An IT Security Strategy for XML Messages using Web Services - Version 1.4b

GIAC Security Essentials Certification (GSEC) Practical Assignment Option 1

Michaela H. Poole
16 December 2002

Abstract

Securing corporate information is a critical business priority for companies. Due to current trends of ongoing staff reductions and quickly emerging new technologies, Corporate Security is unable to keep up and is relying on a partnership with IT to identify and manage new security requirements. IT strategies identify approaches to achieving key business goals. A well documented and clear IT Security Strategy avoids conflicts, redundancy, and omissions with Corporate Security and is mutually beneficial. This document describes a strategy for securing XML messages using Web Services with the key elements of technology, process, and people. The technology element consists of security components and message content. Security components include encryption, decryption, digital signatures, and authentication. Message content includes canonical XML, encryption, buffer overflow, and malicious content. The process security element identifies the infrastructure processes supporting security throughout the life cycle of an XML message, including code reviews and code testing. The people security element includes incident response teams, security training, roles and responsibilities needed to support the technology and process elements. All three elements are necessary to provide a secure corporate environment.

1 Introduction

This strategy is based upon the business requirements to provide security support throughout the life cycle of an XML message and ensure confidentiality and data integrity of XML messages using Web Services. These requirements support the business goal to improve data security. The technology, process, and people elements in this strategy support the business requirements. These elements are equally important. Technology, process, and people combined provide the strong defense-in-depth strategy essential in demonstrating this company's information security preparedness. In the future, "the Securities and Exchange Commission may start requiring companies to disclose their information security preparedness to investors" [Schwartz-1 37].

This strategy does not provide an end-to-end security solution for XML messages using Web Services. The technology, process, and people sections are essential in preventing and/or impeding internal and/or external attacks. The security topics not addressed in this strategy include network, data base, and operating system security.

2 Technology

This section describes several security component and message content technologies used to support the company's business requirements for confidentiality and data integrity of XML messages. The security components section discusses encryption, decryption, digital signatures, and authentication to secure XML messages. The message content section discusses canonical XML, encryption, buffer overflow, and malicious content. The technology components are a vital layer in this company's defense-in-depth strategy.

2.1 Security Components

This section describes how encryption, decryption, digital signatures, and authentication support the business requirements for confidentiality and data integrity. This section does not provide a detailed analysis of all the security components, their strengths or their weaknesses. This strategy recognizes the vulnerabilities of these technologies; however, they provide an additional layer in the company's defense-in-depth strategy. The type and extent of security needed for each XML message is determined during the requirements phase by the business representatives in conjunction with the security teams described in section 4 of this strategy.

Netscape states that eavesdropping, tampering with information and impersonation through spoofing or misrepresentation are key issues that compromise the security and data integrity of XML messages [Netscape]. This article concludes public-key cryptography using encryption, decryption, digital signatures, authentication, or a combination of these components provides the solutions to these issues. While public-key cryptography has security issues, such as key distribution problems, this strategy supports this solution in providing confidentiality and data integrity to XML messages using Web Services.

2.1.1 Encryption and Decryption

Encrypting and decrypting confidential and sensitive data supports the business requirement for confidentiality. Specific data elements, such as social security numbers and salaries, are classified as secret by the company's Corporate Security department and require encryption when transmitted. Other data elements, such as product information, are not classified as secret and do not require encryption. However, secrecy of product information in some instances is necessary thus requiring encryption. Identifying data classified as non-secret that must be encrypted is determined during the requirements gathering phase by the business and security teams. Encryption and decryption resolves many eavesdropping and tampering issues and provides confidentiality to XML messages

2.1.2 Digital Signatures

Digital signatures support the business requirement for data integrity. Hankison states while digital signatures provide assurance of data integrity and non-repudiation, the tools used to implement digital signatures should include the ability to a cancel signature, support multiple signatures proved encryption mechanisms, and provide a timestamp [Hankison]. Digital signatures are required for some company information, such as an XML message communicating classified legal information. Digital signatures resolve many tampering issues and provide integrity to XML messages.

2.1.3 Authentication

This section describes how authentication supports the business requirement for data integrity. “Authentication is the process of determining if a user or entity is who he/she claims to be” [Curphey, et al. 27]. Having authentication safeguards in place is crucial for the recipient of the XML message to trust the origin of the XML message. Authentication resolves many tampering and impersonation issues and provides integrity to XML messages.

2.2 Message Content

This section discusses canonical XML, encryption, buffer overflows, and malicious code. These factors affect XML message performance, confidentiality, and data integrity. XML message content needs to be constructed to support the company’s business requirements for confidentiality and data integrity of XML messages.

2.2.1 Canonical XML

XML messages needing encryption and/or digitally signatures need an XML canonical form generated. Mactaggart states two XML messages can be logically equivalent but physically different textually because of content such as line delimiters and empty tags. He further states that encryption and/or digital signatures should not be invalidated due to logical differences, hence the need to use the canonical form [Mactaggart]. XML canonical form supports the business requirement for data integrity.

2.2.2 Encryption

Time and cost prevents encrypting all XML messages. This strategy recommends the entire XML message be encrypted if 80% of the data requires encryption. This would increase processing time. If less than 80% of the data requires encryption, the data needing encryption should be grouped together at the top of the XML message instead of spread out through out the message. This practice accelerates compile time. The inability to perform searches when subsections of an XML message are encrypted is a drawback identified by Mactaggart [Mactaggart]. Encryption supports the business requirements for confidentiality and data integrity.

2.2.3 Buffer Overflows.

Buffer overflows cause a denial of service attack. Buffer overflows are caused when a memory buffer is needed that is larger than the software can handle, for example 4k of memory is needed, but only 3k is allocated. Buffer overflows can be prevented by allocating more memory than needed and not hard coding the memory size. This strategy requires the code review process to examine XML messages for hard coded memory allocation. Memory must be dynamically allocated. This strategy recommends XML message testing includes buffer range testing as well as testing for under flow and over flow results. For example, if the developers determined the memory allocation is 4k, then test 200 bytes and 100k and monitor the results.

2.2.4 Malicious Content

This strategy defines malicious content as anything in the code causing a denial of service or compromising the confidentiality and/or data integrity of XML messages using Web Services. Malicious code can be intentionally or unintentionally constructed. Code reviews and XML message testing are essential for detecting malicious code before the XML message is sent. Also, when a Web Service receives an XML message, webMethods® states that Web Services should not execute the contents of a message if it contains active content such as ActiveX or Perl scripts because the Web Service could transmit the malicious code to other systems that execute the code [webMethods 17].

3 Process

This section describes the infrastructure processes supporting the business requirements to provide continued security support throughout the life cycle of an XML message and ensure confidentiality and data integrity of XML messages using Web Services. The purpose of these processes is to determine XML message security compliance. Processes provide a standardized way of doing business which allows for the creation and reuse of security data and services. This section describes the processes but does not detail the procedures. The processes discussed in this section are supported by various teams described in section 4 of this document. "Well-designed processes let companies prepare for the majority of attacks" [Schwartz-1 40].

3.1 Project Identification Processes

This section describes actions taken when a project is initially funded. Security needs to be involved from the beginning. The purpose of these processes is to alert security of new projects. You cannot secure an XML message if you don't know it exists.

3.1.1 Project Notification Process

The objectives of this process are to assign Information Security Team (IST) representatives to a project and to notify the project of the assignment. The IST project manager is responsible for this process. The IST project manager must be notified of all newly funded projects in IT by the architecture security role. The IST project manager then analyzes and assigns a Corporate Security representative and an IT Security representative to the project. Project information is then emailed to these representatives. The IST project manager emails the project team the names of their representatives. This information is posted to the IST web site. Keeping everyone informed is essential to providing security. This process supports the business requirement to provide continued security support throughout the life cycle of an XML message.

3.1.2 Project Security Rating (PSR) Process

The objective of this process is to determine the level of involvement in a project required by IT Security and Corporate Security. The project security rating (PSR), as designed for this strategy, is determined by the IST representatives. They analyze the initial project information and determine the PSR. Some projects will have multiple ratings depending upon the security requirements of the project. The IST representatives notify the development team the project PSR via email and post it to the IST web site. This process supports the business requirements to provide continued security support throughout the life cycle of an XML message and ensures confidentiality and data integrity of XML messages using Web Services.

A PSR of 1 requires both IT Security and Corporate Security involvement during the life cycle of the project. Many financial projects would be assigned this rating. A PSR of 2 requires IT Security team involvement during the life cycle of the project with minimal involvement from Corporate Security. Most projects will be assigned this rating. A PSR of 3 requires the project team accesses the Corporate Security web site for project security standards, guidelines, and policies. Projects assigned this rating will have team members who are knowledgeable of the security procedures and requirements. The PSR can change during the life cycle of the project as security requirements change.

3.1.3 Project Security Kick-off Meeting Process

The objectives of this process are to introduce the security representatives to the development team and discuss security processes, policies, standards, and guidelines. The IST representatives present a standardized security briefing and discuss the project PSR. The project needs to understand the security policies and procedures they must follow, why the security measures are important and the ramifications to the personnel if the security measures are not implemented. This process supports the business requirement to provide continued security support throughout the life cycle of an XML message.

3.2 Development Phase Processes

This section describes actions taken when a project using XML messages with Web Services starts the development phase of the project. Reusing approved security code provides accelerated delivery time of secure XML messages and reduces costs.

3.2.1 Requirements Process

The objective of this process is to identify data requiring security, the type of security required, and any other security requirements needed to support the business requirements for confidentiality and data integrity. IST representatives, business analysts, and business representatives determine the security requirements. Threats are analyzed and resolutions determined. “The threat analysis is the process of identifying [as many as possible] risks that can affect the assets” [Peteanu 10]. This process supports the business requirement to ensure confidentiality and data integrity of XML messages using Web Services.

3.2.2 Design Review Process

The objective of this process is to identify potential security problems caused by the design. IST representatives, business analysts, and project developers review the design. Poor design can cause security breaches. This process is an approval process. The IST representatives must review and approve the design. The design needs to match the specifications of the project. If an XML message needs only a name and phone number the design should fail the review if irrelevant information, such as social security number, is included in the design. This process supports the business requirement to ensure confidentiality and data integrity of XML messages using Web Services.

3.2.3 Data Review Process

The objective of this process is to enforce corporate standardization of security components used in XML schemas. An XML schema provides the syntax for an XML message. The data role is responsible for creating standardized authorization and authentication XML schemas. These reusable XML security schemas must be included in all XML schemas using Web Services.

This process is an approval process. When an XML schema is created, it must be reviewed and approved by the data role. New security components identified by a project team will be analyzed by the data role and possibly incorporated into the security schemas for reuse across the organization. Ensuring the XML security schemas are included in every project XML schema is part of the process. When an XML schema has been approved by the data role, the schema is stored in a corporate repository for security purposes. Only the data team has access privileges to change an XML schema after it has been approved and stored in the corporate repository. This process supports the business requirement to ensure confidentiality and data integrity of XML messages using Web Services.

3.2.4 Code Review Process

The objective of this process is to identify security problems caused by the code. IST representatives and project developers review the code. Peteanu states code reviews need to match the code against the requirements, check for common errors such as hidden fields, and ensure secure code relies on secure libraries and subsystems if applicable [Peteanu 28]. This process supports the business requirements to provide continued security support throughout the life cycle of an XML message and ensures confidentiality and data integrity of XML messages using Web Services.

3.3 Testing Phase Processes

This section describes actions taken when a project using XML messages with Web Services starts the testing phase of the project. Testing provides a quality assurance assessment that an XML messages performs as expected and includes all necessary security criteria. A detailed testing checklist is vital. Knowledge of the project specifications is needed by the testing team to ensure the XML messages function as expected.

3.3.1 XML Schema Testing Process

The objective of this process is to determine if a component of an approved XML schema was changed by the developers during construction of the XML message. Often XML schemas need changes after the XML schema has been approved. Under pressure to produce, developers often feel they don't have the time to have the changes reviewed by the data role. These changes could create security risks, thus the discrepancies need to be identified. The testing team is responsible for creating software that compares the approved XML schema with the syntax used in an XML message. This software should be available on the testing team web site to allow developers the opportunity to pre-test their XML messages. This process supports the business requirements to provide continued security support throughout the life cycle of an XML message and ensures confidentiality and data integrity of XML messages using Web Services.

3.3.2 XML Message Testing Process

The objective of this process is to test XML messages for security threats, intentional or unintentional. The testing team needs a comprehensive test plan. For example, a buffer range test alone is inadequate. Both buffer overflow and underflow tests need to be conducted to ensure a denial of service is not caused due to inadequate testing. Reviewing the code for malicious code, intentional or unintentional, is part of this process. This process supports the business requirements to provide continued security support throughout the life cycle of an XML message and ensures confidentiality and data integrity of XML messages using Web Services.

3.4 Production Phase Processes

This section describes actions taken when XML messages with Web Services are in production. Security procedures are critical at this stage to ensure the business requirements for confidentiality and data integrity are maintained.

3.4.1 Monitoring Process

The objective of this process is to monitor XML messages using Web Services while in production. Thorough testing does not preclude a message from becoming a security threat while in production. XML messages should be randomly screened for various security threats. This function is performed by Corporate Security in conjunction with IT. Parts of this operation can be automated using the software created by the testing team described in section 3.3.1. The syntax of a randomly selected production XML message would be compared to the syntax of the approved XML schema residing in the corporate repository described in section 4.1.2.2. This process tests production XML messages to ensure the syntax was not changed due to hijacking. The syntax of a hijacked XML message could have been changed to request confidential information. This process supports the business requirements to provide continued security support throughout the life cycle of an XML message and ensures confidentiality and data integrity of XML messages using Web Services.

3.4.2 Incident Response Process

The objective of this process is taking action when an incident occurs. CIRT, the Computer Incidence Response Team described in section 4, is responsible for handling all incidents involving XML messages using Web Services. This team is comprised of skilled personnel in all areas of XML, Web Services and security. Detailed incident response plans and checklists need to be in place before incidence occurs. Lessons learned meetings after the resolution of an incident are a must. Plans, checklists, and lessons learned meetings provide another layer of defense. Also, the CERT® Coordination Center has identified evaluating the effectiveness of the team as a critical part of the process [CERT]. This process supports the business requirement to provide continued security support throughout the life cycle of an XML message.

3.4.3 Retirement Phase Process

The objective of this process is taking action when an XML message is no longer used. Often when a project is cancelled or an XML message is not needed, the XML message remains active in the production environment. This type of XML message creates a security risk. IST needs to be notified of all cancelled projects or XML messages that are no longer in use. IST works with various teams to ensure the appropriate XML messages are retired. For example, IST would check that all Web Service references to a retired XML message were deleted, thus providing another layer of defense. This process supports the business requirement to provide continued security support throughout the life cycle of an XML message.

4 People

This section describes security roles, responsibilities and training supporting the business requirements to provide continued security support throughout the life cycle of an XML message and ensure confidentiality and data integrity of XML messages using Web Services. These requirements support the business goal to improve data security.

Peteanu recommends dedicated developers trained in security write all company code for security mechanisms, otherwise there will be security holes [Peteanu 27]. This strategy proposes all roles outlined in this document have dedicated highly trained security personnel to support the life cycle of XML messages.

4.1 Roles and Responsibilities

“Having a good security staff won't mean a thing if those security pros aren't effectively integrated into your company, and if they can't develop solid lines of communication” [Schwartz-2]. Clearly defined and documented roles and responsibilities supporting the processes and technology are key factors in successfully integrating security teams into IT.

4.1.1 Corporate Security

This section identifies the roles and responsibilities of Corporate Security that support the IT Security Strategy. Corporate Security is responsible for the end-to-end security of XML messages using Web Services. However, lack of personnel and emerging new technologies requires Corporate Security to team with IT to ensure XML message security. The Corporate Security role:

- Approves or recommends changes for all security related documents created by IT. IT writes XML message and Web Services security policies, standards, procedures, and related security documents because IT knows the content.
- Owns all security policies, standards, procedures, and other related security documents created by IT.
- Publishes security policies, standards, procedures, and other related security documents to the Corporate Security web site.
- Owns the data classification list identifying what data is confidential and restricted. This classification determines the data that must be encrypted such as social security number.
- Member of the IT Computer Incident Response Team (CIRT).

.

4.1.2 IT roles and responsibilities

This section identifies the roles and responsibilities of IT to secure XML messages using Web Services. IT security roles require a high level of expertise in architecture, data design, software tools, development, testing, and incidence response.

4.1.2.1 Architecture Role

This role is responsible for designing the end-to-end security framework for XML messages using Web Services. This role supports project notification processes and technology components. The architecture role:

- Creates the security infrastructure framework securing XML messages using Web Services. This framework creates a unified approach to securing XML messages using Web Services in alignment with emerging industry and security standards such as SAML, the Security Assertion Markup Language. SAML standardizes authorization and authentication information.
- Operates a test lab developing unified security solutions. For example, developing solutions to implement authentication with the various Web Service technologies such as .NET and Glue.
- Owns the corporate approved products list identifying the software that can be used by developers. A standardized toolset enables security solutions to be deployed prior to use by developers. Allowing developers to use any software creates a “catch up” scenario for security, thus increasing the risk for security loopholes.
- Owns and maintains the list of all projects funded by the company.
- Notifies the Information Security Team project manager of all new projects.

4.1.2.2 Data Role

This role is responsible for standardizing security terminology used in XML messages and working with project analysts to determine what and how much security is needed for the project. The Security Assertion Markup Language (SAML) is the industry standard used by this strategy as the source of standard security terminology [SAML]. SAML includes XML schemas containing authorization and authentication components. This role supports development phase processes and technology components. The data role:

- Creates standardized XML security schemas based upon SAML standards. Schemas define the “structure, content and semantics of XML documents” [W3C]. Including these standardized security schemas in all company XML messages is a requirement when using Web Services.
- Approves all XML schemas using Web Services in support of the data review process. All company XML schemas are required to include the standard security components for authorization and authentication. Also, the XML schemas must adhere to corporate standards for naming XML components. Standardized XML component names supports security during the testing process. For example, an XML component named SN might not be recognized as social security number and consequently not encrypted.
- Maintains the corporate XML schema repository in support of the testing and monitoring processes. This repository contains all XML schemas approved by

the data role. The testing process compares project XML message syntax against XML schema syntax in this repository to ensure developers did not change their XML message syntax. Changing syntax after the approval process poses potential security risks. The monitoring process compares XML message syntax against production XML messages ensuring the XML message were not hijacked and altered.

- Creates integrated schemas. Schemas can include other schemas in their entirety or import specific XML components from another schema. Included schemas and imported XML components pose problems when validating schemas for compliance because the included schemas or imported XML components can change. An integrated schema contains no include or import statements. The included and imported XML components are “flattened” into one schema. Integrated schemas are important for capturing point in time to validate schemas during audits since included schemas or imported XML components can change, thus affecting the project schema.

4.1.2.3 Tools Role

This role is responsible for ensuring only authorized personnel use the company approved software to create XML messages and Web Services in support of technology components. The tools role:

- Creates a centralized repository of all XML schema and Web Services software requests tracking who has access to what tools for security purposes.
- Notifies users of software upgrades. Using older versions of software can create security risks.

4.1.2.4 Development Role

This role is responsible for XML message code security. This role programs security components and trains programmers in programming security essentials. This role supports development phase processes.

- Creates security best practices programming documents. With all the new technologies emerging, it is difficult for programmers to have all the knowledge to program secure XML messages.
- Performs code reviews on all XML messages supporting the code review process.
- Trains application developers in corporate application security requirements.

4.1.2.5 Testing Role

This role is responsible for ensuring the XML message performs its task reliably. Testers need to know the purpose and requirements of each XML message to ensure the message performs as expected and no malicious code is present. This strategy recommends creating a team of testers to test the security functions of all XML messages due to the complexity of security issues surrounding the new technologies. This role supports testing processes.

- Writes and owns testing procedures.
- Tests the security portions of XML messages using Web Services.

4.1.2.6 Information Security Team (IST) Role

This role is comprised of personnel from Corporate Security and the various IT Security teams partnering to ensure corporate XML messages using Web Services are secure and trustworthy. This role supports all processes and technology.

- Creates standardized security briefing documentation for presentation at project kick-off meetings. This briefing provides projects with an understanding of project security requirements prior to starting a project and supports the project notification processes.
- Determines the Project Security Rating (PSR) for each project. A PSR determines the level of involvement by Information Security Team.
- Audits XML messages for security compliance. .
- Partners with development teams to analyze and design security into the project.

4.1.2.7 Computer Incidence Response Team (CIRT) Role

This role is a subset of the Information Security Team comprised of at least one member of each of the above roles including Corporate Security. When an incident occurs, all members are informed and updated. This strategy recommends a proactive approach to immediately create a CIRT to avoid what West-Brown calls "the trial-by-fire approach to security incidents" [West-Brown]. She states that most companies have no formal response team in place until a major incident has occurred. CIRT supports the production processes.

- Develops various strategies and best practices documents.
- Develops incident response procedures and checklists.
- Responds to all incidents involving security issues for XML messages using Web Services.
- Conducts "lessons learned" meetings after each incident.

4.2 Security Training for IT

The IT security professional needs specialized skills and training in computer information security. This strategy recommends annual security certifications for all IT security personnel to demonstrate current knowledge of information security. IT needs to budget funding for training and certification. Well trained IT security professionals reduce threats and minimize costly security exposure to the company.

5 Summary

Success of this security strategy is dependent upon the implementation of technology, process, and people elements. They are equally valued and necessary in constructing a defense-in-depth strategy to ensure confidentiality and data integrity of XML messages using Web Services. This strategy supports the business goal to improve data security and supports the business requirements to provide security support throughout the life cycle of an XML message and ensure confidentiality and data integrity of XML messages using Web Services.

6 References

[CERT] CERT®. “Creating a Computer Security Incident Response Team: A Process for Getting Started.” 2002. URL: http://www.cert.org/csirts/Creating-A-CSIRT.html, (November 25, 2002).

[Curphey, et al.] Curphey, Mark, et al. “A Guide to Building Secure Web Applications: The Open Web Application Security Project.” September 21, 2002. URL: http://www.cgisecurity.net/owasp/OWASPBuildingSecureWebApplicationsAndWebServices-V1.1.pdf, (October 5, 2002).

[Hankison] Hankison, Whitney. “Digital Signatures and Web Services: Signing Your Service.” February 13, 2002. URL: http://www.webservicesarchitect.com/content/articles/hankison03.asp. (October 12, 2002).

[Mactaggart] Mactaggart, Murdoch. “Enabling XML security.” September 2001. URL: http://www-106.ibm.com/developerworks/library/s-xmlsec.html, (October 12, 2002).

[Netscape] Introduction to Public-Key Cryptography. (1998). URL: http://developer.netscape.com/docs/manuals/security/pkin/contents.htm (October 12, 2002).

[Peteanu] Peteanu, Razvan. “Best Practices for Secure Development” v4.03, October 2001. URL: http://members.rogers.com/razvan.peteanu/best_prac_for_sec_dev4.pdf, (October 5, 2002).

[SAML] Assertions and Protocols for the OASIS Security Assertion Markup language (SAML) Specification 01 (May 31, 2002). URL: http://www.oasis-open.org/committees/security/docs/cs-sstc-core-01.pdf. (October 26, 2002).

[Schwartz-1] Schwartz, Matthew. “The Homeland Security Imperative.” Enterprise Systems Volume 17 Number 5 (May 2002): 37-42. This article is also available on-line by selecting the May 2002 issue URL: http://esj.com/back_issues/contents.asp?EditorialsID=17 and selecting the article. (November 9, 2002).

[Schwartz-2] Schwartz, Matthew. “Put a Good Security Staff in its Place.” Enterprise Systems (March 2002). This article is available on-line by selecting the March 2002 issue URL: http://esj.com/back_issues/contents.asp?EditorialsID=15 and selecting this article under the Columns category. (November 9, 2002).

[W3C] Architecture domain. (April 2000). URL: http://www.w3c.org/XML/Schema. (September 28, 2002).

[webMethods] webMethods®. “Requirements for Securing Enterprise Web Services.” May 2002. URL: http://www.webmethods.com/whitepaper_email_entry/1,1330,,00.html, enter your email address and select this whitepaper, (September 14, 2002).

[West-Brown] West-Brown, Moira. "Avoiding the Trial-by-Fire Approach to Security Incidents." Newsa2sei interactive Volume 2, Issue 1 (March 1999). URL: http://interactive.sei.cmu.edu/news@sei/columns/security_matters/1999/mar/security_matters.htm, (December 4, 2002).