Sub-Sahara African Academic Research Publications
March, 2023, Editions

JASOR
Journal of Advanced Science and Optimization Research
Vol. 27, No.9, ISSN 2418-9325

A PROPOSED IMPROVED CAPTCHA BASED INTRUSION DETECTION MODEL

ABDULRAHMAN ABDULKARIM; ISHAQ MUHAMMED; FATIMA AHMED ABUBAKAR; ATIKA AHMAD JIBRIN; & SUBERU YUSUF
Department of Computer Science, Federal Polytechnic, Bauchi.

ABSTRACT
Intrusion Detection System is a process of intelligently monitoring events occurring in a computer system or network, analyzing them for signs of violations of a security policy. Its primary aim is to protect the availability, confidentiality and integrity of critical networked information systems. This paper considered and reviewed a CAPTCHA based intrusion detection model. The improved model is designed by creating a method of incorporating signature along with CAPTCHA to clear the controversy identified in the existing model. The improved model is expected to be implemented by the design of an interactive website such as an authentication page. In a future work, results from implemented model would be analyzed and evaluation of the performance against the existing model would be carried out. Higher detection rate and a lower false positive rate are being expected to be achieved.

Keywords: Intrusion Detection System IDS, Signature, CAPTCHA, Intrusion Prevention System IPS

Introduction

With the advancement of the Internet and its capabilities, an increasing number of individuals are getting connected on a daily basis to take advantage of its services. On one hand, the Internet offers great commercial opportunities in terms of reaching end consumers. On the contrary, it

introduces a lot of security threats to a business over the network. Various approaches are employed to assist the security of a business against threats and attacks. However, attackers are discovering new ways and techniques to break these approaches.

Intrusion could take a form of a process where software accesses web content that is protected with username and password, it uses various infiltration procedures to break the username and password. At a broader sense, intrusion may include both human and machine access to an account having web content that is secured with username and password. To overcome this problem, network security provides many techniques and one of the most important techniques is Intrusion Detection System (IDS) as suggested by (Souley & Abubakar, 2018). To achieve more security, the features of IDS, Intrusion Prevention System (IPS) and Honeypot can be combined as proposed by Yesugade, et al., (2016).

Intrusion Prevention System (IPS) is a tool that prevents spyware from entering a system. CAPTCHA is one of the methods employed in IPS. It's used in IPS to prevent unauthorized access to accounts by distinguishing between humans and spyware. With this fact, human being can solve CAPTCHA and gain authorization, spyware cannot.

With advancement in technology, Spyware creation is evolving at a rapid pace, and increasingly sophisticated spywares are designed to bypass CAPTCHA under IPS. Nachar, et al., (2015) attained 57.3% - 76.7% success rate in bypassing CAPTCHA on Yahoo using edge and fuzzy logic segmentation and recognition method. Also, a success rate of 31.75% and 58.75% in solving reCAPTCHA was achieved by Sano, et al., (2015) on Google's reCAPTCHA with continuous visual and audio symbols using sequence recognition method based on hidden markov model (HMM).

Based on the work by Abubakar, et al., (2020), CAPTCHA based IDS was designed and implemented to curb the security failure identified when CAPTCHA was used in IPS. The work integrated CAPTCHA in IDS to detect and identify spywares that bypass and break into the system. However, their method in making the software intruders to believe it is IPS may not be very efficient as some software intruders may attempt login ignoring the CAPTCHA and the textbox provided for it. It was observed in the model

that, a genuine user can mistakenly fill in the CAPTCHA box, hence will be regarded as bot. Furthermore, bots may tend to neglect the CAPTCHA and can be considered been genuine, when this happened the entire system will be penetrated and compromised.

This paper would therefore consider to make an improvement on the work of Abubakar, et al., (2020) by proposing a model that would eliminate the weakness identified in their work to achieve better and more accurate detection rate.

The remaining parts of this paper are organized as follows: Section 2 presents some related work and overview on the related work. Section 3 presents the methodology where analysis of the existing model would be discussed. Section 4 is the presentation and discussion of the proposed model. Finally, Section 5 concludes the paper and presents future work.

Related Work

This section consists of an overview of other researchers' work on related topics. The review of related work is aimed at contributing towards clearer understanding of the nature and meaning of the problem selected for this study.

Abubakar, et al., (2020) proposed a study to design IDS with intelligent redirector using CAPTCHA, a trap for detecting Intrusion by intelligent spywares. The work was set based on a design of an email website which was integrated with the new CAPTCHA based IDS system and hosted online. A dummy honeypot system was designed in which the IP addresses of the software intruders that intruded into the system is being captured. The work was implemented and evaluated based on the performance metrics which includes Detection Rate (DR), Precision (PR), False Positive Rate (FPR), correctly and incorrectly classified instances of the system. Researchers used captured IP addresses as the datasets for the study. The work employed Waikato Environment for Knowledge Analysis (WEKA) and Python to analyze the experimental data. Their findings indicated a high percentage of Detection Rate and a very low False Positive rate as compared to the existing system. However, this system faking software intruders to believe it is IPS may not be very efficient as some software

intruders may attempt login ignoring the CAPTCHA and the textbox provided for it, this will re-direct the intruder to the login authentication and somehow this may have been an intrusion bypassing the fake IPS and the CAPTCHA-trap IDS.

Malav, et al., (2016) proposed a system which combines the concept of Intrusion Detection System (IDS), Intrusion Prevention System (IPS) and Honeypot. Because various exploits are being used to compromise the network. These exploits are capable of breaking into any secured networks. In order to increase efficiency of network security, they introduce Honeypot. Honeypot detect attacks with the help of IDS; trap and deflect those packets sent by attackers. The result of their work indicates that the system handles multiple clients using the concept of Honeypot. They also pointed out that, Intrusion detection system (IDS) monitor whole network and looks for intrusion. When any intrusion occurs Honeypot will be activated. This activated Honeypot will divert the traffic to dummy/virtual servers & back track the source (IP address) or origin of that attack. The drawback of the system is that since it supports multiple clients including an attacker, the system can easily be compromised.

Khudadad & Huang, (2018) carried out a study to compare and explore the latest Anomaly detection methods for WSNs to enhance the workings of IDS in wireless environment. Series of experiments were directed to evaluation and simulate every approach in order to elaborate the effective detecting method. The methods explored were Cluster Based Method, Support Vector Machine (SVM), Naïve Bayes (NB) Method, and the Random Forest (RF) method. Many critical assessments metrics such as Confusion Matrix were used in time to Construct Model, General Classification Ratio and Memory Usage. KDD Cup 99 Intrusion Detection was used as a dataset. Result showed a suggestion to include Data Mining methods to efficiently notice the attacking threads or intrusions into WSN.

The work of El-Mourabit, et al., (2015) has compared and evaluated the newest anomaly detection intrusion techniques used in wireless sensor network, to improve the efficient technique for IDS in Wireless Sensor Network (WSN). According to their findings, the decision of choosing efficient IDS is a compromise between technique employed and

performance metrics. Some critical evaluation metrics were used such as confusion matrix, general classification rate, time to build model, and memory consumption. For implementation, KDDCup'99 intrusion detection dataset on WEKA tool was used. According to their results, it was highly recommended to use the data mining techniques to detect effectively the intrusions and attacks in WSN. Issues such as hierarchical clustering patterns, using machine learning in resource management problem of WSNs, selecting and preprocessing an appropriate dataset are open and needed further research on their work.

Research Gap

Based on the survey and review on related work as discussed above, most of the research work identified security threats from intruders and attackers on the network. The security solutions proposed by most of the researchers were based on intrusion detection using a detection technique or combination of detection technique and a preventive technique. As presented from the work by Abubakar, et al., (2020), their work integrated CAPTCHA in Intrusion Detection System to detect and identify spywares that bypass and break into the system. Therefore, attackers can be detected, prevented and blocked, although it was evident that due to the weakness identified from their work, some software intruders may attempt login ignoring the CAPTCHA and the textbox provided for it, this would re-direct the intruder to the login authentication and somehow this could be an intrusion bypassing the fake CAPTCHA trap Intrusion Detection System.

Methodology

1.1 Proposed Model

The proposed model would be adopted based on the existing model where a CAPTCHA would be incorporated as an IDS in order to deceive spyware and other intruders to assume the system to be a prevention system (IPS). In this model, CAPTCHA would be more regarded as a detection tool by integrating it with a Honeypot in order to capture necessary details of intruding machines. Additionally, but contrary to the adopted model, a

signature would be generated in a separate instance to be matched along with the generated CAPTCHA. The signature would clear the controversy of a genuine user mistakenly regarded as an intruder, also an intruder mistakenly regarded to be legitimate as identified in the review of their work. Below is the architecture of the proposed model show in figure 1

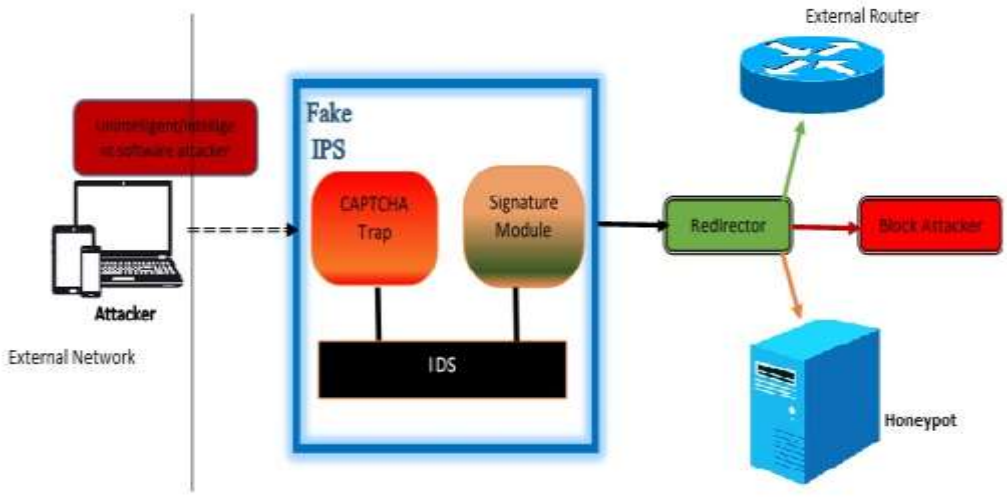

Figure 1 Architecture of the Proposed Model

The proposed model would be implemented by the design of an interactive website such as an authentication page. It is intended to place the proposed model online for a period of time. By putting the system online, it would attract software intruders to visit the site and possibly attempt intruding.

Dataset and Performance metrics

Dataset to be used for the purpose of performance analysis would be a pool of data being captured from the site that would be hosted within a reasonable period of time. Among the data to be used as dataset for the analysis are:

iv. IP address (Hostname)
v. Date of visit
vi. Class (Human/bots)

For the analysis, Naïve Bayes classification technique would be used to develop a model that would be used to classify our collected dataset.

Naïve Bayes classifier technique is based on the so-called Bayesian theorem particularly suited for situation where the dimensionality of the input is high. It is categorized as supervised learning as well as a statistical approach to classification (Stevens, 2016).

This method of analysis was also adopted to evaluate the performance of the existing model where the parameters obtained are as follows:

6. ***Detection rate (DR):*** The ratio between the number of correctly detected attacks and the number of the attacks. $DR = \frac{TP}{TP+FN}$
7. ***False positive rate (FPR):*** It is the ratio between the number of normal instances detected as attack and the total number of normal instances. $FPR = \frac{FP}{FP+TN}$
8. ***Classification rate/Accuracy (CR):*** It is defined as the ratio of correctly classified instances and the total number of the instances. $CR = \frac{TP + TN}{TP+TN+FP+FN}$
9. ***Precision rate (PR):*** Fraction of data instances predicted as positive, which are actually positive. $PR = \frac{TP}{TP+FP}$
10. ***Recall:*** It measures the missing part from precision rate, which is known as the percentage from the real attack covered by the classifier. This is the same as detection rate.
11. ***F-Measure (FM):*** Is the harmonic mean of the precision and recall at a given threshold. It is mostly preferred when only one accuracy metrics is needed as evaluation criterion. $FM = \frac{2}{\frac{1}{PR} + \frac{1}{Recall}}$

Where:

TP (True Positive): Intrusion successfully detected by the IDS.

FP (False Positive): Normal non-intrusive behavior that is wrongly classified as intrusive by the IDS.

TN (True Negative): Normal/non-intrusive behavior that is successfully labeled as normal/non-intrusive by the IDS.

FN (False Negative): Intrusion missed by the IDS, and classified as normal/non-intrusive.

2. Conclusion and Future Work

This paper proposed an improvement to the CAPTCHA based Intrusion detection model by Abubakar, et al., (2020), whereby a method was adopted to use signature incorporated with CAPTCHA in order to overcome the controversy of a genuine user mistakenly regarded as an intruder (bot) and also an intruder mistakenly regarded as legitimate.
In a future work, the improved model would be implemented on an interactive website and results obtained would be analyzed using R studio. R programming language would be used for the analysis on the R studio. At the completion, evaluation of the performance against the existing model would be carried out, a higher detection rate and a lower false positive rate are being expected to be achieved.

References

Abubakar, H., Souley, B., & Ya'u, A. G. (2020). An Improved CAPTCHA-Based Intrusion Detection System Based on Redirector Model. *Journal of Theoritical and Applied InformationTechnology, Volume 98, No. 03*, 429-440.

El Mourabit, Y., bouirden, A., Toumanari, A., & El Moussaid, N. (2015). Intrudion Detection Techniques in Wireless Sensor Network using Data Mining Algorithms: Comparative Evaluation Based on Attacks Detection. *International Journalof Advanced Computer Science and Application, Vol 6, No. 9*, 164-172.

Khudadad, M., & Huang, Z. (2018). Novel Intrusion Detection Methods for Security of Wieless Sensor Netwok. *Journal of Fundermental and Applied Sciences*, 173-189.

Malav, S., Avinash, M. S., Satish, N. S., & Sandeep, S. C. (2016). Network Security Using IDS, IPS, and Honeypot. *Interenational Journal of Recent Research in Mathematics Computer Science and Information Technology, Vol 2, Issue 2*, 27-30.

Milan, Sardana, H., & Singh, K. (2018). Reducing False Alarms in Intrusion Detection Systems – A Survey. *International Research Journal of Engineering and Technology, Volume 05, Issue 02*, 9-12.

Nachar, R. A., Inaty, E., Bonnin, P. J., & Alayli, Y. (2015). Breaking Down CAPTCHA Using Edge Corners and Fuzzy Logic Segmentation/Recognition Technique. *Security and Communication Networks, Vol 8, No. 18*, 3995-4012.

Sano, S., Otusko, T., Itoyama, K., & Okuno, H. G. (2015). HMM- based Attacks on Google's ReCAPTCHA with Continous Visual and audio symbol. *International Journal of Information Processing, vol. 23, No. 6*, 814-826.

Souley, B., & Abubakar, H. (2018). A CAPTCHA – BASED INTRUSION DETECTION MODEL. *International Journal of Software Engineering & Applications, Vol.9, No.1*, 29-40.

Stevens, I., D. (2016). Using machine learning to detect bots in World of Warcraft. *Transactions on networking*19 (5).

Yesugade, K. D., Avinash, M. S., Satish, N. S., Sandeep, S. C., & Malav, S. (2016). Infracstructure Security Using IDS, IPS and Honeypot. *International Engineering Research Journal (IERJ), vol 2, issue3*, 851-855.