SOLUTIONS FOR VARIOUS SECURITY ISSUES AND ATTACKS FACED BY SEMANTIC WEB TECHNOLOGIES: A REVIEW

[1]Neera Chaudhary, [2]Suresh Kumar
[1]Master Scholar, [2]Associate Professor
[1,2]Department of CSE
[1,2]Ambedkar Institute of Advanced Communication Technologies & Research, Govt. of NCT of Delhi, India

Abstract: Semantic Web (SW) is a meaningful web that is in general extended version of the traditional Web. It provides some common infrastructure to both companies and developers. Its services and technologies are being used by large number of companies. Commonly security flaws/attacks faced by SW are untrusted communication network, problem of access control, Network packet sniffing, XPATH injection attack and Denial of service attack etc. So, there is a main requirement to secure and preserve the services of internet providers. It requires to be protected against all sorts of security flaws. In this research article, we have presented all possible attacks on each layer of SW and their solution in detail.

Index Terms **- Semantic Web, Security issues, Security policies, Semantic Web technologies, Attacks.**

I. INTRODUCTION

The explosive growth of the Internet has made huge amounts of information available to decision makers. The information is increasing in the form of four major V's- Volume, velocity, variety and veracity of Big Data. Semantic Web (SW) is a new kind of web where information is clearly understandable with the well-defined semantics [2]. Semantic refers to the meaning of data on the web so that machine could be able to take decision and increase involvement of machine over the web as human. It offers a distributed environment in which far away entities are connected and can interact with each other even if they have no previous interaction ever in past [2]. This is only possible by the valuable information available on the Web. Thus, information plays an important role for connecting many entities in Semantic Web and it must be secure. SW threats are something that lead to a potential serious damage or harm to SW. There are various security flaws and challenges in path of SW security. These flaws and attacks may help intruders to perform vulnerable attacks like Denial of Service Attack, network sniffing, SPAQL injection attack. Various security policies are also being developed for the security purpose in Semantic Web. The policy helps in secure interaction and communication. Policy based interaction on involver, many strategies like one-step policy evaluation, policy driven negotiation and so on may be used [2]. Entities on Semantic Web exchange their security and policies are described using language between entities [2].

As the demand of web is increasing and people are becoming more familiar with Semantic Web technologies. Moreover, it is becoming a reality in real life. It provides flexible and meaning based searching power that can be used by authorized users as well as malicious users. Malicious users use Semantic Web services and technologies for their own benefit and to exploit vulnerabilities in applications [3].

Semantic Web offers the advanced features of World Wide Web. Its semantic power and semantic technologies are being used in all aspect of life [4]. Safety of communicating parties and their reliability and safe reasoning needs to be guaranteed by a trusted third party [4]. In this connection, this paper deals with various security issues and attacks on all layers of Semantic Web and suggests solutions for Semantic Web technologies.

II. SECURITY ISSUES IN SEMANTIC WEB TECHNOLOGIES

Tim Berners Lee and W3C have vision for the new generation of web. Web of linked data is the W3C vision known as Semantic Web. The concept of Linked data of Semantic Web is empowered by various technologies such as RDF, SPARQL, OWL and SKOS. In this section, the security issues on each layer of semantic web are discussed step by step. The current Semantic Web technology contains many layers where each layer involves different kinds of components.

The first layer is URI and Unicode. It is a standard and international collection of unique character sets which is generally used to support multiple languages on web. Thus, it is needed to secure TCP/IP, secure sockets and secure HTTP [5]. At this layer, the main issue for the security of Semantic Web is TCP/IP built on untrusted communication layers.

The second layer is XML layer. It is a scripting language used to create user defined tags. This layer also contains XML namespace and schema definition supports the common syntax on the web which are the important part of this layer. Thus this layer is also important and need to control by unauthorized access. In this layer, the main issue is the access and privilege of XML document for users. That means how much (entire XML documents or parts of documents [5]) access and privilege should be given to users.

The third layer is RDF data interchange layer. RDF data deals with to make sentence in triple format consisting of subject, predicate and object about resource. The main security issues in this layer are RDF and RDF schema and are needed to secure interpretation and semantics [5].

The forth layer of Semantic Web consist of query processing. SPARQL query is a data base query language for SW. It is a semantic query language also known as RDF query language. It needs to be protected for information security access control. Information security access control is the mechanism to deny unauthorized user to access information illegally.

Next layer that resides after query processing is OWL [6]. Ontologies contain descriptive information so they also need to be secured.

Top most layer of Semantic Web is trust and proof. Trust is closely related to security. Trust needs to be secured as it is directly related to the image of an organization, resources and human beings presented in Semantic Web [7].

III. ATTACKS ON SEMANTIC WEB TECHNOLOGIES

Based on the literature surveyed by us, we have found various issues in the Semantic Web. In this section, we are describing some possible attacks on all layer of Semantic Web Technologies (SBT). These attacks are classified as TCP/IP attacks, HTTP attacks, XML attacks, SPARQL injection attacks, RDF attacks, TRUST attacks based on semantic web technologies. It is needed to ensure that security is maintained across all the layers of semantic web stack [7].

1. TCP/IP Attacks

There are mainly three attacks that are being performed by intruders on TCP/IP layer such as Denial of Service attack (DoS), Network packet sniffing, Distributed Denial of Service attack(DDoS). In DoS attacks, multiple requests are being sent to the server by the attackers using fake IP address. In response of requests server reply on those addresses and wait for attacker response as the requesting address is fake and as server is busy in responding. It keeps authorized persons away from accessing server [7]. In packet sniffing / network sniffing invader interrupts and analysis the network traffic being transmitted over the network [7]. In DDoS attack request from multiple system are being sent to the target server or a single system.

2. HTTP Attacks

In Semantic Web, HTTP attacks are of two types: HTTP-GET flood attack and Man - in - the -Middle attack. In HTTP-GET flood attack attackers target the web server by sending various bogus HTTP-GET requests [7]. Man - in - the - Middle attack can be performed in two ways one by session hijacking attack and second by IP spoofing. Here, sniffers are used by the attackers to monitor the communication between the devices. It also collects the data that is transmitted.

3. XML Attacks

There are four types of an XML attack including an XML injection attack, an XPATH injection attack, an XML denial of service attack and an XML parsing attack. In XML injection attack attackers manipulate or compromise the logic of an XML application or service [7]. XPATH refers to the syntax of a XML document that defines various parts of XML document. So, in XPATH injection attack user supplied information is used by the website to construct a XPATH query to access XML data. In XML Dos attack an XML document is being transmitted ture and use all CPU cycles. XML parsers are programs used to read and use XML. XML parsing attack can be performed in two ways: SAX (Simple API for XML) parsing attack and DOM (Document Object Model) parsing attack with multiple digital signatures. It consumes all the resources as the parser will check each signal.

4. RDF Attacks

This attack contains various command injection attacks which may be possible on RDF layer. Command injection attacks are the attacks performed by using SPARQL commands.

5. SPARQL Injection Attacks

Query languages are unsecured and are vulnerable to attacks. The vulnerability appears when users directly input the query series permitting attackers to easily gain control over the executed query. In SPARQL injection attack malicious code are injected in the form of query.

6. OWL Attacks

An attacker can create an ontology that can crash an OWL Parser. So many new types of attacks are possible such as SOAP and XML attacks.

7. TRUST Attacks

They are the attacks that affect the image of the agents presented in Semantic Web. They are of three types as unfair rating, malicious consortium attack and on - off attack [7].

IV. SOLUTION TO VARIOUS SECURITY ISSUES AND ATTACKS

The security at layered architecture of Semantic Web cannot be considered in isolation because an architecture refers to the internal structure of a system but in a certain context that have an important and useful part of the real world representation. Sir Tim-Berner Lee proposed a layered architecture for Semantic Web which is comprehensive, functional, layered (CFL) architecture where there is a layered structure of each system components and each layer represents a group of elements that provides related services. Thus, a single layer cannot focus as a whole security.

As user's data is so important and privacy of user's data must be maintained from unauthorized access, security is required and should be maintained among and across all layers of Semantic Web stack. Since, security is a very challenging and a complex task but it must not be ignored. Thus, it must be required from the beginning level of Semantic Web stacks.

In this section, we have presented the solution for attacks which arises at each layer of SW architecture. The solution for different attacks as under:

A. Solution for TCP/IP security issues is to build a TCP/IP on a trusted communication layer. To avoid TCP/IP attacks flitters or sniffers can be used to filter the network traffic and monitor the traffic against intruders [7].

B. Solution for HTTP attack is to make use of Secure Socket Layer (SSL). To prevent session hijacking and provide security goals like availability of data, integrity, authenticity it is needed to encrypt the communication channel. HTTP's is the extension of HTTP which provides secure channel for information [7].

C. XML layer security issues can be resolved by digital signature and encryption. XML injection can be prevented by properly monitoring and managing any user input before it reaches the main program code.

D. RDF layer can be secured by securing data interpretation and it can be achieved by using abstract interpretation approach for security [10].

E. Query languages can be secured in semantic web using various attack prevention strategies. SPARQL injection attack can be mitigated using parameterized string. It is similar like preventing SQL injection attack [7].

V. CONCLUSION AND FUTURE SCOPE

Security of user's information is an important factor of user's daily life. The information as a communicating message makes strong connection and social network among communicating parties. Semantic Web provides a reliable connection and safe reasoning capability among communicating parties and trusted third party. In this paper, we have discussed various issues and attacks at each layer of Semantic Web and discussed possible solutions for all. This research paper will help to move on further research direction and make a scope of research at specific level of security at each layer on Semantic Web layered architecture. We are developing an infrastructure and techniques to resolve all the attacks faced by SW. Our work is in progress and in near future, we will publish all work for security issues with results.

REFERENCES

[1] Suresh Kumar, Rakesh Kumar Prajapati, Manjeet Singh, Asok De, Realization of Threats and countermeasure in Semantic Web Services, International Journal of Computer Theory and Engineering, Vol.2, No.6, December, 2010.

[2] N K PRASANNA ANJANEYULY ANNA, SHAIK NAZEER, SEMANTIC WEB SECURITY AND PRIVACY, Journal of Theoretical and Applied Information Technology.

[3] Pablo Orduna, Aitor Almeida, Unai Aguilera Xabier Laiseca, Diego Lopez-de-Ipina, Aitor Gomez Goiri, Identifying Security Issues in the Semantic Web: Injection attacks in the Semantic Query languages, https://www.researchgate.net/publication/244994827.

[4] Suresh Kumar, Rakesh Kr. Prajapati, Manjeet Singh, Asok De, Security Enforcement using PKI in Semantic Web, 978-1-4244-7818-7/10/$26.00©2010 IEEE.

[5] Dr. Bhavani Thuraisingham, Security Issues for the Semantic Web, 0730-3157/03 $ 17.00 © 2003 IEEE.

[6] Blake Middleton, James Halbert, and Frank P. Coyle, Security Impacts on Semantic Technologies in the Coming Decade.

[7] Sumit Kumar, Suresh Kumar, Semantic web attacks and countermeasures IEEE International Conference on Advances in Engineering & Technology Research (ICAETR – 2014), August 01-02,2014, Dr. Virendra Swarup Group of Institutions, Unnao, India.

[8] Sabrina Kirrane, Serena Villata and Mathieu d' Aquin, Privacy, Security and Policies: A review of Problems and Solutions with Semantic Web Technologies, 1570-0844/18/$35.00 © 2018 – IOS Press and the authors.

[9] Akliesh Dwivedi, Abhishek Dwivedi, Suresh Kumar, Satish Kumar Pandey, and Priyanka Dabra, A Cryptography Algorithm Analysis for Security Threats of Semantic E-Commerce Web (SECW) for Electronic Payment Transaction System, N. Meghanathan et al.(Eds.): Advances in Computing & Inf. Technology, AISC 178.pp. 367-379©springer-Verlag Berlin Heidelberg 2013.

[10] Isabella Mastroeni, Abstract interpretation-based approaches to Security, EPTCS 129, 2013, pp. 41-65, doi:10.4204/EPTCS.129.4.