Computers and Electrical Engineering 000 (2017) 1–11

Contents lists available at ScienceDirect

Computers and Electrical Engineering

journal homepage: www.elsevier.com/locate/compeleceng

Measuring web service security in the era of Internet of Things☆

Bo Zhou[a,*], Quan Zhang[b], Qi Shi[a], Qiang Yang[c], Po Yang[a], Yinyan Yu[d]

[a] Department of Computer Science, Liverpool John Moores University, Liverpool, UK
[b] School of Information Engineering, ShenYang University of Technology, Shenyang, China
[c] College of Electrical Engineering, Zhejiang University, Hangzhou, China
[d] Institute of Computer Science and Technology, Peking University, Beijing, China

ARTICLE INFO

Article history:
Received 16 October 2016
Revised 14 June 2017
Accepted 22 June 2017
Available online xxx

Keywords:
Web service
Security measurement and evaluation
Quantitative service security
Service level agreement
Linguistic evaluation
Multiple attribute decision making

ABSTRACT

Technologies such as Internet of Things allow small devices to offer web-based services in an open and dynamic networking environments on a massive scale. End users or service consumers face a hard decision over which service to choose among the available ones, as security holds a key in the decision making process. In this paper a base linguistic evaluation set is designed, based on which all the other fuzzy term sets that used for describing security attributes are uniformed and integrated for calculating an overall security value of the services. This work, to the best of our knowledge, is the first practical solution to offer direct comparisons and rankings of network services based on multiple security attributes such as confidentiality, availability, privacy and accountability. We analysed four major cloud service platforms to illustrate the proposed approach.

1. Introduction

In the digital world, a service is defined as a software unit that provides certain functionalities. A web service is a service that is made remotely available to other entities through networks. By using standard communication protocols and languages, web services provide necessary interfaces so that any system can invoke them remotely. The Service-Oriented Architecture (SOA) provides designs and frameworks to offer services as self-contained units. One can invoke a web service, as long as the input satisfies the interface specification, and let the output of the web service to be an input to another service if they need to work together. The most commonly used communication protocol for exchanging information between web services is the Simple Object Access Protocol (SOAP). SOA platforms provide a foundation for modeling new applications, which involves planning, searching for, connecting, and invoking web services.

One of the issues faced by a service consumer is to measure and choose a right service from potentially a very large service pool. Services provided by different providers may offer the same functionality, but they could be very different in terms of cost, quality, or security. Therefore the service consumer faces the dilemma of picking up the most suitable services for his/her application, especially in the era of Internet of Things (IoT) where small devices are made available as service unit through an open and dynamic networking environment in massive scale. Among all the existing works that have been

☆ Reviews processed and recommended for publication to the Editor-in-Chief by Guest Editor Dr. Zhihan Lu.

* Corresponding author.
E-mail addresses: b.zhou@ljmu.ac.uk, b.zhou@hotmail.com (B. Zhou).

http://dx.doi.org/10.1016/j.compeleceng.2017.06.020
0045-7906/

used to quantify and compare web services, we found that most of them focus on the QoS only and the key question of quantifying services based on their security properties remains unanswered [1]. Nonetheless, it is crucial to measure the services from security perspective since one service developed with good faith in its security may not be necessarily good enough for another to use.

In this paper we propose a novel quantitative approach based on fuzzy terms. In particular, we focus on security as it is a big challenge for utilising web services, due to the lack of a common ground and evaluation criteria. It is to use a linguist evaluation method to quantitatively measure services based on their security attributes such as *confidentiality, availability, privacy* and *accountability*. These attributes are formulized into one base linguistic evaluation set and calculated towards an overall security value. In this way the comparison of different services' security becomes possible.

To the best of our knowledge, this work is the first practical approach to target the issue of evaluating web services based on multiple security attributes at the same time. It provides the foundation for further research into this area and has great potential to be extended to solve similar issues faced by other information systems. The calculation is based on information that already exist, e. g., descriptions in the Service Level Agreements (SLAs), thus it is feasible and practical enough to make immediate impact.

The rest of the paper is organised as follows. The next section explains how web service security is presented in current network and the challenges service consumers are facing. Section 3 introduces the linguistic evaluation foundation and the triangular membership function. The next section explains our approach to formulize different linguistic term sets and calculate an overall security value for web services based on multiple attributes. An example is given in Section 5 to illustrate the solution and Section 6 discusses related work. Finally the paper concludes with an outline of future work in Section 7.

2. Web service security

2.1. Security wtih SLAs and WSDL

Web services are normally made available together with a Service Level Agreements (SLA). A SLA is a formal guarantee that has to be accepted by service consumers before the service being used. A SLA can specify the properties of a service across different levels. For example, on business level it can describe what kind of functionality the service is offering and how the users will be charged (cost); on technical level it may describe the number of shutdowns the service might experience each year (QoS).

Security can also be promised as part of the SLA. However its coverage is rather poor to date due to the lack of well defined semantics. The SLAs traditionally focus on the QoS metrics such as a bandwidth guarantee and backup strategy. Even when the security being mentioned, in practice it tends to be written in a natural language with fuzzy terms such as "High", "Good", etc. Therefore it is very difficult for the service consumer to really understand the situation and compare the web services from the security aspect.

Apart from SLA, a web service also describes its interfaces through a Web Service Description Language (WSDL). A WSDL file specifies how to invoke the service, i.e. the input parameters, in order to communicate with the service and the expected output for each of the operations provided by the service. The WSDL file can be generated automatically from the web service code. Based on WSDL specification files, a service consumer can design his/her applications accordingly and use SOAP to call the operations listed in the WSDL files.

Although WSDL is mostly used to specify the functional aspects of a service, it is possible to attach non-functional properties such as security to the WSDL. WS-SecurityPolicy is an extension of WSDL to secure SOAP messages. It utilises standards like SAML, XML Signature , and XML Encryption to achieve the goal of secure communications with web services. WS-SecurityPolicy is different from the Secure Socket Layer (SSL) protocol as the WS-SecurityPolicy only encrypts the content of a SOAP message while SSL can encrypt the entire communication channel. Comparing to SSL, WS-SecurityPolicy is more flexible as it can choose which part of the SOAP message to be encrypted by using which cryptographic algorithm. WS-SecurityPoliy is attached to the WSDL by declaring it in the WSDL.

2.2. Challenges

Despite some efforts from SLA and WSDL, security issue remains a big challenge for web services. The dilemmas faced by a service consumer are in three folds.

- Firstly, security is a broad concept that includes many aspects such as confidentiality and privacy. One service may be stronger than another in terms of confidentiality; while it is also possible that the very same service has weaker protection of privacy. It is a typical multi-criteria issue, which service consumers are not always in the position to resolve due to the lack of expertise.
- Secondly, WS-SecurityPolicy was proposed to secure the SOAP messages. It is well equipped for–but also limited to–the security of communication with web services. Security requirements at higher levels are hard to be expressed by using the WS-SecuirtyPolicy. In contrast, security descriptions in SLAs are more open and inclusive but not always precise, especially in natural language. The situation can get even more complicated when more than one SLA language is involved.
- Finally, although some security modelling and verification techniques allow the service consumer to specify certain security properties that the service has to comply with before the service being used [2], in practice the number of services

Please cite this article as: B. Zhou et al., Measuring web service security in the era of Internet of Things, Computers and Electrical Engineering (2017), http://dx.doi.org/10.1016/j.compeleceng.2017.06.020