

PROTECTION OF INFORMATION TRANSMITTED VIA THE SOAP PROTOCOL.
WEB SERVICE SECURITY (WS SECURITY)

YURY KUVETSKI, IRINA BURACHIONOK

Polotsk State University, Belarus

The article examines the peculiarities of the SOAP protocol, the problems you can face while using this protocol and the methods of their solution. The authors of the article analyse the main modern ways of providing security of the communication process with Web services via the Internet and their realization in the WS Security Standard. The article dwells on necessary measures for providing complete security while using web services.

At all times the process of automatization of different activities is the necessary condition of the development of the society. Nowadays developing the cutting-edge information technologies opens new opportunities for creating new automated systems in all spheres of national economy. Certainly there appear the problems connected with the necessity of increasing the level of security of such systems. Moreover, the choice of methods and means of processing information is defined not only by the importance of the processed information, but also by the composition of automated systems, their structure, the ways of processing information and also by the quantitative and qualitative composition of users and service personnel. Let's consider the system, where the main tasks are the remote compilation and the execution of program code on different web services. The most popular architecture among the modern application developers is the service architecture, because such applications are much easier to maintain and it's easier to solve the problem of zooming, but the problem of security appears, because transmission of data takes place via the net. In this article we are going to regard a variant of a system build, based on the SOAP protocol of transmitting data, and the WS Security Standard.

First of all, let's discuss SOAP. The SOAP (Simple Object Access Protocol) is used for exchanging random structured messages in XML format (Extensible Markup Language) via the cloud computing environment. It can be used with any protocol of an applied level, however more often SOAP is used above the HTTP (Hyper Text Transfer Protocol). Its message in XML format is presented in figure 1 and represents the envelope which contains a header and a body, the body in its turn can contain a fault. Microsoft allows you to use the SOAP Protocol with the help of the WCF (Windows Communication Foundation) [1].



Fig. 1. The Structure of XML Message Transmitted via the SOAP Protocol

Further we will examine three standards of security applied to the XML: authentication, data integrity and data confidentiality. The more detailed diagram is presented in figure 2.




Basic Standart	WS Security		
Basic Mechanisms	Security Token  Authentication	Encryption  Confidentiality	Signatures  Integrity
Constituent Elements	The token profile for the user name.	XML Encryption	XML Signatures
	Profile of the token for certificate X.509	Symmetric Encryption	XML standardization
	Token profile for SAML	Asymmetric encryption	Digest algorithm

Fig. 2. The Structure of Basic WS Security mechanisms

The authentication guarantees that a sender and a receiver are the people who they claim to be, and it proves the authenticity of the sides. It can be realized in different ways. A simple variant is to provide the user's ID and password. A more complicated variant is using the certificate, which contains all the necessary accounting data and is associated with a pair of public and private keys.

To provide the integrity of information, which is exchanged by the sides, and to guarantee that the contents of the message won't be changed or damaged in the process of transmitting data, the data are signed with digital signature (DS) with using the certificate X.509 private key of the sender. Also you can sign SOAP headers of requests to guarantee the integrity of additionally transmitted information.

The third requirement for providing system security is confidentiality. Encryption technology is used to make an exchange of information in requests and web service responses unreadable for strangers. The aim is to guarantee that any attempt to request data while transmitting, in memory or after being saved will require relevant algorithms and security keys for their decryption.

At the moment all these security measures are easily realized and the ways of their realization can depend on the means of transmitting messages or be specific for SOAP protocol. Each of them separately can provide a sufficient level of security but in such cases a system is always at risk. Everyone will have an access to the service without authentication. There exists the possibility of substituting or damaging data without a digital signature. If all the listed above requirements are applied every system can be considered to be secured, whereas the ways of security realization are not so important. Surely there are systems in which you can ignore these rules, for example, if you don't need to restrict an access to a service, you can omit authentication. If the size of a system is limited by sending a request between a user and one point (service), then it is enough to use the HTTPS (Hyper Text Transfer Protocol Secure) and the necessity of encrypting is not needed. The same refers to the digital signature of data, it is not needed if transmitted messages are not valuable or can't damage a system.

Providing integrity, confidentiality and authentication of a message and its sender while maintaining transparency for extension are the main tasks of WS security [2]. It doesn't define any new technologies and is based on existing standards, for example the XML Encryption, the XML Signature, the X.509 certificates and different cryptographic algorithms. Due to the fact that their basic conception is based on message mechanisms, it becomes possible to provide End-to-End Security, for example, by using the Secure Socket Layer protocol instead of the protection aimed at transport. The main standard elements are the following basic mechanisms: security tokens, encrypting, digital signature and timestamps.

Security tokens are applied during authentication and their task is to perform credentials without which authentication is impossible. A user ID and a corresponding password most often perform the role of credentials.

We can give a lot of information on the topic of encrypting but principally we distinguish between two mechanisms of encrypting: symmetric and asymmetric. In the first case a generic key, always available for both sides, is used for encrypting and decrypting; this way is faster. In the second case different keys for encrypting and decrypting are used: a private key remains at with an owner and a public key is freely distributed; this way is

more reliable. Both approaches are often united in the following way: a client who generates a symmetric key, encrypts data of any size by using it, after that the key itself is encrypted with the help of an asymmetric algorithm and is enclosed in a message. Digital signatures are used to confirm the integrity of messages. Due to them you can recognize illegal modifications such as attachment, modification and deletion of data.

In Ws Security this approach is based on the XML Digital Signature standard. The principle of the Digital Signature is based on the creation of checksums with the help of special algorithms, (digests) after that the results are attached to the message and are partly transmitted in an encrypted way.

It's also important to regard the technology of timestamps. The thing is that in terms of the SOA (Simple Object Access) services should perform a definite action in such a way as to maintain an interaction stateless. This peculiarity allows attackers to perform replays, when an attacker sends a whole message again or its separate parts. To be protected from such attacks, it is necessary for a message to have its own unique identifier (Message ID) which a service keeps and takes into account in the following messages.

As a result we can make a conclusion that the SOAP protocol is quite flexible and suitable to use, it allows you to abstract a message with different web services via using their generic interface. Due to the WS Security standard you can provide a sufficient level of system protection against dangers. There has been made a decision to organize a direct communication of a client with web services by using the SSL protocol with a high enough level of security for transmitting data on the Internet directly from the client to the service.

REFERENCES

1. Microsoft. Общие сведения о безопасности [Электронный ресурс] / MDN. – Режим доступа: <https://msdn.microsoft.com/>. – Дата доступа: 10.09.2017.
2. IBM Knowledge Center. WS-Security [Электронный ресурс] / IBM. – Режим доступа: <https://www.ibm.com/support/knowledgecenter/>. – Дата доступа: 10.09.2017.