Security against Web Application Attacks Using Ontology Based Intrusion Detection System

Mr. Harshal A. Karande[1], Miss. Pooja A. Kulkarni[2], Prof. Shyam S. Gupta[3], Prof. Deepak Gupta[4]

[1] Research Scholar, Department of Computer Engineering, Siddhant College of Engineering, Sadumbare, Pune, Maharashtra, India.
[2] Research Scholar, Department of Computer Engineering, Siddhant College of Engineering, Sadumbare, Pune, Maharashtra, India.
[3] PG Co-ordinator and Assistant Professor, Department of Computer Engineering, Siddhant College of Engineering, Sadumbare, Pune, Maharashtra, India.
[4] Assistant Professor, Department of Computer Engineering, Siddhant College of Engineering, Sadumbare, Pune, Maharashtra, India.

---***---

Abstract - ***Dependence on web applications is increasing very rapidly in recent time, but this resulted as web application targeted by cyber crook and hackers. Attacks may occur through the utilization of common security vulnerability in web based applications and programs. Such attacks are strongly essential to reduce some of the harmful consequences on web applications. For e-commerce and many conventional models, web application services become dependable platform. This paper identifies vulnerability attacks caused due to input performed by the user which are not properly validated across the web application also system gives effective defense against application level attacks. Because of web application service has enticed attackers which have made web services prone to various attacks, for this reason proposed system can predict and classify web application attacks. Attacks are classified based on security level of the attacks on security goals. Proposed system identifies vulnerability attacks and provides protection from threats and attacks in web applications.***

Key Words: Cyber Security, IDS, Network Security, Ontology, OWL-S, Semantic web, Web Application.

1. INTRODUCTION

In the internet technology the World Wide Web (WWW) has become an important day-to-day resource for the people. . According to internet usage statistics trends, number of web users has increased approx to 1.9 billion in Jun 2010. The web is day-to-day resource for the people and greatly more used for providing daily basis services like education service, E-commerce area., online reservation, online shopping and many more applications which is designed and perspective of user. So that the network attacks are popular attacks targeted because of narrow understanding of programming, limited security knowledge, and that is means lack of cognizance of the protection. And lack of protection is very harmful for the web application services. Generally web application use the network port 80 is employed. This communication is not protected by IVAs. There are different types of Open Web Security project (OWASP) Vulnerabilities: SQL Injection attacks, Cross Site Scripting attacks, Buffer Overflow attacks etc.

Security Ontology which exists provides taxonomy for threats, vulnerabilities and attacks. Ontology refers to the explicit Specification of the conceptualization of a domain which captures its context. Most ontological approaches are based on signature. The Web Application Security has become increasing very large manner in last decade and become hottest issue due to increase in communication to millions of users globally through divers range of applications. So, Intrusion Detection System is the system which is used to protect such type of systems. Generally Web Scanners provides only first line defense against the web attacks and detect good and well known security flaws those have signature. Result in false alarm and fail to detect critical vulnerability because scanners lack semantic. White list and black list is generally maintained by signature base solutions, which contains signature of begin inputs and signature of malicious attacks vectors. So, because lack of detection false positive and false negative alarm is generated. And that's why there is need of semantic system which can understand the application context, the data and contextual nature of attacks. Again there are two types such as Syntax Based Validation and Semantic Based Validation. Syntax Based Validation provides the size where as Semantic Based Validation may focus on specific data, format and understand potentially dangerous commands. Generally various generic security controls such as signature based firewall, intrusion detection and prevention systems. Proposed system is able to address all these issue through automatically updating of knowledge base. Also proposed systems mitigate the web application attacks effectively and easily capable of defeating the current strategy of novel manipulation of treats and attacks by hackers.

For critical types of issues, the proposed system analyses the web application treats that may be exploited by the attacks. Proposed system is highly able and capable to predict the attacks with respect to vulnerabilities.

2. PROBLEM WITH EXISTING SYSTEM

Most existing intrusion detection Systems are following problems:
The existing IDS developed and designed for validation vulnerability attacks are language reliable. In existing IDS, there are low accuracy and detection rate.

1. Data Overload, is the important problem which is overcome by current IDS.
2. False Positive: normal attacks is mistakenly classified as malicious and treated as attacks.
3. False Negative: IDS does not generate alarm when intrusion actually taking place.

3. CONTRIBUTION

Provide method to predict and classify the Web application attacks. So, basically system is an Ontological based approach which gives and specifies the web application attacks using context of consequences, attacks and vulnerability. Proposed system is efficiently and accurately capable to detecting the web application attacks. Classification of web application attacks are based on their severity level. Proposed system can capture the context of important web application attacks, various techniques are used by the hackers, source and as well as target of the attack, vulnerabilities and controls in terms in policies for mitigation of these attacks. Proposed system gives suggestion for detecting and preventing the attacks.

4. OBJECTIVES

1. Recreated, but rather converted into the final published version. Low False Positive rate and Low False alarm rate is provide.
2. Efficiency and Accuracy increase.
3. Detection of Cyber attacks.
4. Study of Ontological Framework for Intrusion Detection System.
5. Accuracy/Validity of the Model.
6. Task Orientation.
7. Completeness and Conciseness.
8. Clarity.
9. Expandability and Reusability.
10. System performance by using throughput and response time.
11. Ontology Expressiveness.

5. RELATED WORK

Research is basically influenced by related work in ontology based reasoning, also the core concept of semantic systems used to define concepts and relations of domain knowledge.
Raskin et al. (2001) proposed Ontology for achieving data integrity of web resource. They have claimed that by using their ontology, intrusive behavior could be systematically organized to any level of detail. Summarizing a large variety of item sets reduces list of properties, and allow specification of security knowledge, so because of this improvement in prevention and reaction capabilities. Ontology basically focuses on network layer.
Ning et al. (2001) have proposed a hierarchical model for attack specification and abstraction of events for intrusion detection in distributed systems. No any attack modeling formalism is mentioned in the model but it only support network layer attacks.
Undercoffer et al. (2004) proposed a system of traffic centric ontology. In this system there are huge numbers of classes of computer intrusion.
Denker et al. (2005) proposed access control trough ontology developed in DARPA Agent markup language, but this ontology is not fully utilized.
Ontology for information security is proposed by Herzog et al. (2009) models the assets, threats, vulnerabilities, countermeasures and their relationships, with using of OWL reasoner, the system is capable of generate new knowledge. J.McHugh (1998-99) proposed the system that focuses on classification of attacks which is based on protocol layer.
Fenz et al. (2007) focuses on security ontology for certification of ISO/IES 27001 and security guidelines.
Abdoli et al. (2010) have designed on ontology for attacks targeting computers and network and highlighted its importance in information security. For development of the ontology the authors have studied different number of logs and connection that causes network DoS.
Huang et al. (2010) proposed a system that can be used to analyze malware behavior based on ontology, that malware can divide into different layers. To monitor this type of malware they use to change system files for Microsoft windows. They have used SWRL rules for behavior analysis, which help in inference and infer new knowledge that helps in better malware analysis.
Carlos Blanco et al. (2011) provide comparison between various ontological approaches that can be reused.
To depict a simple model of attack attributes is a major problem which is common for all above ontological systems used. Also systems have lack of necessary reasoning ability due to their taxonomical structure. The proposed ontological model of attack detection, allow us to successfully capture the context of their input, which is important in designing and developing mechanisms against web attacks.

6. ONTOLOGY ENGINEERING METHODOLOGY

Ontology design is an iterative process to determine a scope defines classes, properties (relations), axioms, constraints and instances. Our system Ontology has been developed keeping in view. Also gives some objectives like, manage security aspects at various levels, provide a generic solution, enable the reusability of Ontology.

7. PROPOSED SYSTEM

Figure shows various components such as system analyzer, interface engine, rule engine, ontology generator and knowledge base. Ontology generation and rule engine is the major components which are used to generate attack prediction rules. Knowledge base is used to store such concepts like web application attacks, threats etc. Application layer communication layer protocols are used as semantic networks. Every protocol is termed as a conceptualized category in this model. Model presents specific details for each protocol.

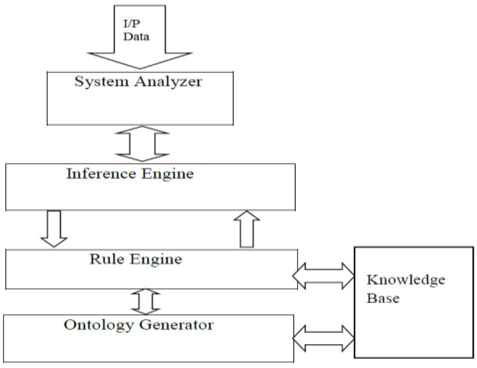

Fig.1. System Architecture

For instance the HTTP concepts in the mode contains all the associated parameters and their relationships which relevant concept by using RFC 2616. HTTP request is a part of HTTP message structure, which again further classified in to request line, Entity Header, Request Header, and payload.

Figure 2 shows the generation of ontology; ontology was created by using Protégé tool. With use of Protégé we have to design Ontology. Protégé is written in java, thus supports running in a wide range of operating systems. It allows users to create and edit ontologies in an application area and it has the building blocks that we expect in developing ontology: classes, relations and instances. Protégé can record ontologies in various formats including RDF/XML, OWL/XML, N-Triples, N3 and Turtle RDF. With the use of this tool ontology are created and it is very helpful to the system to detect the malicious or attack.

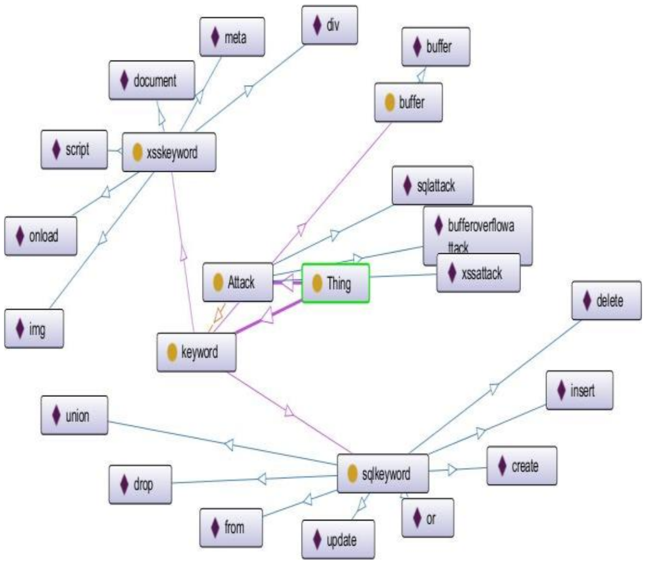

Fig.2.Ontology generation using Protégé.

In the proposed system request is parsed according to the ontological model. Input is checked for encoding, with the use of protégé there are .owl file is generated. So with help of these file system can easily able to detect the malicious or attack.

8. IMPLEMENTATION

In this system we have focused on the HTTP protocol because it is foundation of data communication for World Wide Web (WWW). Logic based context reasoning can be employed on the basis of functionality. In rule based reasoning, semantic rules can be defined that will manipulate the ontology logic. Rules can be defined using standard rule languages or can be written in a variant of a language supported by a specific reasoner.

9. CONSIDERED ATTACKS

1. Analyzer Detection Mechanism (XSS)
2. Protocol Validation Attack
3. SQL Injection Attacks
4. Buffer Overflow.

10. CONCLUSIONS

In this paper we introduced a novel Distributed Intrusion Detection System that used special attack ontology to detect attacks and intrusions. The ontology based system can able to classify web application attacks. Proposed system effectively analyzed malicious attacks. The proposed system again gives suggestions to mitigate and prevent the attacks.

ACKNOWLEDGEMENT

We are glad to express our Sentiments of gratitude to all who rendered their valuable guidance to us. We would like to express our appreciation and thanks to Dr. S. S. Khot, Principal, Siddhant College of Engineering, Sudumbare, Pune. We are also thankful to our family and friends for their encouragement and support. We thank the anonymous reviewers for their comments.

REFERENCES

[1] Harshal A. Karande, Prof. Shyam S. Gupta, “ONTOLOGY BASED INTRUSION DETECTION SYSTEM FOR WEB APPLICATION SECURITY”, IJIRT, Vol.1, pp. 618-624, December 2014.

[2] Harshal A. Karande, Prof. Shyam S. Gupta, “INTRUSION DTECTION SYSTEM FOR WEB APPLICATION SECURITY BASED ON ONTOLOGY”, GJESR 2(10), pp. 98-102, October 2015.

[3] P.Salini, J. Shenbagam, “Prediction and Classification of Web Application Attacks using Vulnerability Ontotlogy”, IJCA, Vol 116-No.21, April 2015.

[4] Razzaq Abdul, Latif Khalid, Ahmad Hafiz F, Hur Ali, Anwar Zahid, Bloodsworth Peter C. “Semantic security against web application attacks”, Information Sciences 2014;254:19e38. Jan 2014.

[5] J. Undercoffer, J. Pinkston, A. Joshi and T. Finin, “A target-centric ontology for intrusion detection”, In 18th International Joint Conference on Artificial Intelligence, pp. 9-15, March 2004.Ding, W. and Marchionini, G. 1997 A Study on Video Browsing Strategies. Technical Report. University of Maryland at College Park.

[6] S. Fenz, G. Goluch, A. Ekelhart, B. Riedl, E. Weippl, Information security fortification by ontological mapping of the iso/iec 27001 standard, in: 13th Pacific Rim International Symposium on Dependable Computing, 2007, PRDC 2007, IEEE, 2007, pp. 381–388.