CS 6301.005
DEVELOPING AND SECURING THE CLOUD

TERM PAPER #1
WS - SECURITY

TABLE OF CONTENTS

1. ABSTRACT

Web Services Security is a one of a series of specification implemented to protect from external attacks by defining security measures. It ensures the security of SOAP (Simple Object Access Protocol) by aiming at protecting the principles of authentication, confidentiality and integrity. The security of web services is of great importance to the overall security of these systems. The security mechanisms should be based on established standards in order to facilitate interoperability. The security mechanisms get updated every once in a while, as new technology gets innovated. So, the WS protocols should be flexible to accommodate enhancements or modifications. The developer can customize a security solution according to the security problems as WS-Security combines different security problems to find the best approach. For example, to enable non-repudiation and authentication features digital signature and Kerberos can be utilized. A developer can select any or combination of both.

2. INTRODUCTION

Web services are independent of operating system and programming languages and also provide services for system integration. They are widely used in cloud technologies and have become one of the most attractive choices for Software as a Service(SaaS). The web service is located across organizational domains and provide loosely coupled services which makes our work much easier.

Extensible Markup Language (XML) is used for integrating various systems in web services. For example, the web service interface can be described using XML based Web Services Description Language (WSDL). The communication of web services is performed using SOAP messages.

Thus, web service-based systems security depends on confidentiality and integrity of XML based SOAP messages used for communication along with their own security services.

Several specifications related to web services and XML security have been recognized and systematized by World Wide Web Consortium (W3C). By avoiding third party or self-defined standards and using widely accepted standards can provide advantage of interoperability and reusability. The rest of this paper is organized as follows: we discuss details of each of the security standards are provided in separate sections.

3. APPROACH

Some of the WS Security mechanism includes utilization of security tokens. The tokens mainly utilize SOAP for messaging for passing security information. They utilize binary or XML to enforce security rules. The authority of these tokens can be implemented by signing the security token as a form of verification. There are 5 token types available namely X.509 certificate, Rights Expression Language (REL), Kerberos, Username Token, SAML.

3.1. The Username Token Profile

The user Token is used as a means to identify a user by his username and his password or its equivalent like RSA key. The password can be hashed and encrypted using SHA-1 to prevent it from attacks. Utilizing timestamp and salt the passwords security can be further reinforced. By utilizing salt (random generated string added to the password) and iterations (no for times a salt is used to on the password) a shared key can be generated which then can be used by the key holder to authenticate.

But, the size of the generated key is 160 bits in an ideal case. Generally, it’s around 48-bits for most of the 8-letter passwords that can be generated using uppercase, lowercase alphabets and numbers. These keys are still susceptible to dictionary attacks.

This does not provide counter measures to prevent a Username Token from being utilized from replay attacks to a different receiver. Therefore, if the same authentication details can be used with multiple receivers, steps against such attacks must be provided. One possible countermeasure is to require the identity of the receiver to be included in the password. But such custom solutions may cause interoperability problems.

3.2. The X.509 Certificate Token Profile

The X.509 certificate token profile is an OASIS specification which defines how to include X.509 certificates in SOAP messages. It also describes the profile on the security token which is defined in standards. The certificate token is used to validate or specify the public key which is used for authenticating messages. The X.509 certificate is used for ownership of certificate token, the authentication of user. The ownership is proved by signing the message using the private key corresponding to it. X.509 certificate also plays an important role in protecting message confidentiality and integrity by applying message signing and encryption.

3.3. The Rights Expression Language (REL) Token Profile

The Rights Expression Language (REL) token profile defines how to include ISO/IEX Rights Expressions in SOAP messages. In XML and Web services, the Rights Expression Language is also called as XML Rights Management Language (XrML). A technical committee is formed in OASIS in order to standardize XrML, this committee was disbanded before reaching an agreement on a standard.

In REL/XrML, licenses used as a form to expression of rights. It grants a Cryptographic key holder some access rights and is signed digitally by the issuer. They may be used to show details of the key holder or provide authorization to perform certain actions (e.g., issuing commands, running scripts). SAML is more widely supported by Web services Security, and there are many others which provide similar features, but using SAML instead as it is more standard.

3.4. The SAML Token Profile

Security Assertion Markup Language is an open standard for exchanging authenticated data among different parties. The SAML token profile defines how the SAML assertions with security headers and references for the assertions in SOAP message. By signing a message with a key specified in SAML assertions, a binding is made between a SAML token and the SOAP message. On the other hand, the receiver trusts an attesting entity may vouch for the message to send for whom the assertion statements apply on behalf of the subject. In this case, the entity which is attesting must make sure that the integrity for SOAP messages are upholded. For example, by using digital signature etc.,

3.5. The Kerberos Token Profile

The Kerberos token is used for message security, specifically with the SOAP message security specification for web services, and is another supported token, such as the username token and the secure conversation token. The Kerberos Token can be used either to sign or/and encrypt the SOAP message. When the Kerberos ticket is referenced as a signature key, the specification defines that the signature algorithm must be a Hashed Message Authentication Code (HMAC). The Kerberos token is limited to AP-REQ message, which allows a client to authenticate a service. The ownership is provided by signing the message using corresponding key, which is similar to the

X.509 certificate. The AP-REQ is obtained outside scope of profile, this kind of functionality is provided using WS-Trust. And the functionality is provided by Kerberos specification.

4. ANALYSIS

Web services play a critical role in modern day technology so much that it has become a part and parcel of everyone’s life. But we have seen or heard about incidents where people or companies getting attacked by hackers and causing a lot of financial loss. This shows the importance of Web Service security in real life. This paper majorly talks about how to combat these issues and following are the results of the analysis obtained from the research done.

For authentication I suggest that using Kerberos as an authorization system for granting services and user name and password with salt and encryption for authentication would cover up each other’s shortcomings mentioned in the description above.

As for web policies REL provides a variety of services which enforce the rules created. Even though OASIS has tried making it a standard, it still isn’t as widely used as SAML. So, to avoid getting interoperability issues I suggest SAML for enforcing policies or rules.

There are many other methods which are not included in the analysis, the utilization of the security implementations mainly depends on the needs of the web service, company policies and its utilization. Finally, the combination of Kerberos, username, salted and encrypted password and SAML for Authorization, authentication and Web policies implementation respectively for best results.

5. CONCLUSION

The above considered security standards are expected to evolve as they gain more experience. As the new web services and patterns become more accepted, new security functionality will be required. For instance, the Web Services Business Process Execution Language (WS-BPEL) defines the business process by specifying the inter connection among other web services by creating complex service. This kind of business process may be defined by some other parties and also involve internal and external services. Thus, to ensure that such processes are in alignment with local security, some methods are required. Regardless of the above discussed security standards, they are applicable to complex services. For instance, securing the interactions or enforcing access control within the service. WS-BPEL is also used to implement web services with fault tolerance.

5. REFERENCES

- https://www.techopedia.com/definition/24385/web-services-security-ws-security

- https://ieeexplore.ieee.org/abstract/document/5208730/references#references

- https://www.ibm.com/support/knowledgecenter/en/SS7JFU_8.5.5/com.ibm.websphere.express.doc/ae/csec_kerb_auth_explain.html

- https://www.ibm.com/support/knowledgecenter/en/SSAW57_8.5.5/com.ibm.websphere.nd.multiplatform.doc/ae/cwbs_samlssoconcepts.html