ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 1, January 2017

# WSIT Security Mechanisms on the Performance of Web Services

[1] Sushma Kakkar,

[1] Department of Electronics and Communication Engineering, Galgotias University, Yamuna Expressway Greater Noida, Uttar Pradesh

[1] sushma.kakkar@Galgotiasuniversity.edu.in

**Abstract: In recent years, in the context of securing of web application layer from attacks by unauthorized users, web security has been viewed. Security of Web services has shown a significant gesture as several specifications have been developed and implemented to meet web services' security challenges. However, the performance of security mechanisms is full of concerns due to additional security content in SOAP messages, the higher number of trust-building message exchanges, as well as additional CPU time to process these additions, we consider and compare the performance of various security measures applied to a simple web service evaluated with different initial message sizes in this paper. The test results shows that security mechanisms for transport layers are considerably faster than security mechanisms for message level. In addition, the effect of adding SAML-tokens is negligible and the performance of SAML-based web services is largely dependent on the underlying security mechanisms. Eventually, compared to Non-STS Mechanisms, the performance penalty for implementing STS security mechanisms is significantly high.**

**Keywords: Security, Service, Web Services, Web.**

## INTRODUCTION

Program language-independent technology that facilitates network-to-network interoperability between system and machine. It has an interface defined using XML objects such as Web Services Description Languages (WSDL)[1]. Using a standardized XML messaging system such as the Simple Object Access Protocol (SOAP)[2], clients and other systems interact with the web service usually communicated in conjunction with other common web standards using HTTP and XML serialization. Nonetheless, the concept of interacting software from different parties poses a security threat. Text communication security is an important issue to consider in web services. It should be possible for the recipient of the text to check its validity and to ensure that it has not been updated. The letter should be sent confidentially to the recipient where it could only be read by the authorized users, know the sender's identity and decide the required activity in the message. The task of protection for web services is to understand and consider the risks of protecting a cloud-based service based on existing security strategies, while at the same time following emerging requirements to fill the gap in security for web services.

Since the interaction between service providers and requesters takes place via XML-based SOAP messages, securing web services tends to make such messages longer than they would otherwise be and therefore allows both sides to be interpreted by XML[3] parsers, That reduces web services efficiency. We discuss the impact of applying different WSIT security mechanisms to the efficiency of web services in this review paper.

*Web Services Interoperability Technology (WSIT):*

WSIT[4] incorporates a number of open web service specifications to support business features such as message routing, efficient messaging, and security. Web services depend on transportation-based encryption such as SSL to provide point-to-point security. WSIT implements WS-Security to ensure the integrity and confidentiality of interoperable message content; even when messages reach their destination endpoint via intermediate nodes. As provided by WSIT, WS-Security is an alternative to the current transportation-level security that can still be used While applying WSIT security mechanisms to enhance the security of web services, this may also lead to an increase in the size and number of SOAP messages exchanged, which may result in an increase in the time of processing and transmitting these messages over the network.

## TEST DESIGN

*Test Scenario and Cases:*

The purpose of this test is to investigate the effect of individual security mechanisms on the performance of web services. Therefore, a simple echo scenario has been designed and implemented to reduce the side effects of unrelated business logic processing. We use a basic JAX-WS echo program consisting of a web service and a database. This example is the peer-to-peer mode test; the client sends different size messages (from 1 Byte to 1MByte) and the web service echoes (send back) the same received message. The test was carried out using various initial message sizes with and without security mechanisms: 1byte to 1 Mbyte. Image. Fig. 1 illustrates the safety mechanisms that have been tested.

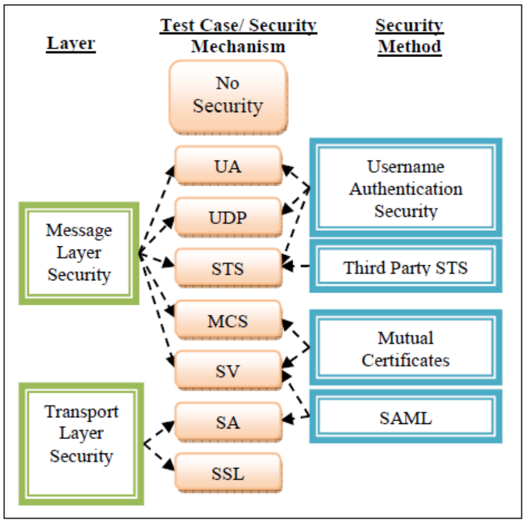

**Fig.1: Security Mechanisms**

*Test Environment and Settings*

In this paper we concentrate on increasing processing time while implementing security mechanisms[5] rather than network latency. As a result, our data is collected from a local machine; web service and customer are installed on a Dell system (RAM Pentium D CPU 2.80 GHz/3 GB) running Microsoft XP. NetBeans IDE 6.5 is used to create web service and customer service. As a web application, the web service is developed and deployed on a Glass Fish 2.2 application server. To represent the client, we used a Java SE application. Before sending the message, the initial data sent from the client to the service is generated randomly to avoid caching. To add security mechanisms to our web service, Metro's WSIT web service stack 1.4 is used.

*Evaluation Metric:*

We calculate the time spent requesting and answering on the client side as round trip time (RTT), using Java's System[6]. Nano Time. We run each test 1000 times and for each case we calculate the average RTT. In 10 different occasions, the test is then repeated. After extracting the highest and lowest averages, the results shown in this paper reflect the overall average. To determine the efficiency overhead for a specific security framework implementation, we compare the results using the Round Trip Time Increment Percentage (RTTIP):

$$RTTIP = \frac{RTT1-RTT0}{RTT0} \times 100\%$$

Where:

- RTT0 is the round trip time without applying any security mechanism deployment.
- RTT1 is the round trip time of the web service with a specific security mechanism i deployment. In our test, we use the following deployments as test cases:
  1. UA: Username Authentication with Symmetric Key.
  2. UDP: Username with Digest Passwords.
  3. MCS: Mutual Certificates Security.
  4. SSL: transport Layer Security.
  5. SA: SAML Authorization over SSL.
  6. SV: SAML Sender Vouches with Certificates.
  7. STS: STS Issued Token

## RESULTS AND DISCUSSION

The results are analyzed using different criteria in this section: security layer (transport vs. message), type of encryption[7] (symmetric vs. asymmetric), use of SAML[8] tokens, and finally type of authentication (direct vs. STS).

### 1. *Transport Security vs. Message Security;*

Figure 2 shows the huge performance gap between UA-represented message level security and SSL-based transportation level security. While the percentage increase of RTT using message level security increases as the data size increases, we can see that the use of transport layer protection is declining. The main justification is that SSL is lightweight because there is no XML parsing involved. Protection of transportation levels should therefore be used if there is no special requirement to use protection of message level, such as a web service chain, unless end-to-end protection is necessary.

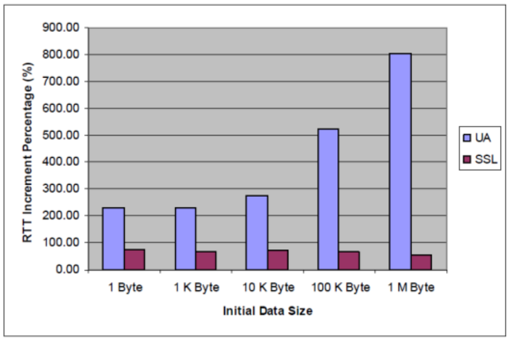

**Fig.2: Transport Security vs. Message Security**

### 2. *Username Tokens vs. Mutual Certificates:*

As shown in Figure 3, the round trip time is increased by about 220-230 percent when implementing username authentication mechanisms when the initial data size is in the range of 1 byte to 1 Kbyte. The UDP performs slightly better than UA because, unlike UA, the username token in UDP is not encrypted when digest passwords are used. In comparison, using MCS for the same data sizes increases the time of the round trip in 380-400%. The difference may be due to the use of symmetric key cryptography[9] by UA and UDP when using asymmetric cryptography by MCS, where symmetric encryption is often faster than asymmetric encryption. On the other side, of course, When large messages are exchanged between the customer and the service (i.e. 1Mbyte), we notice that the difference between UA, UDP and MCS performance decreases dramatically because most of the processing time is spent applying the actual encryption instead of manipulating the keys.

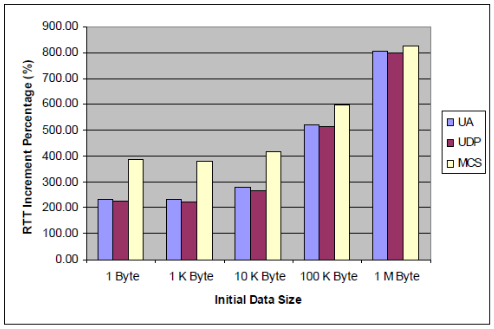

**Fig.3: Username vs. Mutual Certificates**

1. *SAML: Over SSL vs. Mutual Certificates:*

Figure 4 shows that the performance of SAML-based security mechanisms[10] (SA and SV) is primarily dependent on the underlying security system used for data protection (SSL and MCS).

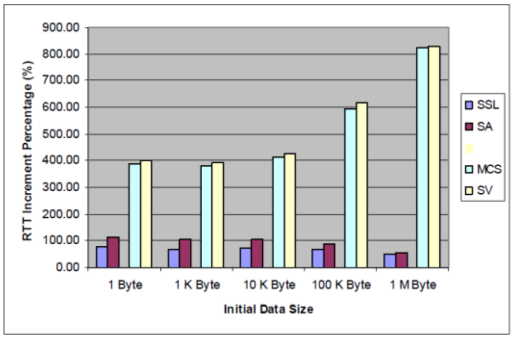

**Fig.4: SAML-Based Mechanisms Compared to their Underlying Security Mechanism**

## CONCLUSION

In this paper, we compared the performance of a number of web services security mechanisms. Our performance evaluation has shown that mechanisms that uses protection at the transport level are always quicker than mechanisms for security at the message level. Furthermore, security protocols at the message level have a problem of scalability if large messages are exchanged, unlike mechanisms based on SSL. The difference is negligible when using very large size messages inside message level security mechanisms based on username authentication. The output can be slightly improved by using digest passwords instead of encrypting the entire username token. The performance penalty for using SAML is very small and largely depends on the underlying security mechanism. Finally, the efficiency of STS security mechanisms is massively lower than Non-STS Mechanisms and should only be used when service and customer are in different areas.

## REFERENCES

[1] I. Melzer and I. Melzer, “Web Services Description Language,” in *Service-orientierte Architekturen mit Web Services*, 2010.

[2] R. G. Côté, “Simple Object Access Protocol,” in *Encyclopedia of Systems Biology*, 2013.

[3] M. Lalmas, “XML information retrieval,” in *Understanding Information Retrieval Systems: Management, Types, and Standards*, 2011.

[4] R. Vinaja, “Web Information Systems and Technologies,” *J. Glob. Inf. Technol. Manag.*, 2012, doi: 10.1080/1097198x.2012.10845614.

[5] H. Suo, J. Wan, C. Zou, and J. Liu, “Security in the internet of things: A review,” in *Proceedings - 2012 International Conference on Computer Science and Electronics Engineering, ICCSEE 2012*, 2012, doi: 10.1109/ICCSEE.2012.373.

[6] F. Sun, J. System, and A. Server, “The Java EE 5 Tutorial,” *System*, 2010.

[7] T. Aggregation and F. C. Encryption, “Journal of Networks,” *Simulation*, 2010.

[8] J. Somorovsky and A. Mayer, “On Breaking SAML: Be Whoever You Want to Be.,” *USENIX Secur. …*, 2012.

[9] P.Andrew, J.Anish Kumar, R.Santhya, Prof.S.Balamurugan, S.Charanyaa, "Investigations on Evolution of Strategies to Preserve Privacy of Moving Data Objects" International Journal of Innovative Research in Computer and Communication Engineering, 2(2): 3033-3040, 2014.

[10] W. J. Buchanan, *Cryptography*. 2017.

[11] P.Andrew, J.Anish Kumar, R.Santhya, Prof.S.Balamurugan, S.Charanyaa, " Certain Investigations on Securing Moving Data Objects" International Journal of Innovative Research in Computer and Communication Engineering, 2(2): 3033-3040, 2014.

[12] J. Arkko, V. Torvinen, G. Camarillo, A.

Niemi, and T. Haukka, “Security Mechanism Agreement for the Session Initiation Protocol (SIP),” *Req. Comments 3329*, 2003.

[13] P.Andrew, J.Anish Kumar, R.Santhya, Prof.S.Balamurugan, S.Charanyaa, " Survey on Approaches Developed for Preserving Privacy of Data Objects" International Advanced Research Journal in Science, Engineering and Technology Vol 1, Issue 2, October 2014

[14] Vishal Jain, Gagandeep Singh Narula, "Improving Statistical Multimedia Information Retrieval (MIR) Model by using Ontology and Various Information Retrieval (IR) Approaches", International Journal of Computer Applications 94(2):27-30, May 2014 having ISSN No. 0975-8887.

[15] Vishal Jain, Gagandeep Singh, Dr. Mayank Singh, “Implementation of Multi Agent Systems with Ontology in Data Mining”, International Journal of Research in Computer Application and Management (IJRCM) May, 2013 page no. 108-114 having ISSN No. 2231 – 1009.1, Issue 3, November 2014