Review Paper on Web Service Security

Lekha V. Bhandari
Computer Science & Engineering
G. H. Raisoni College of Engg. & Management
Amravati, India
lekha_bhandari@rediffmail.com

Avinash P. Wadhe
Computer Science & Engineering
G. H. Raisoni College of Engg. & Management
Amravati, India
aviwadhe@gmail.com

***Abstract* — a web service is a software system that is designed to support machine to machine interoperable interaction of systems over a network. Web services provide a framework for system integration without depending on programming language and operating system. It is widely deployed in current distributed systems and has become the technology of choice. The Web services have become more suitable now for integrating heterogeneous systems and are largely facilitated through its extensive use of the Extensible Markup Language (XML). Hence, the security of Web services based system depends not only on the security of the services but also on the confidentiality and integrity of the XML based SOAP messages that are used for communication. Now-a-days, Web services have generated huge interests in vendors and researchers. A web service is based on existing Internet protocols and open standards, and also provides a flexible solution to various problem of application integration. This paper provides an overview of the web services, web service security and the various algorithms used for encryption of the SOAP messages.**

Keywords: Web service, Web services security, Web services security standards.

I. INTRODUCTION

A web service is a network accessible interface to various application functionalities, built using standard Internet technologies illustrated in Figure 1.

Figure 1. A web service allowing access to application code

In other words, if an application can be accessed over a network using some combination of protocols like HTTP, XML, SMTP, or Jabber, then it is a web service. A web service can also be defined as a software system designed to support interoperable machine to machine interaction over a network. Web services provide a framework for system integration without being dependent of programming language and operating system.

A web service is an interface that is positioned between the application code and the user of that code as shown in figure 2. Web service acts as an abstraction layer, this layer separates the platform and the programming language specific details of how an application code is actually invoked, and this standardized layer shows that any language that supports the web service can also access the application's functionality.

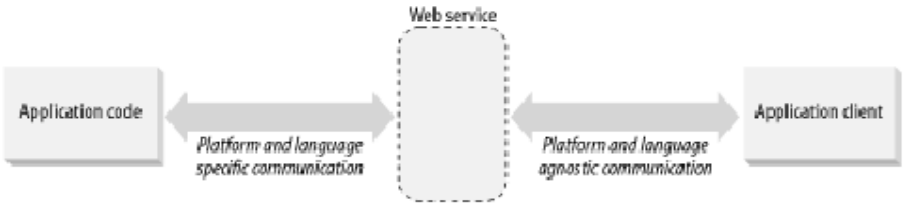

Figure 2. Web services providing an abstraction layer between the application client and its code

Now-a-days the web services that we see deployed on the Internet are HTML web sites. In these, the application services that are the mechanisms for publishing, managing, searching, and retrieving contents are being accessed through the use of standard protocols and data formats like HTTP and HTML. Client applications (various web browsers) that understand these standards can interact with the application services to perform various tasks like ordering books, sending greeting cards, or reading news etc. As this standard based interface provides abstraction, it does not matter whether the application services are written in Java and the browser written in another language like C++, or the application services deployed on a Unix box or any other system while the browser is deployed on Windows. Web services also allow for cross platform interoperability that makes the platform irrelevant and is one of the key benefits gained from implementing web services. There is currently an ongoing effort within the Java community to define an exact architecture for implementing web services within the framework of the Java 2 Enterprise Edition specification. Each of the major Java technology providers such as Sun, IBM, BEA, etc. are all working to enable their platforms for web services support and many significant application vendors such as IBM and Microsoft have completely embraced web services. Today IBM is integrating web services support throughout their Web Sphere, Lotus, and DB2 products, and Microsoft's new .NET development platform is built around web services that are a messaging framework. The requirement placed on a web service is only that it must be capable of sending and receiving the messages using some combination of various standard Internet protocols.

The Web service are in more use and being suitable for integrating heterogeneous systems and is largely facilitated through its extensive use of the Extensible Markup Language (XML). The interface of a Web service is described using the XML based Web Services Description Language (WSDL). The communication is performed using XML based SOAP messages. Hence, the security of a Web services based system depends on the security of the services themselves as well as on the confidentiality and integrity of the XML based SOAP messages used for communication. The Organization for the Advancement of Structured Information Standards (OASIS) and the World Wide Web Consortium (W3C) has standardized several specifications that are related to security in Web services and XML. Now-a-days web services are emerging as a systematic and extensible framework for application to application interaction and are built on top of existing Web protocols and open XML standards. Web services are a new class of Web applications and are self-contained, self-describing, modular applications that can be published, located, and invoked across the Web.

Web services perform various functions that can be anything like from simple requests for information to creating and executing complicated business processes. If a web service is deployed once, it can be discovered and invoked by the other applications or other Web services. The advantage of using Web services is the ability to create applications through the use of loosely coupled and reusable software components; this has fundamental implications in technologies and business applications. The business services can be reorganized and distributed over the Internet and also can be accessed by a wide variety of communications devices. Businesses can be released from the load of complex, low and costly software integration and focus instead on the value of their offerings. In this way, the Internet will become a universal platform where organizations and individuals converse with each other to carry out various commercial activities and to provide value added services. The fences to provide new offerings and entering new markets will be hand down to enable access for small and medium sized enterprises. Dynamic enterprises and dynamic value chains become reachable and may be even fixed for competitive advantages.

The Web services background is divided into three areas — communication protocols, service descriptions, and service discovery and specifications are being established for each. The following specifications are presently most stable in each area:

1. The simple object access protocol (SOAP) that enables communications among Web services. It is fundamentally a stateless and a one way message exchange standard that enables applications to create more difficult interaction patterns like request/response, request/multiple responses, etc. by combining one way exchanges with types provided by an underlying protocol and application detailed information.
2. The Web Services Description Language (WSDL) that provides a formal, computer-readable description of Web services. It provides a model and an XML format for labeling Web services. WSDL defines services as groups of network endpoints or ports.
3. The Universal Description, Discovery and Integration (UDDI) directory that is a registry of Web services descriptions. It provides a mechanism for clients to discover Web services. Web services are important only if potential users may find information appropriate to permit their execution.

II. LITERATURE REVIEW

The amazon web services provided an overview of the various security processes they have used for providing security to web services [1].

Joe M. Tekli, Ernesto Damiani, Richard Chbeir and Gabriele Gianini gave an overview of current research related to SOAP processing performance enhancement that focused on similarity based methodologies, as well as the web service Security optimizations, and XML parallel processing structural designs. Most methods form on the observation that SOAP message exchange usually includes highly similar messages. They identified the collective parts of SOAP messages, to be processed once, only restating the processing for parts which are unlike, and reducing SOAP processing overhead [2].

Nils Agne Nordbotten has provided an overview of recent security standards for XML and Web services. These standards provide a stretchy framework for fulfilling basic security requirements such as confidentiality, integrity, and authentication, as well as more difficult requirements such as, authorization, and federated identities. Various mechanisms such as those provided by Web Services Policy and the Web Services Description Language (WSDL) may also provide appreciated sources of information to an attacker who is trying to find weaknesses in a system. Though XML firewalls may be able to identify messages trying to feat these vulnerabilities, the use of end to end encryption may effectively inhibit such detection [3].

Hongbing Wang, Joshua Zhexue Huang, Yuzhong Qu, Junyuan Xie have presented the basic idea about Web services. They presented three aspects of Web services that are the service security, the service composition, and the service semantics. They are dangerous to the successful utilization of Web services [4].

Doug Tidwell, James Snell, Pavel Kulchenko has mentioned in their book that a critical insight is that web services don’t replace current technology infrastructures. Rather, they help to incorporate existing technologies. If one needs a J2EE application to talk to another application than web services makes it easier. Web services won't completely replace old mainframe system in the back private that nobody ever thinks about anymore. But web service provides cross platform automated access to the mainframe's applications, hence opening new networks of business [5].

III. SYSTEM OVERVIEW

The Web Services architecture is based upon the three roles that interact with each other as service provider, service registry and service requestor. These interactions involve publish, find and bind operations. These roles and operations together act upon the Web Services artifacts that are the Web service software module and its description. A service provider hosts a network reachable software module that is an implementation of a Web service. The service provider describes a service description for the Web service and publishes it to a service requestor or service registry. The service requestor makes use of the find operation to recover the service description or from the service registry and uses the service description to bind with the service provider and raise or interact with the Web service implementation. Service provider and service requestor roles are the logical constructs and a service can reveal characteristics of both. Figure 3 illustrates these operations, the components providing them and their interactions.

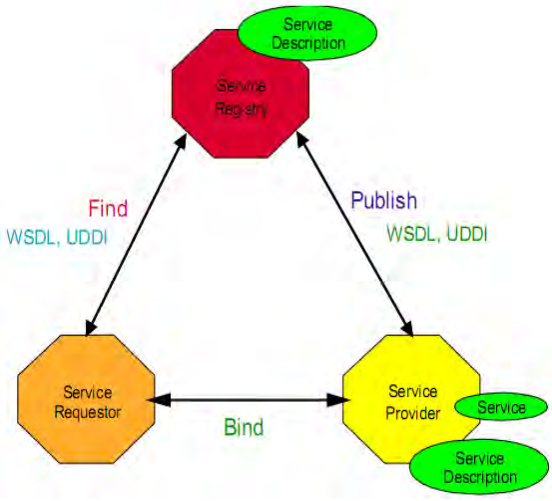

Figure 3: Web Services Architecture

Three Roles in Web Services Architecture

1. Service provider: This is the owner of the service from business point of view and from an architectural point of view; this is the platform that hosts access to the service.

2. Service requestor: This is the business that requires certain functions to be satisfied from business point of view and from an architectural point of view, this is the application that is looking for and invoking or initiating an interaction with a service. The service requestor role can be played by a browser obsessed by a person or a program without any user interface.

3. Service registry: It is a searchable registry of service descriptions where service providers publish their service descriptions. The service requestors find services and obtain binding information in the service descriptions for services during the development for static binding or during execution for dynamic binding. The service requestors can obtain a service description from other sources additional to a service registry, such as a Web site.

A. The Operations in Web Service Architecture

To take advantage of Web Services for any application, the three behaviors should take place:

Publication of service descriptions, finding of service descriptions, and binding of services based on the service description. These behaviors can occur iteratively and these operations are as follows:

1. Publish: A service description needs to be published to be accessible so that the service requestor can find it, where it is published can vary depending upon the requirements of the application.

2. Find: In the find operation, the service requestor recovers a service description directly or requests the service registry for the kind of service required.

3. Bind: A service needs to be invoked. In the bind operation the service requestor invokes or initiates an interaction with the service at runtime using the binding details in the service description to locate, contact and invoke the service.

B. The Artifacts of a Web Service

1. Service: A service is where a web service acts as an interface that is described by a service description and is implemented. It is also a software module deployed on network available platforms provided by the service provider. It exists to be raised by a service requestor. It can also function as a requestor, using other Web Services in its implementation.

2. Service Description: The service description contains the details of the interface and implementation of the services. This includes its data types, operations, binding information and network location. It could also include classification and other metadata to facilitate the various discoveries and utilization made by service requestors. The service description may be published to a service requestor or service registry. The Web Services structural design explains how to instantiate the elements and implement the operations in an interoperable way.

IV. WEB SERVICES SECURITY

In web services background, security means that the recipient of a message should be able to validate the reliability of a message and to make guaranteed that it has not been altered. Web Service Security defines the tool to include integrity, confidentiality, and single message authentication structures within a SOAP message. Web Service Security uses the XML Signature and XML Encryption specifications as well as defines how to include digital signatures, message digests, and encrypted data in a SOAP messages. Web Service Security is apprehensive with security for SOAP messages, and hence web service security clearly builds on uppermost of SOAP. Web service security also makes use of XML Signature and XML Encryption. The Web Services Security provisions aim to provide an outline for building secure web services using SOAP and consist of a core specification and numerous additional profiles. XML Encryption is being utilized to provide confidentiality, while message integrity is provided through the use of XML Signature through which the SOAP message body elements, selected headers or any combination may be signed or encrypted using unlike signatures and encryptions for unlike SOAP roles that because SOAP message headers may be subject to processing and modification by SOAP intermediaries, lower layer security mechanisms such as SSL are unsatisfactory to ensure end to end integrity and confidentiality for SOAP messages. The functionality providing web service security is needed if confidentiality and integrity are required for such messages.

A major performance traffic exist in SOAP message processing and the reason for SOAP performance criticality is because of two reasons as: On one side, SOAP communication creates network traffic, and causes higher potential than the other competing technologies. On the other side, and perhaps more importantly, the generation and parsing of SOAP messages and their conversion to and from in memory application data can be computationally very expensive.

Since the XML encryption doesn't provides security in web services and hence an algorithm can be used to provide security to web services. However, the recent Web services architectures are antagonized with a few

problems like security and many algorithms is used for performing cryptographic operations with symmetric key based security symbols. Current XML encryption used is symmetric key encryption and authenticity of message can't be assured. Public key encryption allows the use of RSA which enables the recipient of a message to verify that the message is really from a particular source. The recipient might receive a message privately so that unauthorized users could not read it, know the identity of the sender and determine whether or not the center is authorized to carry out the operation requested in the message and these are frequently met through encrypting messages. Security is difficult to the adoption of Web services by various enterprises, but the Web services structure does not meet simple security requirements. The point that the Web services involve exchange of messages means that securing the message exchange is an important issue to consider when building and using Web services. On the other side, because Web services allows all the internal systems as well as external systems to communicate on HTTP ports, these application servers are predictably opened up to application level attacks. Some few standards have been introduced to improve the message security problems, including web service security and various other enterprises towards enabling digital signatures on XML messages and the transactions.

There are four basic security requirements that the Web Services security layer must provide as follows:

1. Confidentiality, where information is not made available or disclosed to unauthorized individuals, entities, or processes, and it also guarantees that the contents of the message are not disclosed to unauthorized individuals.
2. Authorization is the yielding of authority, which includes the conceding of access based on access rights and also guarantees that the sender is authorized to send a particular message.
3. Data integrity is the property that data has not been undetectably changed or damaged in an unauthorized manner or by unauthorized users thereby ensuring that the message was not altered accidentally in transit.
4. Proof of origin is indication that identifies the originator of a message or data. It states that the message was transmitted by a properly identified sender and is not a replay of a previously transmitted message. This requirement implies data integrity.

V. SECURITY ALGORITHMS

Web Service security is big challenge for researchers as it requires a strong security algorithm for the encryption of data. The xml encryption scheme is being used presently for encrypting the messages between the different programming languages running on different platforms, but this xml encryption algorithm is symmetric key encryption algorithm and it creates communication overhead, hence there is need to use an asymmetric key encryption algorithm.

The more powerful version of DES is used for high security called Triple-DES. To start encrypting with Triple-DES, two 56-bit keys are selected and the data is encrypted via DES three times, the first time by the first key, the second time by the second key and the third time by the first key once more. This process creates an encrypted data stream that is unbreakable with today's code-breaking techniques and existing computing power, while being compatible with DES. Today, the National Institutes of Standards and Technology considers DES an absolute technology that is suitable only for legacy applications and supports a new standard called Advanced Encryption Standard.

AES is a newer encryption standard and is now the preferred one to use for XML Encryption. AES is a substitution linear transformation network having 10, 12, or 14 rounds, depending on the various key sizes which are currently set at 128, 192, or 256 bits. The block size used in AES is 16 bytes and the data block to be processed is divided into an array of bytes developing a matrix with rows and columns.

Symmetric ciphers uses the same key for encryption and decryption that means both sides need to have it, and it needs to be kept secret, because anyone knowing the key can decrypt all messages encrypted with it. DES and AES are the examples of symmetric ciphers. Asymmetric ciphers use two types of keys, a public key for encryption and a private key for decryption. The advantage is that there is no damage in communicating the public key to anyone because it cannot be used to decrypt any data. Whereas the private key doesn't need to be sent to anyone and is easier to keep secret. RSA is an example of an asymmetric cipher and these ciphers are generally more compute intensive and hence they are hardly used to encrypt messages of large size.

AES and DES are symmetric cipher that means that both parties must know a shared key. The problem of distributing the key is not small, and there exist well known algorithms for doing this. RSA algorithm is an asymmetric key encryption algorithm and is widely known for its security empowerment. RSA involves a public key and a private key. The public key can be known by everyone and is used for encrypting messages. Messages encrypted with the public key can only be decrypted in a reasonable amount of time using the private key. But RSA key size is 1024 and this increases the communication overhead. Hence it can be implemented according to the priority of messages by using the various key sizes of RSA. Lower the priority of messages lower will be the key size, higher the priority of messages higher will be the key size.

Another algorithm used for encryption is SHA-1 algorithm. It produces a 160-bit hash value that is typically expressed as a hexadecimal number that is 40 digits long. SHA-1 is the most widely used of the existing SHA hash functions and is employed in several broadly used applications and protocols. SHA-1 appears to provide greater resistance to attacks as its implementation increases the security.

VI. PROPOSED SYSTEM:

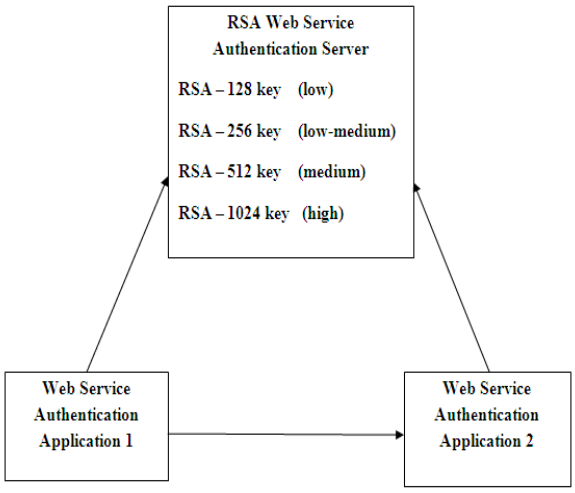

Figure 4: Web Service Secure Communication

Since Web Service security is big challenge for researchers as it requires a strong security algorithm for the encryption of data, the security algorithms mentioned above can be used for key generation and encryption of the messages. The RSA algorithm is known for its security empowerment and hence it can be used for key generation but as there are many challenges in RSA implementation for web services, the proposed system will design a security policy for RSA implementation as shown in the figure 4. There are four types of keys that can be generated with RSA algorithm i.e. 128, 256, 512, 1024 bit key size. Key size will be chosen depending upon level of confidentiality i.e. low, low-medium, medium and high. If a message is not so confidential message then it will be encrypted with 128 bit key. If request message is more confidential like checking balance in bank then it will be encrypted with 256 or 512 bit key. If request message is most confidential like transferring money in bank then it will be encrypted with 1024 bit key. Separate third party secure server will look after for RSA key generation. With this security policy communication overhead will decrease substantially. Whereas SHA-1 will be used for encryption and decryption of the messages as it provides greater resistance to the attacks.

VII. CONCLUSION

In this paper we have presented Web services, an emerging technology for the Web, The web service overview and the various security issues occurred in the implementation of the xml encryption of the messages. The security of web services is an important aspect and hence a security algorithm is required to implement in web services for key generation and encryption decryption of the messages.

The security algorithm described in this paper will be used together in combination for key generation and encryption decryption of the messages which will provide strong security in web services.

REFERENCES

[1] Amazon web services: Overview of Security Processes, June 2013.
[2] Joe M. Tekli, Ernesto Damiani, Richard Chbeir and Gabriele Gianini, “SOAP Processing Performance and Enhancement” IEEE Transactions On Services Computing, Vol. 5, No. 3, July-September 2012.
[3] Nils Agne Nordbotten, “XML and Web Services Security Standards”, IEEE Communications Surveys & Tutorials, Vol. 11, No. 3, Third Quarter 2009.
[4] Hongbing Wang, Joshua Zhexue Huang, Yuzhong Qu, Junyuan Xie, “Web services: Problems and Future Directions”, 2005.
[5] “Programming Web Services with SOAP”, Doug Tidwell, James Snell, Pavel Kulchenko, First edition, December 2001.
[6] Web Services conceptual architecture, By Heather Kreger IBM Software Group, 2001.
[7] Locktyukhin, Max; Farrel, Kathy (2010-03-31), "Improving the Performance of the Secure Hash Algorithm (SHA-1)", Intel Software Knowledge Base (Intel), retrieved 2010-04-02
[8] http://aws.amazon.com/security.

AUTHORS PROFILE

Miss. Lekha V. Bhandari: Persuing M.E (CSE) from G.H Raisoni College of Engineering and Management, Amravati and has done B.E in Computer Science & Engineering from SGBAU, Amravati.

Prof. Avinash P. Wadhe**:** Received the B.E from SGBAU Amravati University and M-Tech (CSE) From G.H Raisoni College of Engineering, Nagpur (an Autonomous Institute). He is currently an Assistant Professor with the G.H Raisoni College of Engineering and Management, Amravati SGBAU, Amravati University. His research interest include Network Security, Data mining and Fuzzy system .He has contributed to more than 20 research paper. He had awarded with young investigator award in international conference and He is also cyber forensic certified.