Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 5, Issue. 1, January 2016, pg.265 – 270

A Comprehensive Model to Enhance Performance of WS-Security Processing

Nidhi Arora[1], Savita Kolhe[2], Sanjay Tanwani[3]

Assistant Professor, Department of Computer Science, M.B.Khalsa College, Indore, India[1]
Senior Scientist (Computer Applications), ICAR-Directorate of Soybean Research, Indore, India[2]
Professor and Head, School of Computer Science and IT, Devi Ahilya University, Indore, India[3]

ABSTRACT

Service Oriented Architecture with Simple Object Access Protocol based Web Services enable flexible software system integration, especially in heterogeneous environments. These web services require proper security when they communicate critical information. These services are exposed to a variety of external threats and attacks. Therefore, security is an important issue for Web Services. Several security technologies and standards are developed to secure web services.

SOAP protocol inherits problems related to XML. SOAP processing performance is one of the issues. Adding security requires extra computations. Lower performance not only affects the efficiency of system but it also affects the availability and quality of web services.

A comprehensive parallel model for stream-based processing of secured web services is introduced to address these issues. It is used as application level gateway to enhance performance of security processing especially for large documents. The architectural design of the comprehensive model is described in detail in the paper. The overall performance of the new model is evaluated on different hardware platforms by conducting tests for different size of SOAP messages with varying levels of security. Significant reduction in the processing time and early detection of attacks is observed by successful implementation of the model.

Keywords: stream based processing, parallel processing, WS-Security, Web Services, SOAP processing

I. INTRODUCTION

Architectural paradigms that were used previously to integrate businesses were required to deal with multiple interfaces. These paradigms faced challenging complexity, non-reusability and redundancy during integration. Service Oriented Architecture (SOA) is an architectural model popular for system integration and interoperation. Web Service (WS) is a current standard for SOA. Web service is a software service over the Internet designed to serve a specific function. Different web services can be integrated to become large complex business processes. The web service has no interactive web interface; rather, it is designed with an aim to support interoperable interaction of business critical processes over Internet. Simple Object Access Protocol (SOAP) is an eXtensible Markup Language (XML) based protocol intended for exchanging information between web services.

The nature of web services processing makes these services prone to many attacks as there are many weaknesses of web services and XML vulnerabilities. Some of these vulnerabilities are that message processing

is driven by a flexible, semi-structured message format i.e. XML codes which are open. Also, availability of WSDL enhances the possibilities of different attacks [1]. Flexibilities in schema like unbounded elements and xs:any elements allows attackers to inject their own XML data and operations in the SOAP messages [2]. The major threats and attacks faced by web services are Denial of Service (DoS) Attack and XML Signature Wrapping (XSW) [2].

Some significant approaches to mitigate such attacks are Inline based approach [3], XML schema validation with streaming [4], security policy validation [5], Schema hardening [6] and XML Spoofing Resistant Electronic Signature (XSpRES) [7] etc. Hardened schema limits the chances of XSW and DoS attacks, thereby enhancing security. Stream based parser starts working as soon as it gets XML data. If streaming parser with SOAP message validation used as application gateway [4][8], it checks for each incoming message before sending it to server and rejects malformed schema invalid messages. In this way it prevents the server from DoS attacks. This approach detects vulnerabilities in XML messages earlier as compared to other methods and also increases robustness against different types of DoS attacks. To secure services from DoS and XML rewriting attacks schema validation and schema hardening is ideal, but due to lack of efficiency these counter measures are not used or avoided in most cases [2].

To address performance issues of SOAP and WS-Security processing, a number of approaches are suggested in the literature. Some of these are –(i) efficient encodings of XML to reduce parsing and de-serialization costs [9][10], (ii) Similarity-based SOAP processing for performance and enhancement [10] (iii) Re-canonicalization [11], (iv) Multicast approach [12],(v) Digest based cashing [13] and (vi) Stream based processing of schema and XML signature validation [4], [8-11] and (vii) parallel programming methodologies used for improving the performance of XML parsers [14,15].

Data parallel model for stream-based processing of secured web services is hence developed [16] in this research work. A combination of pipeline and data parallelism is used. Security component is added to the pipeline of parser in order to perform security processing. The security model has various processing components like Encryption/Decryption and Signature/Verification component. SOAP message parts are distributed among multiple instances of parser running in parallel to balance the processing load on different cores. Schema Analyzer and Partitioning Algorithm have been developed to perform partitioning. These parts are processed in parallel manner with event based SOAP processing model. This parallel stream based WS-Security processing model with hardened schema is discussed in this paper.

II. COMPREHENSIVE PARALLEL STREAM BASED WS-SECURITY MODEL

A Comprehensive Parallel Stream based WS-Security Processing model developed in this work is shown in Fig.1.

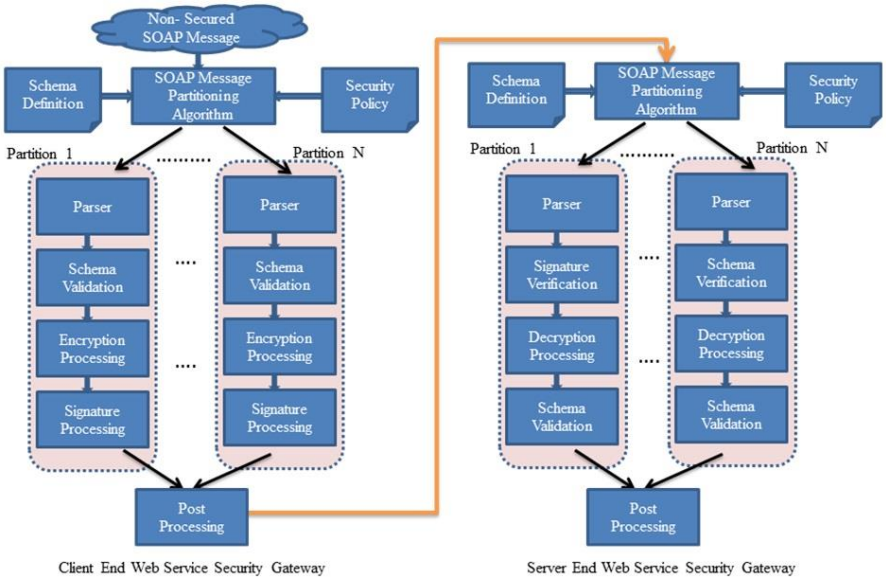

Fig.1. Architecture of comprehensive parallel stream based WS-Security processing model

The Model has following modules-

- SOAP Message Partitioning
- Stream based SOAP Parsing
- Encryption/Decryption Processing
- Signature/verification Processing
- Schema Validation

A. SOAP Message Partitioning

Large SOAP message are divided in schema valid partitions. Partitioning Algorithm and Schema Analyzer is developed [17] which use schema definition to analyze structure of SOAP message. The information obtained is further used by partitioning algorithm to perform splitting task. Dummy Creator is also used to attach dummy tags in order to complete each part as per schema definition. These parts are distributed to different cores for parallel stream based processing. Flowchart of Schema Analyzer is shown in Fig.2.

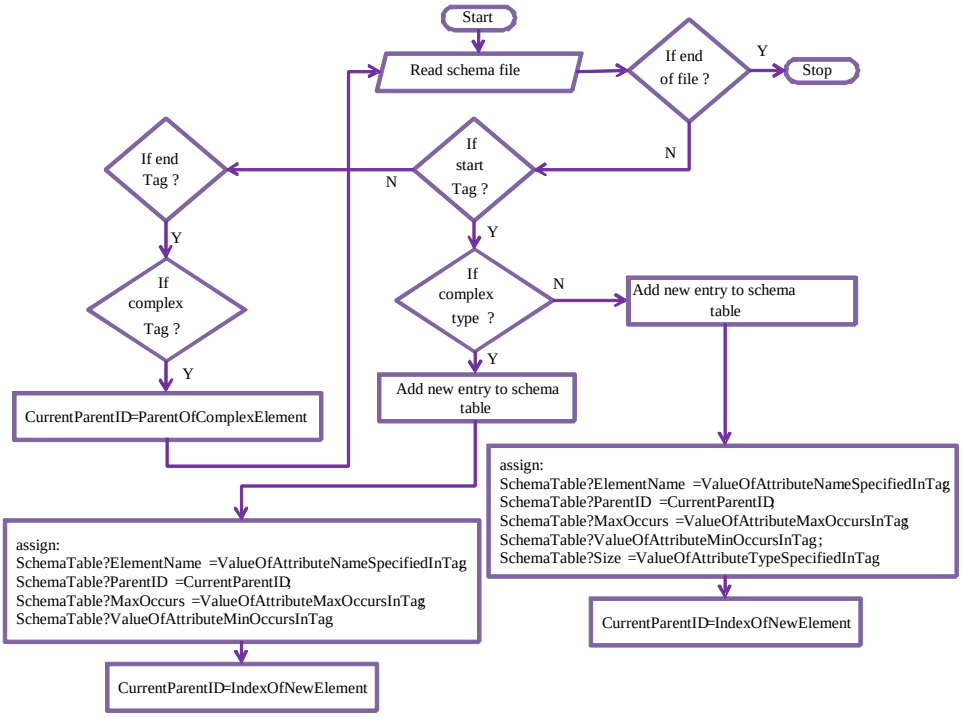

Fig.2. Flowchart for schema analyzer used for partitioning SOAP message into schema valid parts

B. Stream based SOAP Parsing

Different parsing techniques and models exist for processing XML documents. SAX parser is used which has several pipeline modules to perform SOAP message parsing in stream based manner. Data is transmitted from one module of pipeline to another module via XML events. Its memory and processing requirements are low as compared to other models. SAX allows interrupting parsing as and when an invalid element is encountered and therefore, this is very important for the processing of SOAP messages with security elements. As soon as any malicious element is found in SOAP message, it is reported and all the communication with the sender application is blocked immediately, if necessary. Multiple instances of SAX parser are created and distributed among multiple cores.

C. Encryption/Decryption Processing

SOAP messages may carry sensitive and confidential data. XML encryption is a W3C recommendation used to maintain confidentiality of SOAP messages. It specifies that encrypted messages should be wrapped between <Encrypted Data> pair and its supporting tags. Encryption/Decryption module added in pipeline of stream based

parser [16] analyzes events coming from previous module and performs encryption or decryption related operation if required as per security policy.

In our model at client end, it works as Encryption module. XML data is replaced by <EncryptedData> element while encrypting. It generates new events related to <EncryptedData> and supporting tags at the time of encryption. At server end, it works as Decryption module where it removes <EncryptedData> and supporting tags and replaces them with the decrypted data element events at the time of decryption.

D. Signature/Verification Processing

XML-Signature standard assures integrity and authenticity of SOAP messages transactions. Signature processing is performed by Signature/Verification module. *XSpRES* is enhanced with parallel streaming approach and used in this work. At client end signature is created while at server end signature verification processing is done. Detached XML-Signature, Exclusive Canonicalization [18] and FastXPath Expressions [7] are used for efficient and robust SOAP message communication in our model.

E. Schema Validation

Schema validation is required process for early detection of error and intrusion. SOAP message is validated against the schema definition and forwarded to next pipeline module if valid. This is also done in event based manner. Validation is performed prior to encryption at client end but at server end it is performed after decryption. This is because it is not possible to validate message when it is encrypted. Hardened schema is used to prevent SOAP message from the XML signature wrapping attacks. Log is maintained for errors, schema and policy violation in order to take proper decisions about the current communication and further communication with the sender.

III. RESULTS AND DISCUSSION

The performance of comprehensive model is evaluated for Encryption Processing, Signature Processing, Parsing and their combinations. For evaluation purpose, a number of test scenarios have been executed. This includes messages containing - (i) encrypted parts; (ii) signed parts; (iii) encryption as well as signed parts. Web service is invoked with large SOAP message as a whole and then processing is performed with increasing number of partitions viz. 2, 4, 8, 16, 32 and 64. Experiments are conducted on different hardware platforms – single core, dual core, core i5 and i7.

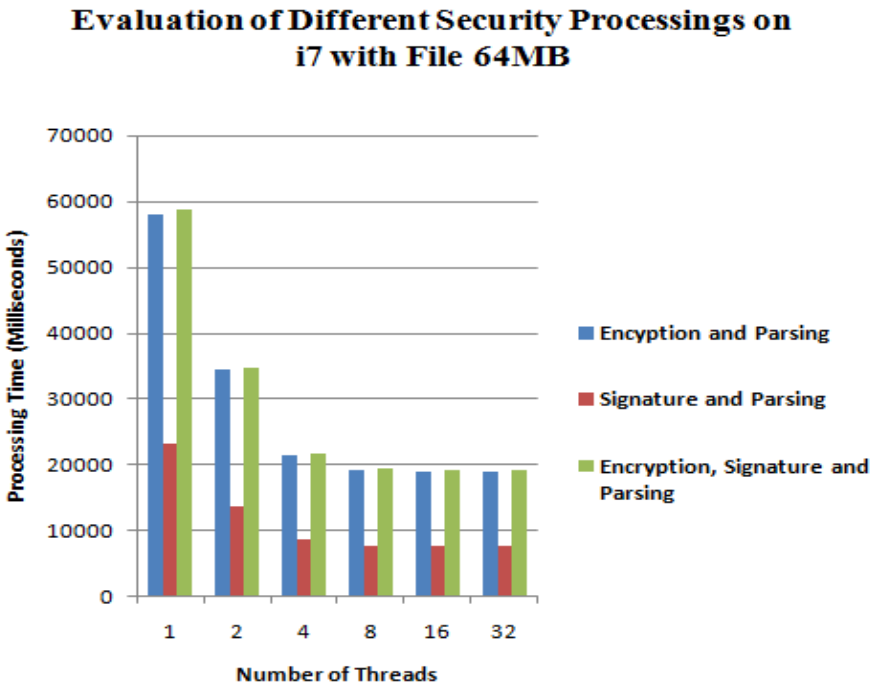

Fig. 3. Performance evaluation of parallel stream based processing of different security functions.

Experimental results in terms of performance enhancement on core i7 with file size 64 MB for Encryption Processing, Signature Processing, Parsing and their combinations are shown in Fig. 3.
Observing the graph (Fig.3) it is clear that signature processing is taking less processing time as compared to encryption processing. Hence the signature processing is faster than encryption processing. Overall Performance of each test case increases as SOAP message is partitioned and run in parallel. The performance at client end is observed to increase from 40% to 67% when number of parts increased from 2 to 32 respectively.

Processing at server end takes 37% more time as compared to processing at client end, but the overall performance improvement is also observed to be raised from 40% to 67% on the server end with increasing number of parts. These results prove that performance improvement is due to partitioning and parallel stream based approach.

IV. CONCLUSION

The comprehensive parallel model with FastXPath expressions, security policy and hardened schema validation in efficient way plays important role in order to avoid several types of DoS and XWS attacks on web services. Parallel stream based approach is combined with *XSpRES* model. It enhances the robustness of model against XWS and DoS attacks. The approach used exhibit that it not only leads to quantitative performance improvements but also has fundamental advantages compared to serial models. It is possible to parse, secure and validate the content in one step with this model, thus detecting attacks rapidly. The comprehensive parallel model significantly enhanced the overall performance of WS-Security processing.

REFERENCES

[1] N. Gruschka, M. Jensen, L. Lo Iacono, and N. Luttenberger, "Server-Side Streaming Processing of WS-Security," In *IEEE Transactions On Services Computing*, Vol. 4, No. 4, 2011.
[2] M. Jensen, C. Meyer, J. Somorovsky, and J¨orgSchwenk, "On the Effectiveness of XML Schema Validation for Countering XML Signature Wrapping Attacks" in *the International Workshop on Secured Services in the Cloud Chair for Network and Data Security, IWSSC*, pp. 7 -13, 2011.
[3] M. A. Rahaman, M. Rits and A. Schaad, "An Inline Approach for Secure SOAP Requests and Early Validation," *In Proceeding of the Open Web Application Security Project Europe Conference (OWASP)*, Leuven, Belgium, 2006.
[4] N. Gruschka, M. Jensen, T. Dziuk, "Event-based Application of WS-SecurityPolicy on SOAP Messages", *ACM, USA*, 2007.
[5] K. N. Gruschka, and L. Lo Iacono, "Vulnerable Cloud: SOAP Message Security Validation Revisited," *In Proceedings of the IEEE International Conference on Web Services*, Los Angeles, USA. IEEE, 2009.
[6] M. Priyadharshini, I. Suganya, N. Saravanan "A Security Gateway for Message exchange in Services by Streaming and Validation," In *International Journal of Innovative Research in Computer and Communication Engineering* Vol. 1, Issue 3, 2013.
[7] C. Mainka, M. Jensen, L. Lo Iacono, and J. Schwenk, "XSpRES: Robust and Effective XML Signatures for Web Services," In *2nd International Conference on Cloud Computing and Services Science*, 2012.
[8] Protecting Web Services from DoS Attacks by SOAP Message Validation, Nils Gruschka, Norbert Luttenberger, 2007
[9] N. A. Ghazaleh, M.J. Lewis, Differential Deserialization for Optimized SOAP Performance. *Proceedings of the ACM/IEEE Conference on Supercomputing*, 2005. pp. 21-31, Seattle, USA.
[10] J. Tekli, E. Damiani, R. Chbeir, and G. Gianini, "Similarity-based SOAP Processing Performance and Enhancement," In *published of IEEE Transactions on ServicesComputing*, PrePrints 1939-1374, DOI : 10.1109/TSC, 2011.
[11] W. Lu, K. Chiu, A. Slominski, and D. Gannon. A streaming validation model for SOAP digital signature. In In 14th IEEE International Symposium on High Performance Distributed Computing (HPDC-14), 2005.
[12] A. Azzini, S. Marrara, M. Jensen, J. Schwenk , "Extending the Similarity-Based XML Multicast Approach with Digital Signatures", Proceedings of the 2009 ACM Workshop on Secure Web Services (SWS'09), 2009. pp. 45-52, Chicago.
[13] Van Engelen R. and Zhang W., "An Overview and Evaluation of Web Services Security Performance Optimizations", *In Proceedings of IEEE International Conference on Web Services (ICWS)*, 2008. pp. 137-144.
[14] Y. Wu and Q. Zhang, "A Hybrid Parallel Processing for XML Parsing and Schema Validation," In *The Markup IEEE International Conference on Web Services.* 2008.

[15] Y. Pan, Y. Zhang, K. Chiu, "Hybrid Parallelism for XML SAX Parsing," In *IEEE International Conference on Web Services*, pp -505-512, DOI 10.1109/ICWS.2008.107,2008.
[16] N. Arora, S. Kolhe, S. Tanwani, "Parallel Stream Based Processing Model for WS-Security", *International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering*, Vol. 4, Issue 1, 2016, pp. 42-46. DOI 10.17148/IJIREEICE.2016.4111
[17] N. Arora, S. Kolhe, S. Tanwani, "A New Partitioning Algorithm to Enhance Performance of SOAP Message Security Processing" , *International Journal of Advanced Research in Computer and Communication Engineering(IJARCCE)*, Vol. 5, Issue 1, 2016
[18] J. Somorovský, "Streaming-based Processing of Secured XML Documents," Ph.D. dissertation, University Bochum, 2009.

