MITIGATING INSIDER THREAT'S IP SPOOFING THROUGH ENHANCED DYNAMIC CLUSTER ALGORITHM (EDPU based HCF)

.

ABSTRACT

Insider Threat has always been a major problem to computer security due to unauthorized system misuse by users in an organization. Understanding the concept and the inherent adverse consequences of the insider threat can assist in postulating mitigating approaches and techniques to the menace. Insider intrusion, from researches, experiences and literature have proved to be more expensive and destructive more than external attacks due the comprehensive understanding of the internal operations of the organization by the perpetrator. Many researchers have explored into the unhealthy nature of insider activity with the aim of eliminating the threat, thereby identifying the various categories as theft of intellectual property, fraud, sabotage, espionage. This work tends to address the menace by studying models for detecting, reducing and eliminating the threat through IP Spoofing in order to propose a better model for the intrusion. Certain experimental research through analysis of network data measurement has shown that HCF (Hop Count Filtering) can discover and discard almost 90% of spoofed IP packets but an improvement on this experiment called DPU (Dynamic Path Update) Based Hop Count Filtering has proved to identify and discard more than 90%. This was carried out in Linux Kernel environment to substantiate the effectiveness of its measurements. However, enhancing enhancing the performance of the DPU-based HCF by reducing the packet size of packets at the point of entry in order to decrease the network traffic, and to permanently discard 100% spoofed packets is the research direction of this work

Keywords: Insider Threat, IP Spoofing, DDOS, TTL, Hop Count

1. INTRODUCTION

The technological advancement in the new digital age we find ourselves *today* evolve with its pros and cons. Its main shortcoming is the security risk. Confidentiality breaches are becoming more common and serious as more sensitive information enters the digital world, The majority of which come from within the organization. Another major security concern is data integrity, the loss of which can lead to more serious problems [1], Security threats can originate both within and outside of an organization. The attacks from insiders, whether from employees, suppliers, or other organization legitimately connected to a company's computer system, pose a more pernicious threat than external attacks [2]. The

review in [3] shows Character Proximity For RFID Smart Certificate System: A Revolutionary Security Measure to Curb Forgery Menace. These insiders understand the organization's internal workings and have full access to all the rights and privileges required to launch an attack that outsiders do not have. As a result, insiders can disguise their attacks as routine operations. It has never been easy to detect and mitigate insider threats, also known as user-based threats. There are a number of behavioral indicators that can reveal the source of a potential threat, which is only the first step in the mitigation process. The decay function will be predicted in Energy Efficient Hierarchical Cluster Head Election Using Exponential Decay Function Prediction [4](Adeniji o.d. IP Spoofing, also known as Internet Protocol Address Spoofing, has been identified as a major source of Spoofed IP. Traffic from malicious network activities, particularly Distributed Denial of Service (DDOS) attacks, continues to pose a significant threat to many networks and the internet [5]. DDOS attacks are attempts to prevent legitimate users from accessing a victim's server or network resources and in Development of DDoS Attack Detection Approach in Software Defined Network Using Support Vector Machine Classifier [6] and *Immune-Inspired Concepts for Intrusion Detection in Cybersecurity Using Neural Networks [7].* Dynamic Flow Reduction Scheme in Software Defined Network Using Two Tags Multi-protocol Label Switching (MPLS) [8] . It is one of the most difficult security issues to address because hackers can use it to crash the computer system and, as a result, the entire IT infrastructure. As a result, the ability to filter spoofed IP packets near victim servers is critical for their protection and avoidance of becoming inadvertent DOS reflectors. An attacker can forge any field in the IP header except the number of hops an IP packet takes to reach its destination. An internet server can easily deduce the hop -count information from the IP Header's Time-to-Live (TTL) field. Using the IP to hop-count mapping, the server can distinguish between legitimate and spoofed IP packets [9,10], review [11] on Route Optimization in MIPv6 Experimental Test Bed for Network Mobility: Trade off Analysis and Evaluation While in [12] demonstrates Zero Day Attack Prediction with Parameter Setting Using Bi Direction Recurrent Neural Network in Cyber Security. This work will improve upon a filtering technique known as Dynamic Path Update Based Hop Count Filtering, which has been used to detect and discard spoofed IP packets. This model has proven to be effective after extensive testing of the routing path between the source and the destination [13]. When a path meets the condition of accurate transmission from the source to the destination, the packet is forwarded to the receiver and the HCF table is updated; otherwise, the packet is drop.

2. MATERIAL AND EXPERIMENTAL DETAILS

IP Spoofing was always caused by DDOS attacks more than two decades ago. It was initially defeated by one of the Filtering techniques known as ingress filtering (August, 2016), which detected spoofed packets but was ineffective. Reflectors were also used to protect against distributed denial of service attacks, but these reflectors did not meet the expectations of several hosts.

Later, the IP trace back mechanism was proposed to detect spoofed senders by using new rooting mechanisms such as "path markers" supported by some or all routers in a network. It was used to identify hosts involved in an attack (M. Ma, "Tabu marking scheme to accelerate iptraceback," Journal of Computer Networks, vol. 50, no. 18, pp. 3536-3549, 2006). In a marking scheme [IEEE Transactions On Dependable And Secure Computing, VOL. 6, NO. 2, April-June, 2009], intermediate routers mark packets probabilistically, allowing the victim network to identify the path taken by the attack packets. IP spoofing has had a significant impact on TCP service, which is widely used. It is safeguarded using a variety of methods. MULTOPS (Multilevel Tree for Online Packet Statistics) is a data structure for detecting DDoS attacks [M. P. Thomer et al, "Multops: a data-structure for bandwidth attack detection," in Proceedings of the 10th USENIX Security Symposium, 2001.]. The basic idea is that the packet rate of traffic in one direction is proportional to the packet rate in the other direction during normal operation.

Hop Count (HC) is the number of hops a packet takes from sender to receiver [A. Hussain et al, "A framework for classifying Denial of Service Attacks in Proc. ACM SIGCOMM, 2003, pp. 99-110]. The IP Time-to-Live (TTL) Field is used to infer HC, which is not typically sent in the IP packet. The main purpose of the IP TTL field is to keep packets from looping indefinitely. TTL is initially set by the sender. The TTL value is decremented by one at each node along the path. The packet is discarded if the TTL reaches zero. The HC can be estimated by subtracting the received TTL value from the closest initial TTL value that is greater than the received packet's. TTL. Typically, these initial TTL values are operating system dependent and limited to a few options. As a result, guessing the initial TTL set by the OS is possible without knowing the OS explicitly. It can even be used to mitigate DDoS attacks.

The logic behind HCF is that an attacker cannot change the number of hops an IP packet takes to reach its destination, but he can alter any field in the IP header. When most randomly spoofed IP packets arrive at victims, they do not have hop count values that are consistent with the spoofed IP addresses. An Internet server, on the other hand, can easily deduce the hop count information from the IP header's TTL field. By clustering address prefixes based on hop counts, HCF constructs an IP2HC mapping table to detect and discard spoofed IP packets.

The server can distinguish between legitimate and spoofed IP packets by using a mapping between IP addresses and hop counts. In light of this, a filtering technique known as Hop-Count Filtering (HCF) was developed to detect and discard spoofed IP packets. HCF builds an accurate IP-to-hop-count (IP2HC) mapping table. HCF is simple to set up because it does not require any help from the underlying network. HCF can identify nearly 90% of spoofed IP packets and discard them with little collateral damage by analyzing network measurement data. It was implemented and tested in the Linux kernel to demonstrate its efficacy through experimental measurements. Dynamic Path Update-based HCF, an improvement on Hop Count Filtering, creates an all-possible IP2HopCount mapping table to detect and discard spoofed IP packets. DPU-based HCF has been able to identify more than 90% of spoofed IP packets through network measurement analysis, and then it checks next possibilities (DYNAMIC) path to reach destination because there are many routing paths between source and destination. If the next path meets the condition, the packet is forwarded to the receiver and the HCF table is updated; otherwise, the packet is discarded. In the existing system (HCF), the receiver only checks the accurate path between the source and the destination; if it does not meet the condition, the packet is discarded.

3. METHODOLOGY

The experimental development of the system is divided into 2: The description is presented below.

Stage 1: consist of a scenario where the default packet filter will filter every packet of information sent by either the sender or attacker. It will reduce the packet size to between 8 or 16 bits before the data is allowed to be stored in the sender buffer. Since the attacker can spoof the sender's identity, he can use his opportunity to bypass the security barriers of the system. This implies that the packets from both the sender and the attacker will be attached with experimental threshold and forwarded to the receiver buffer via the router where each packet is separated into three fields.

Stage 2: This stage involves the following : (i) The sender should be authorised before allowing the packet to be sent with its attached IP address and TTL field. When the data packet is sent to the Buffer, the actual TTL (Time to Live) will be extracted and forwarded to the DPU based HCF (Hop Count Filteing).

(ii) The IP Address from the packet is then mapped with the IP2HC table in order to get the corresponding Hop count (Treshold) with the highest priority. If the experimental threshold (Te) does not match with the corresponding actual threshold (Ta), then the next highest priority will be obtained. This continues until the the nth priority, when the result is given to the buffer.

(iii) The HCF of each packet sent by the sender is obtained from it's corresponding threshold time. The packet along with it's HCF and IP will be sent into the sender buffer. After the router might have received each packet to the receiver system, it stores stores it in it's buffer, which extracts the IP and TTL field while forwarding the IP address to IP2HC table. The information obtained from this table is again forwarded to the receiver while the TTL is checked, together with that obtained from the IP2HC table. Whenever the value is the same, the packet will be considered legitimate or else is discarded. Then, the updated IP2HC table is forwarded to all the system for their IP2HC to be updated also.

The Overall system design is shown below:

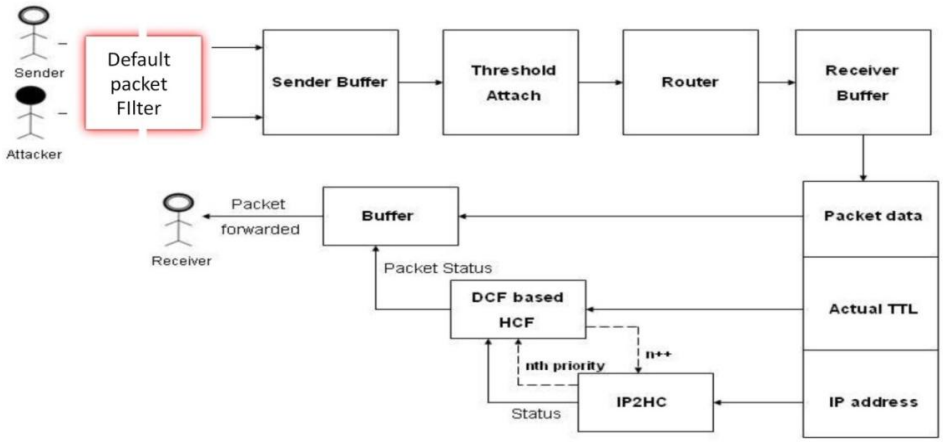

Fig 1: Overall System Design

RESULT AND DISCUSSION

The system was simulated using software and hardware to build the model. The information obtained from the table below shows the forwarded packet to the receiver while also recording the results from the TTL obtained from the IP2HC table. Similar values observed fro the TTL checked and that of the IP2HC table implies that the packet is legitimate and if not is discarded. The updated table is then forwarded to all the system to update their IP2HC table.

Table 1 shows the result captured during the experiment.

Table 1: Sequence of number of packets with Message from Sender to Receiver

Packet Sequence Nos of Messages	Sender Number of Messages	Receiver Numbers of Messages
102	1.00091	1.00133
105	1.00133	1.002221
106	1.002221	1.090260
108	1.089060	1.315440
109	1.314320	1.398141
110	1.315444	1.493260
112	1.35822	1.751512
113	1.398141	2.217725
115	1.492280	2.553430
116	1.750365	2.886511
117	1.751511	3.428802
118	2.216842	3.498451

The table below shows the result for configuration and testing the model. The priority messages with the protocol and TTL was obtained. TCP is marked as the priority protocol during the experiment because of its gain at the Transport layer.

Table 2: Different Protocols of Systems and Time To Live of packets

Message	Sender	Receiver	Protocol	TTL	Priority
102	1.00091	1.00133	TCP	149.5	1
105	1.00133	1.002221	BTR	145	1
106	1.002221	1.090260	TCP	174.5	2
108	1.089060	1.315440	TCP	160	1
109	1.314320	1.398141	CBR	165	1
110	1.315444	1.493260	ADP	174.5	1
112	1.35822	1.751512	TCP	150	2
113	1.398141	2.217725	CBR	144.5	1
115	1.492280	2.553430	CBR	150	1
116	1.750365	2.886511	ADP	149.5	1

117	1.751511	3.428802	BTR	145	1
118	2.216842	3.498451	TCP	174.5	2

5. CONCLUSION:

The default packet filter at the point of entry of data packets into the system is aimed at disallowing spoofed packet from getting to the Receiver Buffer. The reduction in the packet size , thereby decreasing the network traffic will enhance the similarity in the TTL checked from each packet in the receiver buffer to that in the IP2HC table, thereby ensuring the packets entering the systems are not spoofed.

In conclusion, though the Dynamic Path Update (DPU) based HCF can remove more than 90% of illegitimate traffic, the proposed methodology (EDPU based HCF) on implementation will almost eradicate all spoofed packets within the system, thereby increasing the health and effectiveness of the system environment. Effectively deploying this model however, will completely arrest spoofed traffic employed as a tool by cybercriminals to attack the confidentiality, integrity and availability of sensitive data in trusted systems. For future work, hybridizing this technique with other models can be employed as preferred tools in the arsenal of every security team.

AUTHORS' CONTRIBUTIONS

We thank the authors for their support in this research work and effort put in the research.

REFERENCES

1. Toffalini F., Homoliak I., Harilal A., Binder A., Ochoa M. Detection of Masqueraders Based on Graph Partitioning of File System Access Events; Proceedings of the 2018 IEEE Security and Privacy Workshops (SPW); San Francisco, CA, USA. 24 May 2018; pp. 217–227.
2. Alhajjar E., Bradley T. Survival analysis for insider threat. Comput. Math. Organ. Theory. 2021:pg1–17.
3. Eze, C., Adeniji, O.D. *Character Proximity For RFID Smart Certificate System: A Revolutionary Security Measure to Curb Forgery Menace*. International Journal of Scientific and Technology Research IJSTR, 2014, Vol 3 No 66-70.
4. Ojoawo, A.O., Adeniji O.D. *Energy Efficient Hierarchical Cluster Head Election Using Exponential Decay Function Prediction.* International Journal of Wireless & Mobile Networks (IJWMN). 2018,Vol. 10, No. 5. pp 17-31.
5. Georgiadou A., Mouzakitis S., Askounis D. Detecting Insider Threat via a Cyber-Security Culture Framework. J. Comput. Inf. Syst. 2021:pg1–11.
6. Adeniji, O.D., Adekeye, D.B., Ajagbe, S.A., Adesina, A.O., Oguns, Y.J., Oladipupo, M.A. (2022). *Development of DDoS Attack Detection Approach in Software Defined Network Using Support Vector Machine Classifier.* (eds) Pervasive Computing and Social Networking. Lecture Notes in Networks and Systems, 2022, vol 475.pp319-331, Springer.
7. Adeniji, O.D., Ukam, J.J. *Immune Inspired Concepts Using Neural Network for Intrusion Detection in Cybersecurity.* Proceedings of the 20th iSTEAMS Multidisciplinary Trans-Atlantic Going Global Conference. , 2019. pp 119-126.
8. Adeniji O.D. (2022*). Dynamic Flow Reduction Scheme Using Two Tags Multi-protocol Label Switching (MPLS) in Software Define Network*. International Journal of Emerging Trends in Engineering Research. March, 03, Volume 10. No.3**.**
9. Bose B., Avasarala B., Tirthapura S., Chung Y.-Y., Steiner D. Detecting Insider Threats Using RADISH: A System for Real-Time Anomaly Detection in Heterogeneous Data Streams. IEEE Syst. J. 2017; Vol11:pg471–482.
10. Denney K., Babun L., Uluagac A.S. USB-Watch: A Generalized Hardware-Assisted Insider Threat Detection Framework. J. Hardw. Syst. Secur. 2020;4:pg136–149.
11. Adeniji, O.D., Osofisan, A. *Route Optimization in MIPv6 Experimental Test bed for Network Mobility: Trade off Analysis and Evaluation. International Journal of Computer Science and Information Security* IJCSIS, 2020, Vol. 18. No. 5. pp 19-28.

12. Adeniji, O.D., Olatunji, O.O.. *Zero Day Attack Prediction with Parameter Setting Using Bi Direction Recurrent Neural Network in Cyber Security.* International Journal of Computer Science and Information Security IJCSIS, 2020 Vol. 18. No. 3. pp 111-118.
13. Erdin E., Aksu H., Uluagac S., Vai M., Akkaya K. OS Independent and Hardware-Assisted Insider Threat Detection and Prevention Framework; Proceedings of the 2018 IEEE Military Communications Conference (MILCOM2018); Los Angeles, CA, USA. 29–31 October 2018; pp. 926–932.