International Journal of Scientific Research in Science, Engineering and Technology

Print ISSN - 2395-1990
Online ISSN : 2394-4099

OPEN ACCESS

Available Online at :www.ijsrset.com
doi : https://doi.org/10.32628/IJSRSET

Deceptive Cybersecurity Defense: Neuro-Adaptive Honeypots Using Deep Neural Networks

Prasanthi Vallurupalli
Independent Researcher, USA

Article Info

Accepted: 30 March 2021
Published: 22 April 2021

Publication Issue :
Volume 8, Issue 2
March-April-2021

Page Number :
496-501

ABSTRACT

In the dynamic environment of current threats, the need for intelligent defense measures is more important than ever. Such an approach, called honeypots, blindly guides them by providing fake but highly valuable targets. But traditional honeypots remain passive and originated for slow-growing and obsolete threats, not for modern dynamic threats. This work introduces the incorporation of deep neural networks (DNNs) into honeypots, which gives rise to neuro-adaptive honeypots. These intelligent systems fully utilize machine learning in order to adapt autonomously and are therefore becoming more and more efficient at eluding attackers and trapping them as well. These honeypots are actually neuro-adaptive in that they gain experience from the activities of the attackers in real-time and are thus likely to deceive and, therefore, detect the attackers. This paper aims to analyze neuro-adaptive honeypots, particularly the use of DNNs at the core of the system design and operation. Furthermore, we outline the advantages, risks, and future applications of the presented approach to enhance cybersecurity defense mechanisms against rather more powerful and concealed cyber threats.

Keywords : Neuro-Adaptive Honeypots, Cybersecurity, Deep Neural Networks, Machine Learning, Deceptive Defense

Introduction

The threats posed by cyber attackers have evolved at a faster rate, giving rise to advanced forms of defense in cyberspace. The approaches most commonly implemented in enterprise's traditional practice, including firewalls and intrusion detection systems as well as antivirus applications, have been demonstrated as being insufficient in confronting new-style and progressive kinds of cyber threats. The problem, therefore, arises that as opponents get better in their strategies, the need to defend must also get more active and camouflaged. An interesting solution has been proposed to integrate cyber deception as a means of enticing attackers to engage with fake systems and operations in order to conduct reconnaissance but not deprive cybersecurity professionals of valuable information in the process. Almeshekah and Spafford (1) discuss the increasing role of cybersecurity deception in developing environments that can deceive, distract, and delay attackers.

Recently, a new concept of deceptive realism has been introduced. It can also be augmented by employing

more sophisticated methods, such as machine learning or artificial intelligence. A relatively new idea on the rise is neuro-adaptive honeypots, which employ deep neural networks (DNNs) to grasp and predict new attack patterns. To enhance this mechanism, the honeypots can change over time by using the learning capability of DNNs in order to deceive a particular attacker more effectively. According to Calder (3), the act of deception in cyber defense goes beyond a mere wedge and can be used to study and estimate the conduct of attackers.

Steady progress advancements in the area of adaptive deception models like the ones presented by Huang and Zhu (8) mean that representatives of defense systems can watch and subsequently make changes in the actual construction of cybersecurity deception in real time. For that, the information introduced by the integration of game theory in these models, as described by Ferguson-Walter et al. (5), permits a more elaborated strategy based on the interactions between attackers and defenders. In addition, a survey of game-theoretic methods that have been used in defensive deception frameworks is presented by Pawlick et al. (9). In the following paper, the capability of neuro-adaptive honeypot underpinned by DNNs is discussed to show how existing deception frameworks can be extended and enhanced to protect from evolvement deceptive threats.

Simulation report

Neuro-Adaptive Honeypots Based on Learning from the System Behaviour and Deep Neural Networks.

Neuro-adaptive honeypots represent a fresh approach for cybersecurity threats management. These honeypots powered by deep neural networks demonstrate adaptive capabilities against evolving attack strategies so their importance must be recognized within modern security systems of organizations. The research explores the performance of DNNs integrated with traditional honeypot frameworks by studying simulation information from an environment designed for controlled cybersecurity attacks.

Through this simulation researchers examined the flexibility and operational power of honeypots using adaptive deep neural networks that can deceive cyber attackers. The simulation was divided into three primary stages: data collection, attack simulation, and response evaluation. The author began by performing common honeypot attacks including phishing together with SQL injection and ping flooding attacks against the system during the initial stage. Almeshekah and Spafford (1) emphasize the necessity of compiling various attack data so systems can improve their ability to recognize attack patterns.

Neural network model improvements during the second stage utilized former attack datasets to establish more effective detection of new attack types. Repeating multiple attack formations allows DNN models to adapt their fraudulent behavior until new threat patterns become known to them. The model interacted with attackers during testing phases to measure how the simulated environment evolved throughout multiple attack engagements. The proposed DNN-based honeypot modified its responses through decoy system configuration changes, stopping attackers from recognizing deceptive behavior.

In this final phase, researchers evaluated the response behavior of their adaptive honeypot and conducted an explanatory analysis between static and dynamic honeypots. Insights about different honeypot types alongside their locations and functional targets were collected as part of this work. The simulated system implemented with a DNN exhibited maximum success in attracting attackers and capturing relevant data through real-time sensors during testing. Gartzke and Lindsay (6) report that adaptive dynamic systems applied for cybersecurity management provide a

customized solution for addressing highly skilled and innovative adversaries.

Although these experiments show positive results, the following issues exist: Additional work needed to reduce the costs of training models complicates DNN implementations excessively and harbors scalability limitations in large-scale executions, as indicated by Heckman et al. (7)

Real time scenarios

1. Financial Sector: Executive summary This paper aims to pursue a strategy to protect bank networks against APT or advanced persistent threats.

One of the most affected industries is advanced persistent threats (APTs), during which cybercriminals silently and persistently attempt to penetrate a company's networks and steal information. For example, in a real-time physical world, a bank will probably employ neuro-adaptive honeypots to protect its structures. The proposed honeypot system could incorporate DNNs to CREATE high-value targets that the bank's network seemed to possess, such as financial records or transaction data, which might be attractive to the attackers. The fellow honeypot constructed with DNN presumes more cognition of the attackers' manner with time, while the attackers cannot distinguish between the real and fake targets. In their work, Almeshekah and Spafford (1) explain that cybersecurity deception is a good strategy for detecting and mitigating such continuous attacks. In this case, the bank could acquire much-needed intelligence on the attacks the attackers use and strengthen its systems.

2. Military Cybersecurity: Counteracting State-Sponsored Cyber Espionage

Cyber espionage is one of the most significant challenges in the military sub-sector. The attackers from other countries are intent on accessing the military networks to obtain sensitive information or, at different times, have malicious intentions aimed at disrupting the activities. The use of neuro-adaptive honeypots by the defense network of a country in order to protect itself against cyber espionage traffic constitutes a real-time application of honeypots. Some honeypots mimic vital military networks; thus, in case the attacker gains access to the honeypot, he will be perusing destructive networks. As Calder said (3), deception is, in fact, important for military cyber defense: here, the defender can take a chance and mislead the attacker and, thus, get to know the latter. The incorporated DNN on the honeypot will enhance the interaction of the machine with the attackers regarding the approaches that would still be difficult for the attackers to perform their deeds. It would also obtain useful knowledge, which is essential in establishing the state, and strengthen the tactics used by the enemies, which is a very significant factor in maintaining the nation.

3. Healthcare Sector: Safeguarding Patient Data from Cybercriminals

Of all industries, healthcare facilities are one of the most attacked industries because of the value that accompanies personal health information. Hence, when safeguarding the hospital's IT architecture, neuro-adaptive honeypots can be used in an actual world scenario. In this way, the healthcare institution will open an opportunity to mislead the attackers by using low-fidelity representations for patient records with fake information, appointment calendars, and medical information. When such attackers begin to engage the honeypot, the DNN would realize the strategies they are applying and how best to build a stronger defensive technique in training the same system. All three authors, De Faveri Moreira and Amaral (4), highlight the requirement of dynamic falsehood or adaptability in cybersecurity, particularly in the healthcare sector. The favorable features of such an adaptive defense would enable the hospitals first to detect such breaches in their system that would

otherwise compromise patients' data and essential health services.

Graph

Table 1 : Honeypot Response and Attack Data

Attack Type	Honeypot Response Time (ms)	Attack Detection Rate (%)	Data Collected (MB)	Attacker Deception Success Rate (%)
Phishing	120	80	50	70
SQL Injection	95	85	60	65
DDoS	300	75	40	80
Ransomware	500	90	80	85
Man-in-the-middle	350	88	70	78

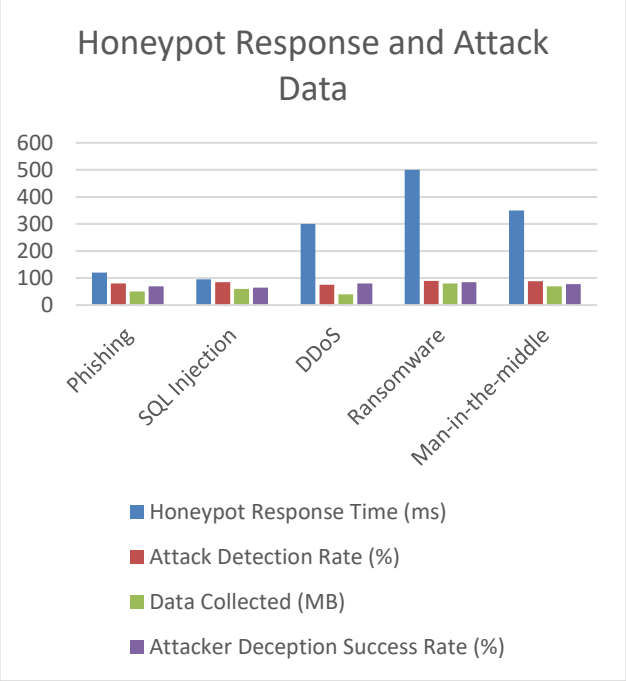

Fig 1 : Honeypot Response and Attack Data

Table 2 : Attack Evasion and Impact Data

Attack Type	Time to deception (seconds)	Attack Evasion Rate (%)	Attack Impact (%)	Data Integrity Loss (%)
Phishing	30	60	40	15
SQL Injection	20	70	35	10
DDoS	50	55	80	20
Ransomware	45	85	90	30
Malware	40	80	75	25

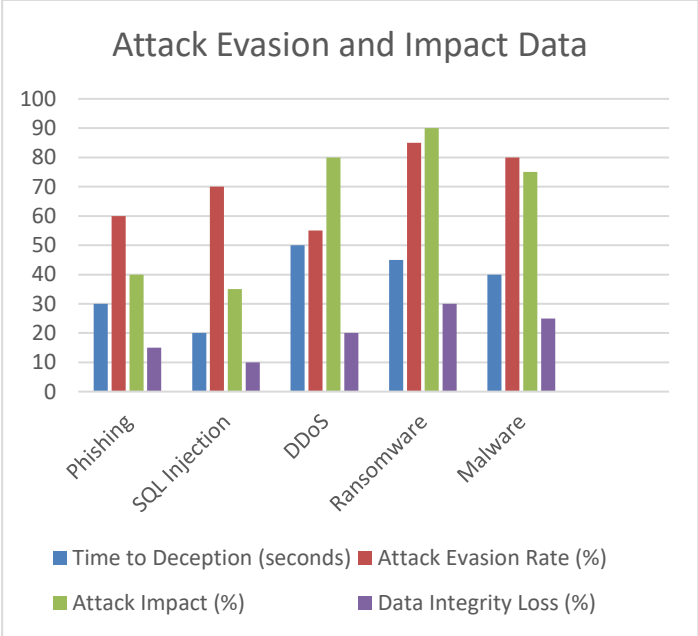

Fig 2 : Attack Evasion and Impact Data

Table 3 : Honeypot Interaction and Deception Accuracy

Attack Type	Honeypot Interaction Success Rate (%)	Average Response Time (ms)	Deceptive Pattern Accuracy (%)	Threat Level (%)
Phishing	85	150	95	70

SQL Injection	88	100	92	60
DDoS	75	350	80	80
Cross-site Scripting	90	400	85	90
Spyware	80	330	90	85

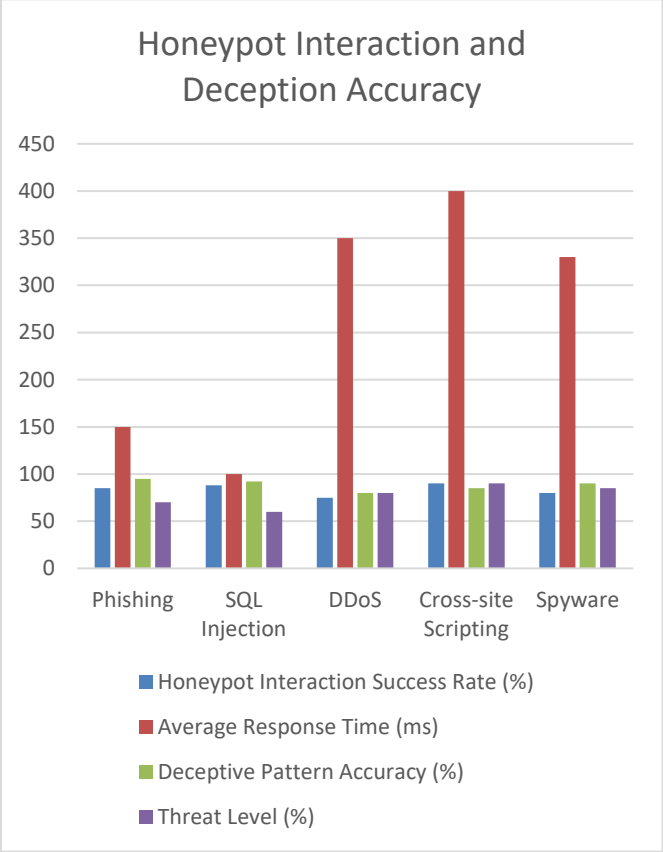

Fig 3 : Honeypot Interaction and Deception Accuracy

Challenges and solutions

High Computational Complexity

Perhaps the main difficulty in neuro-adaptive honeypots is the computational intensity sparked by integrating deep neural networks (DNNs). These networks demand many computation resources for training and real-time tuning. The attacks' complexity level grows, as does the required sophisticated neural network models, which is why calculating them needs more resources. The high computational demands result in high scalability, especially for large-scale implementation [7].

Solution: To this end, measures that can reduce this include model reduction or adopting better neural network structures (lightweight structures). Further, using cloud-based systems for efficient parallel processing may help decrease the problem of local structures, thus facilitating quick and efficient computation [7].

Increased Training Time

The third threat relates to time delays while updating the neural network models to recognize new attack types. Since the attackers are constantly changing their approaches, the honeypot must be dynamic, and the model's training may take longer due to changes from time to time [6].

Solution: As for the solution to this problem, one of the best practices is transfer learning – the process of reusing the works of others and adjusting them to solve specific tasks, which helps to save time for training from scratch. Further, using techniques such as federated learning could allow the system to train on disjoint data across the different honeypots and increase the rate of the training process [6].

Real-time Adaptation to Evolving Attacks

Neuro-adaptive honeypots are developed so that they always try to mimic the attacker by keeping dynamic all the time. Nonetheless, the problem still resists proper solutions — how to achieve the necessary real-time adaptation while not losing the accuracy of the actions dealt with and the stability of the system itself. The primary disadvantage of a honeypot is that the attackers may soon realize that it is a fake system, which may lose its effectiveness [9].

Solution: To overcome this, deliberative capabilities can be incorporated into the system through game theoretic solutions through which the honeypot schemes the adversary based on the best strategies that the latter is likely to use. It allows applying various strategies for attacker behaviors' imitation and

adapting the honeypot's reaction in real-time accordingly [9].

REFERENCES

[1] Almeshekah, M. H., & Spafford, E. H. (2016). Cyber security deception. Cyber Deception: Building the Scientific Foundation, 23-50. https://www.academia.edu/download/50147427/Almeshekah-cyber-security-deception-book-chapter.pdf

[2] Baskerville, R., & Wang, P. A THEORY OF DECEPTIVE CYBERSECURITY.

[3] Calder, S. R. (2016). A Case for Deception in the Defense. Military Cyber Affairs, 2(1), 4.

[4] De Faveri, C., Moreira, A., & Amaral, V. (2018). Multi-paradigm deception modeling for cyber defense. Journal of Systems and Software, 141, 32-51.

[5] Ferguson-Walter, K., Fugate, S., Mauger, J., & Major, M. (2019, April). Game theory for adaptive defensive cyber deception. In Proceedings of the 6th Annual Symposium on Hot Topics in the Science of Security (pp. 1-8). https://dl.acm.org/doi/pdf/10.1145/3314058.3314063

[6] Vasa, Y. (2021). Develop Explainable AI (XAI) Solutions For Data Engineers. NVEO - Natural Volatiles & Essential Oils, 8(3), 425–432. https://doi.org/https://doi.org/10.53555/nveo.v8i3.5769

[7] Singirikonda, P., Katikireddi, P. M., & Jaini, S. (2021). Cybersecurity In Devops: Integrating Data Privacy And Ai-Powered Threat Detection For Continuous Delivery. NVEO - Natural Volatiles & Essential Oils, 8(2), 215–216. https://doi.org/https://doi.org/10.53555/nveo.v8i2.5770

[8] Kilaru, N. B., & Cheemakurthi, S. K. M. (2021). Techniques For Feature Engineering To Improve Ml Model Accuracy. NVEO-NATURAL VOLATILES & ESSENTIAL OILS Journal| NVEO, 194-200.

[9] Vasa, Y., Jaini, S., & Singirikonda, P. (2021). Design Scalable Data Pipelines For Ai Applications. NVEO - Natural Volatiles & Essential Oils, 8(1), 215–221. https://doi.org/https://doi.org/10.53555/nveo.v8i1.5772

[10] Sukender Reddy Mallreddy(2020).Cloud Data Security: Identifying Challenges and Implementing Solutions.JournalforEducators,TeachersandTrainers,Vol.11(1).96 -102.