Volume 3 Issue VI, June 2015
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Detecting Intrusion in Multi –Tier Web Applications Using Double Guard

Stephant Naorem[1], Abhishek Sharma[2]
[1]*M.Tech*, [2]*Assistant Professor*
Department of CSE, Shri Balwant College of Engineering &Technology, Dcrust University

Abstract:-Internet services and applications have increased in both popularity and complexity and such services employ a web server front –end and a back –end. Thus data from web server and database server are prone to be hacked easily which relies to provide more security to web applications..To overcome this issue Double Guard system is used. Intrusion Detection System is used in Double Guard to manages both front end and back end of the multi-tier design and exposes a wide range of attacks with 100% accuracy.
Keywords—DoubleGuard, database server, multi- tier web application, web server

I. INTRODUCTION

Nowadays web services are very much popular in our daily tasks such as as banking, travel, and social networking, are all done via the web. Such services typically employ a webserver front end that runs the application user interface logic as well as a back end server that consists of a database or file server. Due to their ubiquitous use for personal and corporate data, web services have always been the target of attacks. These attacks have recently become more diverse, as attention has shifted from attacking the front end to exploiting vulnerabilities of the web applications in order to corrupt the back end database system. e.g., SQL injection attacks .To protect multi-tiered web services, Intrusion detection systems (IDS) have been widely used to detect known attacks by matching misused traffic patterns or signatures.
Functions of an intrusion detection system are to:

Monitor and analyze the user and system activities.
Analyze system configurations and vulnerabilities.
Assess system and file.
A secured network must have the following three features:

Confidentiality: Only authorized people should be able to access the data that are being transferred through the network. Integrity: The integrity of the data should be maintained starting from its transmission until it is received by the receiver. Availability: The network should be resilient to any kind of attacks.

The three tier architecture is explained bellows:-

A. 1-TIER Web Architecture

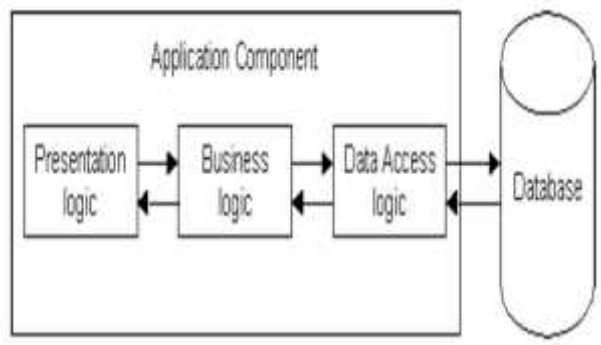


FIG 1- 1-TIER Web Architecture

All 3 layers are on the same machine
All code and processing kept on a single machine

Volume 3 Issue VI, June 2015
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Presentation, Logic, Data layers are tightly connected
Scalability: Single processor means hard to increase volume of processing
Portability: Moving to a new machine may mean rewriting everything
Maintenance: Changing one layer requires changing other layers

B. 2-TIER Web Architecture

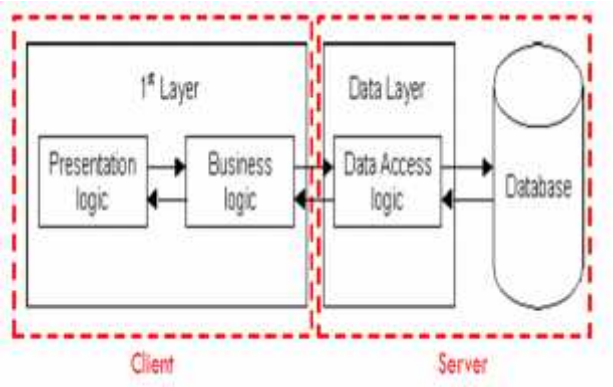


Fig-2 2-TIER Web Architecture

Database runs on Server
Separated from client
Easy to switch to a different database
Presentation and logic layers still tightly connected
Heavy load on server
Potential congestion on network
Presentation still tied to business logic

C. 3 TIER Web Architecture

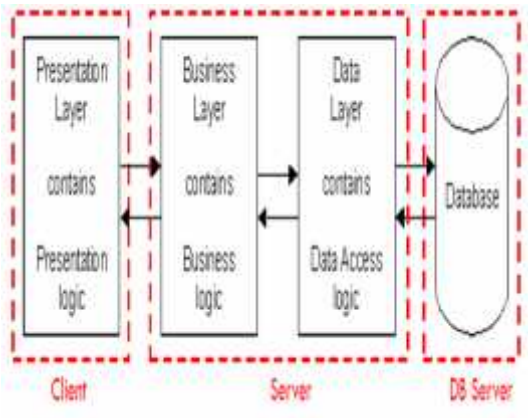


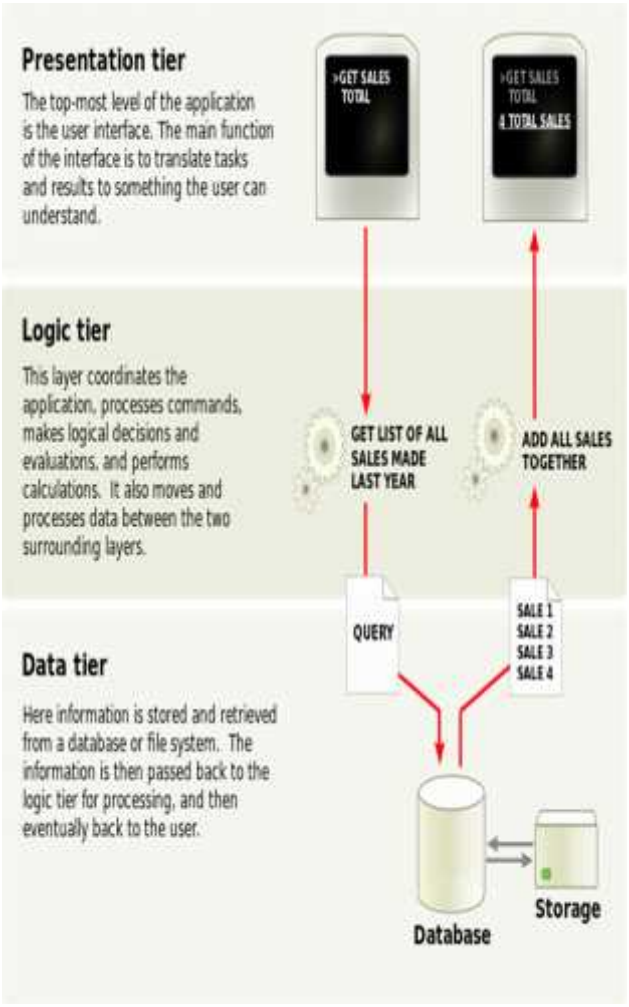
Fig-3 3 TIER Web Architecture

Each layer can potentially run on a different machine

Presentation, logic, data layers disconnected

Volume 3 Issue VI, June 2015
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

A Typical 3 Tier Architecture



II. INTRUSION DETECTION SYSTEM

Intrusion Detection System is a device or software napplication that monitors network and/or system activities for malicious activities or policy violations and produces reports to a Management Station

Limitation - Detecting newly published attacks or variants of existing attacks.

A. Double Guard

DoubleGuard is a system used to detect attacks in multi-tiered web services. This approach can create normality models of isolated user sessions that include both the web front-end (HTTP) and back-end (File or SQL) network transactions. There are two types of network Intrusion Detection System namely: Anomaly Detection and Misuse Detection. Anomaly detection tries to identify new attacks by analyzing strange behaviors in the network. To make this possible, it first has to ``learn" how the traffic in the network works and later try to identify different patterns to then send some kind of alert to the sensor or console. IDS made using this model have higher tendency for raising false alarm, as they often suspicious about all network behavior irrespective of malicious or legitimate.

The misuse or signature-based is the most-used IDS model. Signatures are patterns that identify attacks by checking various options in the packet, like source address, destination address, source and destination ports, flags, payload and other options. The collection of these signatures composes a knowledge base that is used by the IDS to compare all packet options that pass by and check if they match a known pattern.

B. Existing System

An IDS examines network packets individually within both the web server and database system.

The back end database server is often protected behind a firewall while the web servers are remotely accessible over the

internet.
The back ends are susceptible to attacks that use web requests as a mean to exploit back end.

C. Proposed System
Double Guard is a system used to detect attacks in multi –tiered web applications

This approach can create normality models of isolated user sessions that include both the web front-end (HTTP) and back-end (File or SQL) network transactions.

It will employ a technique to assign each user's web session to a dedicated container which is isolated virtual computing environment.We use the container ID to accurately associate the web request with the subsequent DB queries .Thus it can build a casual mapping profile by taking the web server and DB traffic into account.

III. SYSTEM ARCHITECTURE

The concept of Double Guard is based on to making request coming to server Isolated from each other. This architecture will increase system security by mapping all requests coming to server to set of Database query. Double Guard can be apply to at that first point of contact to web server and at last point of contact of web server just before touching to Database layer.

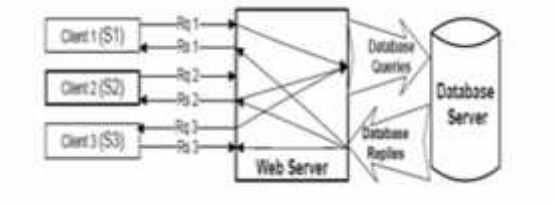


Fig 3.1 classic 3 tier model

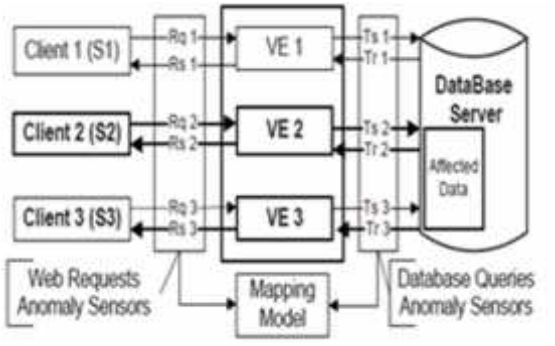
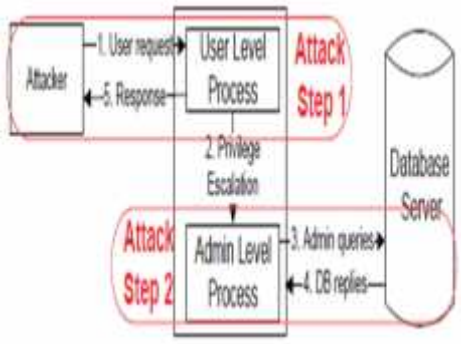


Fig 3.2 webserver instances running in containers

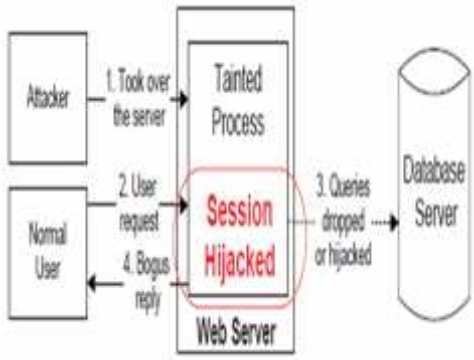
A. Attack Scenarios
DoubleGuard Intrusion Detection System is effective at capturing the following types of attacks:
1) Privilege Escalation Attack



Volume 3 Issue VI, June 2015
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

It shows how a normal user may use admin queries to obtain privileged information.
Now suppose that an attacker logs into the web server as a normal user, upgrades his/her privileges, and triggers admi queries so as to obtain an administrator's data. This attack can never be detected by either the web server IDS or the database IDS.

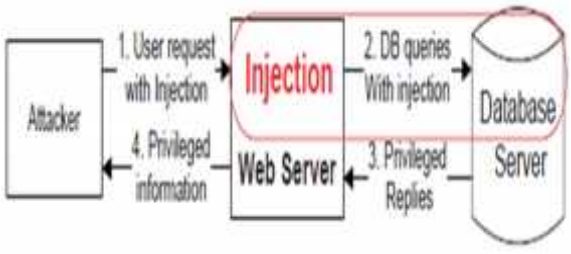
2) Hijack Future Session Attack



A. It illustrates a scenario wherein a compromised web server can harm all the Hijack Future Sessions by not generating any DB queries for normal user requests.
B. This class of attacks is mainly aimed at the web server side.
C. An attacker usually takes over the web server and therefore hijacks all subsequent legitimate user sessions to launch attacks.

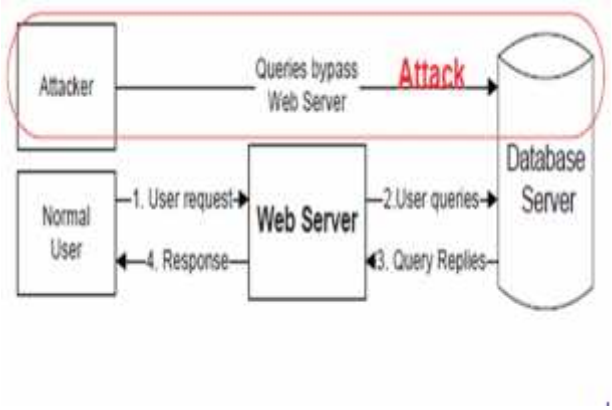
For instance, by hijacking other user sessions, the attacker can eavesdrop, send spoofed replies, and/or drop user requests.

3) Injection Attack



Attacks such as SQL injection do not require compromising the web server. Attackers can use existing vulnerabilities in the web server logic to inject the data or string content that contains the exploits and then use the web server to relay these exploits to attack the back-end database

4) Direct DB Attack



A. It illustrates the scenario wherein an attacker bypasses the web server to directly query the database.

B. An attacker could also have already taken over the web server and be submitting such queries from the web server without sending web requests.

C. Without matched web requests for such queries, a web server IDS could detect neither.

D. Furthermore, if these DB queries were within the set of allowed queries, then the database IDS itself would not detect it either. However, this type of attack can be caught with Double Guard approach

1V. MODELING DETERMINISTIC MAPPING PATTERNS

A. Deterministic Mapping

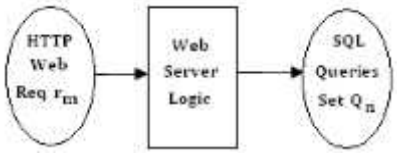


Fig a : Deterministic Mapping Scenario.

This is the most common and perfectly matched patterm . That is to say that web request rm appears in all traffic with the SQL queries set Qn. For any session in the testing phase with the request rm, the absence of a query set Qn matching the request indicates a possible intrusion. On the other hand, if Qn is present in the session traffic without the corresponding rm, this may also be the sign of an intrusion.

B. Empty Query Set

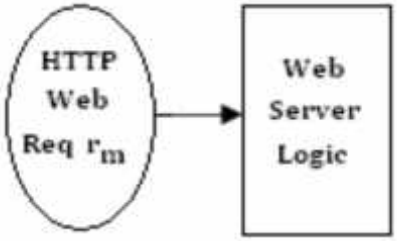


Fig b : Empty Query Set Scenario.

In special cases, the SQL query set may be the empty set.This implies that the web request neither causes nor generates any database queries. For example, when a web request for retrieving an image GIF file from the same webserver is made, a mapping relationship does not exist because only the web requests are observed. During the testing phase, we keep these web requests together in the set EQS.

C. No Matched Request

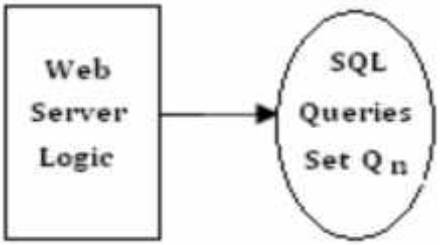


Fig c : No Matched Request Scenario.

Unmatched queries in a set NMR are kept. During the testing phase, any query within set NMR is considered legitimate.

D. Non-deterministic Mapping

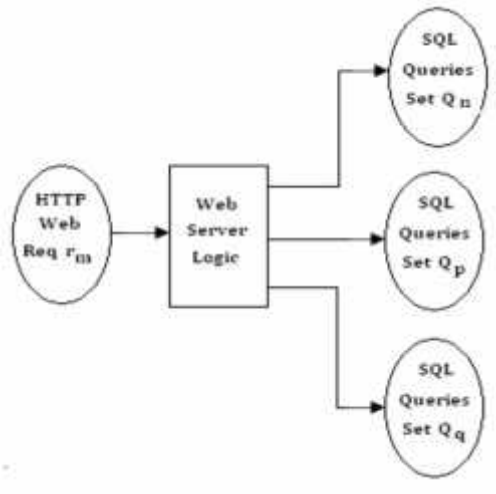


Fig- d Non-deterministic Mapping Scenario.

E. DoubleGuard Limitations

1) Vulnerabilities Due to Improper Input Processing :Once the malicious user inputs are normalized, DoubleGuard cannot detect attacks hidden in the values.
2) Possibility Of Evading Double Guard :It is possible for an attacker to discover the mapping patterns by doing code analysis or reverse engineering, and issue "expected" web requests prior to performing malicious database queries.
3) Distributed DoS : DoubleGuard is not designed to mitigate DDoS attacks. These attacks can also occur in the server architecture without the back-end database.

V. CONCLUSION

In this topic we presented an intrusion detection system that builds models of normal behavior for multi tiered web applications from both front-end web (HTTP) requests and back-end database (SQL) queries.Double Guard form a container IDS with multiple streams to produce alerts.Correlation of different data streams provide s a better characterization of the system for anolamy detection.

REFERENCES

[1] Anley. (2002) "Advanced Sql Injection in Sql Server Applications," technical report, Next Generation Security Software, Ltd.,
[2] Meixing Le, AngelosStavrou, Brent ByungHoon Kang," Double Guard: Detecting Intrusions in Multitier Web Applications", IEEE Transactions on dependable and secure computing, vol. 9, no. 4, July/august 2012.
[3] Barry B.I.A. and H.A. Chan (2009). "Syntax, and Semantics-Based Signature Database for Hybrid Intrusion Detection Systems," Security and Comm. Networks, vol. 2, no. 6, pp. 457-475.
[4] Christodorescu M and Jha S (2003) "Static Analysis of Executables to Detect MaliciousPatterns," Proc. Conf. USENIX Security Symp.
[5] Cova M, Balzarotti D, Felmetsger V, and Vigna G(2007) "Swaddler:An Approach for the Anomaly-Based Detection of State Violations in Web Applications," Proc. Int'l Symp. Recent Advances in Intrusion Detection (RAID '07).
[6] Felmetsger, L. Cavedon, C. Kruegel, and G. Vigna, "Toward Automated Detection of Logic Vulnerabilities in Web Applications," Proc. USENIX Security Symp., 2010.
[7] Felmetsger, L. Cavedon, C. Kruegel, and G.Vigna, "Toward Automated Detection of Logic Vulnerabilities in Web Applications," Proc.USENIX Security Symp., 2010.
[8] T. Pietraszek and C.V. Berghe, "Defending against Injection Attacks through Context-Sensitive String Evaluation," Proc. Int"l Symp.Recent Advances in Intrusion Detection (RAID "05), 2005.