Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 93 (2016) 870 – 877

Procedia Computer Science

6th International Conference On Advances In Computing & Communications, ICACC 2016, 6-8 September 2016, Cochin, India

Web Services Attacks and Security- A Systematic Literature Review

Varsha R Mouli[a*], KP Jevitha[a**]

[a] *Department of Computer Science & Engineering, Amrita School of Engineering, Coimbatore-641112, Amrita Vishwa Vidyapeetham, India*

Abstract

Web Services allow applications to communicate with each other independent of platform and/or language. They are prone to attacks in the form of Denial-Of-Service, XML, XPath, SQL injection and spoofing, making implementation of web service security vital. Though many solutions are proposed for minimizing attacks, there is no single solution for mitigating all the attacks on web services. The objective of this paper is to present a systematic review on the studies of web service security. It is identified that there is lot of research going on in web services, dealing mostly with attack detection as well as identification of vulnerabilities in the services. Denial-of-service attack is found to be the most addressed of all attacks. Solutions were mainly proposed using dynamic analysis, closely followed by static analysis.

Keywords: Web services; Systematic literature review; Attacks; Security

1. Introduction

In the current day, many applications and web pages depend upon web services to seamlessly exchange information among one another. Web services provide a way to transfer dissimilar data over the network helping organizations/individuals reuse functionality across services. There is dynamic relationship between the user and the web service, as there are many scenarios that are user input controlled. This dynamic nature is often a cause of worry. Web services protocols include Simple Object Access Protocol (SOAP), XML-RPC, and JSON-RPC for message communication; Web Service Description Language (WSDL) and Universal Directory and Discovery Integration (UDDI) for web service description and discovery. Frameworks used for creating/developing web services mainly include Apache Axis, .NET and Zend. Due to the variety of protocols and frameworks involved in developing a web service, they become vulnerable and often prone to attacks.

Most web service attacks are XML Injection, XPath Injection, SQL Injection, Spoofing, Denial of Service and Man in the Middle attack[32].

DOS attacks affect the availability of system and its resources to valid requests. Recursive payload takes advantage of extensive XML tag nesting to overload the parsers thus causing XDOS attacks. Coercive payload loads a lengthy XML message into memory that utilizes large amount of CPU resources thus making the server unavailable, contributing to DOS attacks[38].

*Tel.: +91 7418193412; **Tel.: +91 9789797982
**E-mail address:* vrsh.rv@gmail.com ; ** *E-mail address:* kp_jevitha@cb.amrita.edu

doi:10.1016/j.procs.2016.07.265

Injection attacks occur when malicious code is inserted through user inputs to gain access to restricted data. SQL, XPath and XML injections are the most occurring in web services. Though parametrized queries, prepared statements and whitelist validations are often stated as countermeasures, these conventional fixes cannot eradicate the attacks completely[37].

Spoofing is done by masquerading as a valid user and sending requests to bypass any access controls[39].

The purpose of the paper is in presenting the systematic review we have conducted on the existing state of research on web service security. The rest of the paper is structured as follows: approach taken to review this paper is discussed in Section 2. Section 3 depicts the results obtained. Section 4 answers the research questions raised and Section 5 provides the conclusion.

2. Research Approach

This paper performs a detailed analysis of existing studies on web service security published in journals/conferences.

2.1. Research Questions

Listed below is the set of research questions addressed in this study:

Q1: How much research has happened on web service security since 2005?
Q2: What are the web service security issues that are addressed in the research papers?
Q3: What are the techniques proposed to solve web service security issues?
Q4: Which are the web service security areas focused in the research papers?

To answer Q1, a systematic analysis and review on research spanning from 2005 up to 2016 was done. Regarding Q2, we have tried to identify the attacks that each of the paper focuses on .We wanted to identify the proposed models/algorithms/solutions and Q3 aims to answer that. For Q4, we have differentiated between attacks and vulnerabilities and their detection and prevention techniques.

2.2. Requirement Process

To collect the necessary case papers for the study, data repository search was performed. Relevant articles were obtained from each of the repository.

The search terms used were:

- Web service attacks.
- Web service vulnerability.
- Web service attack mitigation.
- Denial of Service attacks.
- XML injection.
- SQL injection.
- XPath injection.
- Web service attack mitigation.

Combination of above mentioned search terms was done using Boolean AND/OR.

Further search was done on the referenced publications in the obtained papers for topics related to web service security.

2.3. Paper Inclusion Standard

Papers with the following criteria were included:

- Papers that describe solution to address the web service security problem.
- Papers that use testing methodologies for vulnerability detection in web services.
- Papers that address web service attack such as SQL/XML/XPath Injection,Spoofing and Denial of Service.
- Papers that are published before April 2016.

2.4. Data Collection

The following data was collected from every individual paper:

- Title of the paper &Year of publication.
- Summary of Paper.
- Type of Web service attack (XML/SQL/XPath Injection, Spoofing, Denial of Service).
- Area of focus (Attack prevention, Vulnerability detection, Attack detection).

3. Results Obtained

Table 1. Summary of review findings.

Ref	Type of Attack	Summary of the Paper	Area of focus
[1]	XPath injection	An architecture that uses a run-time monitoring mechanism to identify malicious queries thus preventing XPath Injection.	Attack prevention
[2]	SQL injection	SQL vulnerabilities in web services is detected based on mutation operator related automated testing approach.	Vulnerability detection
[3]	DOS attack	An adaptable algorithm for testing web services by parsing incoming XML messages for DOS attack.	Attack detection
[4]	SQL,XPath injection	A comparison of existing vulnerability scanners against 300 public web services to identify security flaws.	Vulnerability detection
[5]	SQL,XPath injection	An automated approach for XPath/SQL injection vulnerability detection in web services.	Vulnerability detection
[6]	SQL injection	A systematic approach for web services to detect SQL injection vulnerabilities using penetration testing tool.	Vulnerability detection
[7]	DOS attack	Model an architecture to apply on web services and create a filter defense system to protect against XML based DOS.	Attack detection/Attack prevention
[8]	XML injection attack	An approach is proposed with pluggable API as well as security services in the middleware to detect and overcome XML Injection attacks.	Attack detection
[9]	Spoofing, DOS	An automated pluggable API Model for network level threat detection was proposed.	Attack detection
[10]	DOS attack	A proposed real time agent based classification mechanism for detecting and preventing DOS attacks on web services.	Attack detection/Attack prevention
[11]	SQL,XML, XPath injection	A novel approach to complement existing vulnerability detection by forming sound and precise slices thus identifying false and true positives.	Other
[12]	Spoofing	Proposed a misuse pattern called Spoofing web services to prevent the same attack on web services.	Attack prevention
[13]	XML injection	A hybrid learning, universal approximator model is proposed to detect XML SOAP based attacks on web services.	Attack detection/Attack prevention
[14]	SQL,XML injection DoS attack	An intrusion detection systems based on fuzzy rules is suggested to prevent Injection as well as Denial-of-service attacks.	Attack prevention
[15]	DOS attack	A content introspection framework is suggested to prevent XML based Denial-of- service attack on web services.	Attack prevention
[16]	DOS attack	Effectiveness of a cryptographic authentication technique for access grant to prevent DOS attacks on web services is studied.	Other
[17]	DOS attack	Deploy known DOS vulnerabilities on web services to identify the effect on resources and performance.	Other

[18]	DOS attack	An adaptive approach combining the capabilities of Case Based Reasoning (CBR) as well as multi-agent systems for protecting web services against malicious soap messages.	Attack prevention
[19]	XML injection	A WS-Inject based fault injection technique on web services to identify XML Injection vulnerabilities.	Vulnerability detection
[20]	DOS attack	An architecture based on real time, intelligent agent to use reasoning within a time bound to classify DOS Attacks against web services.	Attack detection
[21]	DOS attack	An automated plug-in based on Black box testing is proposed that can evaluate DOS attacks on web services.	Other
[22]	DOS attack	Propose an approach, for identifying DOS attacks on web services, which are intrusion tolerant.	Attack detection
[23]	DOS attack	A gateway system is proposed based on Schema hardening as well as WSDL Compiler to protect the services from DOS attack by filtering malicious SOAP Messages.	Attack prevention
[24]	SQL,XML injection	An architecture as well as filtering policy is proposed and tested to prevent web service attacks such as Injection, Coercive parsing.	Attack prevention
[25]	DOS attack	A Vector Quantization based Intrusion detection system for DOS Attacks on web services to achieve better true detection rates.	Attack detection
[26]	DOS attack	A mechanism is proposed with adaptive rule updates to detect and mitigate DOS Attacks.	Attack detection
[27]	XML Signature injection	An approach of Schema hardening is discussed for fending XML signature attacks.	Attack prevention
[28]	SQL injection, XPath injection	An approach to prevent SQL/XPath Injection attacks on web services by combining statement learning as well as service protection.	Attack prevention
[29]	SQL injection, XPath injection	A Learning based approach, to detect XPath & SQL Injection attacks based on the concept of anomaly detection.	Attack prevention
[30]	DOS attack	A proposed approach for testing the security of service platforms against DOS Attacks, by multi-phase testing.	Other
[31]	XML injection	A hybrid approach that applies ontology on the knowledge database for knowledge based detection of XML Injection attacks on web services.	Attack detection
[32]	XML injection, DOS attack	Identify the different attacks on web services, suggest techniques to counter the attacks as well as develop a self-adaptive hardening scheme for message validation.	Other
[33]	DOS attack, XML injection	A series of tests are conducted on SOAP requests to identify possible attacks on web services.	Attack detection
[34]	XML injection	A XML Injection attack detection method based on XML based SOAP message tree verification.	Attack detection
[35]	DOS attack	A scheme is identified for defending web services against DOS as well as XML based DOS attack.	Attack detection/Attack prevention
[36]	XML injection	An interception, detection and logging module based system is designed on node counting to detect XML attack.	Attacks detection

4. Exploration

4.1. How much research has happened on web service attacks since 2005?

In this systematic study, we identified relevant papers as shown in Table 1. Fig. 1. (a) depicts the research on web service attacks per year. The research is active and still going on as per Fig. 1. (a). Paper publications is spread across journals and conference proceedings. Out of the 36 papers, 6 has been published in journals, covering areas such as

Computer Science, Network and Information security as well as system engineering. The remaining 30 has been published in various international conferences.

Table 2. Web service attacks vs Area of focus.

Web service attacks	Attack detection	Attack prevention	Vulnerability detection	Vulnerability prevention	Combination
XML injection	4		1	1	1
SQL injection			2		
XPath injection		1			
Spoofing		1			
Denial-Of-Service	6	3			7
SQL,XML injection and DOS		1			1
SQL and XPath injection		2	2		
SQL, XML and XPath injections					1
SQL and XML injections		1			
Spoofing,DOS	1				

4.2. What are the web service security issues that are addressed in the research papers?

There are varied attacks on web services, ranging from injection attacks to Denial of service attacks. The following sections elaborates on them.

4.2.1. SQL Injection Attack

SQL injection attacks are very common in a web service environment. Most of the web services have improperly coded blocks that fail to filter non-validated user inputs. This inject and embed themselves as a parameter in a SQL statement trying to run non-administrative commands. As per Table 2, we can identify that 25% (9) of papers address SQL injection attacks. Among the 9 papers, 77.78% of them (7) discuss on other attacks such as XPath and XML injection as well.

4.2.2. XML Injection Attack

When any service fails to validate malicious XML content, XML injection vulnerability arises. The injection of malicious XML content into any service can alter the working logic. 30.55% of papers (11) discuss XML injection attack along with other attacks.7 papers out of 11 (63.63%) address XML injection attacks alone.

4.2.3 XPath Injection Attack.

XPath injection attack targets services/applications that use XPath as a language to convert user provided input to query XML documents. By sending a malformed user input, unauthorized information such as structure of XML document is obtained.[1,4,5,11,28,29] are the papers published that discuss on XPath based injection attacks. This constitutes 16.67% of the total papers analyzed.

4.2.4 Denial of Service Attack

DOS attack renders the target machine unresponsive by depriving the service of resources. DOS Attacks is addressed in 52.77% of papers (19), amongst which 15.78 %(3) deal with multiple attacks. Papers addressing DOS attacks alone are [3,7,9,10,14-18,20-23,25,27,30,32,33,35]

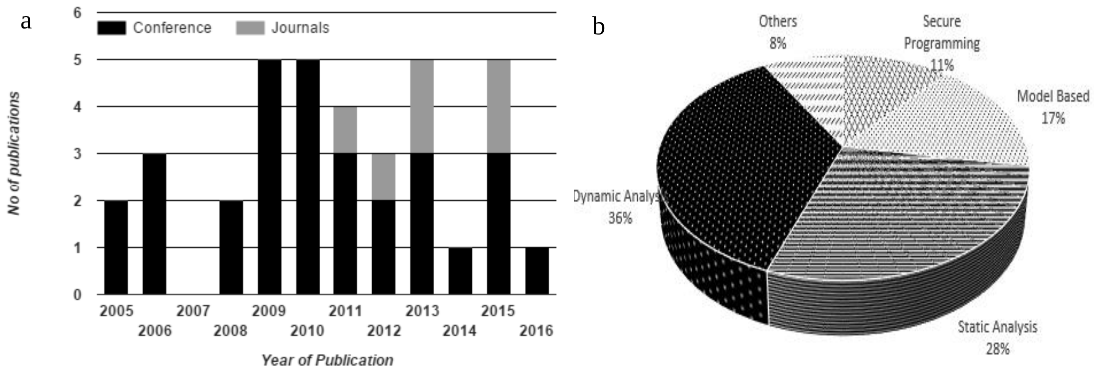

Fig. 1. (a) Publication year vs Publication count; (b) List of techniques used.

Table 3. Comparison between year and attacks.

Year	SQL Injection	XML Injection	XPath Injection	DOS	Others/Combinations
2005				✓✓	
2006				✓✓	✓
2007					
2008				✓✓	
2009	✓			✓	✓✓✓
2010				✓✓✓	✓✓
2011				✓✓✓	✓
2012		✓✓	✓		
2013		✓✓✓		✓	✓
2014	✓				
2015		✓		✓✓	✓✓
2016		✓			

4.3. What are the techniques proposed to solve web service security issues?

4.3.1. Dynamic Analysis

Dynamic analysis technique focuses on identifying output consistency w.r.t to input given in runtime. It is the most suggested technique with 36.11% of articles (13) proposing as a solution technique as per Table 4. It compromises black box testing[3, 4, 6, 21, 29], learning based[2] and schema hardening[32]. Other dynamic techniques are discussed in[17-19, 30, 33, 36]

4.3.2. Static Analysis

Static analysis deals with the code and does not focus on execution. Discrepancies are identified in the code to check for vulnerabilities. Static analysis can be done during the development phase itself. [11] deals with slicing techniques; code analysis in[9, 15]. Flow analysis is discussed in[34]. As seen in table 30.55% of articles (10) focus on static analysis[5, 20,23,28,31]. Static and dynamic analysis study are done in[1].

Table 4. Summary of techniques in the studies.

Techniques	References	No of Papers (%)
Dynamic Analysis	[2-4,6,17-19,21,29,30,32,33,36]	13 (36.11%)
Static Analysis	[1,5,9,11,15,20,23,28,31,34]	10 (27.78%)
Model Based	[7,10,13,14,22,26]	6 (16.67%)
Secure programming	[8,16,24,35]	4 (11.11%)
Others	[12,25,27]	3 (8.33%)

4.3.3. Model Based

As per Fig. 1. (b)., in another 6 studies (16.67%), models are used as solving techniques. [10] uses a case based reasoning model. Fuzzy logic is dealt with in[14]. Intrusion model is used in[22]. Web services attack model is discussed in[26].Other models are proposed in[7, 13].

4.3.4. Secure Programming

Techniques to secure the web service using filters, libraries or secure coding are discussed in 4 papers as per table 4(11.11%).Filtering policy is discussed in[24].Defense system integration into web services for authentication and verification is used in[35].Hash based cryptography measure is included in web service in[16].Pluggable API based security is discussed in[8].

4.3.5. Others

Other approaches like pattern based[12], vector quantization[25] and adaptive rule[27] solutions are discussed in 3 papers as per Table 4.

4.4. Which are the web service security areas focused in the research papers?

This study mainly focuses on two areas: web service attacks and web service vulnerabilities. 20 studies (55.56 %) focus on web service attacks and 6 (16.67%) focus on web service vulnerabilities. 10 papers (27.78%) focus on various combination techniques or attack implementation to test out web service strength as well as evaluate the web service contingency measures. To elaborate further the techniques are further classified into Attack Detection/Prevention, Vulnerability detection/prevention.

Table 2 indicates how the techniques are divided into six groups. Attack detection is the highest individual area with 30.55%, followed by Attack prevention that has papers contributing 25%. This is a positive approach as not only should contingency measures be taken after an attack has occurred, but enough research needs to be done on how to prevent the attack themselves.

Vulnerability detection and prevention is also important and 6 studies (16.67 %) focus on the vulnerabilities. Vulnerability prevention is discussed in[26].

5. Conclusion

Web services have become the primary way in which key information is seamlessly exchanged between applications. This make web service security an essential component and web service attack a serious threat to the integrity and availability of data. We have systematically analyzed 36 papers on web service attacks. Most addressed attacks are Denial-of-Service attacks followed by XML injection attacks. Techniques to deal with attacks predominately focus on attack detection measures. Since web service attacks cannot be completely eliminated, penetration and automation testing should be done as part of every development. This will guarantee added protection as well as lower attacks on web services.

References

1. Asmawi A, Affendey LS, Udzir NI, & Mahmod R Model-based system architecture for preventing XPath injection in database-centric web services environment, *7th International Conference on Computing and Convergence Technology*; 2012. p. 621-625.

2. Appelt D, Nguyen CD, Briand, LC, & Alshahwan N. Automated testing for SQL injection vulnerabilities: an input mutation approach. *International Symposium on Software Testing and Analysis*; 2014. p. 259-269.

3. Altmeier C, Mainka C, Somorovsky J, & Schwenk J. AdIDoS–Adaptive and Intelligent Fully-Automatic Detection of Denial-of-Service Weaknesses in Web Services. *Data Privacy Management, and Security Assurance*; 2015. p. 65.

4. Vieira M, Antunes N, & Madeira H. Using web security scanners to detect vulnerabilities in web services. *IEEE/IFIP International Conference on Dependable Systems & Networks*; 2009. p. 566-571.

5. Antunes N, Laranjeiro N, Vieira M, & Madeira H. Effective detection of SQL/XPath injection vulnerabilities in web services. *IEEE International Conference on Services Computing*; 2009. p. 260-267.

6. Antunes N, & Vieira M. Detecting SQL injection vulnerabilities in web services.*Fourth Latin-American Symposium on Dependable Computing*; 2009. p. 17-24.

7. Chonka A, Zhou W, & Xiang Y. Defending grid web services from xdos attacks by sota. *IEEE International Conference on Pervasive Computing and Communications*; 2009. p. 1-6.

8. Rajaram AK, Babu BC, & Kishore Kumar RC. API based security solutions for communication among web services. Fifth International Conference on Advanced Computing; 2013. p. 571-575.

9. Kumar RK, Kanchana, R, & Babu C. Security for SOAP based Communication among Web Services. *IJCA Proceedings on International Conference on Science, Engineering and Management*; 2013. p. 46-51.

10. Pinzón C, González A, Rubio M, & Bajo J. A Security Proposal Based on a Real Time Agent to Protect Web Services against DoS Attack. *5th International Workshop Soft Computing Models in Industrial and Environmental Applications*; 2009. p. 1-8.

11. Thome J, Shar LK, & Briand L. Security slicing for auditing XML, XPath, and SQL injection vulnerabilities**.** *IEEE 26th International Symposium on Software Reliability Engineering*; 2015. p. 553-564.

12. Muñoz-Arteaga J, Fernandez EB, & Caudel-García H. Misuse pattern: spoofing web services.*2nd Asian Conference on Pattern Languages of Programs* ; 2011.

13. Chan GY, Lee CS, & Heng SH. Policy-enhanced ANFIS model to counter SOAP-related attacks. *Knowledge-Based Systems*; 2012. p. 64-76.

14. Chana GY, Chuaa FF, & Leeb CS. Fuzzy association rules vs fuzzy associative patterns in defending against web service attacks.*12th International Conference on Fuzzy Systems and Knowledge Discovery* ; 2015. p. 524-529.

15. Padmanabhuni S, Singh V, Kumar KS, & Chatterjee, A. Preventing service oriented denial of service: A proposed approach. *International Conference on Web Services*; 2006. p. 577-584.

16 Suriadi S, Stebila D, Clark A, & Liu H. Defending web services against denial of service attacks using client puzzles. *IEEE International Conference on Web Services*; 2011. p. 25-32.

17. Suriadi S, Clark A, & Schmidt D. Validating denial of service vulnerabilities in web services. *4th International Conference on Network and System Security*; 2010. p. 175-182.

18. Pinzón CI, Bajo J, De Paz JF, & Corchado JM. S-MAS An adaptive hierarchical distributed multi-agent architecture for blocking malicious SOAP messages within Web Services environments. *Expert Systems with Applications*; 2011. p. 5486-5499.

19. Salas P, Invert M, De Geus PL, & Martins E. Security Testing Methodology for Evaluation of Web Services Robustness-Case: XML Injection. *IEEE World Congress on Services*; 2015. p. 303-310.

20. Pinzón C, De Paz JF, Zato C, & Pérez J. Protecting web services against dos attacks: A case-based reasoning approach. *Hybrid Artificial Intelligence Systems*; 2010. p. 229-236.

21. Falkenberg A, Mainka C, Somorovsky J, & Schwenk J. A new approach towards DoS penetration testing on web services. *IEEE 20th International Conference on Web Services*; 2013. p. 491-498.

22. Ficco M, & Rak M. Intrusion tolerant approach for denial of service attacks to web services. *First International Conference on Data Compression, Communications and Processing*; 2011. p. 285-292

23. Gruschka N, & Luttenberger N. Protecting web services from dos attacks by soap message validation. *Security and privacy in dynamic environments*; 2006. p. 171-182.

24. Loh YS, Yau WC, Wong CT, & Ho WC. Design and Implementation of an XML Firewall. *International Conference on Computational Intelligence and Security*; 2006. p. 1147-1150.

25. Zheng J, & Hu MZ. Intrusion detection of DoS/DDoS and probing attacks for web services. *Advances in Web-Age Information Management; 2005*. p. 333-344.

26. Mainka C, Jensen M, Iacono LL, & Schwenk J. XSpRES-Robust and Effective XML Signatures for Web Services. *CLOSER*; 2012. p. 187-197.

27. Im EG, & Song YH. An adaptive approach to handle DoS attack for web services. *Intelligence and Security Informatics*; 2005. p. 634-635.

28. Laranjeiro N, Vieira M, & Madeira H. A Learning-Based Approach to Secure Web Services from SQL/XPath Injection Attacks. *IEEE 16th Pacific Rim International Symposium on Dependable Computing*; 2010. p. 191-198.

29. Laranjeiro N, Vieira M, & Madeira H. Protecting Database Centric Web Services against SQL/XPath Injection Attacks. *Database and Expert Systems Applications*; 2009. p. 271-278.

30. Oliveira RA, Laranjeiro N, & Vieira M. Assessing the security of web service frameworks against Denial of Service attacks. *Journal of Systems and Software*; 2015. p. 109, 18-31.

31. Rosa TM, Santin AO, & Malucelli A. Mitigating xml injection 0-day attacks through strategy-based detection systems. *Security & Privacy;* 2013. p. 11(4), 46-53.

32. Patel V, Mohandas R, & Pais AR. Attacks on Web Services and mitigation schemes. International Conference Security and Cryptography; 2010. p. 1-6.

33. Siddavatam I, & Gadge J. Comprehensive test mechanism to detect attack on Web Services. *16th IEEE International Conference on Networks;* 2008. p. 1-6.23.

34. Tao Z. Detection and service security mechanism of xml injection attacks. *Information Computing and Applications*; 2013. p. 67-75.

35. Ye X. Countering ddos and xdos attacks against web services. *IEEE/IFIP International Conference on Embedded and Ubiquitous Computing*; 2008. p. 346-352.

36. Gupta AN, & Thilagam PS. Detection of XML Signature Wrapping Attack Using Node Counting. *3rd International Symposium on Big Data and Cloud Computing Challenges*; 2016. p. 57-63

37. Joseph S, & Jevitha KP. Evaluating the Effectiveness of Conventional Fixes for SQL Injection Vulnerability. *Proceedings of 3rd International Conference on Advanced Computing, Networking and Informatics*; 2016. p. 417-426.

38. Lindstrom P. Attacking and Defending Web Services, White paper, 2004 http://www.spiresecurity.com

39. WS-Attacks, Welcome to WS-Attacks, 2015 http://www.ws-attacks.org/Welcome_to_WS-Attacks