Web Service Message Security in Applications Integration

Syed Umair Hassan*, Farrukh Saleem Sheikh**

*Faculty of Computer Science, Institute of Business Administration (IBA), Karachi, Pakistan

**Faculty of Computer Science, Institute of Business Administration (IBA), Karachi, Pakistan

Abstract-In today's e-business era, organizations are more focusing on Web Services for system integration. Transactions of Web Service are done mainly through plain-text XML formats like SOAP and WSDL, altering them is not a big task. XML Signature and XML Encryption is one way to secure XML documents up to certain level as well as retain the documents structure. Web Service message security cannot be taken as granted. When implementing a web service message security one should know the life cycle of web services and how it is implemented. Also, XML Encryption is described in detail followed by XML Signature. Web services provide us Integrity, privacy, confidentiality, authentication which makes up the building block for web service security. In this, Web services message attacks are discussed and how they can be minimized using different techniques. Web services message security is utmost important in any enterprise application integration and if they are not looked upon seriously then they can bring massive disappointment to the company and to their data as well. We have conducted a survey on Web Service Message Security and our target audience was those people who have some knowledge about Web Services and based on their results we presented our analysis.

Index Terms- Authentication; Authorization; Digital Signature; Integration; SOAP;WSDL;WS Security;XML Signatures; XML Encryption;

I. INTRODUCTION

Concept of web services is not new and since its advent in IT sector it has quickly become the backbone of the IT industry. Web services functionality is to give a response to request over a network and its interface is in a form of XML [1]. Web Service can be used by using SOAP, REST and JSON. Its popularity among the technology industry has led different organizations to amalgamate their software and services from different companies and location into one integrated service which can streamline important process. [2]. They are internet based enterprise applications that are based on XML related standards and communications. All the messages request and response are done using HTTP with XML serialization among other web related standards and all this is governed by SOAP protocol.

To implement the web service, it is necessary to know the life cycle of web service which includes; Definition phase, Service selection phase, Deployment phase and Execution phase[3]. There are many risks associated in XML communication and a valid XML document can still cause troubles like Dos-attack, Buffer overflow, Replay attack, Common injection flaws etc.[4] due to this web service security became an important part as it has become easy for hackers to breach the protocol, so to avoid that, necessary security measures have to be taken which introduces the two standards for XML security - XML signature and XML encryption[5] By doingXML encryption it ensures users authentication, integrity and confidentiality as there were numerous records which needed to be secure like medical records, bank statements and other classified information. XML signature are digital signatures which are obtained by applying digital operation to XML structure and they are not limited to signing XML resources only, they can also be used for signing JPEG file. Though XML signature and XML encryption are the standard which must be taken but there aremanyother techniques also which can counterfeit the attacks like using SSL protocol, Transport Layer Protocol (TLP) and many others.

Web services can work without a WSDL file but it will not be convenient enough, as it will be to use web services with WSDL. These days there are so many XML encryption algorithm available which has redefined the security mechanism for XML security and most of them fall under symmetric and asymmetric encryption algorithms. Advanced Encryption Algorithm (AES) which is a successor of DES, is a symmetric algorithm and it uses 256 bit key for encryption and its main issue is that they can't decrypt the message until all the parties exchange the keys for encryption. RSA which is an asymmetric algorithm uses two independent keys, one for encryption and the other for decryption. RSA is much slower than symmetric algorithm but it can be implemented to 4096 bit keys which is a more secured cryptographic hash function than symmetric algorithm but it will be expensive to run this encryption technology.

In this research, we are going to discuss web service message security and how to cater those security risks in

application integration which is going to be a questionnaire based, in which we are going to ask series of closed questions related to web service message security.

II. BACKGROUND

In early 90's when a new technology of web service was introduced there was no concept of message securities[6]. The only security measure that was considered was the point-to-point transportation securities throughtransportation protocols like https that is using SSL for data or information transportation. At that time, it was required to have a SOAP-level or end-to-end security. The need of this web service message security is fulfilled by developing a protocol in 2006 by IBM, Microsoft and VeriSign named as Web Service Security (WS-Security).

The building blocks of Web service security include[5]

Identification & Authentication	Allow the access to known and verified requester only.
Authorization	Allow only those users who have the permission.
Integrity	Do not Allow to modify the data in unauthorized manner
Non-repudiation	Assurance that either sender or receiver cannot deny about information status.
Confidentiality	Saving agreed restrictions and access levels
Privacy	Confined access to subscribers

TABLE 1 : WEB SERVICE SECURITY BUILDING BLOCKS

The following table will summarize the web service security standards[5]

XML Encryption	Process of encrypting the data and saving in XML (Confidentiality)
XML Signature	Using the public and private key the sender and signing entities are verified (Integrity, Authenticity)
WS-Security	For SOAP security enhancements XML Signature and Encryption technologies are used.
Username Token	For basic authentication
X.509 Certificate	Public Key Infrastructure is use for verification purpose
WS-Policy	Policies or conditions may be applied by web service providers
WS-Addressing	XML Framework for standard specification of message
WS-Trust	Security token renewing, issuing, validation
WS-Secure Conversation	Safe conversation between services

TABLE 2 : WEB SERVICE SECURITY STANDARDS

The basic **XML Signature structure**per[7] is shown in Figure 1, which is as follows:

```
<Signature ID?>
  <SignedInfo>
    <CanonicalizationMethod/>
    <SignatureMethod/>
    (<Reference URI?>
    (<Transforms>)?
    <DigestMethod>
      <DigestValue>
        </Refernce)+
  </SignedInfo>
  <SignatureValue>
    (<KeyInfo>)?
    (<Object ID?>)*
</Signature>
```

FIGURE 1 : XML SIGNATURE STRUCTURE

The basic **XML Encryption structure**per[7] is shown in Figure 2, which is as follows:

```
<EncryptedData id? Type? MimeType? Encoding?>
  <EncryptionMethod/>?
  <ds:KeyInfo>
    <EncryptedKey>?
    <AgreementMethod>?
    <ds:KeyName>?
    <ds:RetrievalMethod>?
    <ds:*>?
  </ds:KeyInfo>
  <CiperData>
    <CiperValue>?
    <CiperReference URI?>?
    </CiperData>
  <EncryptionProperties>?
</EncryptedData>
```

FIGURE 2 : XML ENCRYPTION STRUCTURE

The above Web services securities defined are not enough as there are lot of new attacks registered shows the complexity of XML security have large potential vulnerabilities like XML Signature Wrapping[8].

III. LITERATURE OVERVIEW

Web services are used to provide a Web Application Programming Interface easier which has resulted many loop holes in their security. They come with few issues of their own which can be problematic to someone who doesn't handle them correctly and in the right manner. Web services provide information about all the requests which are offered to the interface by an incoming application and based on that information which is being provided, nature of attack isdecided by the hacker to steal the information hidden in the web service message.

There are many attacks on XML messages that can possibly affect the building blocks of Web Services such as confidentiality, integrity and availability. The most common attacks per[4] and [1] are as follows:

Denial of service is commonly known as DOS-attack. This type of attack is an ancient type of attack in which a web server receives an overwhelming number of requests which causes the web server to be hanged up. Due to the overwhelming number of requests, the target doesn't know how to deal with them and the web server chokes. This type of attack is mostly intended attack but DOS-attack can also occur unintended. DOs attack also has a sibling which is known as DDOS (distributed denial of service) which is a same type of attack as DOS attack but in this attacker targets number of servers until they are choked.

Replay attack is like DOS attack but in this attack, attacker capture and copies the data and replays the same message to a web service. This is the most basic type of attack in which the user does not require to know the contents of the data, also this type of attack is easier to detect since the pattern of the message are repeating over again and again which makes this attack easier to detect.

SQL Injection is a type of attack; attacker inject SQL queries through input of web page which can alter and modify the contents of database. This type of attack is done to get access of the database where the data of the application resides[9]. Attackers can retrieve any important information which can harm the integrity of the database so preventing this type of attack is very important as it can harm your database and your application as well.

Cross-site Scripting Flaw attack is also known as XSS. This type of attack occurs when an attacker transport an infected code to a different end user using web service. Mostly these types of attacks are done through tags which includes <script>, <body>, <img>, <input>etc. where attacker can give reference of external JavaScript or can embed the code within those tags. A successful cross-site scripting attack can expose user's session token.

SOAP messages confidentiality and integrity are provided by XML encryption and signature standards are. XML signature includes two mandatory elements which are <Signed Info> and <Signature Value>. When an attacker who is listening the SOAP, messages moves the original SOAP body to SOAP header and attaches a new SOAP body and enforces the new service removing the original one.**Signature wrapping attack**per [1]:

```
<soap:Envelope>
  <soap:Header>
    <ds:Signature>
      <ds:SignedInfo>
        ....
      </ds:SignedInfo>
    </ds:Signature>
    <soap:Body wsu:Id="body">
      <deleteUser>
        <usr>John</usr>
      </deleteUser>
    </soap:Body>
  </soap:Header>
  <soap:Body wsu:Id="attack">
    <setAdminRights>
      <usr>John</usr>
    </setAdminRights>
  </soap:Body>
</soap:Envelope>
```

FIGURE 3 : SIGNATURE WRAPPING ATTACK

To minimize the security risks to get struck by any of these threats many secure mechanisms has been developed to cater those risks. The two main standards for XML security are XML Signature and XML Encryption.

XML Signature are also known as XML Digital Signature (XDSIG). XML was jointly developed by the W3C and Internet Engineering Task Force (IETF) to optimize digital signature for XML documents, to ensure integrity of XML data [5]. Since XML signature supports other types of data as well so it is also known as "XML aware digital signature"[4].Capturing of digital signature operation results for other XML data is also done by XML signature and it defines its schema as well. XML signature not only provides us to sign the whole document but it can also be used to sign the partial document and to have multiple signatures in a document which is an important feature in distributed environment. XML signature represents the encrypted data in the document not the primary data. There are three types of XML signatures per[5] which are: Enveloped Signature, Enveloping Signature and Detached Signature.

Enveloped XML Signature is the signature in which XML signature is present in the document and is the child element of the object in the document being signed. Enveloped

signature must make sure that their own content of signature element must remain aloof from the data digest and signature value calculations[7]. Basic structure of Enveloped XML Signature per [5]

```
<document>
  ..... Data
  <signature>
    ..... Contains
    reference to the data
    being signed
  </signature>
</document>
```

FIGURE 4 : ENVELOPED XML SIGNATURE

In **Enveloping XML Signature**, the data which is being signed is closed in the <signature> and </signature> tags. <document> and </document> tags are included in the XML Signature as the child element. Basic structure of Enveloping XML Signature per [5]

```
<signature>
  ..... Contains
  reference to the data
  being signed
  <document>
    ..... Data
  </document>
</signature>
```

FIGURE 5 : ENVELOPING XML SIGNATURE

In **Detached XML Signature**, XML Signature is in separate document which is most likely to be non-xml format. Reference of Signed XML Document's location is given in the XML Signature. Also, detached XML Signature can be put to the data objects that are present in the same XML document [7]. Basic structure of Enveloping XML Signature per [5]

```
<signature>
  ..... Contains
  refernce to the data
  being signed
</signature>
```

FIGURE 6 : DETACHED XML SIGNATURE

The contents covered in the digital signatures must be identical on the signature application otherwise a digital signature gets invalid. However, this is not the case of digital signatures on XML document where minoralteration can affect the signed XML fragments if the contents are same to the XML Parser. White spaces which are included in the XML document are of no importance now as they are not being considered during XML Parser. By using XML Signatures, it can help in removing many security problems such as spoofing, falsification.

XML Encryption is a W3C recommendation. It is a mechanism to encrypt data and then to decrypt that encrypted data and eventually showing the results using syntax of XML. It can be used to hide sensitive information in an XML by using cryptographic algorithm. Like XML signature, XML encryption allows the encryption of specific parts of XML document rather than doing all the encryption of that document, it also supports multiple encryption of the data which is an important feature in business sector where different parties must cooperate on certain things[7].
XML encryption and signature both uses Key Info element which provides information regarding what key to use in validating a signature to a recipient or to decrypt the encrypted data. Ciphered data element contains the secret value and it also contains the data reference which needs to be ciphered as shown in Figure 2. To encrypt an XML document usually RSA or triple DES is used. XML encryption ensure that users data is authenticated, remains confidential and integrated but it is practically unimportant to encrypt the data if the same data is sent to a lot of people so for this purpose XML signature ensures the data integrity and user authentication among the group of people where the same data is shared [5].

To resolve Signature Wrapping Attack which is shown in Figure 3, per [1] schema should be hardened and then it should be used for validating the SOAP message. [1] Shows how to counter the **Signature Wrapping Attack** which is shown in Figure 7:

```
<xs:complexTypename="Envelope">
  <xs:sequence>
    <xs:element ref="tns:Header" minOccurs="0" maxOccurs="1"/>
    <xs:element ref="tns:Body" maxOccurs="1"/>
  </xs:sequence>
  <xs:anyAttribute namespace="##other" processContents=lax"/>
  </xs:complexType>
```

FIGURE 7 : SOAP MESSAGE VALIDATION

To counter SQL injections in web Service, per [10], different tools should be used to prevent and check SQL injections like WAVES which is a black box technique and it is very efficient in testing for SQL injection, it also can monitor the application using machine earning technique. SQLDOM can also be used which can protect the database

from un-trusted authorization to databases. SQLDOM uses an API for all the systematic query building. Another tool, which can be used to prevent SQL injection is to use SQL Prevent, it uses an HTTP request interceptor and it modifies the original dataflow when it is deployed on web server making theapplication more secure and securing the database from infected SQL statements.

XML message security issues are not only limited to enterprise applications but they are also very much involved in cloud computing as well where many issues occur like malware attacks in which hackers inject their malicious codes into their cloud service and can remotely access their commands like Sony's PlayStation was a victim of malicious code attack. Wrapping attacks also occurs in cloud.

To protect your Web Services in cloud, your cloud should be private where only limited users can access it.Also, other countermeasures should be taken like enhancing the cloud security policy which can reduce the risk of abuse in cloud. Data should be protected from insiders which can cause the main threat to web services message in cloud by using the tools which include user behavior profiling and decoy technology [11].

IV. SURVEY

A survey is circulatedtoanalyze the Web Service Message Security in Applications Integration. Survey is circulated in software Houses and Financial institutions. Participants were selected among the categories; Software Engineers andIT Professionals and organization's management.

Survey is circulated in such a way that a questionnaire is given to the participants with a short overview about the concerned terminologies. Appendix A is attached for the questionnaire.

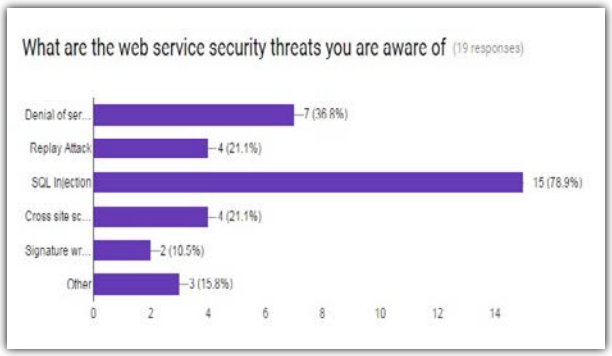

FIGURE 8 : WEB SERVICE SECURITY THREATS

As per our survey results from Figure 8, majority of them choses SQL Injection as the most common web service security threats they were aware of probably because this is the most common attack that happen in enterprise applications.

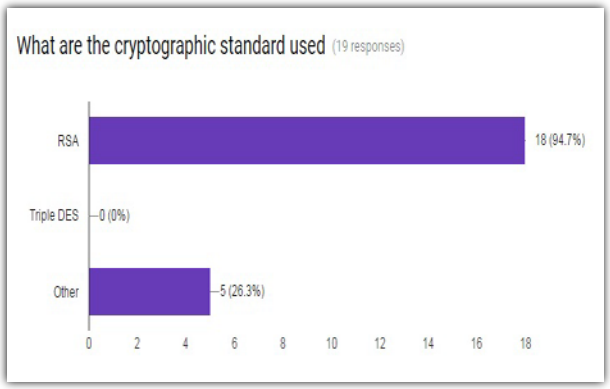

FIGURE 9 : CRYPTOGRAPHIC STANDARDS

As per our survey results from figure 9, majority of them choses RSA as the most common cryptographic standard used in their web service message integration followed by others.

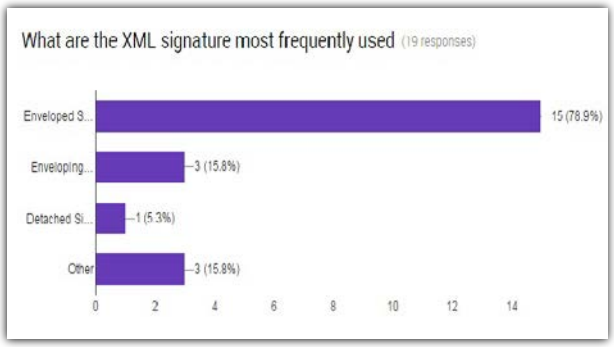

FIGURE 10 : XML SIGNATURES

As per our survey results from Figure 10, Enveloped signature was the most frequently used XML signature by everyone in their web service security where signature is a child element of the data.

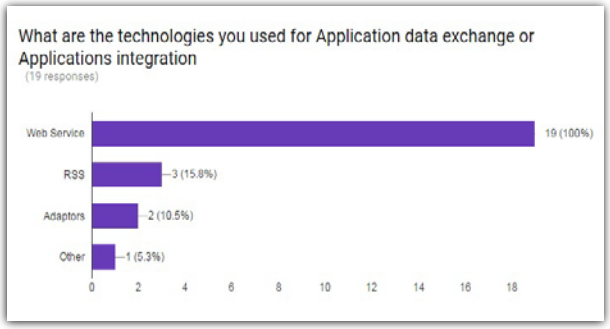

FIGURE 11 : TECHNOLOGIES FOR APPLICATION INTEGRATION

As per our survey results from Figure 11, web service was a clear winner when it comes to application integration

because it provides easy access to the application and provides standards too. It was followed by RSS and adapters.

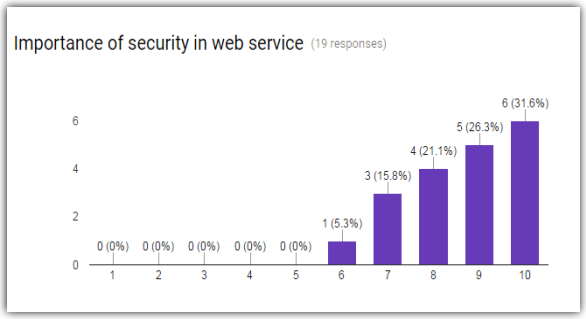

FIGURE 12 : IMPORTANCE OF SECURITY IN WEB SERVICES

As per our survey results from Figure 12, everyone considers the importance of web security as a major part in their application integrations and they can't compromise on it.

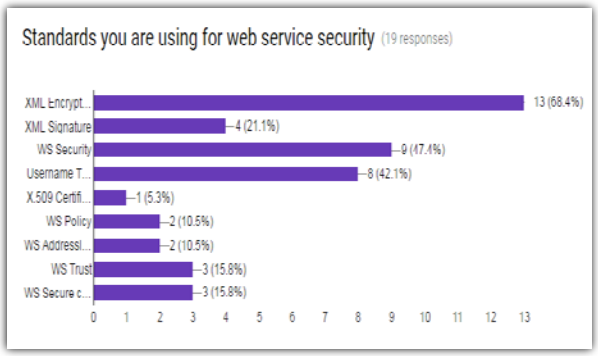

FIGURE 13 : COMMONLY USED SECURITY STANDARDS

As per our survey results from Figure 13, XML Encryption and WS Security was the commonly used security standards in their application integration because XML encryption allows the encryption of specific parts in XML messages and you don't have to provide encryption to whole XML which makes it the most favorable web service security standard.

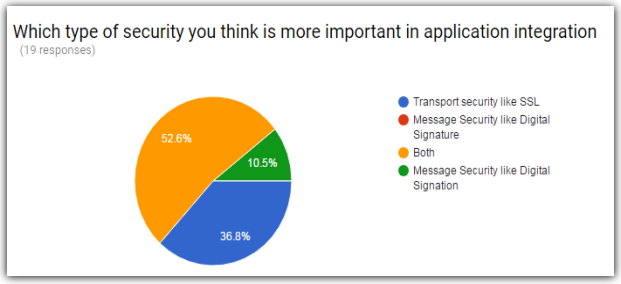

FIGURE 14 : SECURITY IN APPLICATION INTEGRATION

As per our survey results from Figure 14, majority of them choses both end to end and transport level security are important from application integration which is followed by the transport security.

V. ANALYSIS

The following results have been concluded based on responses of the questionnaire.

Question	Result
Web Service Security Threat	Most of the threats are aware out of which SQL Injection is most known threat.
Cryptographic Standards	RSA is the most common standard in Pakistan
XML Signature	Enveloped XML Signature is widely used
Technologies for Application integration	Web Service Technology is the mostly used for application integration
Importance of security in Web Services	Security is a part and parcel of web services
Commonly used security Standards	XML Encryption, XML Signatures and WS Security are commonly used security standards
Security in Application integration	Both end to end and transport level security is in practice

TABLE 3 : ANALYSIS

VI. CONCLUSION& FUTURE WORK

From the above literature overview and questionnaire analysis we have come to the point that in Pakistan, web service is the most successful and frequently used technology for the data interchange among the enterprise applications. However, security concerns are there that are to be resolved using different techniques. A lot of new techniques are coming to cater these security concerns including XML Signatures and XML Encryptions. The awareness about these security concerns and their counter techniques is increasing making the web service more and more robust technology for enterprise application integration.Potential Future work will be to extend all the work which have been done currently in XML message security where it can support encryption in multiple files and it can also be able to define multiple receiver of that XML file which is encrypted. It can also be further improved in cloud computing as well where better security

policy and data management can be done for XML security like for countering XML signature wrapping attack FastXPath can be used which is a subset of XPath to resist all the attacks that are being injected into XML SOAP message

Bibliography

[1] M. Priyadharshini, I. Suganya and N. Saravanan, "A Security Gateway for Message exchange in Services by Streaming and Validation," *International Journal of Innovative Research in Computer and Communication Engineering*, vol. 1, no. 3, pp. 604-612, 2013.

[2] S. K. Lippert and C. Govindarajulu, "Technological, Organizational, and Environmental Antecedents to Web Services Adoption," *Communications of the IIMA*, vol. 6, no. 1, pp. 147-160, 2006.

[3] Q. Z. Sheng, X. Qiao, A. V. Vasilakos, C. Szabo, S. Bourne and X. Xu, "Web services composition: A decade's overview," *Information Sciences*, p. 218–238, 2014.

[4] M. Holtkamp, "The role of XML Firewalls for Web services," 1ST TWENTE STUDENT CONFERENCE ON IT, Enschede, 2004.

[5] R. K. Saravanaguru, G. Abraham, K. Venkatasubramanian and K. Borasia, "Securing Web Services Using XML Signature and XML Encryption," ARXIV, Vellore, 2013.

[6] Wikkipedia, "Wikkipedia," 02 Feb 2017. [Online]. Available: https://en.wikipedia.org/wiki/WS-Security.

[7] A. E.-A. Ahmed and K. Arputharaj, "A Comprehensive Presentation to XML Signature and Encryption," in *International Conference on Recent Trends in Information Technology (ICRTIT)*, Chennai, 2013.

[8] J. Somorovsky, On the insecurity of XML Security, Bochum: Ruhr-Universität, 2013, p. 169.

[9] V. R. Mouli and K. Jevitha, "Web Services Attacks and Security- A Systematic Literature Review," in *6th International Conference On Advances In Computing & Communications, ICACC*, Cochin, 2016.

[10] S. Charania and V. Vyas, "SQL Injection Attack :Detection and Prevention," *International Research Journal of Engineering and Technology (IRJET)*, vol. 03, no. 04, pp. 1496-1501, 2016.

[11] T.-S. Chou, "SECURITY THREATS ON CLOUD COMPUTING VULNERABILITIES," *International Journal of Computer Science & Information Technology (IJCSIT)*, vol. 5, no. 3, pp. 79-88, 2013.

AUTHORS

First Author – Syed Umair Hassan, MSCS, Institute of Business Administration (IBA), suhassan@khi.iba.edu.pk
Second Author – Farrukh Saleem Sheikh, MSCS, Institute of Business Administration (IBA), farrukhsheikh@khi.iba.edu.pk.

Correspondence Author – Waqas Mehmood, wmehmood@iba.edu.pk

VII. APPENDIX A

4/12/2017

Web Service Message Security in Application Integration

A short survey about the importance of web services securities and standards in software industry of Pakistan

*Required

1. Emailaddress*

_____

2. Whatare the web service security threats you are aware of?

   Tick all that apply.

   - [ ] Denial of service
   - [ ] Replay Attack
   - [ ] SQL Injection
   - [ ] Cross site scripting flaw
   - [ ] Signature wrapping
   - [ ] Other: _____

3. What are the cryptographic standard used?

   Tick all that apply.

   - [ ] RSA
   - [ ] Triple DES
   - [ ] Other: _____

4. What are the XML signature most frequently used?

Tick all that apply.

- [ ] Enveloped Signature
- [ ] Enveloping Signature
- [ ] Detached Signature
- [ ] Other: _____

5. Which type of Organization you are working in

Mark only one oval.

- ◯ Software House
- ◯ Bank
- ◯ Research and Development
- ◯ Educational
- ◯ Service Provider
- ◯ Other: _____

6. What are the technologies you used for Application data exchange or Applications integration?

**Tick all that apply.*

- [ ] Web Service
- [ ] RSS
- [ ] Adaptors
- [ ] Other: _____

7. Web Service for Enterprise Integration

Mark only one oval.

1	2	3	4	5	6	7	8	9	10
◯	◯	◯	◯	◯	◯	◯	◯	◯	◯

8. Importance of security in web service

Mark only one oval.

1	2	3	4	5	6	7	8	9	10
◯	◯	◯	◯	◯	◯	◯	◯	◯	◯

9. Factors you are using in web service security

Tick all that apply.

- ☐ Authentication
- ☐ Authorization
- ☐ Integrity
- ☐ Confidentiality
- ☐ Privacy
- ☐ Other: _____

10. Standards you are using for web service security

Tick all that apply.

- [ ] XML Encryption
- [ ] XML Signature
- [ ] WS Security
- [ ] Username Token
- [ ] X.509 Certificate
- [ ] WS Policy
- [ ] WS Addressing
- [ ] WS Trust
- [ ] WS Secure conversion

11. Most important factor/standard of WS security

Mark only one oval.

- Authentication
- Authorization
- Integrity
- Confidentiality
- Privacy
- XML Encryption
- XML Signature
- WS Security
- Username Token
- X.509 Certificate
- WS Policy
- WS Addressing
- WS Trust
- WS Secure conversion

12. Which type of security is more important in application integration *

Mark only one oval.

- Transport security like SSL
- Message Security like Digital Signatures
- Both

Send me a copy of my responses.

Powered by

Google Forms