ISSN 2395-1621

An Analytical Study For Two Way Protection Of Web Services

Mayuri Dugane[#1], Anjali Gore[#2], Suman Sahu[#3], Snehal Londhe[#4]

[1]mdugane203@gmail.com

[2]anjali.gore2@gmail.com

[3]suman.sahu0707@gmail.com

[4]snehalondhe18@gmail.com

[#1234] Dept. of Computer Engineering,

Padmashree Dr. D. Y.Patil Institute of Engineering & Technology College,
University of Pune, Maharashtra, India.

ABSTRACT

Internet services and web applications are intricate as a part and parcel of our life, enabling communication and management of personal information from anywhere .The data from web server and database server are prone to be hacked in the absence of IDS system. Before the concept of IDS the firewall program was used for security purpose. Slower processes, inefficient algorithm and degradable system performance were in light. In case of an attack in which an attacker logs into the web server as a regular user, and access admin queries so as to obtain an administrator's data. The IDS system is unable to detect this attack .A detection technique in which the admin privileges would be more secure and have another method to access it than the normal technique. The static model building algorithm is another way to overcome this disadvantage. The MD5 algorithm is the method followed in this paper which helps in maintaining integrity of files and security related applications .Light weight virtualization technique is the major benefit of IDS system.

ARTICLE INFO

Article History

Received :21st February, 2015

Received in revised form :

25th February, 2015

Accepted :2nd March, 2015

Published online :

5th March 2015

Keywords— DOS attack , SQL injection ,intrusion, detection.

I. INTRODUCTION

The Internet has played a vital role in this fast growing world because consumers use the Internet to shop, bank, entertain, and invest online. The handy mobile devices (smart phones, sensors) give a boost to the use of internet. GSM, GPRS, Wi-Fi connectivity is the heart of today's lifestyle. The e-commerce network is on full crease with lots of sites making customer friendly services and activities. This growing reliance on internet is increasing the potential damage by VARIOUS ATTACKS on the network. Increase in number of complexity in the applications leads to increased number of vulnerabilities. Day by day the attacks are becoming more severe as its exploiting the back end by SQL attacks and corrupting the whole system. The attack on backend is more crucial to handle than that of the front end. Confidentiality and integrity will be devalued if security issues are not implanted.

However,, there is small work performed on multi-tiered Anomaly Detection (AD) systems which generate network behaviour models for both web and database network interactions. In some multi-tiered ARCHITECTURE, the web servers are remotely accessible over Internet but the back-end database server is always protected behind a firewall.

The back-end systems are susceptible to attacks that use web requests as a way to exploit the back-end. Integrity Guard combines several highly sophisticated digital security mechanisms that also covers whole classes of potential attacks. Integrity Guard achieves many goals at a time: Digital security measures enables new design and test methods that lead to thorough security systems. But it cannot be implemented effectively in all software's .To protect multi-tiered web services,(IDS) have been widely used to detect known attacks by matching misused signatures.

The IDS system would be implemented in the attack scenarios like privilege escalation attack, hijack future session attack, direct database attack, AND INJECTION attack. If we come across a situation in which a regular user is logged in the system and he triggers admin queries which violates the admin rights .Here the admin data is not safe and the situation needs to be handled by IDS system .The system would not be able to distinguish between the normal user and the culprit. Another case in which the web server is attacked by any hacker which controls the future sessions of the SERVER, THE data may be misused any bluff message can be passed which may lead to huge losses. All the request send by the client will be responded in an unconventional way leading a corrupt network .The direct database attack illustrates the scenario wherein an attacker bypasses the web server to directly query the database .In this the source itself is been hacked

II. Literature Survey

Growing internet use leads to make a more secure network .The vulnerabilities which may make the system corrupt or risk on user privileges and confidential data need to be handled by a model proposed as IDS..

The author N.Jaisankar1 [1] describes the mobile agent paradigm , in which mobile agents communicate with their own environment and other agents according to their own volition. User activity and program operations are handled in this paper. Security principles like agent privacy and integrity, agent and server authentication ,authorization and access control ,metering, charging and payment mechanisms are followed. The eye catching colour mechanism is used where if the user access unauthorized application the simulation changes from green to red detecting intrusion in the system. Moreover, an agent system must provide functions to capture agent state and only few languages allow externalizing the state at such a high level. Thus further enhancements are needed in [1].

K. karthika [2] narrates a technique of detecting wide range of threats and reducing false positives .Also it has specified the detection accuracy when we tried to model static and dynamic web requests with the back-end file system and database queries. For static websites, we built awell-correlated model, which proved to be effective at detecting different attacks. This technique is true for dynamic requests where both information retrieval and updates to the back-end database occur using the web server which is front end. When our prototype is deployed on a system that employed Apache server, and a MySQL back end ,a blog application. This Double Guard was identifying a wide range of attacks with minimal false positives. For that a large number of parallel running Apache instances should be maintained similar to apache threads that server would maintain in Scenario without containers. If a session is timed out, the apache instance should be terminated along with its container.

Shyam in [3] proposes a method in which a normal multitier application of frontend and backend correlation is build with individual intrusion detection system. but dual protection which will allowed multiple input requests to produce alert.
The implementation will be by using the virtulization technique where the information flow and session requests would be isolated.The sequence of activities performed are user control, session monitoring ,mapping HTTP queries with SQL queries ,showing attack log takes place in the model. But practically such a casual mapping between web server traffic and database server traffic is not possible since it is not attributed to user sessions.

Binal Patel[4] introduces an idea of password guessing attack algorithm. In this idea, for each possible shift of pattern (P) relative to text (T) the brute-force pattern matching algorithm compares the pattern P with the text T, until either a match is found, or all placements of the pattern are tried. But it not able to capture the screen of Web Application at client machine and pass to admin record so that Admin can take decision about the user process. This should be in very secure manner using more complex concept and should be used some more new recent technique so that other hacking can be also prevent.

By extending the general IDS system, the concept of Virtual Guard was described in [5]. This is achieved by isolating the flow of information from each web server session with a lightweight virtualization. It forms container based IDS with multiple input streams to produce alerts. Here the containers are recycled based on events or when sessions time out, which requires storage and memory management

III. Proposed Methodology

The proposed system assumes that both database server, web server are vulnerable to various attacks such as privilege escalation attack, hijack future session attack, Injection attack. The three attack scenarios are described below-

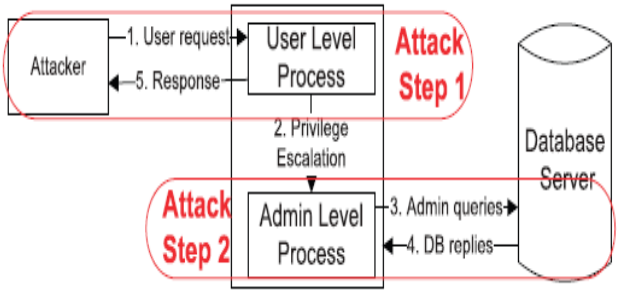

Fig. 1 – Illustrates privilege escalation attack

In this attack the user escalates its privilileges to admin level and causes misuse to admin data.

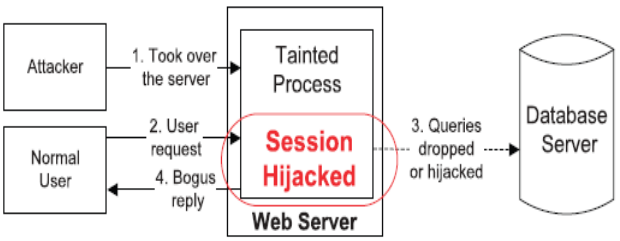

Fig. 2 – Illustrates Hijack Future Session Attack

Fig 2.deccribes the attack in which control over the server is taken by attacker and then through this hijacked session it communicates to the server.Thus getting fake reply.

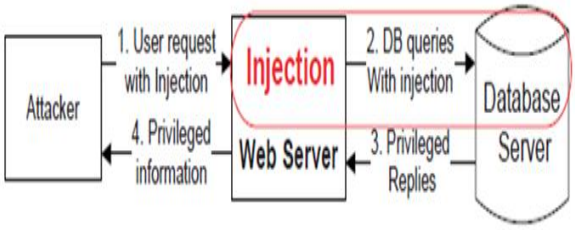

Fig. 3 – Illustrates Injection Attack

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.

Thus through this concept we can detect intrusions and create a secure network

IV. Conclusion

The increased use of smaller and costless wireless devices has simultaneously increased the vulnerabilities in unsupervised and hostile environment. [2] Narrates a distributed intrusion detection system that can protect the system from frontend as well as backend attacks. In this paper we built a prototype web application to test the mechanisms to protect the complete web application both at server side and database side. The IDS sensors can detect wide range of attacks and prevent them. We built a model to correlate HTTP request to corresponding SQL commands to be executed in database server

References

[1] N.Jaisankar1, Intelligent Intrusion Detection System Framework Using Mobile Agent.

[2] K .Karthika, To Detect Intrusions in Multitier Web Applications by using Double Guard Approach.

[3] Shyam A Gade, Front End and Back End Database Protection from Intruders in Distributed Web Application

[4] Binal M. Patel ,Intrusions Detection in Three tier Web Applications using Double Guard System

[5]Ajinkya Nikam Virtual Guard: Intrusion Detection System on Static and Dynamic Web Applications

