International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 1, 2017 ISSN: 2348-6600
Reference ID: IJCS-160 PAGE NO: 968-973
Sri Vasavi College, Erode Self-Finance Wing 3rd February 2017
National Conference on Computer and Communication NCCC'17
http://www.srivasavi.ac.in/ nccc2017@gmail.com

DOUBLEGUARD: DETECTING INTRUSIONS IN MULTI-TIER WEB APPLICATIONS

N.Saranya, M.Phil Scholar,
Mrs. A. Lavanya, Assistant Professor, Department of Computer science
Sri Vasavi College [Self Finance], Bharathiar University, Erode-638 316, India.
saranyanalls@gmail.com

ABSTRACT

Network attacks are increased in number and severity over the past few years, intrusion detection system (IDS) is increasingly becoming a critical component to secure the network. Intrusion detection is the process of monitoring and analyzing the events occurring in a computer system in order to detect signs of security problems. Intrusion Detection Systems has the additional job of triggering alarms toward this security problem and some of it automated in the role of triggering or doing an action on behalf of the network administrator. The goal of intrusion detection system (IDS) is to provide another layer of defense against malicious (or unauthorized) uses of computer systems by sensing a misuse or a breach of a security policy and alerting operators to an ongoing attack.

Keywords: Intrusion Detection System, Anomaly Detection, Web Server, Attacks, SQLIA, Classification of SQLIA.

1. INTRODUCTION

DoubleGuard, techniques is IDS system that models are the network behavior of user sessions across both the front-end web server and the back-end database. By monitoring both web and subsequent database requests, it's able to ferret out attacks that independent IDS would not be able to identify. Implement the Double Guard using an Apache web server with MySQL and lightweight virtualization.

Then collected and processed real-world traffic over a 15-day period of system deployment in both dynamic and static web applications. Double Guard is able to expose a wide range of attacks with 100% accuracy while maintaining 0% false positives for static web services and 0.6% false positives for dynamic web services.

2. RELATED WORKS

The attacker's objective for using the injection technique is lies in gaining control over the application database. In a web based application environment, most of the web based applications, social web sites, banking websites, online shopping

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 1, 2017 ISSN: 2348-6600
Reference ID: IJCS-160 PAGE NO: 968-973
Sri Vasavi College, Erode Self-Finance Wing 3rd February 2017
National Conference on Computer and Communication NCCC'17
http://www.srivasavi.ac.in/ nccc2017@gmail.com

websites works on the principle of single entry point authentication which requires user identity and password. A user is identified by the system based on his identity. This process of validation based on user name and password, is referred as authentication. Web architecture is general entry point authentication process. In general client send a HTTP request to the web server and web server in turn send it to the database layer. Database end contains relational tables so queries will be proceeding and result will be send to the web server. So entire process is database driven and each database contains many tables that are why SQLIA can be easily possible at this level. SQL Injection is a basic attack used for mainly two intentions: first to gain unauthorized access to a database and second to retrieve information from database. Function based SQL Injection attacks are most important to notice because these attacks do not require knowledge of the application and can be easily automated.

Databases always contain more valuable information; they should receive the highest level of protection. Therefore, significant research efforts have been made on database IDS, and database firewalls. These software's, such as Green SQL work as a reverse proxy for database connections. Instead of connecting to a database server, web applications will first connect to a database firewall. SQL queries are analyzed; if they're deemed safe, they are then forwarded to the back-end database server. The system proposed in composes both web IDS and database IDS to achieve more accurate detection, and it also uses a reverse HTTP proxy to maintain a reduced level of service in the presence of false positives. However, found that certain types of attack utilize normal traffics and cannot be detected by either the web IDS or the database IDS. In such cases, there would be no alerts to correlate. Analyzing only network traffic that reaches the web server and database. assume that no attack would occur during the training phase and model building.

3. MODELING OF DYNAMIC PATTERNS

In contrast to static web pages, dynamic web pages allow users to generate the same web query with different parameters. Additionally, dynamic pages often use POST rather than GET methods to commit user inputs. Based on the web server's application logic, different inputs would cause different database queries. For example, to post a comment to a blog article, the web server would first query the database to see the existing comments. If the user's comment differs from previous comments, then the web server would automatically generate a set of new queries to insert the new post into the back-end database. Otherwise, the web server would reject the input in order to prevent duplicated comments from being posted (i.e., no corresponding SQL query would be issued.) In such cases, even assigning the same

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 1, 2017 ISSN: 2348-6600
Reference ID: IJCS-160 PAGE NO: 968-973
Sri Vasavi College, Erode Self-Finance Wing 3rd February 2017
National Conference on Computer and Communication NCCC'17
http://www.srivasavi.ac.in/ nccc2017@gmail.com

parameter values would cause different set of queries, depending on the previous state of the website. Likewise, this non-deterministic mapping case (i.e., one-to-many mapping) happens even after we normalize all parameter values to extract the structures of the web requests and queries. Since the mapping can appear differently in different cases, it becomes difficult to identify the entire one to-many mapping patterns for each web request.

Moreover, when different operations occasionally overlap at their possible query set, it becomes even harder for us to extract the one to- many mapping for each operation by comparing matched requests and queries across the sessions.

4. INTRUSION DETECTION MODULE

In this module, Intruder is detected and his activities have been noted. Generally, using the information about the capture time of each packet, last sent packet and its length can be identified. So analyzing this overall information an intruder can be detected.

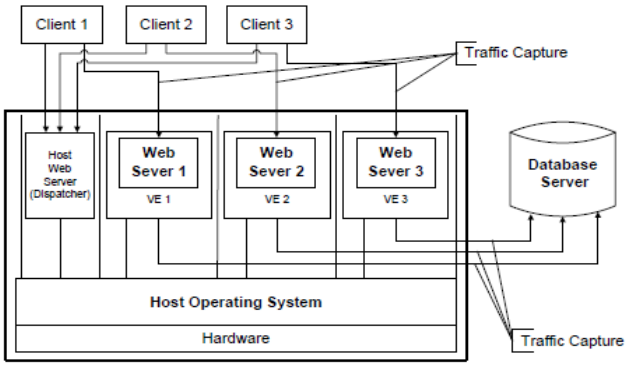

Figure: The overall architecture of our prototype

Usually an intruder login and does all his activities. This is stored in the database and can be used to detect the abnormal usage. Subsequent request can be noted and an intruder can be identified. Based on the usage, an Network layer is depicted.

5. DOUBLE GUARD TECHNIQUE

1. Double guard provides high security since the usage of session for each subsequent web request. A session is dedicated to container which refer to the disposable server and a container ID is provided for each client.

2. If any one session is attacked by intruder, others remain unaffected.

It is very useful to identify attacks like session-hijacking, SQL injection attack etc.

3. It not only provides security but also provides isolated information flow.

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 1, 2017 ISSN: 2348-6600
Reference ID: IJCS-160 PAGE NO: 968-973
Sri Vasavi College, Erode Self-Finance Wing 3rd February 2017
National Conference on Computer and Communication NCCC'17
http://www.srivasavi.ac.in/ nccc2017@gmail.com

4. It does not depend on time basis and hence provide a complete secure system. It provides an alert system which operates on multiple feeds of input.

5. It does not require any input validation as it looks for the structure of request not on the input parameter.

SQLIA is a server type of web vulnerability, which impacts badly on web applications. In this section, a novel model for SQLIA prevention is proposed. As mentioned in previous section, several models are proposed for prevention of SQLIA, but they are not applicable for all type of injection attacks. SQLIA prevention via double authentication through tokenization is an approach to control SQLIA.

In this paper, propose a new model names as Double Guard. In this model the system will identify the input. The input may be of two types it may be a request for certain service or information and it may be accepted or rejected by the system, and another one is Query which is generated to find out some specific information

If the query is syntactically correct it will display information, even then none of that type of information store in database it will display this information also the system store.

6. CHALLENGES

Intrusion detection systems aim at detecting attacks against computer systems and networks or in general, against information systems. Building IDS is a complex task of knowledge engineering that requires an elaborate infrastructure. There are various challenges that IDS faced today and which need to concentrate while building IDS.

7. CONCLUSION

In this paper, presented an intrusion detection system that builds models of normal behavior for multitier web applications from both front-end web (HTTP) requests and back-end database (SQL) queries. In the previous approach used independent IDS to provide alerts unlike. Double Guard which forms container-based IDS with multiple input streams to produce alerts, such correlation of input streams provides a better characterization of the system for anomaly detection because the intrusion sensor has a more precise normality model that detects a wider range of threats.

This flow of information from each web server session is lightweight virtualization. Furthermore, Quantified the detection accuracy of our approach when attempted to model static and dynamic web requests with the back-end file system and database queries. To built a well-correlated model for static websites, which our experiments proved to be effective at detecting different types of attacks. It also showed that this held true for dynamic requests where both retrieval of information and updates to the back-end database occur using the

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 1, 2017 ISSN: 2348-6600
Reference ID: IJCS-160 PAGE NO: 968-973
Sri Vasavi College, Erode Self-Finance Wing 3rd February 2017
National Conference on Computer and Communication NCCC'17
http://www.srivasavi.ac.in/ nccc2017@gmail.com

web server front end. When deployed our prototype on a system that employed Apache web server, a blog application, and a MySQL back end, Double Guard was able to identify a wide range of attacks with minimal false positives which depended on the size and coverage of the training sessions is used. In this project use TDT4 method to provide effective summarization methods to extract the core parts of detected topics, as well as graphic representation methods to depict the relationships between the core parts. Applied together, the two techniques, called topic anatomy, can summarize essential information about a topic in a structured manner. When the Future can retrieve information from scan by using our voice instead of typing text. The user can search through voice; the system will recognize this voice and provide essential information about a topic.

REFERENCES

[1]R. Ezumalai, G. Aghila, "Combinatorial Approach for Preventing SQL Injection Attacks", 2009 IEEE International Advance Computing Conference (IACC 2009) Patiala, India, 6-7 March 2009.

[2] Asha. N, M. Varun Kumar, Vaidhyanathan. G of Anomaly Based Character Distribution Models in th,"Preventing SQL Injection Attacks", International Journal of Computer Applications (0975 – 8887) Volume 52– No.13, August 2012

[3] Yuji Kosuga, Kenji Kono, Miyuki Hanaoka, Hiyoshi Kohoku-ku, Yokohama, Miho Hishiyama, Yu Takahama, Kaigan Minato-ku, "Sania: Syntactic and Semantic Analysis for Automated Testing against SQL Injection" 23rd Annual Computer Security Applications Conference, 2007, 1063-9527/07, 2007 IEEE

[4] Prof (Dr.) Sushila, MadanSupriyaMadan, "Shielding Against SQL Injection Attacks Using ADMIRE Model", 2009 First International Conference on Computational Intelligence, Communication Systems and Networks, 978-0-7695-3743-6/09 2009 IEEE

[5] A S Yeole, B BMeshram, "Analysis of Different Technique for Detection of SQL Injection", International Conference and Workshop on Emerging Trends in Technology (ICWET 2011) – TCET, Mumbai, India, ICWET"11, February 25–26, 2011, Mumbai, Maharashtra, India. 2011 ACM.

[6] Ke Wei, M. Muthuprasanna, Suraj Kothari, "Preventing SQL Injection Attacks in Stored Procedures".Proceedings of the 2006 Australian Software Engineering Conference

[7] Debasish Das, Utpal Sharma, D. K. Bhattacharyya, "Rule based Detection of SQL Injection Attack", International Journal of Computer Applications (0975 – 8887) Volume 43– No.19, April 2012. [17] NTAGW ABIRA Lambert, KANG Song Lin, "Use of Query

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 1, 2017 ISSN: 2348-6600
Reference ID: IJCS-160 PAGE NO: 968-973
Sri Vasavi College, Erode Self-Finance Wing 3rd February 2017
National Conference on Computer and Communication NCCC'17
http://www.srivasavi.ac.in/ nccc2017@gmail.com

Tokenization to detect and prevent SQL Injection Attacks.

[8] Kai-Xiang Zhang, Chia-Jun Lin, Shih-Jen Chen, Yanling Hwang, Hao-Lun Huang, and Fu-Hau Hsu, "TransSQL: A Translation and Validation-based Solution for SQL-Injection Attacks", First International Conference on Robot, Vision and Signal Processing, IEEE, 2011.