Second International Conference "Mathematics Days in Sofia"
July 10–14, 2017, Sofia, Bulgaria

Contemporary Cryptographic Methods for Secure Web Services

Malinka Ivanova

Informatics Department, Faculty of Applied Mathematics and Informatics
Technical University of Sofia, Bulgaria
m_ivanova@tu-sofia.bg

Keywords: web services, security, cryptographic methods

Development of web technologies and their wide adoption in different areas leads to the increased usage of web services. Web services are software components that in most of the scenarios support machine-to-machine communication, performing actions when they are utilized by web applications. Currently, the most widely used web services are the REST (Representational State Transfer) web services, because of their simpler implementation in comparison to SOAP (Simple Object Access Protocol)- and WSDL (Web Service Definition Language)-based web services that require more complex realization. Anyway, their implementation is always based on XML placed in a SOAP envelop and the problem related to the development of secure XML is from the highest importance [1].

The most probable threats and attacks related to SOAP messages address issues like modification of the message, reading a message, sending false message to a service to be well-formed in a way that will not cause the utilization of security claims, or sending false message to a service that will force the generation of incorrect client request [2]. The realization of web service security is achieved through the use of different algorithms for encoding and digital signing [3]. According to the WS-Security specification, separate header and body blocks as well as their sub-structures could be encrypted/signed as a symmetric key which could be additionally shared between two sides or it could be encrypted and placed in the message [4]. The XML Encryption specification recommends which algorithm for what purpose is to be applied: for block encryption the following ones are recommended: TripleDES, AES-128, AES-256 and AES-192 algorithms; for key agreement – Diffie & Hellman algorithm; for Key transport – RSA-v1.5 and RSA-OAEP; for message authentication – XML Digital Signature [5].

The aim of the talk is to explore and summarize the best practices in the area of achieving web service security by means of cryptographic algorithms. Solutions and recommendations in specifications, technical and research papers concerning threats and attacks against web services at XML level and their prevention and protection are analysed. The performed analysis is foreseen as part of designing a methodology for realization of secure web services.

References

[1] Paul Adamczyk, Patrick H. Smith, Ralph E. Johnson, Munawar Hafiz, REST and Web Services: In Theory and in Practice - chapter from the book REST: From Research to Practice, Springer New York, 2011, ISBN 978-1-4419-8302-2, pp. 35-57.

[2] Esmiralda Moradian and Anne Håkansson, Possible attacks on XML Web Services, IJCSNS International Journal of Computer Science and Network Security, vol.6 No.1B, January 2006, pp. 154–170.

[3] Martin Abadi and Bogdan Warinschi, Security Analysis of Cryptographically Controlled Access to XML Documents, Journal Journal of the ACM, vol. 55, Issue 2, May 2008, Article No. 6, pp. 1–29.

[4] W3C XML Encryption Syntax and Processing version 1.1. 11 April 2013. http://www.w3.org/TR/xmlenc-core1/.

[5] W3C XML Signature Syntax and Processing, Second edition. 10 June 2008. http://www.w3.org/TR/xmldsig-core/.