Credibility Verification of RESTful Web Services Based on Behavior Declaration

Xue-jun YU¹,a and Miao-chen LIU²

¹,²School of Software Engineering, Beijing University of Technology Beijing, China

a58218350@qq.com

Keywords: Behavior declaration, RESTful, Web services, Credibility.

Abstract. Representational State Transfer (REST), a kind of current mainstream framework, fit the needs of the people very much. But the research on the credibility of REST is not enough. In this paper, we will define the behavior declaration of RESTful Web services by the study of the characteristics of RESTful Web services and the definition of the credibility. We take a Web Services platform as an example; use the credibility behavior declaration to guide its credible verification.

Introduction

Web services are software organizations or applications published in the Web, can provide a variety of support to the user [1]. The traditional Web services are based on XML, SOAP and WSDL-UDDI technology, also known as the service based on the RPC model. Most of the traditional Web services use HTTP as a transmission protocol, in some extent misused the original intention of the HTTP protocol, and almost do not use any features of HTTP.

REST (Representational State Transfer) is a term proposed by Dr. Roy [2], it is a new Web architecture style based on the existing Web architecture specification with some new features added. It can reduce the complexity of Web application development, improve the system's flexibility. It is addressable, cacheable and connectivity, it is the summary of the most successful elements of web [3]. RESTful Web services take full advantage of the HTTP protocol, the operation of all resources is achieved through the HTTP protocol. In recent years, more and more attention to RESTful has been paid than traditional Web services, the global search trend of the two terms in Google Trend from 2004 to the present as shown in Figure 1.

![Figure 1. The global search trend of RESTful and Web services.](image)

At present, the relevant research about Web services, especially the RESTful Web services, is not very perfect. Compared with the traditional software testing, Web
service testing has many new features and faces complex problems, including the running environment sensitive, complex network environment and the diversity of remote call methods. In [4,5], they reviewed the requirements of the current Web services test, the problems and the current situation of the research, and classified the related research from their respective perspectives. In [6], they established a credible attribute model of the Web services: TIM-WS, described the relationship between the credible attribute and its measure factor, combined the self-learning of neural network with the global optimization of genetic algorithm, designed a credible Web services measurement model EPTMM and its basic algorithm ANNGA.

In this paper, according to the characteristics of the RESTful Web services, we design a behavior declaration which is different from the traditional one, put forward a credibility verification process model for the RESTful Web services based on the behavior declaration.

Credibility Verification Process Model for the RESTful Web Services Based on the Behavior Declaration

Credibility test for RESTful Web Services means mining the credibility test features of RESTful Web services based on the characteristics of RESTful Web Services, then test on these feature points to verify the credibility of the RESTful Web Services.

The credibility verification process model for RESTful Web Services based on the behavior declaration as shown in Figure 2. In this paper, the credibility test is based on the credibility behavior declaration, which runs through the whole credibility test process. We analyze the core features of RESTful Web services first, and obtain the credibility demand based on these features to generate the credibility behavior declaration. Then generate the test cases according to the credibility behavior declaration, do the test by these test cases. Finally, we will obtain the credibility level as test result which has been marked in the credibility behavior declaration and determine whether the RESTful Web services is credible. We will give the test results back to the users and the results will be used as the direction of the next operation.

Figure 2. The credibility test model of RESTful Web services based on trusted behavior declaration.

Credibility Demand Acquisition

The core features distinguish the REST architecture style from other architecture styles which based on the network is it emphasizes that there must be a unified interface between the components. The unified interface here refers to the standard action (GET, POST, PUT, HEAD, DELETE, etc.) provided by the HTTP protocol to CRUD operations to the resources. REST API is the interface which expose the system resource to the outside, it will publish the valuable information as the resource through the exposure URI. Every resource and every message will release an URI, that means each resource corresponds to a unique resource identifier.
These URI will expose some important information from our system, it is likely to have some influence on the credibility. In this paper, the credibility demand acquisition of the RESTful Web services needs to start from these exposed URI.

**Generating the Credibility Behavior Declaration of RESTful Web Services**

Ordinary credibility behavior declaration is divided on different software behavior, such as the behavior declaration of disk access and registered access, they need to verify different information.

The RESTful Web services access resources by using different HTTP actions and produce different request message. In this paper, the credibility behavior declaration will be classified according to different HTTP actions. The credibility behavior declaration must include two parts at least:

1) Operations of resources by different HTTP actions;
2) Sensitive information.

**Credibility Test**

In this phase, the behavior declaration is defined.

The test cases are generated according to the behavior declaration; the behavior declaration and the program are stored in the same directory. It will determine the credibility level to the request according to the behavior declaration when there is an external request system resource, then return the determine result to the users.

**The Credibility Behavior Declaration of RESTful Web Services**

The credibility behavior declaration of RESTful Web services contains two parts, and will use XML format.

**The Constraint of HTTP request**

The RESTful Web services access resources by using different HTTP actions and produce different request message. In this paper, the credibility behavior declaration will be classified according to different HTTP actions and generated in different formats. This behavior declaration should include follows at least:

1) HTTP request method type. the GET method contains `<RequestLine>` and `<Header>` at least, and the POST method should also include `<Content>`;
2) Security Level;
3) Constraint of parameter number: Depending on the request method type in the `<RequestLine>` or `<Content>`.

The main body format is shown as below:

```xml
<HttpRequestInfo>
  <RequestMethod>//GET or POST and other methods
    <RequestLine>
      <RequestLineTestItem1>...</RequestLineTestItem1>
    </RequestLine>
    <Header>
      <HeaderTestItem1>...</HeaderTestItem1>
      <HeaderTestItem2>...</HeaderTestItem2>
    </Header>
    <Content>
      <ContentTestItem1>...</ContentTestItem1>
      <ContentTestItem2>...</ContentTestItem2>
    </Content>
  </RequestMethod>
</HttpRequestInfo>
```
The Constraint of Sensitive Information

Sensitive information part constrains the sensitive resources address, sensitive statements, etc. according to the access. The main body format is shown as below:

```xml
<SensitiveInfo>
  <Path>
    <PathItem>…</PathItem>
    <Authority>…</Authority>
    <SecurityLevel>Safty/Dangerous/Suspicious</SecurityLevel>
  </Path>
  <Sentence>
    <SentenceItem>…</SentenceItem>
    <Authority>…</Authority>
    <SecurityLevel>Safty/Dangerous/Suspicious</SecurityLevel>
  </Sentence>
</SensitiveInfo>
```

Case Analysis of Credibility Test of Restful Web Services

In order to verify the validity and practicability of the above model, we choose a nursing Web Services platform which is put into use as a sample. This platform is a RESTful Web services platform, including the order information services, nurse information services and other related information services. This Web services platform provides all the services to the user (including consumers, nurses and the bank). Users apply the services from the platform through the mobile phone or PC, the services platform will feedback the results to the user after processing information.

Credibility Demand Acquisition

There are a lot of money trade in this system; Token verification method used to verify user identity; Mobile phone number, password and other information should be encrypted before transmission; Add agreed prefix and suffix after the encryption; Using JSON as data transmission format; The backstage management system and the interface are stored in the same server. Based on the above features, in addition to the credible verification of API request, the credible test to this RESTful Web services platform should include verification of Token, encrypted prefix and suffix, sensitive address, sensitive statements (SQL injection, etc.).

Define the credibility declaration

In this paper, we will introduce the credibility declaration by a GET request and the sensitive information section. The server address is represented by "XXX". The credibility declaration as shown in Fig. 4, 5:
Credibility test

Design the credibility test case for the RESTful Web services platform based on the credibility behavior declaration which has been declared. In this paper, PostMan is used as a tool to simulate some request actions, and obtain the results of the verification, the test cases and test results as shown in Tab. 1.

Figure 4. The credibility behavior declaration for the GET method.

```xml
<HttpRequestInfo>
  <GET>
    <RequestLine>
      <URL>http://xxx/GoldenNurse/rest/order/orderDetail?phone=phone*EncryptedPhone*pwd=EncryptedPwd*orderID=OrderId</URL>
      <Version>HTTP/1.1</Version>
      <ParameterNum>3</ParameterNum>
    </RequestLine>
    <Header>
      <Accept>application/json</Accept>
      <Connection>close</Connection>
    </Header>
    <SecurityLevel>Safy</SecurityLevel>
  </GET>
  <GET>
    <RequestLine>
      <URL>http://xxx/GoldenNurse/rest/order/orderDetail?phone=EncryptedPhone*pwd=EncryptedPwd*orderID=OrderId</URL>
      <Version>HTTP/1.1</Version>
      <ParameterNum>3</ParameterNum>
    </RequestLine>
    <Header>
      <Accept>text/javascript, */*</Accept>
      <Connection>keep-alive</Connection>
    </Header>
    <SecurityLevel>Suspicious</SecurityLevel>
  </GET>
</HttpRequestInfo>
```

Figure 5. The credibility behavior declaration for the sensitive information.

```xml
<SensitiveInfo>
  <Path>
    <PathItem>http://xxx/GoldenNurse/managementSystem/*</PathItem>
    <Admin>EncryptedAdminName=EncryptedAdminPwd</Admin>
    <SecurityLevel>Safy</SecurityLevel>
  </Path>
  <Path>
    <PathItem>http://xxx/GoldenNurse/managementSystem/*</PathItem>
    <Admin></Admin>
    <SecurityLevel>Dangerous</SecurityLevel>
  </Path>
  <Sentence>
    <SentenceItem>password='1' or '1'='1'</SentenceItem>
    <SecurityLevel>Dangerous</SecurityLevel>
  </Sentence>
</SensitiveInfo>
```
Table 1. Test cases and test results.

<table>
<thead>
<tr>
<th>num</th>
<th>method</th>
<th>request parameters</th>
<th>result</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>GET</td>
<td><a href="http://xxx/GoldenNurse/orderDetail?phone=phoneaf987w3q45hsdg9end&amp;Pwd=pwd4jh5df9g8345k8g7end&amp;orderId=159390">http://xxx/GoldenNurse/orderDetail?phone=phoneaf987w3q45hsdg9end&amp;Pwd=pwd4jh5df9g8345k8g7end&amp;orderId=159390</a></td>
<td>Safety</td>
</tr>
<tr>
<td>2</td>
<td>GET</td>
<td><a href="http://xxx/GoldenNurse/rest/orderDetail?phone=af987w3q45hsdg9&amp;Pwd=4jh5df9g8345k8g7&amp;orderId=159390">http://xxx/GoldenNurse/rest/orderDetail?phone=af987w3q45hsdg9&amp;Pwd=4jh5df9g8345k8g7&amp;orderId=159390</a></td>
<td>Suspicious</td>
</tr>
<tr>
<td>3</td>
<td>POST</td>
<td><a href="http://xxx/GoldenNurse/rest/order/newOrder">http://xxx/GoldenNurse/rest/order/newOrder</a></td>
<td>Safety</td>
</tr>
<tr>
<td></td>
<td></td>
<td>phone=phonesdtfg8345jfg9843j87346jht8345jgtend&amp;Pwd=pwd984jg84wkhdk5end&amp;personId=pId8r90o3efjvbb78g9end&amp;title=&quot;WhoCanHelpMe&quot;&amp;locationId=348392&amp;cost=200.00&amp;hospitalId=4929084&amp;departmentId=10005&amp;orderDescription=&quot;IWantToSeeADoctor&quot;</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Header:sdttf8345jfg9843j87346jht8345jgt.984jg84wkhdk5u9ek54ny7tsp2ngiui</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>GET</td>
<td><a href="http://xxx/GoldenNurse/rest/order/orderDetail?phone=phoneaf987w3q45hsdg9874jg891kgj4k513end&amp;Pwd='1'or'1'='1'&amp;orderId=159390">http://xxx/GoldenNurse/rest/order/orderDetail?phone=phoneaf987w3q45hsdg9874jg891kgj4k513end&amp;Pwd='1'or'1'='1'&amp;orderId=159390</a></td>
<td>Dangerous</td>
</tr>
</tbody>
</table>

Conclusion

In the period of rapid development of network science and technology, Web Services plays a more and more important role in our life. Credible demand for Web services is also increasing. So, it is an important work to verify the credibility of the Web Services, especial the RESTful Web Services.

In this paper, we, beginning with the characteristics of RESTful Web services and the definition of the credibility, define the behavior declaration for the RESTful Web services. Taking an on-line APP as an example, using the credibility behavior declaration to guide its credibility verification.

The next step of the research work should include: Carry out a more extensive trusted need to the Web services, not limited to the HTTP actions; Automated generation of credibility test cases, expand the test case library and more efficient test.

References


