AJMAS

https://alqalam.utripoli.edu.ly/science/ eISSN 2707-7179

Original Article

A Systematic Mapping Study on Web services Security Threats, Vulnerabilities, and Countermeasures

Laila Bubaker [1]*, Aisha Yousef [1], Walid Algariani [2]

[1] *Department of Computer, Faculty of Science, University of Omer Al Mukhtar, Albyda, Libya.*

[2] *The Higher Institute for Comprehensive Occupations, Albyda, Libya.*

ARTICLE INFO

https://doi.org/10.5281/zenodo.4460572

* ***Laila Bubaker***: *Department of Computer, Faculty of Science, University of Omer Al Mukhtar, Albyda, Libya*

Tel.: (+218) 923424852

laila.haduth@omu.edu.ly

Received: *07-01-2020*

Accepted: *20-01-2021*

Published: *24-01-2021*

Keywords: *Web Services Security, Systematic Mapping Study, SOAP Message, Attacks, Vulnerability.*

ABSTRACT

Web Services (WS) Technology during the past few years for heterogeneous systems integration, has become the reference architecture for those systems. Since it is extremely important nowadays for companies to make applications communicate over the internet, they are vulnerable to attacks in multiple forms. These attacks include SQL injection, XML injections, denial of service, XSS attacks, XPath, and spoofing, which makes implementing web service security critical to secure valuable data stored on computers and servers during data exchange operations over a network. Although web services provide many suggestions as solutions to reduce attacks and provide an element of security, there is no single solution to mitigate all attacks on it. This paper aims to present a Systematic Mapping Study (SMS) on web service security attack and suggested solutions to protect against them. There is still much research conduct in the field of web services security, which are dealing with the types of attacks and how to detect and limit them. SQL injection and a denial-of-service attack were found to be the most addressed of all attacks followed directly by XML injection. Proposed solutions for dealing with attacks were mainly focused on detection procedures for attacks using techniques such as XACML, SAML, and SOAP Enhancement.

Cite this article: *Bubaker L, Yousef A, Algariani W. A Systematic Mapping Study on Web services Security Threats, Vulnerabilities, and Countermeasures. Alq J Med App Sci. 2021;4(1):91-100.*

INTRODUCTION

A web service is a set of protocols and open standards used to exchange data between applications or systems. Web services have taken an important and effective role in building and integrating e-business applications and allowing information system technologies to communicate in an interoperable manner [1]. The communication is performed using XML based SOAP messages. Subsequently, the security of a Web services-based system relies on the security of the services themselves also on the confidentiality and integrity of the XML based SOAP messages utilized for communication [2]. Web services provide SDL (Services Description Language), SOAP (Simple Object Access Protocol), and UDDI (Universal Description, Discovery, and Integration). In other words, a web service is a network-accessible interface to various application functionalities, built using standard Internet technologies. The W3C Web Service Architecture Group described that WSDL is specified in XML format, it describes the interfaces to

a Web services implementation in terms of the format of the messages, binding of the abstract messages to a concrete protocol, and address of the endpoint. Additional standards, WSDL and UDDI, were developed to support the description and discovery aspect of the Web services [3]. In their recent research paper found, UDDI is a registry standard for Web services providers to publish their Web services. It could be used by Web services consumers to discover Web services developed by Web services providers [4]. A web service is a network-accessible interface to various application functionalities, built using standard Internet technologies [5], as showed in Figure 1.

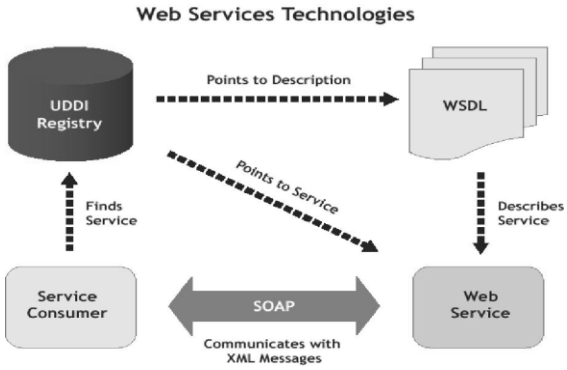

Figure 1: Web Services Technologies.

Organization of The Document

The paper is organized as follows: **Section 1** introduction: provides an overview of Web services implementation and standards. **Section 2** Background: provides an overview Web Services Architecture as well as a listing of several WS attacks. **Section 3** Research Methodology: Specifying Research Question, Conduct Search for Primary Studies, Study of relevant paper, Data Extraction and Classification**. Section 4** Results Obtained from SMS. **Section 5** Exploration: answer research questions. **Section 6** Conclusion

BACKGROUND

Web Services, is considered a universal client/server architecture that allows disparate systems to communicate with each other without using proprietary client libraries. The client and the server could be in heterogeneous technologies" [6]. The Web Services architecture depends on the three roles that cooperate as service requestor, service provider, and service registry. These interactions include find, publish, and bind operations. Moreover, these operations and roles together act upon the Web Services artifacts that are the Web service software module and its description. A service provider hosts a software module that is a network-accessible and it is an implementation of a Web service. The service provider produces a services description and move it to a service registry or service requestor. The service requestor can recover the description of the service using the find operation, and then use the service description to make a connection with the service provider and enhance the interaction with the web service implementation. The functions of both service provider and service requestor are providing logical combinations and the service can reveal the characteristics of each. Figure 2 shows these processes, the components they provide, and their interactions [5].

A vulnerability in web service system is a threat that an attacker can exploit to destroy systems or steal information. Most of the web service attacks are SQL Injection, XML Injection, XPath Injection, Spoofing and Denial of Service [6]. To decrease those drawbacks and improve the Security level of transmission and exchange of data, many researches address these issues in order to find a proposed solution, and many techniques have appeared; for instance, Security assertion markup language (SAML), XML Signature, XML Encryption [7] as indicated in table 4.

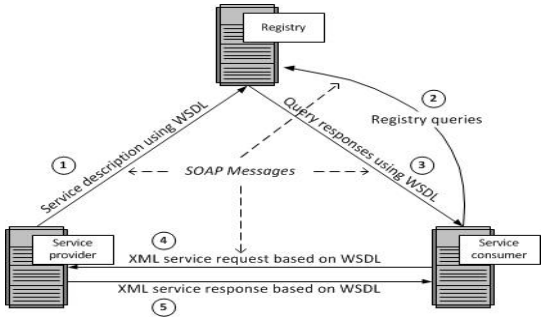

Figure 2: Web Services Architecture

RESEARCH METHOD

This paper adapts and applies Systematic Mapping Study to current studies on web service security published in conferences and journals to answer a four research questions. Figure 3 displays the steps of the SMS process (i.e. study planning, searching for studies, study selection, assessing study quality, data extraction, data classification, analysis, and reporting) [8].

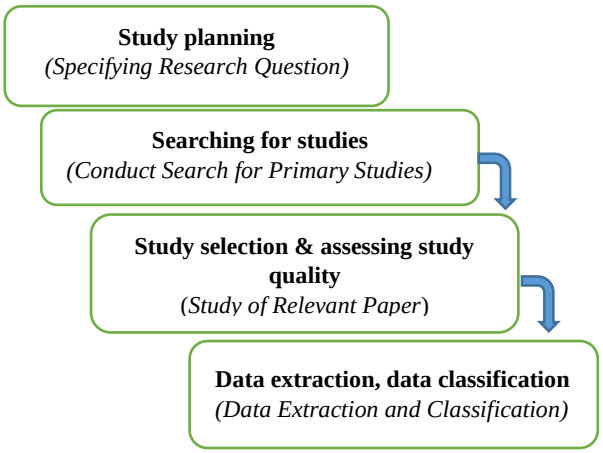

Figure 3: Process Steps for Systematic Mapping Studies.

Specifying Research Question (RQs)

Defining of RQs is a critical part of the planning process. In this study addressed a set of s listed below:

Q1. How much research has been conducted on the Web service from 2002 to 2020?

Q2. What are significant issues in web service security that are covered in the research papers?

Q3. What are proposed solutions to solve web service security issues?

Q4. What are areas of web service security do the research papers focus on?

Conduct Search for Primary Studies (All Papers)

There are a number of approaches uses to identify relevant primary studies for inclusion in the SMS. In this, paper the researchers focusing on two methods Automated Searching and Manual Searching. In the Automated Searching, researcher uses resources like digital libraries and indexing systems; and Manual Searching they are focusing on selected journals and conference proceedings. There are a number of databases researchers use when performing SMSs, in this paper using four of them, which are IEEEXplore, the ACM Digital Library, Science Direct and SpringerLink. The preliminary study and the compilation of previous studies on the subject of the research was carried out through the electronic searches that we referred to above. It was divided into two phases, the first through search engines such as Google Scholar and Research gate, where the search was conducted using general search strings on the topic using terms or phrases such as web service, definitions of web services, web service security, and security standard. Combination of a mentioned search terms was done using Boolean AND/OR. Second, searching through the digital libraries, which helped researchers refine the research and compile a preliminary study on the topic using keywords in the research questions. We obtained 119 initial studies from scientific Database (digital libraries) illustrated in the table 1 and figure 4 below:

Table1: Publication counts from Digital Library

Database	Years of covered area		Number of Studies obtained	Include
	Issues	Solutions		
IEEE Xplore	19	11	30	26
ACM Digital Library	17	14	31	22
Science Direct	21	7	28	18
Springer Link	13	17	30	27

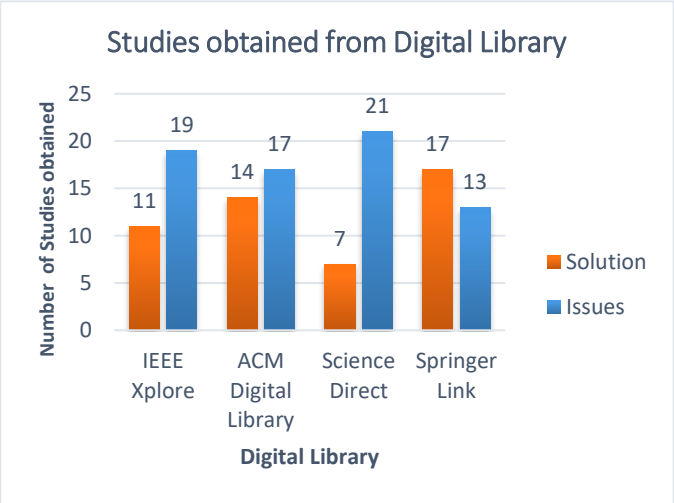

Figure 4: Studies obtained from Digital Library

Table 2: Main Journals and Conferences Covering Web Service Security Topics.

No	Conference Name	Journal Name
1.	7th International Conference on Web Engineering **ICWE 2007**	Programming and Computer Software
2.	4th International Conference on Global e-Security **ICGeS 2008**	International Journal of Information Security
3.	International Conference on Information Computing and Applications ,**ICICA 2013**	International Journal of System Assurance Engineering and Management
4.	2nd International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment, **DIMVA. 2005**	Empirical Software Engineering
5.	20th International Conference on Database and Expert Systems Applications	Procedia Computer Science
6.	19th European Conference on Genetic Programming, **Euro GP 2016**	Journal of Systems and Software
7.	4th International Conference on Computing Communication and Automation **(ICCCA)**	Future Generation Computer Systems
8.	3rd International Conference on Instrumentation, Communications, Information Technology and Biomedical Engineering **(ICICI-BME)**	Information Security Technical Report
9.	3rd International Symposium on Multidisciplinary Studies and Innovative Technologies **(ISMSIT)**	Information and Software Technology
10.	2nd International Conference on Inventive Systems and Control **(ICISC)**	Journal of King Saud University - Computer and Information Sciences
11.	**IEEE** 16th Pacific Rim International Symposium on Dependable Computing	Journal of Systems Architecture
12.	International Conference on Advances in Engineering & Technology Research **(ICAETR - 2014)**	Electronic Notes in Theoretical Computer Science
13.	IEEE International Conference on Web Services	IEEE Latin America Transactions
14.	4th International Conference on Network and System Security	
15.	8th IEEE International Conference on Computer and Information Technology	
16.	IEEE Eighth World Congress on Services	
17.	**IEEE/IFIP** International Conference on Dependable Systems & Networks	
18.	International Conference on Technical Advancements in Computers and Communications **(ICTACC)**	
19.	IEEE International Conference on Services Computing	
20.	IEEE 26th International Symposium on Software Reliability Engineering **(ISSRE)**	
21.	The International Conference on Engineering & MIS **ICEMIS**	
22.	12th ACM Conference on Computer and Communications Security **CCS05**	
23.	Computer and Communications Security **CCS**	
24.	**iiWAS** the 11th International Conference on Information Integration and Web-based Applications & Services	
25.	**ISSTA** International Symposium on Software Testing and Analysis	
26.	**ICWET** International Conference & Workshop on Emerging Trends in Technology	

Study of relevant paper (include and exclude)

After identifying an initial collection of papers based on the research procedure described above, we selected the most suitable set of papers to be eventually included in the SMS. At this step if we have to read the full text of all applicant papers, the task of selecting the most acceptable studies will be time consuming. We begin by analyzing the titles and the abstract of the candidate papers referred to in Table 1 above to determine relevance and eliminate any papers that are clearly irrelevant. There are various ways where the abstract and title of some papers does not have enough detail to make a decision. First, we studied the introduction and conclusion, then the entire paper. In order to construct a decision document, abstract, introduction, and conclusion do

not always contain enough detail. Second, we perform a partial reading of the paper if it seems relevant. Last, on some papers, if the abstract was very short or the proposed solution was not fully described in then we did a full reading of it.

Defining acceptable inclusion and exclusion criteria is a vital aspect of the selection process directly related to web service security. The following points provides some of the Inclusion Standard used by the authors of the papers included which are 86 papers.

- The papers conducted experiments to detect types of attacks.
- The papers describe vulnerability in web services security.
- The papers provide proposed solutions to address and reduce web service issues.

Data Extraction and Classification

We developed a classification scheme for research styles in terms of types of papers. The articles arranged and classified into six categories, a table (3) and figure 5 give pieces of information about them. The most popular papers were Experimental studies with (32%) and the second used types are Solution proposals with around (17.19%) compared with 14.16% Review papers category. In addition, the number of Case Study papers was less in the rate approximately as (12%), while the other categories (Evaluation, Analysis, Compare and Contrast, Survey) were the least popular 7%, 6%, 4%, 3% respectively.

Overall, figure 3 demonstrates that the researchers use experimental studies significantly more time than Solution proposals, and slightly more time Review and Case Study papers. Lastly, the Suggestion article was the least common with 1% of the papers.

Table3: Distribution of Paper Category by number

Paper Category	Solution	Issue	Total
Solution Proposal	17	0	17
Experimental studies	8	21	29
Review Paper	6	8	14
Evaluation	3	3	6
Case Study	2	9	11
Analysis	1	4	5
Suggestion	1	0	1
Compare and Contrast	1	3	4
Survey	0	3	3

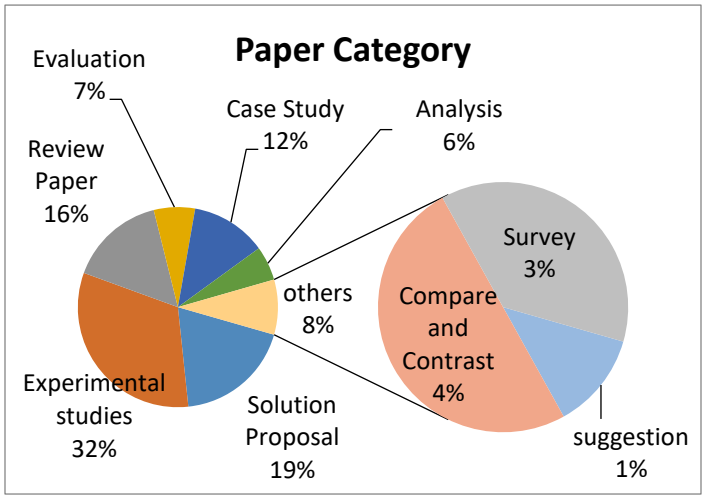

Figure 5: Distribution of Paper Category

RESULTS

The most important information obtained from the included papers are summarized in this table that divided to (References, Focus Areas, Definitions and Types), also this information is categorized to three types which are (Security standard, Web Service security issue, Web Service security solution) as illustrated below. The importance of this table is that it is a basic reference for this research, and it includes an explanation of all focus areas, and it is the main source from which the authors set out to answer the questions of this study.

Table 4. Summary of review findings.

Ref	Focus Area	Definition	Type
[2] [9]	Confidentiality	Where information is not made available or disclosed to unauthorized individuals, entities, or processes, and it, guarantees that the contents of the message are not disclosed to unauthorized individuals .	Security standard
[2] [10]	Authentication	The yielding of authority, which includes the conceding of access based on access rights and guarantees that the user is authorized to use the service or the sender, is authorized to send a particular message.	Security standard
[6]	vulnerabilities	It is a weakness that allow the threats to happen, that could be because of weak design, Inappropriate coding techniques, Security Misconfiguration.	WS security issue
[11]	XML injection	It is a technique used by attackers to insert XML script into XML document to manipulate of XML content and structure, also to change the intended logic of the application.	WS security issue
[12]	SQL injection	It is a code injection technique used by attacker to inject malicious code with in SQL statements to change or delete the database queries.	WS security issue
[13]	XPath /XSS	Attackers convert an original XML message by un-authorized access to insert, remove, or modify the message content or construct a new fake message to fool the receiver into believing it to have come from authorized sender.	WS security issue
[14] [6]	Denial of service	An attacker does a small amount of work on a message that causes the target system to devote all its resources to a specific task so that it cannot provide any services to valid requests. These threats exploit weaknesses in confidentiality, integrity, authentication, and availability protection within an existing infrastructure	WS security issue
[6]	Spoofing	The most organized network traffic pass-through port 80 or 443 to access the web application. the traditional network firewalls do not block the SOAP message that the transport via HTTP (port80) or HTTPS (port443)and do not check whether there is any malicious content in the SOAP message, attackers in general can manipulate the SOAP message	WS security issue
[6] [14] [15] [16]	Security assertion markup language (SAML)	Defines a framework for authentication and authorization exchange of information between partners of e-commerce. The components of SMAL are assertions, protocols, buildings, and features. There are three kinds of assertions, which are attribute, authentication, and authorization	WS security solution
[14] [16] [17] [18]	XML access control markup language (XACML)	This specification provides a common language for illustrating access control policies in XML expressions. It provides the technique for defining the set of rules and politics that determines what users can access through the network	WS security solution
[9] [19]	SOAP message enhancement	Microsoft issued web services enhancement (WSE) which is the first toolset to support the implementation of security within the soap messages, WSE provides a class (Microsoft. Web. Services. Soap Context) and an interface to be allowed to address the WS - security soap headers and other headers on incoming Soap messages Soap. Soap messages might be authenticated and it might be encrypted totally or partially.	WS security solution
[6] [20]	XML Signature	XML Signature specifies the syntax and processing, rules for applying digital signatures to any XML data. According to the W3C, "XML Signatures provide integrity, message authentication, and/or signer authentication services for data of any type, whether XML Signatures can be used to ensure that the content within an XML document has not been changed or altered in any way during the transaction process.	WS security solution
6] [21]	XML Encryption	creating XML syntax to represent encrypted content and the information for decryption. With this standard, an XML document would be partially encrypted which effectively means only the sensitive portions of the XML document are encrypted. Different portions can be encrypted with different keys so that the same XML documents can be distributed to various recipients. Once the XML document is encrypted this way, tags indicating the beginning and end of the encrypted information will appear within the document.	WS security solution
[14] [22]	WS-security tokens	Web Service-Security tokens help to secure information within the soap message and how to identify the receiver of the message identifier and verify the sender to be authenticated and authorized. There are several types of WS-Security Tokens such as Username Tokens, X.509 Tokens, SAML Tokens and Kerberos Tokens.	WS security solution

EXPLORATION

Q1. How much research has been conducted on the Web service from 2002 to 2020?

To answer this question, we used a systematic study to identify relevant papers, and research was done in time spanning from 2002 up to 2020. Fig 6. The chart indicates the number of studies obtained on web service security and attacks per year. Paper publications are spread across conference proceedings and journals. From the pie chart below, it is clear that the majority of obtained papers are conference papers with 67%, and the rest of the papers are journal by 33% with twenty percent difference between the two. Distributed between 26 international conferences and 13 journals as shown tables 2. Covering areas such as Information Security, software engineering, Computer systems, and Information Sciences as well as Networks.

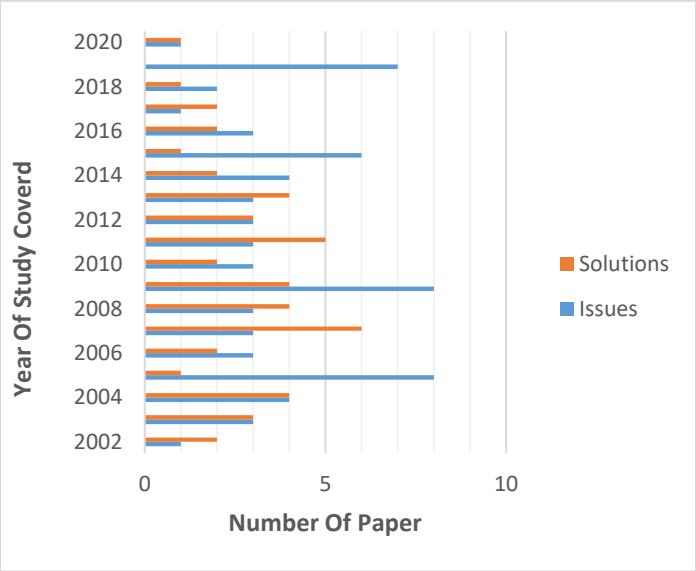

Figure 6: Number of Studies obtained by year (Issues & Solutions)

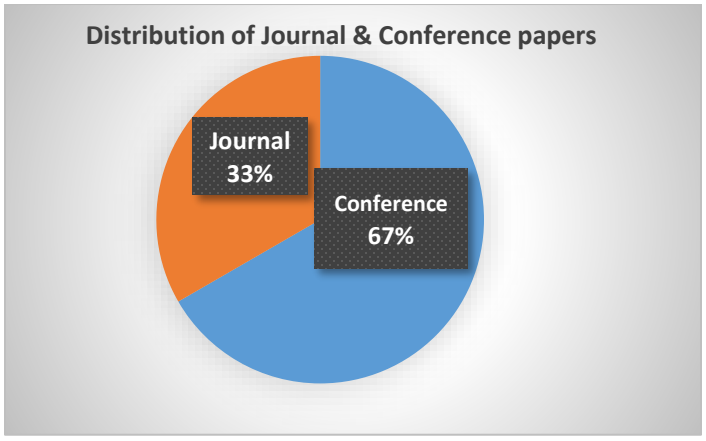

Figure 7: Distribution of Journal & Conference

Q2. What are significant issues in web service security that are covered in the research papers?

From the publications obtained, we found there are six types of attacks on web services, ranging from denial-of-service attacks to injection attacks as illustrated in table 5. SQL Injection and DoS attacks are the most discussed issues in the research papers with around (26%) most of those papers were in 2005 and 2009 with 11 numbers to each as per in figure1 above, as well as 20 % of those papers, discuss SQL injections with other attacks such as XPath and XSS injection. Followed by XPath with a rate of 21%. XML injections and XSS attacks were close in the percentage of 12% and 10%; spoofing Attacks are addressed in 5% of papers.

Table 5: Comparison between issues and year.

Year	SQL Injection	XMl Injection	XPath	SQL Xpath	XSS/ SQL Injection	DoS attack	spoofing
2004	✓			✓			
2005	✓		✓	✓			
2006							
2007							
2008						✓✓	
2009			✓	✓✓			
2010			✓	✓		✓	✓
2011	✓✓			✓		✓	
2012					✓✓		✓
2013	✓				✓	✓	
2014	✓✓				✓✓✓	✓	
2015		✓		✓✓✓		✓✓	
2016	✓✓			✓		✓	
2017		✓					
2018	✓		✓				
2019	✓✓	✓✓				✓	
2020						✓	

Q3: What are proposed solutions to solve web service security issues?

Table 6 provides that the proposed solutions divided into six solutions and technologies. (SAML) the most discussed technologies in the papers with (23%) the majority of those papers were in 2007, the same number of papers was about (XACML) distributed almost evenly over the years as illustrated in table 6. Then followed by XML Encryption that contributed by approximately (19%) of the studies then XML Signature by 14%, the least popular were (SOAP Enhancement) and (WS-security tokens) by 12%, 9% respectively. In several papers, the researchers used to connect some of these suggested solutions in the same study such as employing SAML and XACML together or applying XML signature and XML Encryption to improve the level of web service security.

Table 6: Comparison between Solutions and year.

Year	SAML	XACML	SOAP Enhancement	XML Signature	XML Encryption	tokens
2002				✓	✓✓	
2003				✓		✓
2004	✓✓		✓			
2005				✓		
2007	✓✓✓✓✓	✓✓	✓			✓
2008	✓✓	✓			✓	
2009				✓		
2010		✓				
2011		✓	✓		✓✓	
2012		✓			✓✓	
2013		✓	✓	✓		✓
2014	✓	✓	✓	✓	✓	
2016		✓		✓		
2017			✓			
2020		✓				

Q4. What are areas of web service security do the research papers focus on?

The main focus areas of this study on web services security issues, vulnerabilities and suggested solutions of researchers. The pie chart visualizes that the 48 papers (56%) focus on web service issues and vulnerabilities, and 38 studies (44%) focus on proposed solutions to enhance web service security.

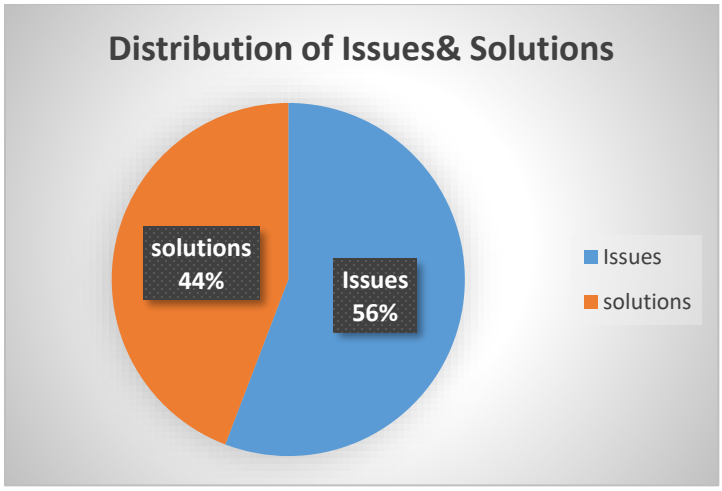

Figure 8: Percentage between Issues and solutions (include papers)

CONCLUSION

To sum up, the Systematic Map Study was used to analyze 86 papers in web services security distributed between 48 papers that address issues and types of attacks, and the rest of the papers were descanting about the most important types of solutions to these attacks. Paper publications are from four types of digital libraries spread across journals and conference proceedings.

We found the publications that dealt with problems outnumber those that deal with solutions by 56% to 44% respectively. Most targeted attacks are denial of service attacks and SQL injection followed directly by XML injection and the rest of the types. The techniques for dealing with attacks mainly focus on detection procedures for attacks using techniques such as XACML, SAML, and SOAP Enhancement. This will ensure additional protection as well as fewer attacks on web services because there is no final solution to completely eliminate these attacks.

Conflict of Interest

There are no financial, personal, or professional conflicts of interest to declare.

REFERENCES

[1] Graham S, Daniels G, Davis D, Nakamura Y, Simeonov S, Brittenham P, et al. Building Web services with Java: making sense of XML, SOAP, WSDL, and UDDI. SAMS publishing. 2004. ISBN-13: 978-0672326417.

[2] Bora A, Bezboruah T. A comparative investigation on implementation of RESTful versus SOAP based web services. International Journal of Database Theory and Application. 2015;8(3):297-312.

[3] Chinnici R, Moreau J-J, Ryman A, Weerawarana S. Web services description language (wsdl) version 2.0 part 1: Core language. W3C recommendation. 2007;26(1):19.

[4] Gottschalk K, Graham S, Kreger H, Snell J. Introduction to web services architecture. IBM systems Journal. 2002;41(2):170-7.

[5] Shravani D, Varma PS, Rani BP, Rao KV, Kumar MU. Web Services Security Architectures for Secure Service Oriented Analysis and Design,". International Journal of Computer Trends and Technology, ISSN. 2011:2231-803.

[6] Diouri O. Web Service Security Overview, analysis and challenges. International Journal of Computer Science Issues (IJCSI). 2014;11(5):124.

[7] Jagruti B, Nidhi P, Pandya D, editors. A Survey on Webservice Security Techniques. 2018 4th International Conference on Computing Communication and Automation (ICCCA); 2018: IEEE.

[8] Petersen K, Feldt R, Mujtaba S, Mattsson M, editors. Systematic mapping studies in software engineering. 12th International Conference on Evaluation and Assessment in Software Engineering (EASE) 12; 2008.

[9] Garcia DZG, de Toledo MBF, editors. Web service security management using semantic web techniques. Proceedings of the 2008 ACM symposium on Applied computing; 2008.

[10] Mani GR, Rao GRK. Web services security and e-Business. Idea Group Publishing, Hershey; 2007.

[11] Tao Z, editor Detection and service security mechanism of xml injection attacks. International Conference on Information Computing and Applications; 2013: Springer.

[12] Thomé J, Shar LK, Briand L, editors. Security slicing for auditing XML, XPath, and SQL injection vulnerabilities. 2015 IEEE 26th International Symposium on Software Reliability Engineering (ISSRE); 2015: IEEE.

[13] Laranjeiro N, Vieira M, Madeira H, editors. Protecting database centric web services against SQL/XPath injection attacks. International Conference on Database and Expert Systems Applications; 2009: Springer.

[14] Moralis A, Pouli V, Grammatikou M, Papavassiliou S, Maglaris V, editors. Performance comparison of Web services security: Kerberos token profile against X. 509 token profile. International Conference on Networking and Services (ICNS'07); 2007: IEEE.

[15] Shin D, Jeong J, Shin D, editors. Design and Implementaion of a Single Sign-On Library Supporting SAML (Security Assertion Markup Language) for Grid and Web Services Security. International Conference on Grid and Cooperative Computing; 2003: Springer.

[16] Yin H, Zhou J, Wu H, Yu L, editors. A SAML/XACML based access control between portal and web services. The First International Symposium on Data, Privacy, and E-Commerce (ISDPE 2007); 2007: IEEE.

[17] Singh NK, Nayak SK. The Threat Detection Framework for Securing Semantic Web Services Based on XACML. Advances in Computational Intelligence and Communication Technology: Springer; 2020. p. 139-47.

[18] Priyadharshini M, Yowan J, Baskaran R, editors. Security Enhancement in Web Services by Detecting and Correcting Anomalies in XACML Policies at Design Level. International Symposium on Security in Computing and Communication; 2014: Springer.

[19] Chakroborti D, Nath SS, editors. Web service performance enhancement for portable devices modifying SOAP security principle. 2017 20th International Conference of Computer and Information Technology (ICCIT); 2017: IEEE.

[20] Mainka C, Jensen M, Iacono LL, Schwenk J, editors. Making xml signatures immune to xml signature wrapping attacks. International Conference on Cloud Computing and Services Science; 2012: Springer.

[21] Seak SC, Siong NK, editors. A file-based implementation of XML encryption. 2011 Malaysian Conference in Software Engineering; 2011: IEEE.

[22] Indu I, PM RA, Bhaskar V. Encrypted token-based authentication with adapted SAML technology for cloud web services. Journal of Network and Computer Applications. 2017;99:131-45.