© 2018 IJSRSET | Volume 4 | Issue 8 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
Themed Section : Engineering and Technology

Technique for Detecting Zero Day Attack by using Signature based and Knowledge Based Method

Gajanan P Bherde[1], Dr. M. A. Pund[2]

[1]Department of Computer Engineering, K. J. Somaiya College of Engineering, Mumbai, Maharashtra, India

[2]Department of Computer Science & Engineering, PRMIT&R, Badnera, Amravati, Maharashtra, India

ABSTRACT

Now a days web services have been increasingly adopted which has been targeted by the attackers. The underlying technologies used by them bring known vulnerabilities to this new environment. The classical approach for attack detection either produce high false positive detection rates or cannot detect attack variations leading to zero-day attacks.In this paper we are working on the zero day attacks detection techniques, 'zero day attack' refers to the hole in software i.e the unknown vendor in the software. This security hole is exploited by the hackers before vendor becomes aware of any attack. In recent system, researchers fail to fix the zero day attacks in the system. In this paper system used two methods to detect the zero day attacks. The methods are signature based and knowledge based detection method. For building the knowledge based strategy system can use the ontology technique. Ontologies can help build a strategy-based knowledge attack database. A novel hybrid attack detection engine brings together the main advantages of knowledge- and signature-based classical approaches.

Keywords : Zero Day Attack, Xml, Hackers, Signature Based Technique

I. INTRODUCTION

Now a days, web services have been widely used as a distributed system on the internet, as they offer a standard means of interoperation among distinct software applications running on a variety of platforms and frameworks.There are number of technologies used for web services which are SOAP, HTTP and XML which favored the deployment of well-known weaknesses in this new environment.

In this paper basically we discussed about the XML injection attacks, these are the types of attacks in which some change in the XML internal components aiming to compromise the web service application. These attack can be prevent by using the signature based detection system. Signature is a payload that identifies an attack through a specific malicious context. Signature-based detection systems usually lead to a low software-detection mistake rate, namely false positive rate [3]. However, one important limitation of signature-based attack detection is that it does not detect new (unknown) attacks, even if small variations of a known payload.

Another way to protect web services from injection attacks is through knowledge-based detection systems [4], which apply a technique usually based in some kind of behavior. For instance, two distinct classes are modeled, one for normal behavior containing all expected actions that define such profile and another class for attacks, which involve actions that are not considered normal. Knowledge-based detection techniques can detect new attacks, but they mostly produce a high false positive rate in their detection.

Classical Approaches for Detection Systems

- Signature based detection:

Classical System uses Signature based detection technique. A signature is a payload that identifies an attack through some specific malicious context. Signature based detection systems usually lead to low software detection mistake rates namely, false-positive rates.

- Knowledge-based detection systems:

Another way to protect Web services from injection attacks is through knowledge-based detection systems,
which apply protection based on some kind of previously known and cataloged behavior. Usually, two distinct classes are modeled: one for normal behavior, containing
all expected actions that define such a profile and another for attacks containing actions that aren't considered normal.

In this paper we implemented the two system for detecting the attack the technique implement are: signature based and knowledge based detection system. The implementation flow of the proposed system is as follows:

1. Read the dataset of the client side.
2. Send data to the server for attack detection.
3. At server side it receive data, by using JPCAP it separate out the IP and TCP packets
4. Apply XML data files to ontology(For generating ontology protage 5.0 tool is used).
5. For attack detection two different methods are used: signature based and knowledge based.
6. Signature Based : Detection is depend upon
   i. Depend on previous store attacks in ontology database.
   ii. It compare the i/p file with all attacks store in the database.
7. Knowledge Based: Signature based method fails to detect the new attacks. Knowledge based detection system detect the new attacks and stored in the database by using SPARQL.

II. LITERATURE REVIEW

In this section discussed the survey done on attack detection techniques, ontology techniques.

This paper [1] applies ontology to build a strategy-based knowledge attack database. It is a novel hybrid attack detection engine, bringing together the main advantages of signature and knowledge-based classical approaches. Moreover, it is capable of mitigating
zero-day attacks for XML injection, with no false positive detection rate.

The Major Task of an IT professional is to integrate diverse application. The problem with DCOM, CORBA or APIs type of integration is that, it is rigid and breaks up with application up gradation and thus needs refractory. The enhanced connectivity and flexibility attributed to Web Services comes at the cost of increased security risks, since XML is essentially text. Research data shows that 70% of attack paths that has been closed by fire walls over the past decade will again be reopened by the XML web services[2].

The advance in Web technology has lead to more and more applications being deployed over the Web service (WS) platform. However, the inherent security weaknesses of the WS platform have lead to these WS-based applications being vulnerable and targets for attacks. This paper identifies and describes the various vulnerabilities and security threats pertaining to WS. After examining the various existing defending mechanisms for WS, it is found that they are not adaptive and adequate in counter-measuring the WS attacks. An adaptive intrusion detection and prevention (ID/IP) framework to protect the WS against attacks related to SOAP/XML/SQL is thus introduced. Through illustration by examples, the framework demonstrated that by making use of agents that act as sensors, data mining techniques such as clustering, association and sequential rule coupled with fuzzy logic to further analyze and identify anomalies, is able to exhibit the adaptive nature of capturing anomalies and avoiding false alarms [3].

In this paper we discuss the problem of mapping relational database contents and ontologies[4]. The motivation lies in the fact that during the latest years, the evolution in Web Technologies rendered the addition of intelligence to the information residing on the Web a necessity. We argue that the addition of formal semantics to the databases that store the majority of information found in the Web is important, in order to make this information searchable, accessible and retrievable. The key technologies towards this direction are the Semantic Web and the ontologies. We analyze in this paper the approaches that have so far been presented in order to exploit the prospects that such collaboration promises. We set the theoretical and practical boundaries of the mapping problem, we delve into the tools that altogether comprise today’s state of the art, and we provide a discussion about the benefits and the drawbacks of the existing approaches. We discuss the feasibility and viability of applying the mappings in real world applications as well as the directions that the evolution of current implementations should follow. We conclude by presenting the requirements that should be met in order to provide a more powerful next generation of mapping frameworks.

In paper [5] present our model as a target-centric ontology that is to be refined and expanded over time. We state the benefits for going dependence upon taxonomies, in favor of ontologies, for the classification of computer attacks and intrusions. We have Specified our ontology using the DARPA Agent Markup Language and have prototyped it using DAML Jess KB. We present our model as a target-centric ontology and illustrate the benefits of utilizing an ontology lieu of a taxonomy, by presenting a use case scenario of a distributed intrusion detection system.

In this paper, we describe WS security threats and state that they have to be analysed and classified systematically in order to allow the development of better distributed defensive mechanisms for WS using F/IDS. We choose ontologies and OWL/OWL-S over taxonomies because ontologies allow different parties to evolve and share a common understanding of information which can be reasoned and analysed automatically. We develop the security attack ontology for WS and illustrate the benefits of using it with an example[6].

In this paper we propose using syntax embedding to prevent injection vulnerabilities in a language-independent way. Injections form a very common class of security vulnerabilities. Software written in one language often needs to construct sentences in another language, such as SQL, XQuery, or XPath queries, XML output, or shell command invocations. This is almost always done using unhygienic string manipulation, whereby constant and client-supplied strings are concatenated to form the sentence[7].

Security is the main concern and a challenging problem of Web services. In the recent years, XML-sensitive security appliances, such as XML firewalls or

Web service firewalls, have been introduced to protect services. However, attackers can still compromise web services and do their malicious actions. Intrusion detection systems (IDS) are appropriate for defence in depth; and sit behind of firewalls in the security structure of an enterprise. However, network IDSs fail to detect attacks in Web service layer. In this paper, we propose an intrusion detection system for web services (WS-IDS), to detect malicious behaviors of the requesters of a typical web service. This idea is motivated by considering the inability of the existing IDSs to detect the attacks in web service layer. WS-IDS can be used in addition to other security appliances for web services, such as web service/XML firewalls[8].

III. PROPOSED SYSTEM

Proposed System Overview

System for XML injection attacks detection is designed here. In this kind of attack produce some change in the XML's internal components that aims to compromise the Web service application. This can be achieved by, for instance, injecting malicious content into an XML message, such as invalid XML characters.

Figure 1 shows the architectural view of system. This system is implemented as client server application with Socket Programming.

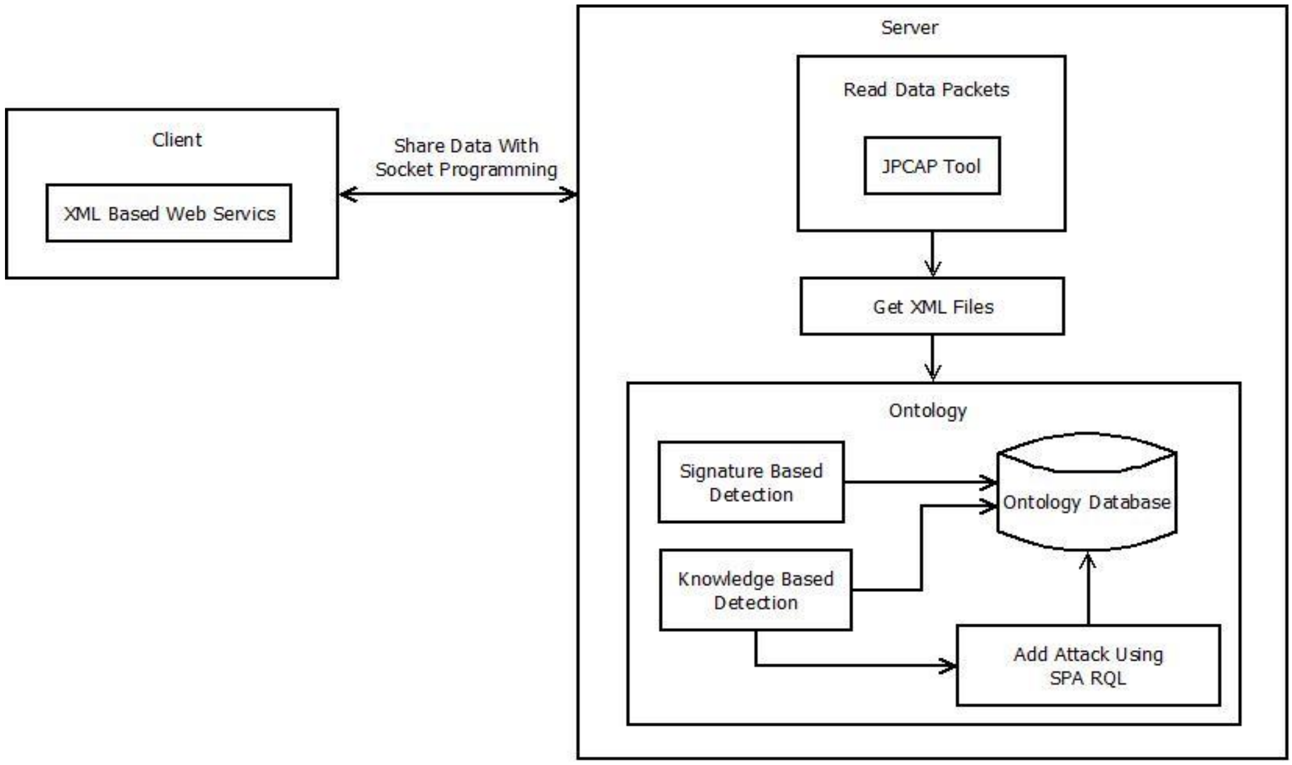

Figure 1. System Architecture

Initially, Server read the data packets from client. With the help of JPCAP tool, IP and TCP data is filtered out and extract the XML files separately. After this, XML files will passed through ontology to detect the attacks.

Ontology is designed using the Protege tool and the Web Ontology Language (OWL; www.w3.org/TR/owl-features).

For Attack identification and detection, strategy based approach is used. It is the combination of signature based detection and knowledge based detection.

1. Signature Based Detection:

A signature is a payload that identifies an attack through some specific malicious context. Signature based detection systems usually lead to low software detection mistake rates—namely, false-positive rates. However, one important limitation of signature-based attack detection is that it doesn't detect new unknown attacks, even if they have only small variations from a known payload.

Such type of detection techniques are effective to detect those attacks that have been already detected in previous detection task. These techniques validate each newly arrived packet with list of already detected known attacks. This technique is not capable of recognizing the zero day attacks. The execution steps of this technique are as follows:

Steps of Signature based attack detection:
Step 1: Store all known attacks in ontologies database in signature format.
Step 2: Read input file or client file at server side.
Step 3: Convert input file content into signature format.
Step 4: Input file content in signature format compare with all attacks stored in ontologies database.
Step 5: if signature matched with the attacks then attacks detected.

2. Knowledge Based Detection:

Another way to protect Web services from injection attacks is through knowledge-based detection systems, which apply protection based on some kind of previously known and cataloged behavior.5 Usually, two distinct classes are modeled: one for normal behavior, containing all expected actions that define such a profile, and another for attacks containing actions that aren't considered normal. Knowledge.

This type of attack detection system knows the information about system vulnerabilities and previous attack description and also able to detect the suspicious behavior of users. It contain two classes such as normal and abnormal behavior. Normal behavior define as the profile of user and another class contain the abnormal behavior of attacker. If new attack is found, it is added into ontology by using SPA RQL.

This system can detect the following types of attacks:

1. XML Injection Attack

XML is also affected by Cross-site scripting attacks. In this attack, unapproved malicious commands are transmitted from attacker.

2. Denial of Service Attack (DoS)

In computing, a denial-of-service attack (DoS attack) is a cyber-attack where the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet. Denial of service is typically accomplished by flooding the targeted machine or resource with superfluous requests in an attempt to overload systems and prevent some or all legitimate requests from being fulfilled.

3. Mitnick Attack

Computer security is an important factor in our information world with Internet and digitally owned materials. Over the past twenty years, network security has evolved continuously. More secure implementations are invented to replace old less secure implementations. Kevin Mitnick was able to hack into Tsutomu Shimomura's X-Terminal computer due to early implementation of TCP connection, which was not really secure at that time. With a huge desire of curiosity, Mitnick did something that no one has ever done before him. He exploited the trusted relationship between two computers by performing man-in-the-middle attack under a spoofed identity.

4. Semantic Attack

In a semantic URL attack, a client manually adjusts the parameters of its request by maintaining the URL's syntax but altering its semantic meaning. This attack is primarily used against CGI driven websites. Consider a web-based e-mail application where users can reset their password by answering the security question correctly, and allows the users to send the password to the e-mail address of their choosing. After they answer the security question correctly, the web page will arrive to the following web form where the users can enter their alternative e-mail address

5. X Query Attack

This is a functional programming language. It convert the collected data into XML format also provides the extensions to other formatting data. This attack happens when the data is entered by malicious source.

6. X Path Injection Attack

XPath Injection is a type of attack. It corrupt the application which is developed by using XML path language queries (XML path). This language can select the nodes from XML documents. This type of attack happens, if Xpath query for data is developed using user supplied information on web site. Attacker simply add corrupted information on web site and easily find out the structure of XML data and can access the data.

IV. CONCLUSION AND FUTURE SCOPE

A Web services administrator can consider the informative messages for investigation, aiming to tune the detection system, ensuring that the proposal approach doesn't produce false positives during detection. In this work designed the system for attack detection and identification by using the signature based and knowledge based method. This system is the combination of signature based and knowledge based system. For this detecting and preventing the attack ontology is used. By using ontology attack is detected.

V. REFERENCES

1. Thiago Mattos Rosa, Altair Olivo Santin and Andreia Malucelli "Mitigating XML Injection Zero -Day Attack through Strategy", publication in IEEE Security and Privacy in 2013.
2. Siddavatam and J. Gadge. Comprehensive Test Mechanism to Detect Attack on Web Services. 16th IEEE International Conference on Networks, p. 1-6, 2008.
3. C. G. Yee, W. H. Shin, and G.S.V.R.K. Rao. An Adaptive Intrusion Detection and Prevention (ID/IP) Framework for Web Services. International Conference on Convergence Information Technology, p. 528-534, 2007.
4. N. Konstantinou, D. Spanos, and N. Mitrou, "Ontology and Database Mapping: A Survey of Current Implementations and Future Directions," J. Web Eng., vol. 7, no. 1, 2008, pp. 1–24.
5. J. Undercoffer et al., "A Target-Centric Ontology for Intrusion Detection," Proc. IJCAI-03 Workshop Ontologies and Distributed Systems, Morgan Kaufmann, 2004, pp. 47–58.
6. A. Vorobiev and J. Han, "Security Attack Ontology for Web Services," Proc. 2nd Int'l Conf. Semantics, Knowledge, and Grid (SKG 06), IEEE CS, 2006, p. 42.
7. M. Bravenboer, E. Dolstra, and E. Visser, "Preventing Injection Attacks with Syntax Embeddings," Science of Computer Programming, vol. 75, no. 7, 2010, pp. 473–495.

8. M.S.A. Najjar and M.A. Azgomi, "A Distributed Multi-approach Intrusion Detection System for Web Services," Proc. 3rd Int'l Conf. Security of Information and Networks (SIN 10), ACM, 2010, pp. 238–244.
9. Z. Li et al., "Hamsa: Fast Signature Generation for Zero-Day Polymorphic Worms with Provable Attack Resilience," Proc. 2006 IEEE Symp. Security and Privacy (SP 06), IEEE CS, 2006, pp. 32–47.
10. J. Undercoffer et al., "A Target-Centric Ontology for Intrusion Detection," Proc. IJCAI-03 Workshop Ontologies and Distributed Systems, Morgan Kaufmann, 2004, pp. 47–58.
11. Z. Maamara, N.C. Narendrab and S. Sattanathan. Towards an ontology-based approach for specifying and securing Web services. Information and Software Technology, p. 441-455, 2005.
12. A. Vorobiev and J. Han. Security Attack Ontology for Web Services Proceedings of the Second International Conference on Semantics, Knowledge, and Grid, 2006.