20Authorization%20Assertions-Feb15.pdf

[11] Kobielus, James. "Microsoft supports SAML, sort of". Dec. 8 2002. URL: http://www.nwfusion.com/columnists/2002/0812kobielus.html

[12] Darmawan, Budi et al. "Tivoli Web Solutions: Managing Web Services and Beyond". Jan. 28, 2002. URL: http://publib-b.boulder.ibm.com/Redbooks.nsf/RedbookAbstracts/sg246049.html?Open

[13] … “The Role of Availability in the Microsoft® .NET Initiative”. http://www.stratus.com/whitep/net/future.htm

[14] Armstrong, Eric, “The Java™ Web Services Tutorial”. Feb. 19, 2003. URL: http://java.sun.com/webservices/docs/1.1/tutorial/doc/index.html

[15] http://www.feapmo.gov/fea.asp

[16] http://www.feapmo.gov/feaTrm2.asp