International Journal of Recent Advances in Multidisciplinary Topics
Volume 2, Issue 3, March 2021
https://www.ijramt.com | ISSN (Online): 2582-7839

Intrusion Detection Using Double Guard System

S. Rithik Kumar[1*], B. Vignesh Jawahar[2], M. Vijaya Kumar[3], S. R. Janani[4]
[1,2,3,4]*Department of Computer Science and Engineering, SNS College of Technology, Coimbatore, India*

***Abstract*: In today's world we have many issues in internet security and privacy. We use internet in travelling, social media, banking, study etc. But we often face the problems with the privacy of the network system. To accommodate this increase in applications and data complexity, web services have introduced the multi-tiered design in which the web server runs the application front-end logic and as well as data is updated to database or file server. IDS plays a vital role in computer security technique. But it also has its own limitations. To overcome those limitations Double guard technique is introduced. We implemented double guard using IIS (internet information and service manager), with the software's such as SQL Server, Visual Studio, .NET and programming language Java Script. This project presents Double Guard, an IDS system that describes the network behavior of user sessions across both the front-end web server and the back-end database. By handling both web and subsequent database requests, it is possible to prevent the attacks that an independent IDS couldn't. Along with this we use Virtual Split Memory that separates code and data into different memory spaces. Finally, this system will detect intrusions in multi -tier applications and prevent it, enhancing the internet security and privacy.**

***Keywords*: IDS, Double guard system, IIS, Web server.**

1. Introduction

In few years, web applications and web services has reached to an extent of being used and also getting more complicated in maintaining and manipulating. Qusay I. Sarhan and Idrees S. Gawdan [15] Web Applications and Web Services, a Comparative Study nowadays banking, travel, social networking, and online shopping is being depending upon web. According to Nicholas Gallinelli, front end and back end development [11] the architecture is divided as front end and back end, where front end is called as user interface and back end is called as database server which deals with data storing, manipulating and retrieving it. Personnel and corporate data have been targeted by hackers(attackers) as its importance and its need is highly valued. According to Daljit Kaur and Parminder Kaur Dr. Empirical Analysis of Web Attacks [2] data attacks have become very common nowadays, also the intention of the hackers also changed from attacking the front end to back end that means accessing the background data. For example, Bank details. J. Jabez and B. Muthukumar Dr. Intrusions Detection System(IDS)[7] our IDS system looks after both user end(front end) and also back end (database server). Intrusion detection system is used to identify attacks by comparing patterns that were misused and also signatures to protect multi-tier web application. The IDS methods has the capability of identifying the attacks by using machine learning, comparing the current abnormal network traffic behaviour with the previous network behaviour phase. Leixing Le, Angelos Stavrou, Brent Byung Hoon Kang [8] explains about double guard IDS system in brief.

2. Literature Survey

In detecting of intrusions and online malicious data hijacking multiple methods and approaches are applied like Abnormal detection and misuse detection. M. Christodorescu and S. Jha [9] explains about the static analysis of executables to detect malicious pattern. G. Kim, S. Lee, S Kim [5] in relation to analytical methods, the Intrusion Detection System can be categorized into two Abnormal Detection, and the other is Misuse Detection or Signature Detection.

1) Anomaly detection

According to Przemyslaw Berezinski, Bartosz and Marcin Szpyrka [13] Anomaly systems acclimate the opposite approach, to find what is normal, and then know the divergent from the normal behavior. These deviations are examined as anomalies or possible intrusions. Yunlu Gong, Shingo Mabu, Ci Chen [19], illustrates about misuse detection using genetic network programming. T. Kanungo, DM Mount [17] tells about the efficient k-means clustering algorithm analysis and implementation.

2) Misuse detection

Misuse detection systems applies preceding knowledge on attacks to glance on any attacks traces. Ozgur Depren, Murat Topallar, Emin Anarim, M. Kemal Ciliz [12] by identifying the misuse they detect intrusions. Yunlu Gong, Shingo Mabu, Ci Chen [19] develops the misuse detection using genetic network programming. It tells about networking. The example for this detection is signature rule. In signature detection, attack signatures are desired in the monitored source.

3) Clustering

In anomaly detection and misuse detection clustering

*Corresponding author: rithikkumar611@gmail.com

methods can be applied. According to Ravi Ranjan and G. Sahoo Arranging the clusters in ascending order to largest clusters according to their distances. T. Kanungo [6], DM Mount tells about efficient k-means clustering algorithm analysis and implementation. H. Shah, J. undercoffer, A. Joshi [6] illustrates about fuzzy clustering for intrusion detection. Mohammed Shojafar, Rahim Taheri and Zahra pooranian [10] the clusters which have maximum numbers of instances which are presented in largest one are marked as normal. Shi na, Liu Xumin and Guan Yong [16] choose the first K1 clusters so that the number of instances in these sum up to 1/4'N, and mark them as normal, where 'called as normal instances. Mark other clusters as malicious. As clustering is done heuristics are used to mark up each other clusters as malicious or normal. Youguo li and Haiyan wu [20] illustrates about the clustering method based on k-means algorithm. To encounter attacks in test data sets self-labeled detection clustering is used.

4) Intrusion Detection System Based on Improved K-means Clustering: Algorithm

Here we use K-Algorithm in which complexity and dependency is denoted in algorithm as K. The Improved form of algorithm is clustering algorithm which the above one puts forward. A. Likas, N. Vlassis, J. J. Verbeek [1] explains about Data classifications accuracy is improved a lot by this algorithm which experiment shows and detection performance importantly. Maximum number of attack detection is done and efficiency is good by this algorithm.

3. Proposed Methodology

To overcome the above limitations, we use the method called Virtual Split Memory. Subsequently, data injection is the process of inducing attack codes.

1) Virtual split memory

Virtual split memory describes about the translation of virtual address into physical address and stores to the main memory. Here the cache memories are directed to the secondary memory.

2) Privilege escalation attack

Privilege escalation attacks exploit defects and security subjection with the point to elevating access to a network, applications, and complimentary systems. The types of attacks are horizontal and vertical privilege escalation attack. Vertical escalation attacks in which hackers perform process as the motive which are similar to users. Horizontal attacks get access to accounts with less allowance needed an escalation of privileges, admin execution process.

3) Hijack future session attack

This attack attempted by the middle person/attacker. Username and password are accessed by the third person without the knowledge of user and misuse them. But in my double guard technique this type of attack is not possible. End-to-end encryption is made between user's browser and web server using secure HTTP or SSL. VPN can also be used for making end-to-end encryption. So using this technique we can prevent this kind of attack.

4) SQL injection attack

In spite of accessing user session, the attacker directly contacts with web server to attain the username and password pair of any normal user to exploit the back end database. This type of attacks can be prevented by validating user data or input, safe guard the data by using special types of symbols. Force the statements and parameterization, induce stored data algorithm in database, actively organize patches and packs. Imply virtual or physical firewall, use strong OS and application, imply pertinent privileges and strict access.

5) Session fixation attack

In session fixation attack, the attackers try to take the ID of a victim's session after the user login's. The attackers will already attain the valid session and tries to enforce the victim to use that certain sessions for his/her purposes. It can be avoided through regenerating the session ID at authentication, allow only server generated session ID's, replace the session ID's, imply strong logout function.

4. Conclusion

To overcome the limitations of previous IDS, we use the method called Virtual Split Memory. Attacks like data injection are induced, which the hackers input their script code into data source. However, the attack code in the data space cannot be accessed for execution as instructions are only retrieved from the code space. In this project, present an approach to diversity system. We make isolated memory locations for both database and user end so that attacks like data injection will not take place.

References

[1] A. Likas, N. Vlassis, J. J Verbeek "The global k-means clustering algorithm".
[2] Daljit Kaur and Parminder Kaur. "Empirical Analysis of Web Attacks".
[3] D. Wagner and D. Dean." Intrusion detection via static analysis.
[4] Five common web application vulnerabilities. http://www.symantec.com/ connect /articles/five- common-web- application-vulnerabilities.
[5] G. Kim, S. Lee, S. Kim, "A novel hybrid intrusion detection method integrating anomaly detection with misuse detection".
[6] H. Shah, J. Undercoffer, A. Joshi, "Fuzzy clustering for intrusion detection."
[7] J. Jabez and B. Muthukumar, "Intrusions Detection System (IDS)."
[8] Leixing Le, Angelos Stavrou, Brent ByungHoon Kang. "Double Guard: Detecting Intrusions in Multi-tier Web Applications," IEEE transactions on dependable and secure computing.
[9] M. Christodorescu and S. Jha."Static analysis of executables to detect malicious pattern".
[10] Mohammed Shojafar, Rahim Taheri and Zahra pooranian, "Automatic clustering of attacks".
[11] Nicholas Gallinelli, "Front end and back end development."
[12] Ozgur Depren, Murat Topallar, Emin Anarim, M.kemal Ciliz, "An intelligent intrusion detection system".
[13] Przemyslaw Berezinski, Bartosz and Marcin Szpyrka, "Entropy-Based network anomaly detection."
[14] Ravi Ranjan and G. Sahoo, "A new clustering approach".
[15] Qusay I. Sarhan and Idrees S. Gawdan, "Web Applications and Web Services: A Comparative Study".
[16] Shi na, Liu Xumin and Guan Yong, "An improved k-means clustering algorithm".
[17] T. Kanungo, D. M. Mount, "Efficient k-means clustering algorithm analysis and implementation."
[18] V. Chandola, A. Baneerjee, V. Kumar, "ACM computing surveys (CSUR)."
[19] Yunlu Gong, Shingo Mabu, Ci Chen; "Misuse detection using genetic network programming".
[20] Youguo li and Haiyan wu, "A clustering method based on k-means algorithm".