ISSN 2395-1621

A Survey on Dual Security protection for Web Server Using Signature Identification

Sunil Gambhire[#1], Chetan Dasare[#2], Pramesh Shaha[#3], Sumit Shinde[#4]

[1]sunilgambhire99@gmail.com

[2]cdasare6@gmail.com

[3]prameshshaha@gmail.com

[4]sumit_shinde@yahoo.com

[#1234]Pune University, Universal COE, Pune

Maharashtra, India.

ABSTRACT

The use of internet has increased enormously in last decade, due to the introduction of handheld devices like, mobiles and tablets. As a result of this, the internet services and applications have increased as well. These applications includes, accessing the personal information from anywhere. But, by providing such access, internet service providers invited large number of attacks and frauds. Thus, a multi-tier technique for internet services was introduced. In this, the webservers were used to handle the front end of the applications, while, the file servers or databases handled the data for users. But these multi-tier services were soon tackled by different attacks, as the attacked end changed from front to the back end. The Intrusion Detection Systems, also known as 'IDSs', examines the network packets at both ends, i.e. Webserver and database systems, individually. But still, the security in multi-tiered Anomaly Detection (AD) systems has a great possibility of studies. To overcome these situations and make internet services more secured, a new IDS system is proposed, called as 'Double Guard'. Here, the user sessions at both, front-end and back-end sessions are secured. The current IDSs do not able to identify the attacks on multitier systems, unlike the Double Guard, which monitors both, front-end and the back-end. We are using the signature identification for detecting intrusion at the places where an attack can be performed. This technique is helpful to identify the intrusions and defend the multitier network architecture.

Keywords: Intrusion Detection Systems (IDSs), web services, multitier architecture, security.

ARTICLE INFO

Article History

Received : 26th January, 2015

Received in revised form :

2nd February, 2015

Accepted : 4th February, 2015

Published online :

11th February 2015

I. INTRODUCTION

Web services and multitier architecture

In a network, a web service is a technique for electronic devices to communicate with each other. The W3C defines the web services as, 'a software system, which is developed to support the electronic devices to interact in interoperable environment over a network' [1]. Nowadays, different software's are used by organizations for management. The data is often needed to be exchanged between the software systems. The web service is the technique, needed for this data exchange over the network. The web service never provides the GUI to the user, unlike the traditional systems, like, web server/web page system. Instead, they share the business logic, data and/or processes across a network. But, a web service can be added to a GUI.

In multitier architecture, the presentation, business logic and data storage are physically separated. Thus, it also called as, client-server architecture. The three-tier architecture [2] is the very popular and widely used multitier architecture. The multitier architecture allows the developer to develop a reusable application. When the application is divided into the tiers, it can be modified separately, rather than to modify all the application.

a. Security in multitier architecture

Nowadays, variety of platforms supports the millions of software applications to be built and run. These applications can be accessed by all users, like, developers, employees, end users or professional hackers etc. due to this uncontrolled access, the internet applications are more prone to the unauthorized usage and attackers. The threat may include,

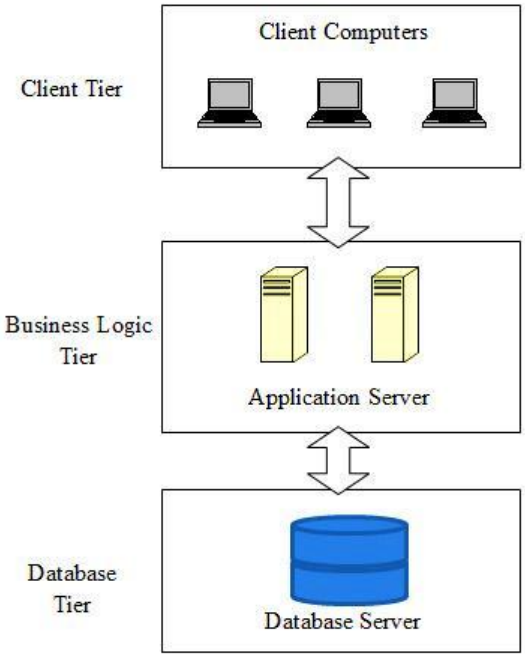


Figure 1 – 3-tier architecture

stealing confidential and private data, applying the heavy traffic on services, creating false data, corrupting the system, modifying the application usage etc. These threats may compromise the security on multiple access points, like from own user to the user interaction. The own user may also be a threat to the applications. The security compromise may also target various computing resources, i.e. hardware and software components. Multitier architecture can face the security breach at each and every tier. Presentation tier and data server tier, i.e. front end and the back end, are widely exposed tiers.

Most of the current systems takes of the security in multitier architectures by monitoring teach tier individually. Thus, they are not much of the security for the multitier architectures. Hence, we are providing a system which will take care of the security in the multitier architectures.

The remaining paper can be sorted out as: Section II gives the quick survey of the current systems in the field of multitier security, with their drawbacks. In section III, contains the system, that is been proposed in this paper. Finally, the section IV contains briefly reviewed conclusion of the paper

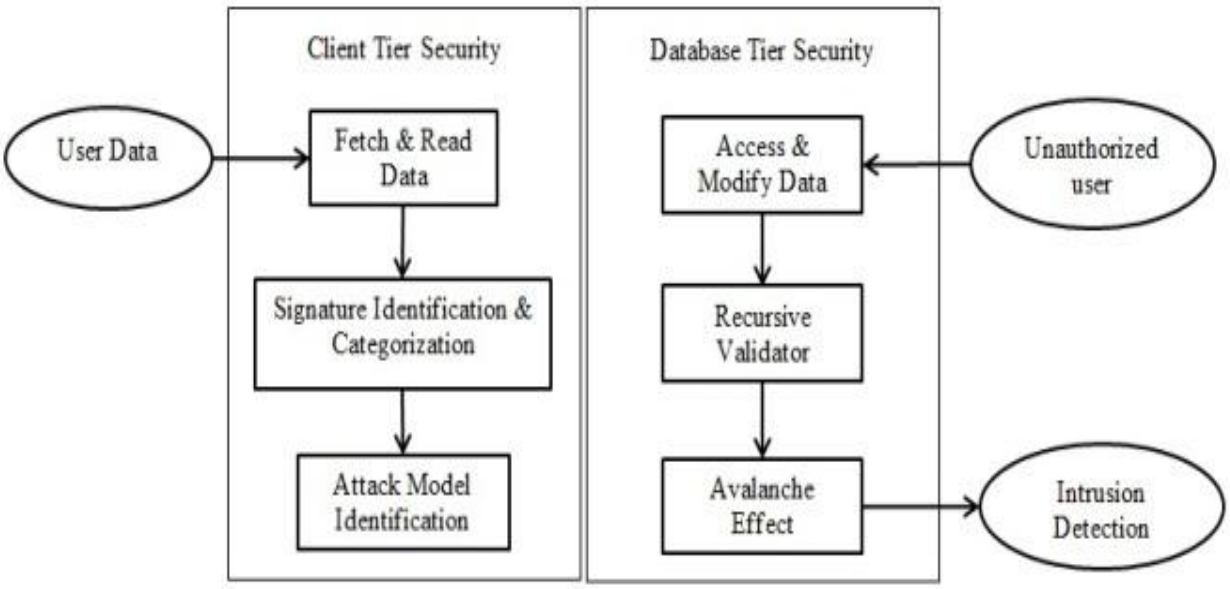
II. LITERATURE SURVEY

The IDS in a network is classified into two broad categories; they are, first, the Anomaly Detection and second, the Misuse Detection. The correct and acceptable static form and dynamic behavior definition and characterization are the prime requirement of the anomaly detection. This stored definition is then used to detect the abnormal behavior in the network [3]. The difference between the correct and anomalous forms of data and code is needed to be accurately defined for better performance. The behavioural models can be built in two different ways. First is by using historical data to perform statistical analysis [4]. Second is, by specifying the behavioural patterns using the rule-based approach [5]. The Temporal information is used by IDS, as in [6] for intrusion detection. This technique correlates the events on the basis of time. This makes the system inefficient, as the independent and concurrent events might be considered as correlated events mistakenly.

The intrusions and vulnerabilities were detected by some previous approaches, using statistical analysis of source code or executable [7]. Some techniques, like in [8] rather tried to dynamically track the flow of information to find the intrusions. Another approach to handle the SQL injection or Cross Site Scripting injection (XSS) attacks is to validate the input [9].

For isolating the objects and enhancing the security performance of the system, virtualization is used in many approaches. The techniques like, Parallels Virtuozzo [10], OpenVZ [11], and LinuxVServer [12], all used the lightweight virtualization. All these techniques are somehow based on the concept similar to the containers. By using the containers, a group of processes can still look as if, they have their own dedicated system, but somehow they are sunning in the separate environment. But, the lightweight container provides with added performance advantages over the virtualization and para-virtualization. A single physical host is capable of running the thousands of containers. The system in [13] provides isolates the different instances of applications by using the lightweight virtualization. For segregation and inhibition of adversaries, such virtualization techniques are widely used. In our system, we have only used the IDs of containers for separating the session traffic. They are helpful for extraction and identification of relationships between database query events and the web server requests.

Another widely acknowledged technique is CLAMP [14]. It is an architecture which prevents the network from leaking the information, even though the attacks are present. It guarantees that the code running behalf of the user is the only part in the system which accesses the sensitive data of user. For this purpose, CLAMP separates the code at web server tier and data at the database tier.



III. Proposed Methodology

In this paper, we are proposing a new technique to detect the attacks in multitier web services, called as 'Dual Guard'. The proposed technique is based on [15]. We are developing a method which is able to generate normality models of each user sessions. These sessions not only includes the web front end, i.e. HTTP, but also includes the back end consist of either files or SQL, of transactions in the network. In dual-guard, to achieve above mentioned security, we have used the light-weight virtualization technique. This technique provides separate virtual computing environment, called as 'containers' to each user's web session. In our technique, we are intended to generate new containers dynamically; we also intend to recycle the used containers.

Now, the web requests are needed to be accurately associated to the subsequent database queries. For this purpose, we have used the container IDs. This creates an instrumental mapping profile, which serves both web server and database traffic. For the basic operations provided by web service, first we will create a separate training model while developing the mapping model, in case of dynamic web pages. We are using the signature identification techniques to detect the intrusions in the network. Correct signature patterns will be stored in the system, while the current packets in the network will be checked against these signature patterns. If the patterns are different then the intrusion is detected. Figure 2 shows the proposed system architecture.

IV. Conclusion

Nowadays, the use of internet has increased enormously, and so does the use of diverse web services over the internet. As the use of web services increased, the attacks on them have also increased. The attacks may include the user information theft, SQL injection etc. Thus, a system is needed to secure the web services for users and for the service providers. Hence, a technique called 'Dual Guard' is proposed in this paper. It not only secures the front end (web pages) from attackers, but also secures the back end (database or files). It uses the signature identification technique to find the intrusions in the network. It protects the system from SQL injection attacks as well.

Though, we don't assume that we have provided a complete solution for the web services' security; so, further study is required in this field due to diverse types of attacks are made almost every day. So, more security is required

References

[1] "Web Services Glossary", W3C, Feb 2004.

[2] "What Is 3-Tier Architecture And Why Do You Need It?" SIMCREST, blog.simcrest.com/what-is-3-tier-architecture-and-why-do-you-need-it/, accessed on 28th Jan, 2015.

[3] T. Verwoerd and R. Hunt, "Intrusion Detection Techniques and Approaches", Computer Comm., vol. 25, no. 15, pp. 1356-1365, 2002.

[4] G. Vigna, W.K. Robertson, V. Kher, and R.A. Kemmerer, "A Stateful Intrusion Detection System for World Wide Web Servers", Proc. Annual Computer Security Applications Conf. (ACSAC '03), 2003.

[5] M. Roesch, "Snort, Intrusion Detection System," http://www. snort.org,2011.

[6] A. Seleznyov and S. Puuronen, "Anomaly Intrusion Detection Systems:Handling Temporal Relations between Events," Proc. Int'l Symp.Recent Advances in Intrusion Detection (RAID '99), 1999.

[7] M. Christodorescu and S. Jha, "Static Analysis of Executable to Detect Malicious Patterns," Proc. Conf. USENIX Security Symp, 2003.

[8] R. Sekar, "An Efficient Black-Box Technique for Defeating Web Application Attacks," Proc. Network and Distributed System Security Symp. (NDSS), 2009.

[9] D. Bates, A. Barth, and C. Jackson, "Regular Expressions Considered Harmful in Client-Side XSS Filters," Proc. 19th Int'l Conf. World Wide Web, 2010.

[10] "Virtuozzo Containers,"

www.parallels.com/products/pvc45/, 2011.

[11] OpenVZ, wiki.openvz.org, 2011.

[12] Linux-VServer, linux-vserver.org/, 2011.

[13] Y. Huang, A. Stavrou, A.K. Ghosh, and S. Jajodia, "Efficiently Tracking Application Interactions Using Lightweight Virtualization," Proceedings of First ACM Workshop Virtual Machine Security, 2008.

[14] B. Parno, J.M. McCune, D. Wendlandt, D.G. Andersen, and A. Perrig, "CLAMP: Practical Prevention of Large-Scale Data Leaks," Proc. IEEE Symp Security and Privacy, 2009.

[15] M. Le, A. Stavrou, And B. B. Kang, "DoubleGuard: Detecting Intrusions in Multitier Web Applications", IEEE Transactions On Dependable And Secure Computing, Vol. 9, No. 4, March 2014 2013.

