ISSN:0975-9646

Efficiently Detection of Intrusion in Multi-tire Web Applications Using DoubleGuard: A Survey

Prerna U. Randive

Computer Engineering Department, Savitribai Phule Pune University
Shivajinagar, Maharashtra, India

***Abstract*— now a day most of the work is done by internet. So web application have now become a essential part of daily life, such as online shopping, banking, social networking, enabling communication and management of personal information from anywhere. To acclimatize this increase in web application and data complexity, web services have shifted to multi-tire design. Wherein the web server executes an application front-end logic and data is outsourced to database or file server. DoubleGuard is an IDS system used to detect and prevent attacks. The behaviour network of user sessions around both the front-end web server and back-end database is modelled by an IDS system. DoubleGuard is able to detect attacks by checking web and consequent database requests. System builds interrelated models for static websites for detection of various types of attacks. This system verified that this kept true for dynamic requests. Where extraction of information and updates in back-end database occurs using the web server front end. This system prevents both web server and database server by providing security.**

***Keywords*—DoubleGuard, Multitier, Session, Attacks, Web server.**

I. Introduction

Web services have been rapidly increased around the world in relation to its popularity and complexity. Internet is used in different daily need tasks such as online shopping, banking, social networking, enabling communication and management of personal information from anywhere. These web services which are used on web to run the application user interface logic for front end and server which stores database or file server for efficient data are backend server. Due to the pervasive use of web services, which is spread everywhere for personal and corporate data they have been targeted for the malicious purpose. Due to turning of attention from attacking to front-end to exploiting vulnerabilities of the web application in order to violet the back-end database system by using SQL injection.

A profusion of Intrusion Detection System (IDS) currently examined the network packets individually within web server and database system. However there is less work being done on multitier anomaly detection that creates models of network behaviour. It is for both web as well as database networks interactions. In such architecture that is multitier architecture, the back-end database server is often prevented behind a firewall which is used as guard while web servers are obtainable remotely over the internet. Unfortunately, though back-end is prevented from direct remote attacks, back-end systems are vulnerable to attacks that make use of web requests as a means to destroy the back-end. Intrusion Detection Systems used to identify known attacks by the help of matching misused traffic-patterns or signature for protection of multitier web services. Unknown attacks by detecting abnormal network traffic that deflects from the normal traffic can be detected by class of IDS that uses machine learning.

OpenVZ can be used to implement DoubleGuard container that is suitable for many web applications and having good performance overhead, if server is already overloaded then there is 26 percent overhead. The DoubleGuard architecture is suitable for profiling of casual mapping and future session hijacking attacks. Dedicated container may be used for each client session due to if an attacker may be able to adjust single session but the loss is limited to adjusted session only, other user session are untroubled by this.

The relationship between request received by web server and requests those are generated for back-end database server is casual for website that do not allow modification of content from users. These web sites are static web application. Casual mapping depends upon web application's size and functionality but does not on content changes that can be executed in controlled environment. The web applications which allow fixed back-end database server modifications those are dynamic web applications. These applications allow HTTP requests that includes variable which depend on user input. Therefore have to model casual relationship between front-end and back-end will not always deterministic one and depend on application logic. The back-end query can be change depend on parameter value which is passed in HTTP request and application logic.

In some situation same application's primitive functionality can be generated by many different web applications. Due to these cases, the obtaining casual mapping between web server and database request can range from one to many based on value of variable passed in web request. To forward this challenge while composing casual mapping model for dynamic web pages an individual training model is triggered for basic request those are supplied by web services.

II. Related Work

There are some methods used to detect and prevent from vulnerabilities. From these methods web application program can improve them to reduce vulnerability. Some techniques are described below.

DoubleGuard [1] proposed by Meixing Le, Angelos Stavrou, and Brent ByungHoon Kang. DoubleGuard is an intrusion detection system that is used to create models of normal behaviour for the multi-tiered web applications from front-end web (HTTP) request and back-end database (SQL) query. DoubleGuard forms container-based IDS with the multiple input streams to generate and create alerts. By monitoring both web and consequent database requests, it is able to find out attacks. This DoubleGuard implemented using the Apache web server with the MySQL and light weighted virtualization. Using DoubleGuard is able to expose and detect wide range of multiple attacks with 100 percent accuracy. While maintaining, for static web services 0 percent false positives and for dynamic web services 0.6 percent false positives.

Swaddler: An Approach [2] Proposed by Marco Cova, Davide Balzarotti, Viktoria Felmetsger, and Giovanni Vigna. Swaddler is used to identification of attacks against web applications which are based on the analysis of the internal application state. Swaddler first models values of session variables in association with critical execution points in web application. Authors also introduced novel detection model that relies on multi-variable invariants to identify web-based attacks. In this method also developed a prototype of our system for the PHP language and evaluated it against various real world applications. Attack detection is done by leveraging the internal, hidden state of a web application. Attacks like violate its intended workflow, confirming our hypothesis that any insecure state usually corresponds to an anomalous state.

A.S. Gadgikar has suggested negative tainting approach [3]. It is used to preventing SQL attacks without change in existing code and it also helps to reduce time and space complexity. Negative tainting approach has benefit like it does not require any costly hardware and can work with any type of database like oracle, SQL etc. This technique consist of detecting vulnerable spot from web application, then lastly inserting the newly identified SQL injection attacks to improve accuracy of the system.

Mihai Christodorescu Somesh Jha has suggested Static Analysis to Detect Malicious Patterns [4] presents a unique review on malicious code detection. Authors regard malicious code explosion as an obfuscation deobfuscation game among malicious code writers and researchers performing on malicious code identification. Malicious codes writers try to obfuscate the malicious code for subvert malicious type of code identifiers, such as antivirus application software. Authors evaluate the resilience of the 3 commercial virus scanners against to the code-obfuscation attacks. Result is virus scanners can be subverting by a simple obfuscation transformation. He also modelled architecture for detection of malicious patterns in executables that are resilient to common obfuscation transformation.

Evaluation of Web Security Mechanisms using Vulnerability & Attack Injection [5] proposed by José Fonseca, Marco Vieira, Henrique Madeira. He proposes a methodology and the prototype tool to evaluate web application for the security mechanisms. He also shows implementation of Vulnerability & Attack Injector Tool (VAIT) which allows the automation of entire process. This tool is helped to run the set of experiments that demonstrate the feasibility as well as effectiveness of the proposed methodology. The injection of the both vulnerabilities and attacks is indeed the effective way to calculate security mechanisms and to point out their weakness as well as improvement.

Nidhi Srivastav Rama Krishna Challa Proposed Novel Intrusion Detection System [6]. In this paper, presented layered framework integrated with neural network to compose an effective intrusion detection system. This system has performed with Knowledge Discovery & Data Mining (KDD) 1999 dataset. The proposed system has high attack identification accuracy and less false alarm rate.

TDFA technique is proposed by Vahid Aghaei Foroushani A. Nur Zincir-Heywood [7]. TDFA includes of three main components: Detection, Traceback, and Traffic Control. In this technique, the goal is to place packet filtering as near to the attack source. By doing this the traffic control component at the victim side aims to set up limit on packet forwarding rate to victim. This type of mechanism used to reduce the rate of forwarding the attack packets and hence improves the throughput of legitimate traffic. So TDFA used to reduce the attack traffic to prevent the quality of service for the legitimate traffic.

III. DOUBLEGUARD SYSTEM ARCHITECTURE

To make effective mechanism to find out intrusion in multitier web application, DoubleGuard system makes use of lightweight process containers declared to as ‘containers’, as impermanent, destruction servers for client sessions. It is probable to initialize thousands of containers on single physical machine, and these virtualized containers may be discontinued, returned, or quickly reinitialized to serve new sessions. In the classic three-tier model database side, it is not able to represent which transaction corresponds to which client request. The conversation among the web servers and the database server is not unattached, and we can hardly recognize the relationships among them.

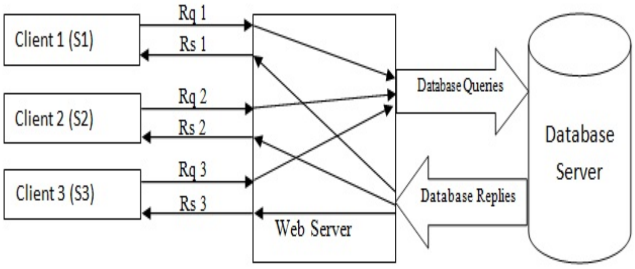

Fig -1: Classic three-tier model. The web server works as the front-end with the file and database servers works as the content storage backend

This container based and session-unattached web server architecture upgrades security performances as well as supply us with the detached information flows that are partitioned in each container session. It grants us to identify mapping among the web server requests and subsequent database queries and to exercise such a mapping model to detect anomalistic behaviours on the session /client level.

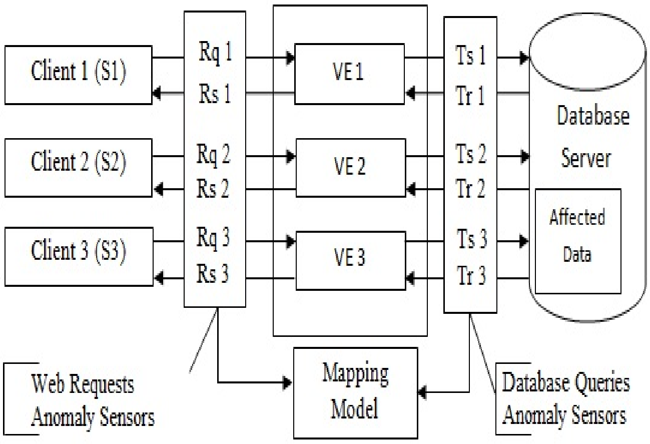

Fig -2: Web-server instances coming in containers

When the mapping model created, it helps to detect unnatural behaviours. Web request and database query within each session would be in consonance with the model. If there survive any request or query that withstands the normality model within a session, after that the session will be used as attack.

A. *Attack Scenarios*

There are various kinds of attacks on web server and database server; DoubleGuard approach can capture the following attacks.

1) *Privilege Escalation Attack:* Privilege is permissions given to user, what a user is allowed to do. Another factor is privilege escalation; it means that a user receives privileges they are not denominate to. This privileges can used to detect files, review of personal information, change information and install unwanted programs such as virus. Privilege escalation consists of two types of form.

1. Vertical privilege escalation: It is with less privilege user can used site administrative functions are the vertical privilege escalation.
2. Horizontal privilege escalation: It is when an application permits the attacker to gain access over resources which generally prevented from an application or user.

2) *Hijack Future Session Attack*: These attacks are mainly done on web server site. The attacker firstly takes over the web server and hence hijacks all subsequent legitimate user session to do attack. This attack does not happened by database queries for normal user requests by this attack. Attacker can eavesdrop, delete user requests and can send spoofed replies. A session hijacking attacking can also be the spoofing attack, exfiltration attack, packet drop attack and replay attack.

3) *SQL Injection Attacks:* This attack does not happen on web server, as attacker use vulnerabilities in web server logic to inject the back-end database. This SQL injection attacks gives unauthorized access to database by giving input which consist of malicious code included in to the query, further that query is treated like input, by this attack attacker can modify database.

4) *Direct DB Attack:* It is not impossible for the attacker to bypass the web server as well as firewalls and make connection directly with database. Without sending a web request, an attacker can taken over web server and submit such query from web server without matched the web requests. For such query, web server IDS could detect neither, further if these queries within the set of allowed query IDS itself would not identify it.

5) *Denial of Service Attacks:* The Attacks, which is predetermined attempts to halt legitimate users from accessing a specific network resource.

B. *DoubleGuard Limitations*

1) *Vulnerabilities Because of Improper Input Processing:* Cross-site scripting is one of the attacks in which attacker embed malicious client scripts through legitimate user inputs. In DoubleGuard, all of the user input values are formalized so as to construct a mapping model depend on the structure of HTTP requests and Database queries as the malicious user input are normalized, DoubleGuard could not identify attacks hidden in the values. So, DoubleGuard presents an approach to detect web attacks based on characterization of input values.

2) *Distributed DoS*

DoubleGuard is not developed to decrease DDos attacks. These attacks can also appearing in server architecture that without back-end database.

IV. Various Schemes Used In Implementation Of DoubleGuard System

A. *Intrusion Detection System*

Intrusion Detection System is used to detect attacks against computer systems, networks and against information system. It is very difficult task to provide confirmable secure information system and preserve them in safe state for their entire lifetime and it is for every utilization. Due to the adversity of ensuring that an information system has developed in the computer security field. For a given environment IDS dynamically supervise the action happens in an environment, it decides whether these actions are suggestive of an attack or incorporate legitimate use of the environment.

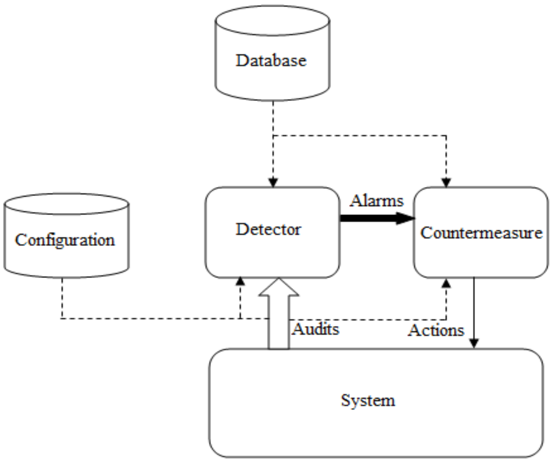

Fig -3: Simple intrusion-detection system

Hence tools Cops and Satan are not IDS, these can be considered as configuration analyzers, even there features worked for detection of intrusions. IDS can be described as detector that processing information approaching from system that is to be prevented. Three types of information can be used by detector first one is the long-term information related to the method which is helped to detect intrusions. Second one is configuration information it is about the current state of the system. Third is audit information that describes events that appear on the system. The main work of detector is that remove unnecessary information from audit trail and represent a synthetic view of the security related actions taken by users based on liability that these actions can be examined symptoms of an intrusion a conclusion is built.

1) Advantages of intrusion detection system:

1.Accuracy: Accuracy of intrusion detection system is based on detection of attack depend on mismatch types and signature. To find out these attacks in multi-tire web application an IDS make use of IDS and database IDS.

2.Easier to deploy: It is easier to deploy because it does not affect existing system or infrastructure.

3.Performance: The performance is based on the rate at which audit events are processed. If performance is good then it can also helps to find out real-time attacks.

4.Timeliness: An IDS performs its analysis as early as possible, so that security officer can take action before much damage has been done and also to protect attacker from defeating the audit source and IDS itself.

2) Limitation of IDS: The limitation of IDS is consists of difficulty of collection of required information on well known attacks and putting it beside with new vulnerabilities and environments. Another one limitation is attacker can do attack directly on back-end database server.

B. GreenSQL

GreenSQL provides a unified, ready to use database security solution for all organization. It offers security to database and acceleration solution this consist of simplified management along with this it provides low maintenance, threat update subscriptions and rewards.

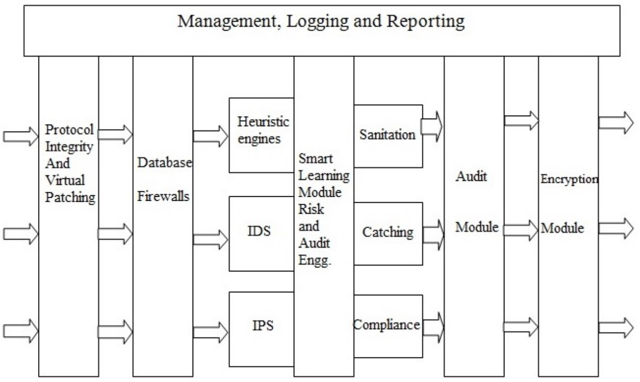
Management, Logging and Reporting
Protocol Integrity And Virtual Patching
Database Firewalls
Heuristic engines
IDS
IPS
Smart Learning Module Risk and Audit Engg.
Sanitation
Catching
Compliance
Audit Module
Encryption Module

Fig -4: Simple GreenSQL Architecture

For implementation of GreenSQL need of devoted hardware, virtualized on database server and application server. GreenSQL is very fast and secure, it can make safe and accelerate any database I less time while it is in learning mode. GreenSQL automatically creates a policy to prepare real time compliance based on usage of database. GreenSQL also can be hides database server and after hiding it will act as proxy server for users. GreenSQL also make use of IDS to detect known as well as unknown attacks. Alerts are generated for every attack on information system, which alerts provided by GreenSQL. It also hides or covers sensitive information from users.

1) Features of GreenSQL:

1.Security: GreenSQL offers security by making use of database firewalls, IPS/IDS and virtual patching. These firewall that are table based or query virtual patching is one of the technique to prevent database application from known or unknown attacks.

2.Auditing: GreenSQL accommodates advanced auditing to MySQL, postgreSQL and MicrosoftSQL databases supplies the option to make a policy based auditing and having a detailed information related with the view or change in database, column or table. Database activity auditing only represent who did, what did and when did. It also supplies view that is after alter and before alter both related with database, column or table.

3.Caching: It offers out of box database catching for procedures and queries, and for supporting MicrosoftSQL, postgreSQL and MySQL. Caching process can be enabled or disabled per entire during installation of GreenSQL or per rule, database, table or even the query.

4.Masking: out of box database masking can be provided by GreenSQL, postgreSQL and MySQL. Masking can be done for covering information like IP, source address, application name, application user and time frame.

2) Limitation of GreenSQL: There is limitation related to GreenSQL like it is unable to detect some kinds of attacks like privilege escalation attack, web server aimed attack, direct DB attack.

V. FUTURE WORK

The main aim is efficiently detection of intrusion to protect multi-tier web application. In future work, the objective is to prevent and detect attacks by using Artificial Intelligence and adds one more level that maintains log. It consists of blacklist that keeps information regarding attacks. In this way, some modification will be do in existing DoubleGuard to increase its reliability, performance in case of static and dynamic web sites both. Finally it will able to expose or detect a wide range of multiple attacks with high accuracy.

VI. CONCLUSION

An Intrusion detection system has creates models of normal behaviour for multi-tier web applications from both front-end web requests and back-end queries. Unlike previous techniques that correlated alerts produce by independent IDS. DoubleGuard and forms a container based IDS with the help of multiple input streams for producing alerts. For anomaly detection correlation of the streams of input supplies a good characterization of system.

Because wider range of attacks can be detect by intrusion sensor with its precise normality model. This achieved due to isolating flow of information from each and every web server session with a light weighted virtualization. For static websites, a well associated model is created to detect various types of attack. And for dynamic website requests, extraction of information and updates to the backend database occurs by using the web server front-end. So, DoubleGuard is able to detect the wide range of multiple attacks with minimal false positive. The number of false positives depends upon the size and coverage of training sessions happened.

References

[1] Meixing Le, Angelos Stavrou, and Brent ByungHoon Kang, “DoubleGuard: Detecting Intrusions in Multitier Web Applications,” IEEE Transactions on Dependable and Secure Computing, Vol. 9, No. 4, July/August 2012.

[2] Marco Cova, Davide Balzarotti, Viktoria Felmetsger, and Giovanni Vigna, “Swaddler: An Approach for the Anomaly-based Detection of State Violations in Web Applications”.

[3] A.S. Gadgikar, “Preventing SQL Injection Attacks Using Negative Tainting Approach,” 2013 IEEE International Conference on Computational Intelligence and Computing Research, 978-1-4799-1597-2/13/$31.00 ©2013 IEEE.

[4] Mihai Christodorescu Somesh Jha, “Static Analysis of Executables to Detect Malicious Patterns”.

[5] Jose Fonseca, Marco Vieira, Henrique Madeira, “Evaluation of Web Security Mechanisms using Vulnerability & Attack Injection,” IEEE Transactions on Dependable and Secure Computing.

[6] Nidhi Srivastav, Rama Krishna Challa, “Novel Intrusion Detection System integrating Layered Framework with Neural Network,” 2013 3rd IEEE International Advance Computing Conference (IACC), 978-1-4673-4529-3/12/$31.00_c 2012 IEEE.

[7] Vahid Aghaei Foroushani A. Nur Zincir-Heywood, “TDFA: Traceback-based Defense against DDoS Flooding Attacks,” 2014 IEEE 28th International Conference on Advanced Information Networking and Applications greensql, http://www.greensql.net/, 2011.

[8] H. Debar, M. Dacier, and A. Wespi, “Towards Taxonomy of Intrusion-Detection Systems,” Computer Networks, vol. 31, no. 9, pp. 805-822, 1999.

[9] Muthu Kumara Raja, Bala Sujitha.T.V, “Intrusion Detection System in Web Services,” International Journal of Science and Research (IJSR), India Online ISSN: 2319-7064, Volume 2 Issue 2, February 2013.

[10] Lwin Khin Shar, Hee Beng Kuan Tan, “Defeating SQL Injection,” Published by the IEEE Computer Society.

[11] Narmadha.S, Deepak Lakshmi Narashima, “Multilayer Intrusion Detection System in Web Application Based Services,” Narmadha.S et al. / International Journal of Engineering and Technology (IJET), Vol 5 No 2 Apr-May 2013.

[12] K.Karthika, K.Sripriyadevi, “To Detect Intrusions in Multitier Web Applications by using Double Guard Approach,” International Journal of Scientific & Engineering Research Volume 4, Issue 1, January-2013 ISSN 2229-5518.

[13] Bogadhi Swetha, A .Kalyan Kumar, “Detection of Intrusion in Multitier Web Application: A Perspective View,” International Journal of Computers Electrical and Advanced Communications Engineering Vol.1 (3), ISSN: 2250-3129.