Spatial Signature Method (SSM) Against XML Signature Wrapping Attacks

Madihah Mohd Saudi[1,2*], Nurzi Juana Mohd Zaizi[2] , Khaled Juma Ahmed Sweese[2] and Azreena Abu Bakar[2]

[1]CyberSecurity and Systems (CSS), Institute Science Islam (ISI), Universiti Sains Islam Malaysia (USIM), 71800 Nilai, Negeri Sembilan, Malaysia.

[2]Faculty of Science and Technology (FST), Universiti Sains Islam Malaysia (USIM), 71800 Nilai, Negeri Sembilan, Malaysia.

Abstract. Living in cyber world with revolutionizes of Industrial 4.0, most of the users and organisations prefer to sell and buy products or services via website online transaction. This online transaction is done through a messaging protocol (SOAP) and signing entire SOAP (SESOAP) using Extensible Markup Language (XML). XML is implemented to secure the SOAP contents by applying the signing method called as XML Digital signature. However, the XML digital signature has issues related to XML signature wrapping (XSW) attacks specifically on Sibling Value Context and Sibling Order Context attacks. Therefore, this paper proposes an enhanced method called as Spatial Signature Method (SSM) which aims to resolve the limitation of SESOAP from the aspect of XSW attacks. It proposes new parameters for XML digital signature inspired by the concept of ratio and space in biotechnology to detect the XSW attacks. The experiment was conducted in a controlled lab by using the Ubuntu Linux system and PHP programming. Based on the comparison made with SESOAP and ID Referencing method (IDR), SSM has proven to defend against the XSW attacks. For the future work, the spatial signature method can be forged with more extensive spatial information for the digital signature and to integrate it with web services.

1 Introduction

Simple Object Access Protocol (SOAP) is a protocol used in handling information exchange between clients and servers for web services. While XML digital signature protects the SOAP from XML signature wrapping (XSW) attacks. Unfortunately, XSW attacks specifically sibling value context and sibling order context attacks are able to exploit SOAP [1-4]. As for sibling value context or known as security header injection, the message is attached to a different ancestor which change the meaning entirely and it is within the security header. While sibling order context or known as namespace injection, exploits the order of the messages, which affects its meaning and implication. In order to solve these attacks, signing entire SOAP (SESOAP) and ID Referencing (IDR) have been developed, but it is time consuming, affects the web services performance and are not able to encounter the XML signature wrapping attacks completely such as multiple assertions and multiple signatures. The XSW attacks started in the year 2013, where it launched attacks to the Amazon online website and until now still a challenge to be solved by the web developer. Hence, in this paper, a new method called as Spatial Signature Method (SSM) is proposed to countermeasure against the XSW attacks. It is inspired by the concept of space and ratio in the biotechnology field and the principle is used to detect abnormality for XML digital signature and to combat the XSW attacks.

This paper is organized as follows: Section 2 presents existing work related to XWS attack detection techniques. Section 3 describes the methodology used in this research. Section 4 presents the results of experiments carried out in this research. Section 5 includes the summary and potential future work of this paper.

2 Related Work

There are several approaches against XWS attacks and these are summarised in Table 1. There are four types of XSW attacks which are simple ancestry context, optional element context, sibling value context (security header) and sibling order context (namespace injection), where most detection methods are only encountering simple ancestry context and optional element context attacks. As for sibling value context and sibling order context attacks, only IDR and SESOAP are able to encounter these attacks, though these two techniques cannot encounter XSW attacks completely [5]. Therefore, SSM is developed and proposed in this paper to fill in the existing gaps and challenges in encountering XSW attacks. Another main concern is time processing or known as performance to form the XML digital

* Corresponding author: madihah@usim.edu.my

signature itself. Details of this issue can be referred at [6].

Table 1. Comparison between existing XSW attacks detection techniques and limitation.

Method	Description	Limitation
XPath Expression [7]	1) It selects complex node sets based on the XPath specification and uses timestamp as a reference.	1) Expression complexity definition. 2) Performance impact due to all nodes must be traversed and evaluated according to expression definition. 3) Security risk. 4) Performance – low.
Inline Approach [8]	1) The first solution for early detection of XSW attacks by adding a SOAP account as a new header element for SOAP message to encounter XSW attacks.	1) No verification and standardization of the proposed SOAP account. 2) Able to detect certain XSW attacks. 3) Performance – low.
ID Referencing (IDR) [9,10]	1) It uses the URI reference within the XML signature element and refers to the signed data. 2) It involves two steps verification, which are reference validation and signature validation.	1) Signed object can be relocated with valid signature value. 2) Exploitation can be done via adversary attack. 3) Able to detect certain XSW attacks. 4) Performance – high.
FastXPath [11]	1) It points the signed subtree and increases the XPath speed function.	1) XPath expression issues cannot be solved. 2) Performance – high.
SESOAP [1]	1) It secured the SOAP message by applying digital signature.	1) Time consuming for hashing with high computational resource. 2) No update for the signed message. 3) Able to detect certain XSW attacks. 4) Performance – very low
Spatial Signature Method (SSM)	1) It is proposed in this paper to detect all XSW attacks and inspired by the concept of ratio and space in biotechnology 2) Faster performance in creating the digital signature than SESOAP.	1) Performance – high.

Xu et al. [12] hypothesized that the imbalance of two opposing effects in lung cancer cells, represented by yin and yang genes. It determines a patient's prognosis. Yin and yang genes are compared based on the expression data from normal lung and lung that is infected by cancer. The proposed Spatial Signature Method (SSM) is inspired by the concept of ratio and space in biotechnology, where specific set of critical points are extracted for the digital signature to build up the spatial method. The mapping between the ratio signature model and the SSM can be found in Table 2. The SSM concept is inspired from the notion of ratio signature, which exploits the relative difference of certain measures to ascertain a particular diagnosis.

Table 2. Mapping Ratio Signature Model to SSM

Ratio Signature Model	Spatial Signature Method (SSM)
It uses 2 imbalanced groups of genes (Yin and Yang) in lung cancer cells to detect and decide towards tumor cells.	XSW attacks to SOAP message leads to imbalance for the whole message. SSM will detect any of these attacks and decide what to do with the attacks.
Yin and Yang balance status in lung cells is referred as the ratio.	SSM selects a collection of specific points as spatial identity from the original message. Any changes to the spatial information can be detected by SSM.
The ratio is referred as the location and total number of the gene expression.	SSM defines the location and size (total number) of the original message from the SOAP message.

3 Methodology

The overall processes involved in this experiment are summarised in Figure 1. The components involved in this experiment are depicted in Table 3.

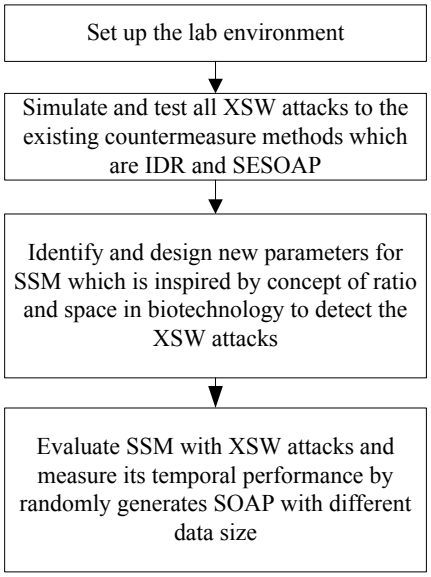

Fig. 1. Overall research processes.

Table 3. Experimentation Setup

Entity and Specification	Purpose
PC i3 Core, 2.27 GHz, 4 GB RAM, Linux Ubuntu 14.04 (OS)	PC to run coding for the experiment
PHP	To implement source code
Open SSL	To provide various cryptography functions
Apache server	To provide efficient, secure and extensible server
Message Size (Kb) 50, 100, 150, 250, 750, 1050,1350,1650, 1950, 2250, 3150	Dataset size for the testing

An example of the SSM creation is illustrated in Figure 2(a)~(b), where it is being attached before the close header.

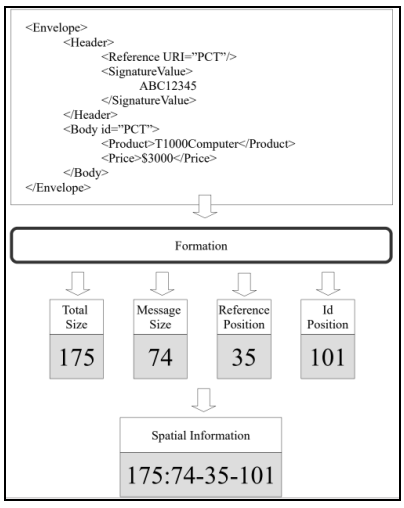

Fig. 2(a). Illustration for SOAP Message extraction and formation of SSM.

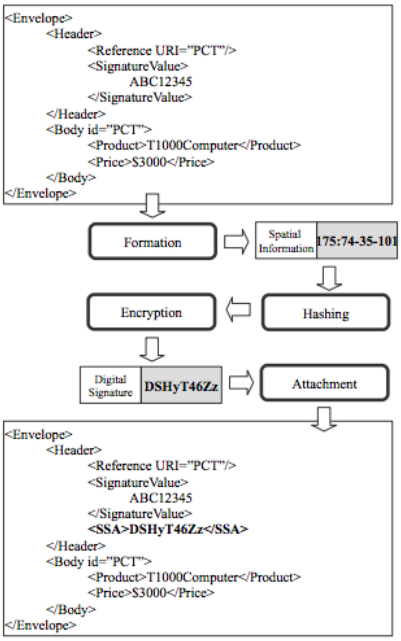

Fig. 2(b). Illustration for SOAP Message extraction and formation of SSM.

4 Finding

For evaluation purpose, four XSW attacks have been launched and the results are as the following. As for the simple ancestry context attack, SSM has successfully detected this attack, which leads to validation process failed, and tampered message is rejected. This process is illustrated in Figure 3.

For optional element attack, SSM has successfully detected the tampering message. This attack tried to change the total size of the entire SOAP message. This is simplified and illustrated in Figure 4.

As for the sibling value attack, SSM has successfully detected this attack, which leads to validation process failed, and tampered message is rejected. This process is illustrated in Figure 5. SSM solved the unprocessed <*Security*> tag within the spatial information, which can lead to changes of spatial information value.

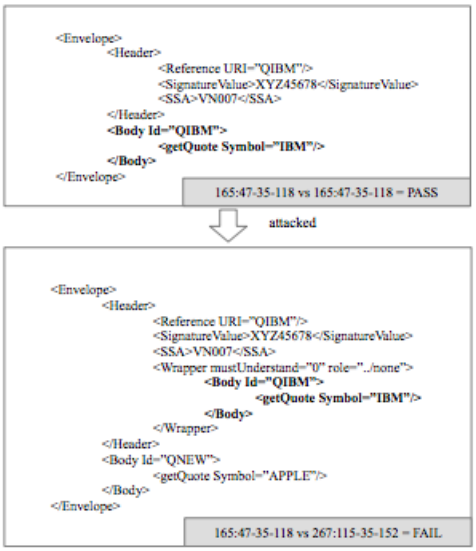

Fig. 3. SSM has defeated the simple ancestry context attack.

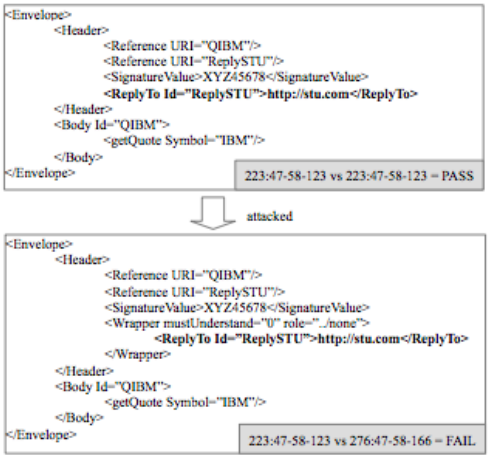

Fig. 4. SSM has detected the optional element attack.

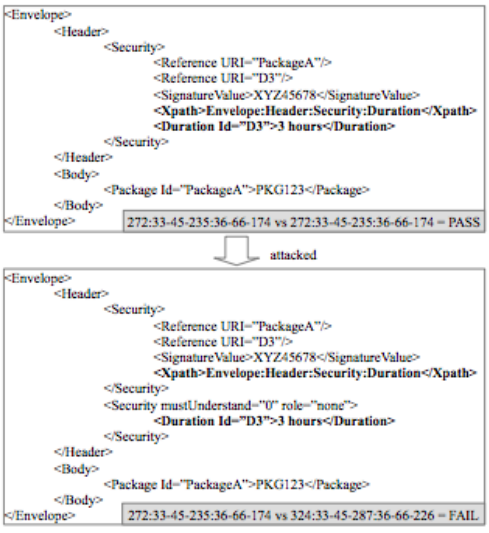

Fig. 5. SSM has detected the sibling value attack.

As for the sibling order attack, SSM has successfully detected this attack, which leads to validation process failed. This process is illustrated in Figure 6. When the information being reordered by the attacker, SSM has detected the changes.

Based on the above testing for the XSW attacks, SSM has successfully detected all of these attacks compared to SESOAP and IDR.

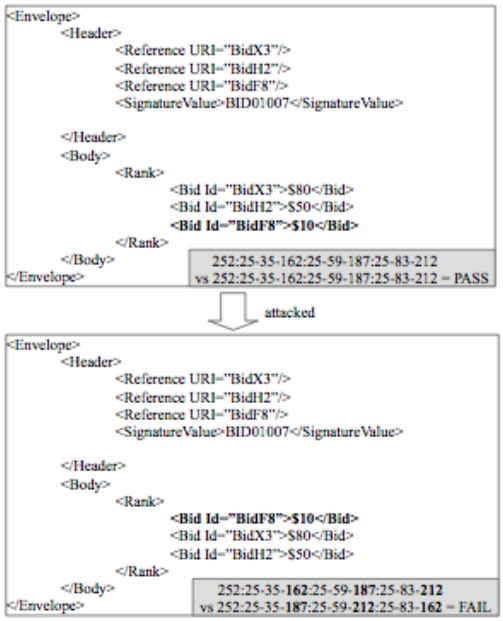

Fig. 6. SSM detected the sibling order attack.

5 Conclusion

Spatial Signature Method (SSM) is inspired by the notion of ratio signature model in cancer detection. Reasoning analogically, the XSW attacks can be perceived as a cancer which innately destructive to the body and in a form of anomaly to the XML message. These XSW attacks would be destructive to the web services. Based on the evaluation conducted, SSM has successfully detected all the XSW attacks which are very beneficial and a great contribution to the web security area. For future work, SSM can be forged with more extensive spatial information for the digital signature and can be integrated with web services.

Acknowledgement

The authors would like to express their gratitude to Universiti Sains Islam Malaysia (USIM) for the support and facilities provided. This research paper is funded under grant: [PPP/USG-0116/FST/30/11716].

References

1. H. R. Kouchaksaraei, A. G. Chefranov, *Countering Wrapping Attack on XML Signature in SOAP Message for Cloud Computing*", International Journal of Computer Science and Information Security. **11**, 7 (2013)
2. M. McIntosh, P. Austel, *XML signature element wrapping attacks and countermeasures*, *ACM*

Proceedings of the 2005 Workshop on Secure Web Services. 20-27 (2005)
3. n.a. “XML Signature Wrapping - Optional Element in Security Header”, WS-Attacks.org. <http://www.ws-attacks.org/XML_Signature_Wrapping_ Optional_Element_in_Security_Header>. Accessed: 12 December 2017.
4. n.a. "XML Signature Wrapping - with Namespace Injection", WS-Attacks.org. <http://www.ws-attacks.org/XML_Signature_Wrapping_with_Namespace_Injection>. Accessed: 12 December 2017
5. H. R. Kouchaksaraei, *Vulnerability in cloud computing. Securing SOAP message using SESoap method*. Doctoral Dissertation, Eastern Mediterranean University - Doğu Akdeniz Üniversitesi (2013)
6. K. G. A. Sawesi, M. M. Saudi, N. B. Azman, *New Countermeasure Approach on XML Digital Signature Against Wrapping Attack*. Advanced Science Letters. **23**, 6 (2017)
7. M. Bartel, J. Boyer, B. Fox, B. LaMacchia, E. Simon, “XML Signature Syntax and Processing Version 1.1”. World Wide Web Consortium (W3C). <https://www.w3.org/TR/xmldsig-core1/> accessed: 20 June 2014.
8. M. A. Rahaman, A. Schaad, M. Rits, *Towards secure SOAP message exchange in a SOA*. *Proceedings of the 3rd ACM workshop on Secure web services*, Alexandria, Virginia, USA (2006)
9. T. Berners-Lee, R. Fielding, L. Masinter, *Uniform resource identifiers (URI): Generic syntax*. (1998)
10. A. Nadalin, C. Kaler, K. Lawrence, R. Monzillo, P. Hallam-Baker, *Web services security: SOAP message security 1.1*. OASIS Standard (2006)
11. S. Gajek, M. Jensen, L. Liao, J. Schwenk, *Analysis of Signature Wrapping Attacks and Countermeasures*. IEEE International Conference on Web Services, ICWS 2009. Los Angeles, CA, USA (2009)
12. W. Xu, G. Jia, N. Cai, S. Huang, J. R. Davie, M. Pitz, L. Murphy, *A 16 Yin Yang gene expression ratio signature for ER+/node− breast cancer*. International Journal of Cancer. **140**, 6 (2017)