International Journal of Information Security and Privacy
Volume 12 • Issue 1 • January-March 2018

A Proposed SOAP Model in WS-Security to Avoid Rewriting Attacks and Ensuring Secure Conversation

Rajni Mohana, Jaypee University of Information Technology, Solan, India

ABSTRACT

Service oriented architecture is a current and popular software engineering paradigm providing agile web services to consumers in a dynamically changing enterprise environment. The SOAP messages are used to establish communication between the web services which are vulnerable to rewriting attacks and insecure conversation. XML Signature as specified in WS-Security provides security to the contents of the SOAP messages but is insufficient. This paper proposes a SOAP model where rewriting attacks can be avoided and a secure conversation can be established as well. This paper recommends three steps, firstly using shared key for encrypting timestamp in the message body for generating corresponding signature; Secondly, using value referencing both for signature validation and message processing; and finally encrypting the whole SOAP body instead of sending an open SOAP Message in the network to prevent unauthorized access. The paper concludes that the proposed model successfully detects rewriting attacks and establishes secure conversation in the to-and-fro message transmission.

KEYWORDS

Rewriting Attacks, Web Services, Wrapping Attacks, WS-Security

INTRODUCTION

Service-Oriented Architecture (SOA) is a new paradigm for reorganizing or reusing old applications into web services. Web services are self-describing platform independent computational elements, which are accessible through standard interfaces. It can be assembled in complex compositions using standard messaging protocols (Rolland, 2010). In SOA environment, one has to integrate various web services and enable a secure conversation among them, to provide a better Business to Business (B2B) / Business to Business (B2C) application with agility. One of the ways of communication between web services is based on Extensible Markup Language (XML) message called Simple Object Access Protocol (SOAP) given in w3.org/TR/xpath20/. Web services make use of SOAP to tie heterogeneous business systems together. This provides an opportunity for organizations to create and deploy distributed applications without being concerned about the hardware platform, the operating system (OS), the programming language, or the network topology (Liu, 2008). Thus, SOAP provides platform and language neutrality.

The challenging part of system integration is SOAP message exchange in a secured and meaningful manner. These messages are very well prone to attacks leading to several issues such as unauthorized access and identity theft. These attacks are basically referred as XML rewriting attacks (Sinha 2008). Rewriting attacks are also called as wrapping attacks because it involves changing the

DOI: 10.4018/IJISP.2018010107

content of the SOAP message without invalidating the signature (Gajek, 2009). Rewriting attacks are done by injecting a faked element inside the structure of the SOAP message so that a valid signature covers the unmodified element whereas faked one processes the application logic. The message is processed according to the path whereas the signature is validated according to the Message body ID. This method is called as *Id* referencing which creates a scope for the rewriting attacks. As a result, an attacker can easily perform an arbitrary web service request pretending as a legitimate user. The challenge is to provide a solution to rewriting attacks. (McIntosh, 2005) showed that the content of a SOAP message is protected by an XML Signature as specified in WS-Security which can be easily altered without invalidating the signature. The *XML rewriting attack is* possible because the referencing schemes used to locate parts of a SOAP message document differ between the signature verification function and the application logic (Gajek, 2009). Replay attack, redirection attack and multiple security header attack are the three types of attacks. (Sinha, 2008) lists out types of rewriting attacks their impact on SOAP messages.

Motivation

Consider a scenario of online shopping (Figure 1), when a client puts a request on the portal, a SOAP message is sent to the inventory to check for the stock, if its available then the details of it is appended to the SOAP message, and the message is further forwarded to billing department. The billing department further prepares the invoice according to the incoming SOAP message, appends the bill information to the SOAP message and sends the message to the shipping department, which takes care of shipping the details to the right person by placing the order to the manufacturer's web service. Now all are authorized to access the SOAP message and are trusted for communication. The problem arises when an authorized user breaks the trust in midway of the path or if an attempt is made to modify the message and further enacting as if he is not the constructor of the message. Hence, it's required to check whether there is any breach of trust.

Using WS-Policy and other standards effectively on SOAP helps escaping XML rewriting attacks (Gajek 2009). However, incorrect usage and incorrect application of the standards by programmer is very likely which leads to vulnerabilities like rewriting attacks and insecure conversations. Related research work in this area by various authors does highlight on how to avoid a wrapping attack.

Figure 1. Scenario of online shopping