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

.

ABSTRACT

Insider threat is a menace to computer security as a result of unauthorized system misuse by users of an organization. A recent study jointly published by the United States Secret Service and Carnegie Mellon University confirms the prevalence of computer crimes perpetrated by insiders across America's organizations. Insider attacks can be more destructive and costly than attacks from the outside as the perpetrator often has deep understanding of and convenient access to a plethora of an organization's computer resources. Through analysis using network measurement data, HCF has been discovered to identify and discard close to 90% of spoofed IP packets while the Dynamic Path Update-based Hop Count Filtering proved to discard more than 90%. This was implemented and evaluated in the Linux kernel in order to demonstrate its effectiveness with experimental measurements. However, enhancing the performance of the DPU-based HCF by reducing the packet size in order to decrease the network traffic, and to permanently discard 100% spoofed packets is the research direction in this work

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

1. INTRODUCTION

This days live in the digital age is like anything, this new reality has its merits and demerits. Its major deficiency is the security risk. As more sensitive information gets into the digital world, confidentiality breaches are becoming more common and significant, most of which occur from within the organization. Data integrity is another important security concern, the damage which can result into more serious problems [1] Security threats can come from inside or 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 have knowledge of the internal workings of the organization, and full possession of all the rights and privileges required to mount an attack that outsiders lack. Consequently, insiders can make their attacks look like normal operations. Curbing and mitigating insider threats, which is also known as User-Based threats has never been an easy task. There are a number of behavioral indicators that can reveal where a potential threat is coming from, which is just the beginning of the mitigation process. Energy Efficient Hierarchical Cluster Head Election Using Exponential Decay Function Prediction in [4] will predict the decay function. IP Spoofing, otherwise known as Internet Protocol Address Spoofing which has been discovered to be a major source of Spoofed IP Traffic remains a significant threat to many networks and the internet, originating from malicious network activities especially Distributed Denial of Service (DDOS) attacks [5]. It is one of the most difficult security problems to address because it can be used by hackers to crash the computer system and consequently a whole IT infrastructure. Thus, the ability to filter spoofed IP packets near victim servers is essential for their protection and prevention from becoming involuntary DOS reflectors. and in Development of

DDoS Attack Detection Approach in Software Defined Network Using Support Vector Machine Classifier [6] (Adeniji o.d. et al, 2022) and *Immune Inspired Concepts Using Neural Network for Intrusion Detection in Cybersecurity in [7]* (Adenijio.d. et al, 2019).Dynamic Flow Reduction Scheme Using Two Tags Multi-protocol Label Switching (MPLS) in Software Define Network in [8] (Adeniji o.d. et al, 2022). Although an attacker can forge any field in the IP header, he cannot falsify the number of hops an IP packet takes to reach it's destination. An internet server can easily infer the hop – count information from the Time-to- Live (TTL) field of the IP Header. Using the IP to hop-count mapping, the sever can distinguish spoofed IP packets from legitimate ones [9] .The review in [10] on Route Optimization in MIPv6 Experimental Test bed for Network Mobility: Trade off Analysis and Evaluation while the information in [10] (Adeniji o.d. et al, 2020) shows Zero Day Attack Prediction with Parameter Setting Using Bi Direction Recurrent Neural Network in Cyber Security in [11].

It is on this premise that a filtering technique called the Dynamic Path Update Based Hop Count Filtering which has been employed to detect and discard spoofed IP packets will be enhanced in this work. This model has proved effective through thorough checking of the routing path between the source and the destination [12]. When a path satisfies the condition of an accurate transmission from the source to the destination, the packet is forwarded to the receiver and update the HCF table, otherwise the packet is discarded.

2. MATERIAL AND EXPERIMENTAL DETAILS

It was observed over two decades ago, IP Spoofing had always been due to DDOS attacks. It was initially overcome by one of the Filtering techniques known as ingress filtering (August, 2016) that detected spoofed packet but was not much effective. Reflectors also were used to protect against the distributed denial of service attacks but these reflectors did not fulfill several hosts' expectation. An approach, called the IP trace back mechanism was later proposed to detect spoofed senders using new rooting mechanism such as "path markers" supported by some or the entire router in a network. It was used to identify the hosts which were involved in an attack for marking scheme to speedup iptraceback", packets are marked probabilistically by intermediate routers, hence facilitating the victim network to identify the path traversed by the attack packets. A Comparative Analysis of Latency, Jitter and Bandwidth of IPv6 Packets using Flow Labels in [13]. TCP service which has been used to a great extent has been affected by IP spoofing. It is protected by various methodologies. *A Comparative Analysis of Latency, Jitter and Bandwidth of IPv6 Packets using Flow Labels in [14].*

The Multilevel Tree for Online Packet Statistics (MULTOPS) provides data structure for DDoS attack detection in which a data-structure for bandwidth attack detection was implemented. The basic idea is that during normal operation, the packet rate of traffic in one direction is proportional to the packet rate in the other direction. DDOS Attacks is an attack to prevent legitimate users from using a victim's server or network resources. Hop-Count Filtering was subsequently proposed and developed for Internet servers to get rid of spoofed IP packets . Hop Count (HC) is defined as the number of hops a packet traverses as it moves from the sender to the receiver. HC is not usually sent in the IP packet but is rather inferred from the IP Time-to-Live (TTL) Field. The main function of IP TTL field is to prevent packets from looping forever. The sender sets the initial value of TTL. Each node on the path decrements the TTL value by one. If the TTL reaches zero, the packet is discarded. The receiver can estimate the HC by subtracting the received TTL value from the closest initial TTL value bigger than the received packet's TTL. Usually, these initial TTL values are operating system dependent and are limited to few possibilities. Therefore, guessing the initial TTL set by the OS is possible without explicitly knowing what the OS does. It can even be used to prevent DDoS attacks. The rationale behind HCF is that an attacker cannot alter the number of hops an IP packet takes to reach its destination, though he can forge any field in the IP header. The most randomly- spoofed IP packets, when arriving at victims, do not carry hop count values that are consistent with the IP addresses being spoofed. On the other hand, an Internet server can easily infer the hop count information from the TTL field of the IP header. Exploiting this observation, HCF builds an IP2HC mapping table to detect and discard spoofed IP packets, by clustering address prefixes based on hop counts. *Detection and Mitigation of Flood Attacks in IPv6 Enabled Software Defined Networks in [14] can address the problem.* Threat Detection Approaches with IoT{15,16**]. *Detection and Mitigation of Flood Attacks in IPv6 Enabled Software Defined Networks [17].*** However, the significant roles of encryption algorithms are numerous and essential in information security[18]. A Model for Intrusion Detection in Cybersecurity using Random Forest Algorithm in [19]. Using a mapping between IP addresses and their hop-counts, the server can distinguish

spoofed IP packets from legitimate ones. In the light of this, a filtering technique, called Hop-Count Filtering (HCF)—which builds an accurate IP-to-hop-count (IP2HC) mapping table—to detect and discard spoofed IP packets was developed. HCF is easy to deploy, as it does not require any support from the underlying network. Through analysis using network measurement data, HCF can identify close to 90%of spoofed IP packets, and then discard them with little collateral damage. It was implemented and evaluated in the Linux kernel, to demonstrate its effectiveness with experimental measurements in [20, 21]. Dynamic Path Update based HCF which is an improvement on the Hop count Filtering technique builds an all possibilities of IP2HopCount mapping table to detect and discard spoofed IP packets. Through analysis using network measurement, DPU- based HCF has been able to identify more than 90% of Spoofed IP packets, and then it check next possibilities (DYNAMIC) path to reach destination because there are many possibilities of routing path between source and destination [22,23]. While the next path satisfies the condition, then packet is forwarded to the receiver and update the HCF table else packet is discarded. In existing system (HCF), receiver check only accurate path between source and destination if it does not satisfy the condition, the packet is discarded.

3: METHODOLOGY

The description of the developed model was divided into phases and an experiment was conducted as discussed below.

The Stage 1: consist of a scenario were 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 easily evade the security barriers of the system, it also stores the data spoofing the sender's identity. So, both the sender's and the attacker's packets will be attached with experimental threshold and forwarded to the receiver buffer via the router where each packet is separated into three fields.

The Stage 2: The data packet is sent to the Buffer. The Actual TTL (Time To Live) packet is extracted and forwarded to the DPU based HCF (Hop Count Filter) and the IP Address from the packet is mapped with the IP2HC table to get the corresponding Hop count (Threshold) with the highest priority. When the experimental threshold (Te) does not match with the corresponding actual threshold (Ta), then the next highest priority is obtained. This is followed by the nth priority, Te and the result is given to the buffer. The sender should be authenticated before allowing it to send the packet, with its attached IP address and TTL field. With each packet sent by the sender, the HCF is obtained from it's corresponding threshold time. The packet along with it's HCF and IP will be fed into the sender buffer. The router receives each packet to the receiver system. Receiver stores each packet in it's buffer, it extracts the IP and TTL field, while forwarding the IP address to IP2HC table. The figure below shows the developed model.

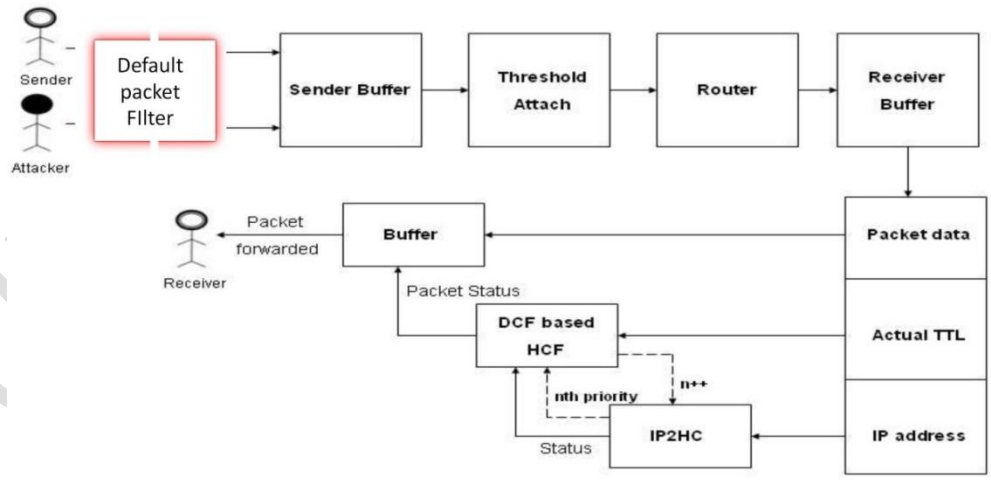

Fig 1: Overall System Design

4: RESULTS 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 the TTL is checked with the TTL obtained from the IP2HC table. When the value is the same, the packet is considered legitimate or else is discarded. The update IP2HC table is forwarded to all the system for their IP2HC to be updated. Table 1 provide the result captured during the experiment.

Table 1: Sequence of Number of packet 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 of the model. The priority messages with the protocol and TTL was obtained. TCP is mark as the priority protocol during the experiment because of it 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

4. 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 obtained from the IP2HC table, thereby ensuring the legitimacy of the packet entering the systems. In conclusion, though the Dynamic Path Update (DPU) based HCF can remove more than 90% of spoofed 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.

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. 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.
8. 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.
9. 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**.**
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.
14. *Olabisi,A.A.,* Adeniji, O.D., *Enangha,A.,. A Comparative Analysis of Latency, Jitter and Bandwidth of IPv6 Packets using Flow Labels. Afr. J. MIS*, 2019, Vol.1, Issue 3, pg. 30- 36.
15. Homoliak I., Toffalini F., Guarnizo J., Elovici Y., Ochoa M. Insight into Insiders and IT: A Survey of Insider Threat Taxonomies, Analysis, Modeling, and Countermeasures. ACM Comput. Surv. 2018;pg 52:30..
16. Kim A., Oh J., Ryu J., Lee K. A Review of Insider Threat Detection Approaches with IoT Perspective. IEEE Access. 2020;8:78847–78867.
17. **.** Ashimi, O. Q., Adeniji, O.D. *Detection and Mitigation of Flood Attacks in IPv6 Enabled Software Defined Networks. Advances in Research* Journal, 2020, Vol. 21. No. 8. pp 1-9..
18. Logunleko, K.B. , Adeniji, O.D., Logunleko, K.B. *Comparative Study of Symmetric Cryptography Mechanism on DES, AES and EB64 for Information Security* Int. J. Sci. Res. in Computer Science and Engineering, 2020, Vol.8, Issue.1, pp 45-55.
19. Adeniji, O.D .,Adeniji A O. (2021), A Model for Intrusion Detection in Cybersecurity using Random Forest Algorithm. *Afr. J. Comp. & ICT, Vol. 14, No. 2, pp. 46 –51.*
20. Le D.C., Zincir-Heywood N., Heywood M.I. Analyzing Data Granularity Levels for Insider Threat Detection Using Machine Learning. IEEE Trans. Netw. Serv. Manag. 2020;17: pg 30–44.

21. S. Venkatramulu et al IP spoofing controlling with design science research methodology AIP Conference Proceedings 2418, 030075 (2022)
22. Wasko S., Rhodes R.E., Goforth M., Bos N., Cowley H.P., Matthews G., Leung A., Iyengar S., Kopecky J. Using alternate reality games to find a needle in a haystack: An approach for testing insider threat detection methods. Comput. Secur. 2021;
23. Yuan S., Wu X. Deep learning for insider threat detection: Review, challenges and opportunities. Comput. Secur. 2021.