A Steganographic Method For Secure Communication And Access Control Using Web Service Container

Authors
B.Padmini¹, Dr. N. Chandra Shekar Reddy²

¹Student, M.Tech CSE Dept, Institute of Aeronautical Engineering, Hyderabad-500043, Andhra Pradesh, India,
²Professor, CSE Dept, Institute of Aeronaucal Engineering, Hyderabad-500043, Andhra Pradesh, India
Email- P_Badarvada@Yahoo.Com, naguchinni@gmail.com

ABSTRACT:

Digital stenography is an art of hiding communication. Security is the important aspect for any software system. It is mandatory for securing communication and access the control in the business applications. This paper focuses, on two aspect (1) Firstly the web container is created for web services, then the web security framework (WSF) offers effective securing communication is done i.e. sending security tokens as a part of SOAP messages to authorized users only. (2) Stenography method is used for SOAP messages; this method is based on rearranging order of XML element according to a secret message.

1. INTRODUCTION

Web services provide a new kind of distributed middleware services. Web services provide standard interface as well as communication protocol and also effective service integration. It is important for secure communication as well as access control.

Due to lack of web security standards and its implementation. On the other hand, the primary secure technologies are included such as SSL (Secure Socket Layer), VPN (Virtual Private Network) and HTTP authentication. But these cannot satisfy any type of web secure communication for permission management by associating rules. Therefore information can be exchanged between peer using SOAP messages.

A SOAP message in a XML document contains text. Stenography used for text files and Xml documents. So of the messages may be infeasible. The new Stenography embed secretive information.

Stenography is combined with cryptography to increase the security for exchanging secret information between people as well as over world using internet. Therefore it is called as the terrorist tool.

Web service exchange data in the form of XML documents, simple object access protocol (SOAP) messages
provide data transport, this provides the efficient communication over web client and systems interact with web services using XML messaging.

Our attempt to provide secure communication and also access control. Web container is designed to offer an effective solution, in secured communication the authorized permission delegation. Finally authorization requires enforcement and authorization constraint based assessment and delegation is also required.

2. RELATED WORK

There are number of stenography studies in comparison of audio, video and image based. Por and Delina [9] improved the open space method proposed by [5]. Therefore, they proposed a hybrid steganography method for text by combining both inter-word spacing and inter-paragraph spacing methods. Thus, whitespaces between words and paragraphs in right-justification of text are used for data hiding in order to increase the embedding capacity. However, the cover text was dynamically generated according to the size of the secret message.

Shirali-Shahreza [3] proposed a new steganography method for texts. This method is based on the different spelling of some words in English between UK and US. For example, “centre” has different terms in UK (centre) and US (center).

The model proposed in [4] defines a text steganography method base on substituting the words which have different terms in UK and US. For example, (Gas) has different terms in UK (Petrol) and US (Gas)

Liu et al. [5] proposed a text steganography method to be used in online chat. This method is based on an Internet meme named typoglecymia, which means that changing the order of word’s middle letters has a slight to no effect on the ability of skilled readers to understand the text (e.g. Guitar and Guiatr). Therefore, it used the redundancy found in the interior letters’ order. Since this letter randomization equals to the common error made by chatters due to high speed typewriting, it is likely to be used in online chats, where the text usually contains mistakes.

However, the previous studies provide text steganography method, which are not necessarily applicable in SOAP messages context due to the fact that SOAP messages are exchanged and monitored by computer systems rather than humans. Using misspelled or alternative words in SOAP messages would result in the SOAP parsers not being able to handle the SOAP messages received because they do not comply with the expected semantic.

To the best of our knowledge, there are only a couple of studies and examples of research regarding information hiding in XML files. Inoue et al. [8] proposed five steganography methods to be used with XML files. These steganography methods are summarized as follows:

The empty elements are represented according to the secret bit; either a start-tag immediately followed by an end-tag (<img></img>), or an empty-element tag (<img/>). This technique can embed one bit per empty
element.
According to the secret bit, we can either add a white space before the close bracket (<tag >), or delete
(normal with no added spaces) this white space (<tag>). This technique can embed one bit per tag.
Two elements may or may not be exchanged according to the secret bit. Thus, one bit per an exchange of
two elements can be hidden.
The order of attributes in an element can be exchanged to hide the secret data. Thus, one bit per an exchange
of the attributes order can be hidden.

3. WEB SERVICE CONTAINER
Web service is an abstraction to wrap application to web services. Web services container consists of three
key layers.
1. Logical resource layer for wrapping web service and implementation on COTS.
2. A web service supporting layer for runtime management and security.
3. Tool layer for discovery, deployment of web services.
To provide a secured environment web container provide secure communication and access control
mechanism.

![Web Service Container Secure Communication](image_url)

**Fig 1:** Web Service Container Secure Communication
An Intermediate way for achieving security is relayed on secured transport layer. This is provides security only in a secure channel. When the secured transport layer is not able to control the message, VPN provides protection to the web service container, but it is limited to a Final slope. As web services will be registered in UDDI, so web service container does not demand to use VPN. New secure communication requires selective encryption end-to-end security, security based application layer.

Web service framework (WSF) applies on application layer. Figure 1 shows that this architecture adds a SOAP message on both server side and client side of the web service container.

Client message process is a serial of message processors such as Security processor, digital signature processor, Authentication processor, Encryption processor.

Server message process is a serial of message processor such as Security processor, Authentication processor, Decryption processor, Signature validation processor and access control processor

Finally the message passing is done on the transport layer protocol by HTTP etc.

**Control Access**

Role-Based Access (RBC) is accepted as an alternative for protection techniques. The idea of setting permission and assigning the role to user is widely adopted in many commercial systems and is suitable for the web service container. A hierarchical RBC is associated with permissions and these permissions are mandatory. However hierarchical RBC are not enough for the web service container delegation are necessary. Some users can have their own roles, but other users want to delegate one user permission to accesses web service

### 4. INFORMATION HIDING IN SOAP MESSAGES

The SOAP is designed to exchange structured information (i.e. SOAP messages) over many protocols is distributed as well as decentralized environments. This protocol uses XML technologies to define messaging protocol that is independent of any programming languages.

A SOAP message is an XML document, which consists of envelop, header body and fault elements."Envelop" is the root element that defines XML document as a SOAP message. Specific information is defined within the “header” element. Header contain SOAP processors either to understand header or to reject SOAP messages. Actual data is defined in the “Body” element.
The design and implementation of data hiding method monitors SOAP message after the serialization of the senders endpoint before it is sent, the analyses of its elements and the secret messages are embedded. When SOAP message arrives at the end point, the secret message is extracted by using stegno key.

**Fig 2:** SOAP message. Stenography Architecture for SOAP Messages

```xml
<? xml version="1.0">
<soap:envelop
xmlns:soap=http://schemas.xmlsoap.org/soap
>
<soap: header>…….</soap:header>
<soap:body>
 <soap: fault>……</soap:fault>
</soap: body>
</soap:envelop>
```

**Fig 3:** Soap Stegnography Architecture
4.1 Embedding Procedure
In this procedure the hiding of secret message with SOAP message consists of six steps.
1. Retrieving of the entire SOAP message.
2. Analysis of the contents will be done, and then identifying the entire element be alone by rearranging the SOAP message that is suitable for embedding process.
3. Elements that were hidden in data (M) are calculated.
4. Merging every sub-element by a reflective symbol for secret message.
5. All the symbols of secret message are hidden in SOAP message, then the sub-elements N+1 will arranged to indicate secret message.
6. If N>M is only the part of the secret message that is sent by SOAP message and sub-element will be re-arranged and indicate the hidden data

4.2 Extracting Procedure
The receiver extracts hidden data and analyzes the contents of the eligible element by using the secret key to reveal the hidden symbol
1. Receiving the SOAP message and checking its validity.
2. Calculating the elements that were used in the data hiding.
3. Extracting of the hidden symbols is done and the analysis of the sub-elements of each and every element in the SOAP message.
4. Process is stopped if the extracted symbol is not a stego SOAP message.
5. If the extracted symbol displays “continue” the new SOAP message is captured and step 1 is analyzed.
6. The next symbol is extracted until the secret message is embedded.

5. CONCLUSION
Web service frame work offer effective solution for secure communication, in this the ability of security tokens for SOAP messages and also web service Container is created.
The stenography manipulates the SOAP protocol and monitors the SOAP message after serialization. The SOAP elements are analyzed and embed the secret message according to a stego key and by using the secret key the SOAP message is embedded by the receiver.
6. REFERENCES

1. Information Hiding in SOAP Messages: A Steganographic Method for Web Services by Bachar Alrouh, Adel Almohammad, Gheorghita Ghinea

2. Secure Communication and Access Control for Web Services Container by Yu Peng, Quanyuan Wu

