ISSN 2348 – 8034
Impact Factor- 3.155

GLOBAL JOURNAL OF ENGINEERING SCIENCE AND RESEARCHES

INTRUSION DTECTION SYSTEM FOR WEB APPLICATION SECURITY BASED ON ONTOLOGY

Mr. Harshal A. Karande[*1] and Prof. Shyam S. Gupta[2]
[*1]Research Scholar, Computer Engineering, Siddhant College of Engineering, Sadumbare, Pune, India.
[2]Prof. Shyam S. Gupta, PG Coordinator, Computer Engineering, Siddhant College of Engineering, Sadumbare, Pune, India.

ABSTRACT

Internet is rapidly increases and blow up exponentially and become more significant in our day to day life. But web applications on internet are not safe; those web applications are targeted by cyber crooks and hackers. By capturing the context of the contents security systems modeled using ontology proposes new class of solution which is highly effective in detecting web application attacks. This paper gives the effective defense against the web application attacks. The proposed system is ontology based system that can predict and help to classify web application attacks and focus on specific portion of the request and response where a vulnerability and malicious script is possible and detect HTTP protocol specification attacks.

Keywords: *Cyber Security, Network Security, Ontology, attacks, web applications, security measure.*

I. INTRODUCTION

With the use of web applications and web services information shearing is rapidly increases. Because of that e-business are enlarged and again it is dangerous for web applications in term affecting the security goals as integrity, availability and efficiency. Various techniques are taken to control the attacks with different security mechanism such as IDS, Scanners etc. Now a day's developers knows the information about threats and attacks, and there for they can easily identify the attacks and mitigate them.

Ontology for the web application provides information about threats and attacks but lack to infer the knowledge to predict the attacks and does not classify the vulnerability. So, for this type of issue the proposed approach analyses the vulnerabilities and attacks. Proposed system is able to detect the attacks with easy manner. Ontological approach for security is effective to identify vulnerabilities.

In our work we are going to providing a unique way to detect malicious attacks. This paper gives the given contribution

- Our solution is an ontological based approach that specifies the web applications attacks.
- Depending upon severity level of web applications attacks are classified.
- Proposed system gives effective result for detection of web application attacks.

Proposed system can be further more efficient for getting several case of input validation attacks, so that this concept reduce the analysis time and likewise increase the effectiveness of the overall system. Propose system mitigate the web application attacks effectively and efficiently and capable the current strategy of novel manipulation of attacks by the hackers.

II. RELATED WORK

Ontology for information security proposed by Herzog models the assets, threats and vulnerabilities and their relationships. The system generates new knowledge through inference and using OWL reasoner.

Carlos Blanco et al. present a systematic review of existing security ontology proposals. The survey shows that various security ontology is developed for each phase of software life cycle and for reusability.

Undercoffer provides better usage of ontology system to gather domain knowledge, protect network layer attacks and ignore web application attacks. The proposed approach detects vulnerabilities and malicious attacks.

III. ONTOLOGY METHODOLOGY

Ontology design is an iterative process to determine the scope and define the concepts, properties, axioms, constraints and instances.

Objectives related to the system are as follows:

- Detailed description of all important security concepts.
- Provides a generic solution for various environments.
- Ontology reusability.

Layered approach of Ontology:

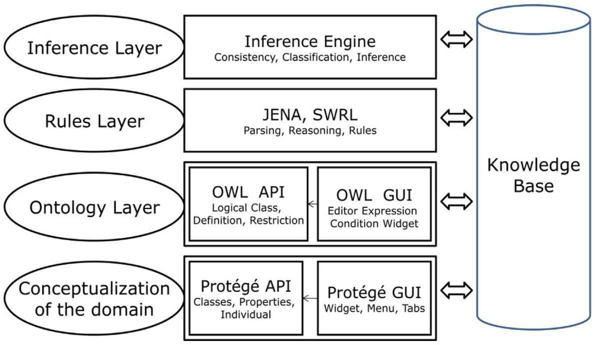
Inference Layer
Inference Engine
Consistency, Classification, Inference
Rules Layer
JENA, SWRL
Parsing, Reasoning, Rules
Ontology Layer
OWL API
Logical Class, Definition, Restriction
OWL GUI
Editor Expression Condition Widget
Conceptualization of the domain
Protégé API
Classes, Properties, Individual
Protégé GUI
Widget, Menu, Tabs
Knowledge Base

Figure 1: Layerd Approach for Ontology

A layered approach has been used for ontology design in the knowledge base that depicts the tools and technologies which have been used, as shown in below figure The bottom-most layer represents the conceptualization in which concepts of our domain in question i.e. web security, are defined in the form of classes, properties and individuals either dynamically or through interaction with the tool's Graphical User Interface.

The ontology layer facilitates the expression of classes in logical form (i.e. predicate logic) and defines restriction upon the classes by using OWL (web ontology language) through interaction with OWL GUI. The inference (top-most) layer drives additional knowledge from the defined ontology and provides the ability to check the uniformity and arrangement of concepts (classes).

The layer representing Rules uses Semantic Web Rule Language (SWRL) and Jena API for parsing, reasoning and rule generation. In addition the Jena API allows query construction for retrieving information via simple protocol and resource query language (SPARQL).

IV. PROPOSED METHOD

In this section detailed descriptions of the components in the proposed system are discussed.

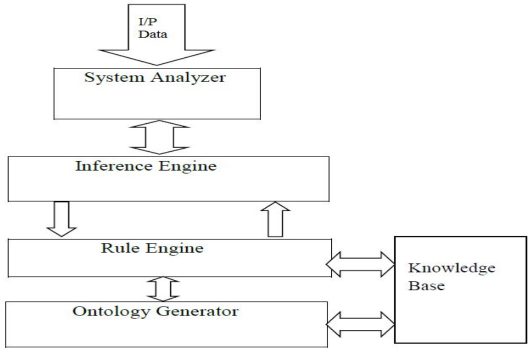

Figure 2: Architecture diagram for proposed system.

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.

The system can be used to gather Knowledge about the threat which exploits the malicious attacks to security. Data collection is also main component in the system. So the function of this component is to gather the required information.

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. 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.

V. ATTACK DETECTION

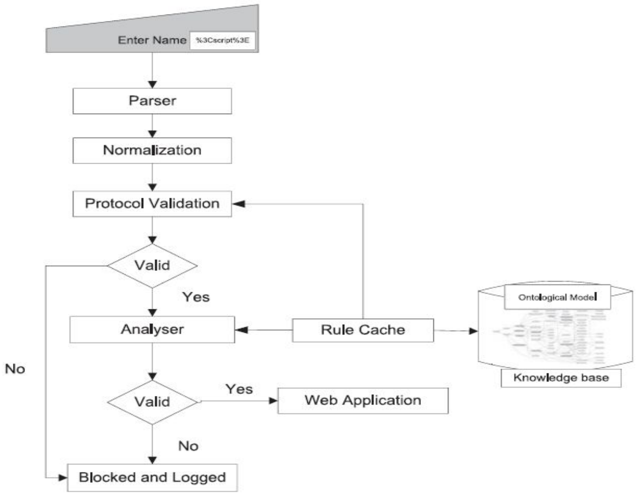

Figure 3: Web Attack Detection

In the proposed system, HTTP request parsed according to ontological model is stored in the Knowledge base. Input is checked for encoding. In case it is encoded it would be first decoded and then would be checked for anomaly After the normalization module the request is passed on to the Protocol Validation and Analyzer module where it is matched against the semantic rules that are generated by ontological models in the knowledge base for identifying malicious content in input validation. Protocol Validation module caters to the violation of protocol specification whereas the Analyzer handles all other Web application attacks. If the input content matches any of the rules the request is blocked and a log is made for the said attack.

VI. RESULT & DISCUSSION

In this paper new methodology developing a framework that makes attacks on network servers and discovers security vulnerabilities in software system and allows security administrators to determine the problems. To show this model application is built that a new methodology that takes protocol requirement aspects from the server and carryout various attacks on the server and detect malicious attacks.

In this paper proposed system detects various types of structured query language injection attacks, cross-site scripting attacks, vulnerabilities, malicious attacks, and also prevention methods. The prediction rate of proposed system result are compared against security ontology and represented as figure.

Figure shows the comparison of detection of the attacks. The attack classification is also compared with the existing system. This section shows our proposed ontological model is advanced to previous model to detect malicious attacks and vulnerabilities.

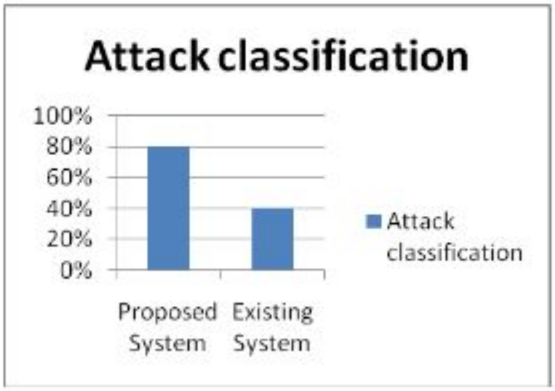

Figure 4: Comparison f Attack Classification

The results show that the capability and attack detection rate of our proposed system are better than the existing system.

VII. CONCLUSION

Whenever web application was proposed to have both a secure and insecure description then find the possible outcomes could be examined. The only vulnerabilities that would be reported would be imprecisely recognized the probable vulnerabilities.

The ontology based system can predict and classify web application attacks. Proposed system effectively analyzed malicious attacks. The proposed system again gives suggestions to mitigate and prevent the attacks. As the future work the proposed system can be reused to detect the web application attacks.

VIII. ACKNOWLEDGEMENTS

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. 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. *A. Herzog, N. Shahmehri, C. Duma, An Ontology for information security, Techniques and applications for advanced information privacy and security: Emerging organizational, Ethical and human Issues(2009) 278-301.*

3. *Carlos Blanco, Joaquin Lasheras, Eduardo Fernandez Medina, Rafael Valencia-Garcia and AmbrosioToval, "Basis for an integrated security ontology according to a systematic review of existing proposals", Computer Standards and Interfaces, Vol. 33, No67, pp.372-388, june 2011.*

4. *J. Undercoffer, J. Pinkston, A. Joshi and T. Finin, "A target-centric ontology for intrusion detection", In 18th International joint Conference on Artificial Intilligence, pp- 9-15, march 2004.*

5. *P. Salini, J. Shenbagam, "Prediction and classification of Web Application Attacks using Vulnerability Ontology", IJCA (0975-8887).*

6. *Grosof Benjamin, Dean Mike,SWRL: a semantic web rule language combining OWL and RuleML.Journal W3C member submission 2004;21:70.*