

Federal Institute of science and Technology
Angamaly
Mookkannoor

Worst-Input Mutation Approach to Web Services Vulnerability Testing Based on SOAP Messages

Reg No: **82904**
Guide : **Simi Stephen**

Bimal Varghese
bimalvv2005@gmail.com

March 16, 2015



Introduction

SOA

Web Service

Web Service Testing

Related Works

Automated Robustness Testing

Perturbation Based Testing

Message Exchange by SOAP Bundling Framework

Using Data Perturbation

Adaptive Random Testing

XML Perturbation

Combinatorial Mutation

API based security solutions

Taxonomy of Web Attacks

Base Paper

Worst-Input Mutation Approach

Proposed Methods



SOA

- ▶ An architectural style that aims to achieve loose coupling among interacting software agents.
- ▶ Service Provider & Service Consumer are implemented via software agents
- ▶ **Service:** A unit of work done by a service provider to achieve some end result for a service consumer.
 - ▶ A Service can be accessed without the knowledge of underlying implementation



Web Service

- ▶ Popular way of implementing a SOA.
- ▶ Way of Integrating web based applications using standards such as XML, SOAP, WSDL & UDDI
 - ▶ **XML** for Tagging the Data.
 - ▶ **SOAP** for Transferring the Data.
 - ▶ **WSDL** for Describing available Service.
 - ▶ **UDDI** for Listing what services are available.



To ensure quality and reliability of Web Service, proper testing must be conducted

Difficulties

- ▶ Difference in developing application environment.
 - ▶ Unable to test web service unless it is deployed
- ▶ Lack of User Interface forcing tester to go for automatic testing methods.
- ▶ Large number of concurrent user access enforcing performance and scalability testing.
- ▶ Involvement of different users like Service provider, Publisher and Users, all need to be involved at different stages of testing.

Related Works

[1] Automated Robustness Testing of Web Service

Evan Martin, Suranjana Basu, Tao Xie



Evan Martin et al in the paper **Automated Robustness Testing of Web Service** present a framework for automatically generating and executing web service request.

Method

Consist of 3 steps

1. Code Generator

1.1 Generate necessary code to implement a service consumer

2. Test Generation

2.1 Generated test class is supplied to a test generation tool such as JCrasher inorder to generate JUnit test.

3. Test Execution

3.1 Invoke test case and call web service.
Collect response from web service.



Advantages

- ▶ Easy framework for automatically invoking web service given a service provider's WSDL
- ▶ Leverage existing automated unit test generation tools to generate unit test cases.
- ▶ No knowledge of underlying service implementation is required.

Disadvantages

- ▶ Generalized black box testing method.
- ▶ Cannot categorize generated errors.
- ▶ Cannot identify errors within data
Eg: Age=-10

[2] Exploring Perturbation Based Testing for Web Service

Lourival F de Almeida and Silvia R Vergilio



An extended approach based on XML message perturbation has been proposed by **Lourival F de Almeida and Silvia R Vergilio** in their paper **Exploring Perturbation Based Testing for Web Service**.

- ▶ Utilized SOAP Perturbation operators and a Web service Testing tool (**SMAT-WS**)

SOAP Perturbation Operator

SOAP perturbation primitive operators are

1. *Null* (n)
2. *Incomplete* (n)
3. *Inversion* (n)
4. *ValueInversion* (n)
5. *Mod_Len* (n)
6. *Space* (n)



Advantages

- ▶ Consider SOAP message perturbation for Web service Testing.
- ▶ Consider various data perturbation operators for testing
- ▶ Created a Testing tool (SMAT-WS) for testing Web Services

Disadvantages

- ▶ Designed mutation operators is not sufficient for comprehensive testing.
- ▶ Issues related to amount of test cases generated by the operators is not considered.

[3] Efficient Web Services Message Exchange by SOAP Bundling Framework

Toshiro Takase, Keishi Tajima



- ▶ A SOAP message bundling framework is Proposed.
- ▶ Framework enables bundling of multiple messages into one message.
- ▶ Application developers do not have to consider the service granularity for performance reasons.



Advantages

- ▶ Existing service providers do not have to re-implement their service application.
- ▶ Bundling framework generates new operations for all combinations of the original operations in the WSDL
 - ▶ If original WSDL has N operations, 2^{N-1} operations are generated.

Disadvantages

- ▶ Existing service requesters have to change their application a little to take advantage of the bundled operations.
- ▶ Multiple Interdependent functions are not considered.

[4] Generating Test Cases for Web Services Using Data Perturbation

Jeff Offutt & Wuzhi Xu



- ▶ Existing XML messages are modified based on rules defined on the message grammars, and then used as tests.

- ▶ Data perturbation uses 2 methods to test Web services:

Data value perturbation:

modifies values according to the data type.

Interaction perturbation:

classifies the communication messages into two categories:

RPC communication and data communication



Advantages

- ▶ Both RPC and Data communication are tested.
- ▶ Request messages were modified by mutation operations.

Disadvantages

- ▶ A few special values were considered in the mutation process.

[5] Adaptive Random Testing: the ART of Test Case Diversity

Tsong Yueh Chen , Fei-Ching Kuo, Robert G. Merkel, T.H. Tse



13

- ▶ Many program faults result in failures at contiguous areas of the input domain, known as failure patterns.
- ▶ For detecting such patterns, ART systematically filters randomly generated candidates.



Adaptive Random Testing

Principle

- ▶ Given a set of previously executed test cases that have not revealed any failures, new test cases located away from these old ones are more likely to reveal failures.

Types of ART methods

- ▶ Fixed Size Candidate Set ART (FSCS-ART):
Candidate with largest distance from current Test case is considered next.
- ▶ Restricted Random Testing (RRT):
Create Exclusion zone for current test case.
Take random selection if it lie outside the zone.



Identifying Failure Pattern using ART

1. Take samples from the set of all possible inputs to the software under test.
2. Execute samples one by one, and determine whether the outputs from each sample match the software specification
3. If not, a software failure is revealed and existence of fault is detected.
4. Select test data so as to maximize the number of distinct faults detected.

[6] Testing Web Services by XML Perturbation

Wuzhi Xu, Jeff Offutt and Juan Luo



- ▶ Web services uses XML to describe and transmit data.
- ▶ XML schema is utilized to generate data formats and test cases.
- ▶ Some applications and web services do not validate XML messages against an XML schema, and sometimes no schema exists.



XML Data Model

- ▶ An XML schema can be modeled as a tree.
XML tree $T = (N, D, X, E, n_r)$, where:
 - ▶ N is a finite set of elements and attribute nodes.
 - ▶ D is a finite set of built-in and derived data types.
 - ▶ X is a finite set of constraints (integrity and representation).
 - ▶ E is a finite set of edges.
 - ▶ n_r is the root node.

The formal model for XML schema's defines three elements in the tree:

- ▶ Nodes
- ▶ Datatypes
- ▶ Edges

Schema perturbation operators systematically modify these three elements.

Schema Perturbation Operators

Schema perturbation Operators are

- ▶ $\text{insertN} (e, e'_p, e'_c, n')$
- ▶ $\text{deleteN} (n)$
- ▶ $\text{insertN D} (n_p, e'_p, n', e'_c, d')$
- ▶ $\text{deleteN D} (n)$

[7] Combinatorial Mutation Approach to Web Service Vulnerability Testing

Qing Li , Jinfu Chen , Yongzhao Zhan, Chengying Mao, Huanhuan Wang



Combinatorial mutation testing focuses on using combinations of at least two faulty input data parameter to find faults within the software

- ▶ A set of operators that can be combined are presented
- ▶ SOAP message is obtained by parsing the WSDL file, and data perturbation techniques are adopted to generate simple initial test data.
- ▶ a combinatorial testing algorithm is developed.



Mutation Operator Design

Two perturbation policies which directly act on the SOAP message are used

- ▶ Data Value perturbation :
modifies values in SOAP messages according to their data types
- ▶ Interaction perturbation :
consider the data values and data relationships



Combinatorial Testing Strategy

1. Analyze the Web service methods, and identify the associated methods as directly associated and indirectly associated methods.
2. For associated Web service methods, invoke different sets of mutation operators according to the type of parameters. Then call the appropriate combinatorial testing approach to generate combinatorial test cases.
3. Based on the combinatorial mutation testing strategy , combinatorial mutations CTCG algorithm to Web service vulnerability testing based on SOAP message mutations is proposed

[8] API based Security solutions for Communication among Web Services

A. Kanchana Rajaram, B. Chitra Babu, and C. Kishore Kumar R



2 existing web service attacks are considered.

1. Message Alteration Attack (MAA)
2. XML Injection Attack (XIA)

Proposed solution consists of

- ▶ **Middleware services:**
containing set of security service
- ▶ **Domain web service:**
set of pluggable API's



Advantages

- ▶ Encrypts all the outbound messages
- ▶ Installable Plug-ins as API

Disadvantages

- ▶ High overhead of encryption and decryption
- ▶ Attacks like Reply of Message Attack and Denial of service attack is not considered.

[9] A New Taxonomy of Web attacks suitable for efficient encoding

Gonzalo Alvarez, Slobodan Petrovic



24

- ▶ A taxonomy of web attacks taking into account some important features of each attack category.
- ▶ A model of Web attacks based on the concept attack life cycle is created.

Every stage of the attack life cycle defines

1. Entry Point
2. Vulnerability
3. Service
4. Action
5. Length
6. HTTP element
7. Target
8. Scope
9. Privileges



Vulnerability

Code Injection

1. Script Injection
2. SQL Injection
3. Xpath Injection

Base Paper

Worst-Input Mutation Approach to Web Services Vulnerability Testing Based on SOAP Message

Jinfu Chen, Huanhuan Wang, Dave Towey, Chengying Mao, Rubing Huang,
Yongzhao Zhan



Proposed an approach based on SOAP message mutation and the worst-input technique.

Methods Discussed

- ▶ Worst Input Mutation:
Utilizing characteristics of SOAP message.
- ▶ Automatic Test Case Generation:
Test Case Generation based on Farthest Neighbor (TCFN) algorithm
- ▶ A prototype Web Service Vulnerability Testing Tool is implemented



Basis of mutation object is SOAP, which is a message protocol based on an XML document.

eRTG

a Regular Tree Grammar with 6 tuples $\langle E, N, DT, P, A, n_s \rangle$

- ▶ E finite set of elements.
- ▶ N finite set of non-terminals.
- ▶ DT finite set of data types defined as {int, string, bool, numerical, char, object}
- ▶ P finite set of production rules.
- ▶ A a 2-tuple $\langle n, \text{type} \rangle$
 - ▶ **n** : number of parameters.
 - ▶ **type** : parameter type.
- ▶ n_s is the starting non-terminal



Mutation Operator

Given a set of all element instances N , a mutation operator is $r=f(n_1, n_2 \dots n_i)$, where f is a function, $i \geq 1$, each $n_1, n_2 \dots n_i \in N$, and has an arbitrary data type, and r outputs the mutated $n_1 \dots n_i$ with the same data type as the input $n_1 \dots n_i$.

Security Rule

Vulnerability of Web services is $VWS=G(r)$, where $r=f(n_1, n_2 \dots n_i)$ is the mutation operator for the tested Web service.

$G(r)$ represents the vulnerability that is triggered by r , and $n_i \in N$ are the Web service input parameters.



Farthest Neighbour Approach

Similar to the Concept of Adaptive Random Testing (ART):

- ▶ Many program faults result in failure manifesting in contiguous area of the input domain.
- ▶ If previous test case not reveal a failure, new test cases should be as far from the already executed non-failure test cases as possible.

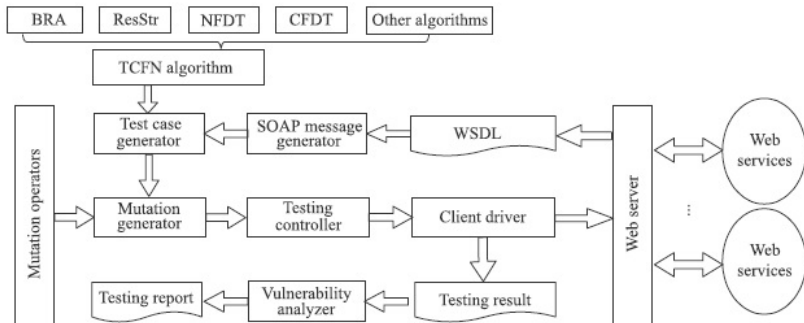
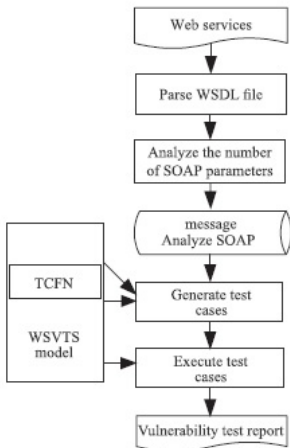


Fig. 2 The WSVTS framework.

Flow Chart



Proposed Methods



Propoesed Modification

- ▶ Based on the [9], XPath Injection is an important vulnerability among web service.
- ▶ The base paper works on data part of web service and is not considering XPath Injection attacks.
- ▶ The base paper is modified so as to identify Xpath Injection Attacks.
- ▶ XML structure of the SOAP message is mutated so as to identify the Xpath Injection Attacks.



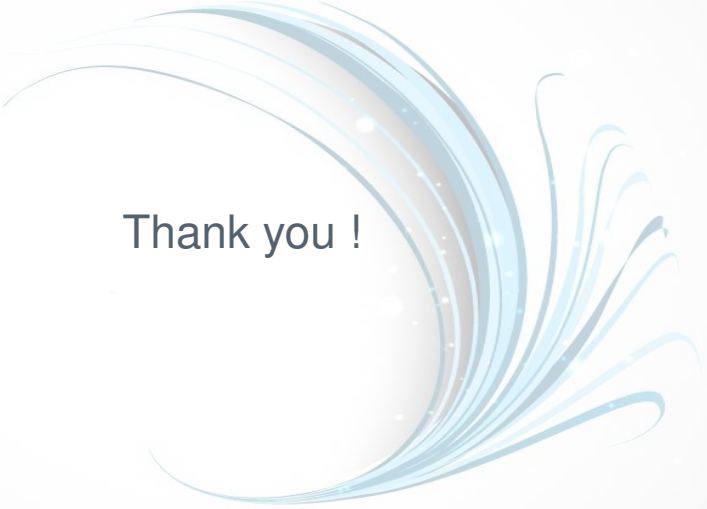
- ▶ Web service Testing is conducted by considering mutation approach.
- ▶ Xpath Injection attack of web service is tested by considering SOAP message mutation approach.



- 1 Automated Robustness Testing of Web Service.
Evan Martin, Suranjana Basu, Tao Xie
- 2 Exploring Perturbation Based Testing for Web Service
Lourival F de Alemeida and Silvia R Vergilio
- 3 Efficient Web Services Message Exchange by SOAP Bundling Framework
Toshiro Takase, Keishi Tajima
- 4 Generating Test Cases for Web Services Using Data Perturbation
Jeff Offutt & Wuzhi Xu
- 5 Adaptive Random Testing: the ART of Test Case Diversity
Tsong Yueh Chen , Fei-Ching Kuo, Robert G. Merkel, T.H. Tse
- 6 Testing Web Services by XML Perturbation
Wuzhi Xu, Jeff Offutt and Juan Luo



- 7 Combinatorial Mutation Approach to Web Service Vulnerability Testing
Qing Li , Jinfu Chen , Yongzhao Zhan, Chengying Mao, Huanhuan Wang
- 8 API based Security solutions for Communication among Web Services
A. Kanchana Rajaram, B. Chitra Babu, and C. Kishore Kumar R
- 9 A New Taxonomy of Web attacks suitable for efficient encoding
Gonzalo Alvarez, Slobodan Petrovic



Thank you !