Name : - Shendage Supriya Hanmant

Roll NO :- 17423

Subject :- Web Service

CASE STUDY: - REVIEW PAPER ON WEB SERVICE SECURITY

INTRODUCTION:-

Forty years ago, computers began to be connected to the Internet and data transfer among computers was already common. Since then, Internet has evolved to form a huge information space, in which users can move transparently from one machine to another. In the field of application programs, a similar development is ongoing. Distributed computing has been used as long as there have been computer networks. But at present, distributed applications are increasingly viewed and constructed as one vast computing medium .Applications which interacts between different machines to provide orchestrated services have now been deployed on a large scale. Introduce security concerns that do not exist in traditional distributed messaging techniques like RMI and CORBA. This is because the SOAP based XML messages can bypass easily traditional firewalls and this could lead to gain access to sensitive systems for non -authorized users just using the interfaces provided by the WSDL files for service description for example. The object of this paper is to explain the principles of web services architecture. It presents the concepts, standards, and the required infrastructure. It discusses and analyzes the limitations of this architecture from the security view giving also light on the challenges surrounding this aspect related to this technology.

DEFINITION OF WEB SERVICE :-

"A web service is any piece of software that makes itself available over the internet and uses a standardized XML messaging system. XML is used to encode all communications to a web service. For example, a client invokes a web service by sending an XML message, and then waits for a corresponding XML response

WEB SERVICES SECURITY:-

To secure Web services, a range of XML-based security mechanisms are needed to solve problems related to authentication, role-based access control, distributed security policy enforcement, message layer security that accommodate the presence of intermediaries. This is a principal condition to make Web services widely adopted, since no company wants to risk exposing their applications and business flows with no damage. Standardization organizations are proposing specifications in order to make these services more secure as traditional Security techniques doesn't provide security against Application level communication as they works on the Lower levels of the OSI stack of message transfer specially on transport layer. The most important standards are:

1) XML Encryption 2) XML Signature 3) WS-Security 4) WS-Policy 5) WS-Security Policy

WEB SERVICES SECURITY REQUIREMENT:-

There are many security challenges for adopting Web services. The objective is to create an environment, where message level transactions can be conducted securely in an end-to-end fashion during transit and data storage. The requirements for providing end-to-end security for Web services are summarized in

Requirement	Explanation
Authentication	Authentication is needed in order to verify the identities of the requester and provider agents. In some cases, the use of mutual authentication may be needed since the participants may not necessarily be directly connected by a single hop. Several methods can be used to authenticate services (can be combined) including: passwords, certificates, Lightweight Directory Access Protocol (LDAP), Kerberos, and Public Key Infrastructure (PKI)
Authorization	Authorization is needed in order to control access to resources. Once authenticated, authorization mechanisms control the requester access to the requested resources on the system
Data Integrity and Data Confidentiality	Data integrity techniques ensure that information has not been altered, or modified during transmission without detection. Data confidentiality ensures that the data is only accessible by the intended parties. Data encryption and digital signature techniques are used for this purpose. It must be verified in End-to-End manner
Non-Repudiation	It is a security service that protects a party to a transaction against false denial of the occurrence of that transaction by another party. It used to resolve probable disagreement.
Audit Trails	Audit trails are needed in order to trace user access and behavior. They can ensure system integrity through verification. It is often not possible to prevent the violation of obligations. Instead, if an audit guard detects a policy violation, some form of retribution or remediation must be enacted.
Distributed Security Policies	The architecture must be able to provide a security policy and enforce it across heterogeneous platforms with varying constrains and privileges

THE WEB SERVICE PROTOCOL STACK:-

Web services are built by using various related technologies. Illustrates the stack of standards on which web services are generally based on.

- **Service transport :** The service transport layer delivers messages between applications. This layer usually implements hypertext transfer protocol (HTTP), Simple Mail Transfer Protocol (SMTP) or file transfer protocol (FTP).
- **XML messaging :** This layer is responsible for encoding messages in a common XML format so that messages can be understood at both parties. This layer includes XML-RPC and SOAP
- **Simple object access protocol (SOAP) :** SOAP is a simple XML-based messaging protocol responsible for transferring data between different web services. SOAP allows communication among interacting web services by implementing a request/response model
- **Service description WSDL :** The purpose of this layer is to define the public interface of a specific web service and its description. WSDL is based on XML

- **Service discovery :** The service discovery layer registers services into a common repository and provides an easy publish/find mechanism. This layer is often implemented via Universal Description, Discovery, and Integration (UDDI) Service orchestration:

PERFORMANCES:-

Using WS-Security implies using signing and encryption. Those operations are costly in matter of resources (CPU and Memory) they can cut application throughput between 5 percent and 50 percent. A solution for this overhead could be the use of a dedicated hardware call XML Firewalls. Those hardware systems provide performance as they allow real-time processing of huge documents. But they cannot always be used as an optimal solution as this quality comes with a price and also they cannot be easily integrated with the already existing back-end software infrastructure.

CONCLUSION:-

We have seen that web services constitute a sort of automated services which communicate via Internet and rely on open Internet-based standards. We have seen also that Web services are invoked using messages instead of APIs or file formats. This works due to the independence of the service interface through the WSDL standard from the implementation. Nevertheless, web services are also subject to some limitations which include low performance, weak transaction management facilities but more critical, an immature and incomplete security framework although the presence of the WS Security framework that we presented and give a critical analysis. . It is important de note that Web Service security represents a key requirement for today's distributed interconnected electronic world. To date, the problem of security has been investigated very much in the context of standardization efforts; these efforts, however, been concentrated in adapting existing security techniques, such as encryption, for use in Web Services