Bulletin of Electrical Engineering and Informatics
Vol. 10, No. 1, February 2021, pp. 274~282
ISSN: 2302-9285, DOI: 10.11591/eei.v10i1.2670

DEH-DoSv6: A defendable security model against IPv6 extension headers denial of service attack

Marlon A. Naagas[1], Alvin R. Malicdem[2], Thelma D. Palaoag[3]
[1]Central Luzon State University, Science City of Munoz, Philippines
[2]Don Mariano Marcos Memorial State Univeristy, Phlippines
[3]Univeristy of the Cordilleras, Phlippines

Article Info

Article history:

Received Mar 15, 2020
Revised Jun 2, 2020
Accepted Aug 23, 2020

Keywords:

IPv6 denial of service
IPv6 emerging threat
IPv6 evasion technique
IPv6 extension headers
IPv6 security model

ABSTRACT

With the rapid depletion of IPv4 protocol in these recent years, the IETF introduced IPv6 as a solution to address the exhaustion, however, as a new protocol exists, new characteristics have been introduced and new threats have been discovered. Extension Headers are the new characteristics of IPv6 that have an emerging and re-emerging security threats that are needed to be taken into consideration during the full migration to the IPv6 network. This study revealed that up to this moment, the popular vendors are still vulnerable and doesn't have any default protection to deal with extension headers' denial of service attack (DoS). Also, this study leads to the development of new security model which creates a new solution to address the emerging threats of IPv6 extension headers' DoS attack. Moreover, the results of this study show that our proposed security model is more effective in terms of neutralizing the unwanted traffic causing evasion attack by filtering, rate-limiting and discarding the malformed packets of prohibited extension headers' payload versus the traditional router protection.

Corresponding Author:

Marlon A. Naagas,
Information Systems Institute,
Central Luzon State University,
Science City of Munoz, NE, Philippines.
Email: manaagas@clsu.edu.ph

1. INTRODUCTION

The Internet community was threatened by the fundamental resource scarcity issue of IPv4. Four out of five (APNIC, RIPE, LACNIC, ARIN) of the regional internet registries (RIRs) have run out of freely available IPv4 address space. As a result, the internet engineering task force (IETF) defines the specifications of the IPv6 protocol [1] however, some of the specifications can be ambiguous and incomplete in certain areas or some security implications have not been considered at the time of writing. Therefore, unforeseen security issues can occur after the protocol is developed and deployed. These fine nuances between the specifications and practical deployments are explored by hackers and security researchers. The IETF sometimes revises the protocols but in some instances the IETF leaves it up to the deployers of IP systems to correct the specifications' deficiencies [2].

One of the unforeseen security issues that the implementors must take into consideration are the IPv6 extension headers. These are just one of the protocol's new characteristics that contain additional information that is utilized by network devices such as routers, switches, and endpoint hosts to determine how to process or manage an IPv6 packet [3]. However, there are one or more classifications of security vulnerabilities of an IPv6 extension header, these are: Evasion of security controls, denial of service attack

(DoS) due to processing requirements, DoS due to implementation errors and extension header-specific issues. Packets that use IPv6 extension headers may have a negative performance impact on the handling devices if proper rules or controls are not in place. The attacker can perform sending a large amount of IPv6 traffic that uses IPv6 extension headers with the intention of performing DoS attack [4, 5]. Negative performances mentioned previously may affect the performance of devices such as routers, firewalls, and network intrusion detection systems (NIDS) [6, 7] by exhausting the devices' resources that cause the network to crash.

Many studies proposed the solution to address the issues through hardening the network infrastructure, however, their solutions were to directly drop/reject/block the malformed packets containing extension headers in the router's forwarding plane once they enter the network or a plane ACL solution. However, these kinds of techniques will affect the operational and interoperability of other protocols if blocked [6], that is why careful filtering is needed while securing your infrastructure. To address these issues, our study provides an IPv6 security model for protecting the network from undesired or malicious traffic without compromising the functionalities of the other protocols. The remainder of the paper is organized as follows. Section 2 elaborates further on the motivation for this work, and discusses similar work found in the literature. Section 3 describes the experimental setup for designing and implementation of DEH-DoSv6 security model. Section 4 presents the results of our evaluation. Lastly, section 5 concludes and presents future direction of this study.

2. MOTIVATION AND RELATED WORKS

Some of the institutions such as businesses and universities around the globe are still in the migration stage and only enables IPv6 for their major products and services, however, one question to ask is: are they really ready for this major transition from a security perspective? Security in internet protocol version 6 (IPv6) is one of the major issues in the world of networking today. In our recent research, we found out that even the well-known network devices and firewalls had a major issue [8] in handling IPv6 security especially in the denial of service attacks using the extension headers' vulnerabilities. However, no permanent solutions and no generic model [9] from the IPv6 community has been developed but just a "quick and dirty" solution that can be applied by preventing the acceptance/sending of some of the IPv6 extension headers using proper firewall rules [10]. Devices should be configured to drop IPv6 extension headers that are not used in your environment such as destination options header, hop-by-hop, etc. and/or fragmentation. This "solution" should be considered only as temporary since they actually suppress some of the IPv6 added functionality and thus, should be applied only after ensuring that this functionality is actually not needed in the specific environment [11, 12].

To address the aforementioned issues, we present a new security model that maintains the strict separation of protecting the forwarding and router control plane hardware and software. Our approach provides a model for protecting a router's control and forwarding plane from undesired or malicious IPv6 traffic without compromising the functionalities of the other protocols if blocked. In this line, all valid control plane traffic is identified and once the legitimate traffic has been identified, a filter is implemented in front of router's forwarding plane. That filter counteracts with unidentified or malicious packets from reaching the router's control plane and even apply rate-limits that is set at normal degree. Ultimately, stateless network protection is applied on both control and forwarding plane of the router by control plane policing (CPP) and infrastructure access list (iACL) [13].

3. DESIGN AND IMPLEMENTATION OF DEH-DOSV6 SECURITY MODEL

The design and implementation of the proposed security model is presented in this section. The design model is consisted of two parts, first the proposed DEH-DoSv6 router architecture design, and second, DEH-DoSv6 traffic classification model.

3.1. Router architecture design

With the proposed security model, we maintain the architectural design of the modern-day router [3] with a separation of control plane and forwarding plane hardware and software. The forwarding plane is in charge of receiving a packet on the incoming interface and works on identifying the packet's IP next hop and defines the best outgoing interface going to the destination and then forwards the packet to its proper interface, whereas a router control plane assists the transmission and control functions. However, the control plane level is more subject to security vulnerabilities of being flooded by a DoS attack than forwarding plane because the traffic is processed directly destined to the router management functions. Through this concept, we added a new layer of security mechanisms by implementing DEH-DoSv6 traffic classification model in

the front of router forwarding plane, see Figure 1. The model works as a traffic classifier by filtering or rate-limiting the legitimate or illegitimate traffic that would be switched from the incoming interface to the forwarding plane layer up to the router control plane all the way to the final destination. The model simply works as it allowed the transmission of the legitimate traffic from the group of IPv6 addresses followed by discarding all the illegitimate that violates the filter rule set. With this method, it avoids the unsolicited traffic from overwhelming the router resources on the interface where the forwarding plane and control plane are connected. Moreover, the added layer will also be effective in segregating the traffic by checking first the address prefix before transmission to the forwarding plane because this kind of technique is more helpful in finding the right outgoing interface where the traffic is intended to be sent. In addition, the filters serve as a forensic tool for the analysis of possible attacks that would be used by the security analyst as important artifacts for future defense preparation. Finally, as RFC 6192 [3] advised, in the actual network environment, in-depth monitoring and predicting of exhaustive list traffic reaching the router control plane is necessary for day to day operation. The model complements the advice of the RFC by allowing all the traffic initially for auditing purposes before applying any appropriate filters or rate limits.

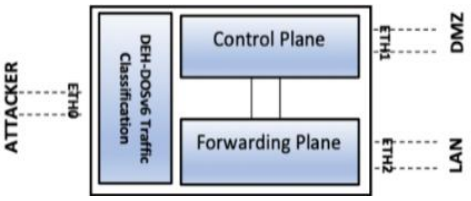

Figure 1. Proposed DEH-DoSv6 router protection architecture design

3.2. Design trade-offs of the proposed DEH-DoSv6 traffic classification model

IETF releases many RFC's related to the filtering of IPv6 packets containing extension headers [3, 4, 7, 9, 14-18]. However, it only provides common practices on how to handle and control security threats by administering proper packet filters in general. From this general perspective, we collect the best practices that comply with the requirements of IETF-RFCs in order to design an appropriate model to fill in the gap on hardening the IPv6 network. Also, this model completes and complements the design consideration for protecting the IPv6 network against denial of service attack from the packets containing malicious extension headers. The proposed DEH-DoSv6 traffic classification model as shown in Figure 2, presents how a filtering policy will protect the router control and forwarding plane in order to harden the IPv6 network against DoS attack specifically the extension headers' security flaws.

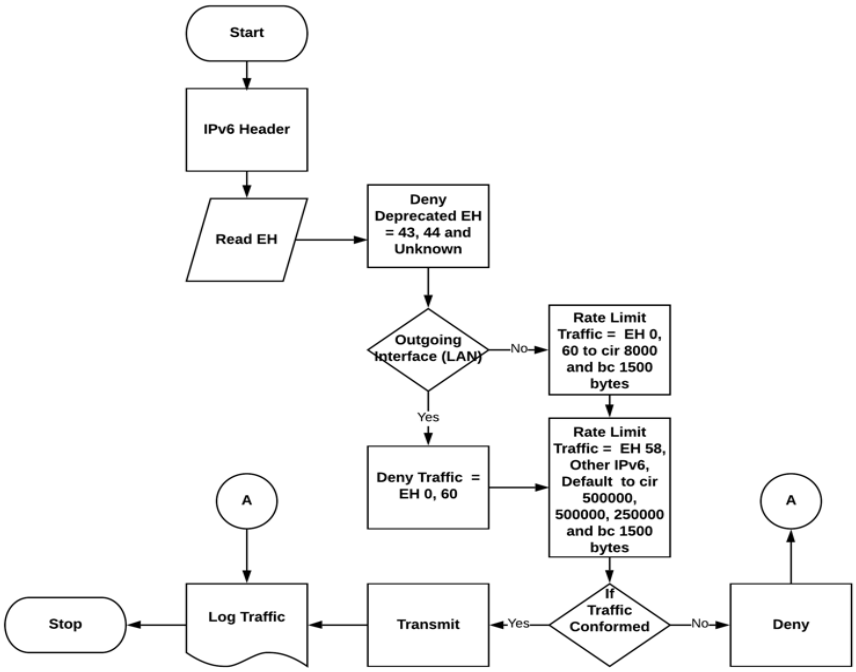

Figure 2. Proposed DEH-DoSv6 traffic classification model

In designing the protection method, we ensure that traffic classification parameters and packet flows are designed to comply with the requirements set by the RFCs. RFCs are the publications that describe the standards, technologies and protocols about network communication including the internet. The model considers two independent processes, first, the traffic classification wherein the traffic is matched by the filters, second, the policy actions taken on the classified traffic wherein the traffic would be dropped, permitted, rate-limited by the router. On the other hand, our filtering policy imposed at the edge of an enterprise network (transit network) where the policy usually follows a "black-list" approach wherein only packets with obvious harmful effects are dropped and rate-limited. This is a good practice in order to mitigate the threat before it reaches the target destination. Section 3.2.1 to 3.2.5 presents the design trade-offs that were used in this study.

3.2.1. Dropping of IPv6 fragments

Fragments can also be used by the attackers to launch attacks against end systems that do not process fragments correctly. For the deployment where fragmentation is needed in the operations, dropping of all fragments destined to the router control plane may not be feasible [3] however, virtual fragment reassembly (VFR) technique is more appropriate in this deployment, this feature reassembles fragmented packets, examines out-of-sequence fragments, and puts them back into the proper sequence. If there are problems with the fragments, it will block the packet accordingly. Moreover, for the deployments that never allow fragmented datagram in the router control plane level, dropping all fragments going to the router control plane may be reasonable [19]. Subsequently, many attacks depend on IP fragmentation such as denial of service attacks, this attack executes by creating a flooded IPv6 fragments to the target host causing resources depletion [2, 7, 8, 20].

3.2.2. Dropping of routing header 0 in control plane level

Routing header 0 (RH0) is no longer required in the IPv6 implementation. Blocking of packets containing of RH0 has no operational implication because it was already deprecated by IETF. However, allowing this traffic has a serious security implication because RH0 can be exploited using traffic amplification which might be used as denial-of-service attack [15].

3.2.3. Dropping of unknown extension header

Several intermediate devices allow the packets that contain unknown options by simply ignoring any extension headers that they do not understand. These devices forward these packets without knowing that this might be part of a malformed or a crafted packet [2, 7]. However, excessive transmission of unknown headers may lead to security implications that could be leveraged as a large-bandwidth covert channel. As a solution, intermediate devices should drop the entire packets that contain extension headers that are unrecognized [2, 7, 21].

3.2.4. Dropping and rate-limiting of HBH and DOH traffic

Hop-by-hop options (HBH) header and destination options header (DOH) both have the same structure; however, they are intended to be used for different purposes. The HBH options header must be processed by every host along the network path, whereas the destination option header is only processed at the destination host [19]. Dropping of packets containing any of these extension headers are challenging and debatable because discarding packets containing any one of these could break any of the protocols [7] that rely on them for proper functioning such as some information that is useful to a router's forwarding plane and control plane such as router alert option [17]. Within the HBH options header, the router Alert option is also a potential security issue [8]. If used improperly, this could cause performance problems for a router receiving a large number of packets containing the Router Alert hop-by-hop option. Discarding the packet containing Router Alert option may help the router control plane to mitigate this security issue [22].

IETF released some guidelines on how to handle the HBH options [7, 14, 20] such as, "if a packet containing HBH options should be dispatched at the control plane level and the packet should be rate-limited before dispatching". IETF also clarifies the requirements of limiting and dropping of packets with respect to HBH options [16]. IETF also noted that you should protect the router by applying REQ4 and REQ7, where REQ4 states that " IPv6 Implementations should protect against DoS attacks that are propagated through HBH options by enabling this protection by default and without special configuration [16, REQ4] and [16, REQ7] stated that "HBH options traffic should be limited as many as 2056 bytes and if the router receives a packet containing more than the set limit, the packet should be dropped" [16, REQ7]. Limiting and discarding HBH options during the implementation is barely legal with respect to aforementioned guidelines, however it is a good practice that the discarding of HBH and DOH options will only depend on the behavior and requirements of your network environment such as a network requiring to process MIPv6 protocol for wireless roaming design, discarding destination option header for this type of protocol is not feasible [23], in this case our model implements network segmentation in order to satisfy with respect to the requirements of

not affecting the operational functionalities of the other protocols, if the traffic is intended to a local area network (LAN) where organization assets are highly protected to DoS attack, the aforementioned rules are highly applicable however, if your network sits in the science of DMZ [24] where traffic is designed to optimize network performance for research applications by removing obstacles that traditional networks place on data transfer and with a minimal hindrance for firewalls, allowing of all traffics containing HBH and DOH headers are applicable.

Moreover, one or more options padding is another shared characteristic of HBH and DOH contained, however the use of padding typically is not needed because the header and option headers are already aligned on an 8-octet boundary [19]. PadN options are required to have a 0-byte payload [19], so if these fields contain any information, it is an error or something deliberate. These padding options could be used to contain information as part of a covert channel [7]. These padding options could also cause other problems, such as firewall resource consumption, if they are used incorrectly [8]. Therefore, it is a good idea for firewalls to check that PadN options contain no payload and that the data within the padding is not part of some type of attack. Therefore, firewalls should drop packets that have multiple padding options as well as packets that have more than 5 bytes of padding. Furthermore, firewalls should also drop padding that has anything other than 0s in the data field [2].

3.2.5. Dropping and rate-limiting of ICMPv6 and other legitimate traffic

Though ICMPv6 plays an important role in starting and keeping communications at the interface level as well as for sessions at remote nodes, allowing passing of entire ICMPv6 traffic poses danger to your network [22, 25]. These ICMPv6 packets can be used to cause DoS [26] in many ways that can cause dropped connections simply by just sending error messages and excessive amount of ICMPv6 packets to the destination sites. In the event that rogue messages can be sent out to break into a link, there is a possibility that even valid addresses or traffic are dropped [27]. To protect routers from random and excessive traffic, a rate limiter of 5000 kbps [10] for ICMP and 5000 kbps for other traffic have been set as a solution and 2500 by default. This can also be used to safeguard against the TCP SYN flooding attacks and other DoS attacks that waste away router control plane resources [3].

3.3. DEH-DoSv6 traffic classification model implementation

The traffic classification model was implemented and tested in cisco router. Cisco was chosen because it has a feature called control plane policing (CoPP), this tool has a major impact on protecting the control plane level by creating filters, rate-limits, and bandwidth constraint that can be configured to control the packet flow and set restrictions to simplify traffic sent to and from the control plane; it helps ensure that the router's CPU is used as best as possible. It also prevents the router processor from getting bogged down by overwhelming router resources in an effort to harmfully affect performance. It is also guaranteed that in times of attack of extremely sending of high load of payloads which exists during a DOS attack, the router can still be managed so that attack remediation can take place.

Modular QoS CLI (MQC) command structure was used to create class maps and a policy map for structuring the legitimate control-plane traffic. The resulting policy map is applied to the virtual control-plane interface using the service-policy command under the control policy configuration. Two different traffic directions (inbound and outbound) for the service policy as it is applied to the control plane. If the inbound direction is identified, the service policy controls the packets received on the control plane. If the outbound direction is identified, the service policy controls packets sent by the router. The input direction is generally preferred as the method to prevent attack packets from reaching the control plane. Output policies would be able to rate-limit the packets that the router sends in response to an attack. Controlling what the control plane of a router sends can help control what responses the router sends and can help to silently discard packets.

4. RESULTS AND DISCUSSION

To perform the DoS security tests, two controlled network environments were established. These environments serve as a playground in order to analyse the behaviour of the network during the attack. Cisco and Microsoft Windows 8.1 were chosen as a test device and operating system because these two brands are the most popular in their category and are widely used today, however, on the technical perspective, the modern day router architecture was present in Cisco whereas the router design maintains a strict separation of forwarding and router control plane hardware and software. The network environment includes the use of two operating systems where the attacker uses kali linux and the victim uses Microsoft Windows with the corresponding IPv6 addresses and network connectivity as well as Cisco router as edge router. The network environment is presented in Figure 3.

Figure 3. Exprimental set-up topology

Ten (10) attack scenarios from our previous research [8] are performed with 10 sets of occurrence per attack, this is best describe as, DOS=AV * Iteration where DoS is the type of attack, AV is the attack vectors used and iteration is the number of times that attack vectors were executed. To simplify the tests, we used the ICMPv6 echo request as attack payloads. By using this upper-layer protocol, this provides a clear indication that the attacker reaches the target by getting an ICMPv6 echo reply message. As a result, seven out of ten (7/10) attacks successfully penetrated the Cisco router, see Figure 4 for the complete list of router tests summary. The victim OS responded to the attacker's request with ICMPv6 echo reply message. This kind of network behavior indicates that the router allowed the malformed packets with the payloads of extension headers chain, multiple padN's, overlapping fragments and router header 0, to be passed on the router control and forwarding plane as shown in Figures 5 and 6. Therefore, this kind of scenarios signified that the attack vectors used easily bypassed the default security mechanisms of the said router. On the other hand, even though the victim OS doesn't respond to the attacker with ICMPv6 echo reply, still, the unwanted payloads are still received by the victim. Moreover, Figure 7 shows that our model worked successfully against the above-mentioned attacks, as you can see no traces were found in the captured packet and this means that all unwanted payloads were discarded on the router control and forwarding plane level.

Threat-ID	Attack Vectors	Results	Remarks
EH-A1	Hop-By-Hop Extension Header with multiple large arbitrary payload in PadN option data at the IP Level - Covert Channel.	Success	With ICMPv6 echo request and reply
EH-A2	Hop-By-Hop Extension Header mixing with multiple fragmentation header and destination header with large arbitrary data at the IP level Covert Channel.	Success	With ICMPv6 echo request and reply
EH-A3	Destination Option Extension Header Test with multiple large arbitrary payload in PadN option data at the IP Level - Covert Channel.	Success	With ICMPv6 echo request and reply
EH-A4	Mixing of multiple fragmentation header and destination header with large arbitrary payload at the IP level - Covert Channel.	Success	With ICMPv6 echo request and reply
EH-A5	Mixing Multiple and Various Extension Headers per datagram in atomic fragments.	Success	With ICMPv6 echo request and reply
EH-A6	Mixing of different extension headers in fragment and unfragmented part with a layer 4 payload.	Success	With ICMPv6 echo request and reply
EH-A7	Overlapping Fragments using Chiron.	No Response	No overlapping fragments more than 1280 bytes
EH-A8	Fragmentation Overlapping using Paxson/Shankar Model.	No Response	Tiny Fragments Received
EH-A9	Amplification Type-0 Routing header (RH0).	No Response	RH0 Error Message Received
EH-A10	Type-0 Routing header within Hop-By-Hop Extension Header and a fragmented Destination Options header.	Success	With ICMPv6 echo request and reply

Figure 4. Complete list of router tests summary without DEH-DoSv6 traffic classification model

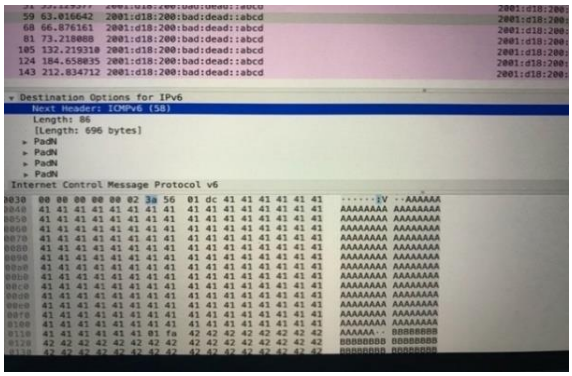

Figure 5 Network behavior during HBH with multiple PadN-covert channel packet capture

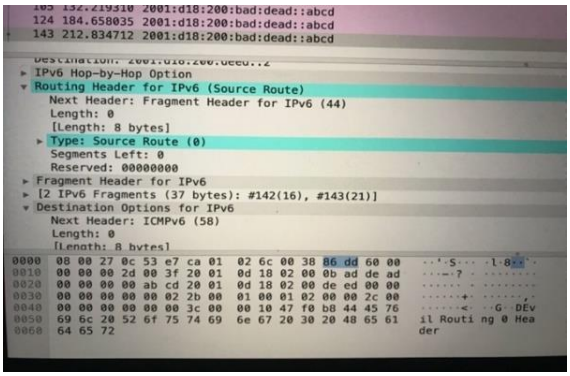

Figure 6. Network behavior during router header 0 attack

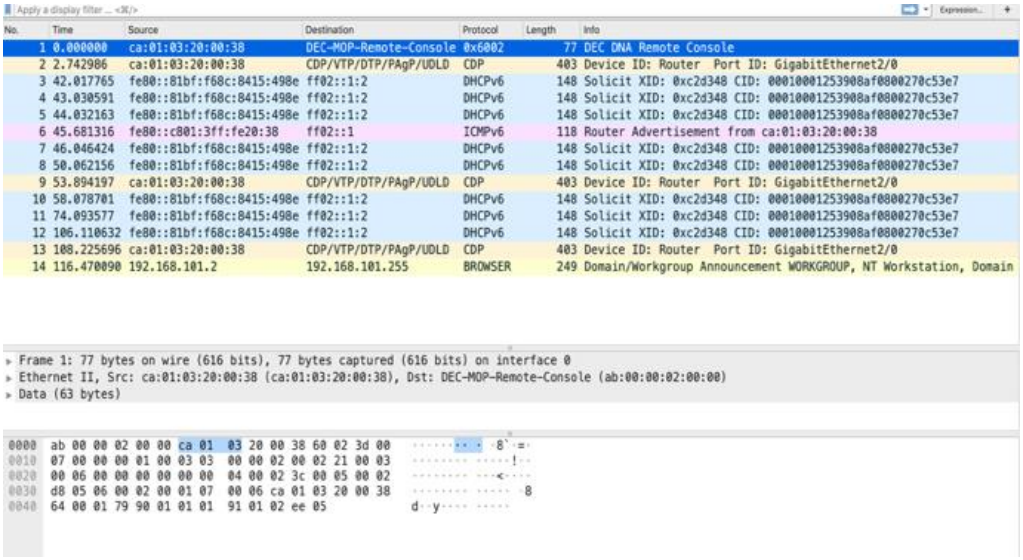

Figure 7. Network behavior with DEH-DoSv6 model implementation

To show the effectiveness of our proposed security model in dealing with the DoS attack, we replicate the implementation of the proposed solution of the other security researchers and compared the results against our model. Their solutions are implemented in the router forwarding plane layer using the access list (ACL) method blocking or discarding the extension headers directly [10, 11, 12]. Figure 8 shows the summary of the router penetration tests and as a result, the router-type 0 or RH0 extension header generates 30 RH0 packets on the actual traffic while ACL recorded 10 RH0 packets only, on the other hand, our proposed model recorded 30 RH0 packets which is the same as the actual RH0 traffic. For the IP fragments test, 130 overlapping packets were generated in the actual traffic and DEH-DoSv6 security model allows blocking of an exactly 130 packets containing overlapping fragments, ACL only blocked 90 fragments. 40 packets containing an actual traffic for the Unknown Headers were also recorded in the test. Only 20 packets having Unknown Headers were discarded by the ACL while 40 packets were discarded by DEH-DoSv6.

For HBH and DOH extension headers, 98 and 150 actual traffic were generated, while 64 and 100 traffic containing HBH and DOH were blocked by our model and ACL only blocked 20 HBH and 20 DOH traffic. This means that some packets exceeded the rate-limits, or it contains a multiple PadN's that will cause a covert channel. Finally, 360 traffic of ICMPv6 were also discarded by DEH-DoSv6 from the actual traffic of 547, whereas, ACL only discarded 270. ICMPv6 and other legitimate traffics could also be used by the attacker to deny network services such as flooding attack that decreases network performance if this protocol is not used properly. Therefore, the results are very clear that the existing solution (ACL only) is not enough in protecting the IPv6 network in general and the router in particular. Moreover, the results also show that our

proposed security model is more effective in terms of neutralizing the unwanted traffic causing DoS attack by filtering, rate-limiting and discarding the malformed packets of prohibited extension headers' payload. In addition, this also served as an alert counter and plays an important role as a forensic tool for the security analyst in order to analyze the possible threats and serve as a basis for the creation of future countermeasures.

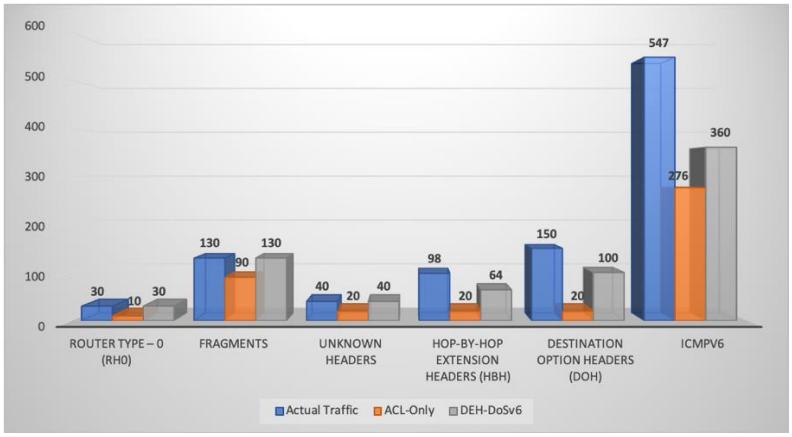

Figure 8. Complete list of router penetration test summary with DEH-DoSv6 security model

5. CONCLUSION

Based on the findings, the conclusions are hereby presented. Extension headers are the new characteristics of IPv6 that has an emerging and re-emerging security threats and is needed to be taken into consideration during the full migration to the IPv6 network. The study revealed that up to this moment, the popular vendors are still vulnerable and doesn't have any default protection to deal with extension headers' denial of service attack. With the above mentioned IPv6 extension headers' vulnerabilities, this study leads to the development of a new security model which creates a new solution to address the emerging threats of IPv6 extension headers' denial of service attack. Moreover, the test results also show that the DEH-DoSv6 security model is very effective in protecting the IPv6 network against the emerging threats of IPv6 extension headers. For the future direction, this is to recommend extending the implementation of DEH-DoSv6 traffic classification model to other router platforms.

REFERENCES

[1] M. A. Naagas, N. A. M. Jr, and T. D. Palaoag, "IPv6 campus transition: A Central Luzon State University case study," Bulletin *of Electrical Engineering and Informatics*, vol. 9, no. 3, 2020.
[2] S. Hogg and E. Vyncke, "*IPv6 Security*," 1st ed, Indianapolis, Indiana, *USA: Cisco Press*, pp. 576, 2009.
[3] D. Dugal, C. Pignataro and R. Dunn, "Protecting the Router Control Plane", IETF Request for Comments: 6192, 2011
[4] F. Gont, "Operational Implications of IPv6 Packets with Extension Headers", [online]. Available: https://tools.ietf.org/html/draft-gont-v6ops-ipv6-ehs-packet-drops-03, 2016.
[5] S. Paliwal, "Denial of Service and Distributed Denial of Service Attack on the IPV6: A Review", *International Journal of Innovative Research in Technology*, vol. 6, no. 1, pp. 474-780, 2019.
[6] F. Gont and W. Liu "draft-ietf-opsec-ipv6-eh-filtering-06 - Recommendations on the Filtering of IPv6 Packets Containing IPv6 Extension Headers", [Online]. Available: https://tools.ietf.org/html/draft-ietf-opsec-ipv6-eh-filtering-06, 2018.
[7] E. Zack, "Firewall Security Assessment and Benchmarking IPv6 Firewall Load Tests", IPv6 Hackers Meeting #1," [online]. Available: http://www.ipv6hackers.org/meetings/ipv6-hackers-1/zack-ipv6hackers1-firewall-security-assessment-and- benchmarking.pdf, 2013.
[8] M. Naagas and A. Malicdem, "Denial of Service (DOS) Attack: An Analysis to IPv6 Extension Headers Security Nightmares", unpublished.
[9] Carpenter, B. and S. Jiang, "Transmission and Processing of IPv6 Extension Headers", IETF Request for Comments: 7045, 2013.
[10] A. Atlasis, "The Impact of Extension Headers on IPv6 Access Control Lists Real-Life Use Cases", [Online]. Available: https://www.secfu.net, 2015.
[11] A. Atlasis, "Security Impacts of Abusing IPv6 Extension Headers", Media.blackhat.com, 2012. [Online]. Available: https://media.blackhat.com/ad-12/Atlasis/bh-ad-12-security-impacts-atlasis-wp.pdf.
[12] A. Atlasis, "Evasion of High-End IPS Devices in the Age of IPv6," Blackhat.com, 2014. [Online]. Available: https://www.blackhat.com/docs/us-14/materials/us-14-Atlasis-Evasion-Of-HighEnd-IPS-Devices-In-The-Age-Of-IPv6-WP.pdf.

[13] Cisco, "Protecting Your Core: Infrastructure Protection Access Control Lists," Document ID: 43920, [Online]. Available: http://www.cisco.com/c/en/us/support/docs/ip/access-lists/43920-iacl.html in 12th July 2015.
[14] F. Gont, " Operational Implications of IPv6 Packets with Extension Headers," [Online]. Available: https://tools.ietf.org/html/draft-gont-v6ops-ipv6-ehs-packet-drops-03Tools.ietf.org, 2016.
[15] J. Abley, P. Savola and G. Neville-Neil, "Deprecation of Type 0 Routing Headers in IPv6," *IETF Request for Comments: 5095*, 2007.
[16] F. Baker and R. Bonica, "IPv6 Hop-by-Hop Options Extension Header," [Online]. Available: https://tools.ietf.org/id/draft-ietf-6man-hbh-header-handling-01.html, 2016.
[17] Partridge, C. and A. Jackson, "IPv6 Router Alert Option," *IETF Request for Comments: 2711*,1999.
[18] A. Pilihanto, "A Complete Guide on IPv6 Attack and Defense," *SANS Institute*, 2012.
[19] S. Deering and R. Hinden "Internet Protocol, Version 6 (IPv6) Specification," *IETF Request for Comments: RFC 8200*, 2017.
[20] F. Gont, "Security Implications of Predictable Fragment Identification Values," *IETF Request for Comments: 7739*, 2016.
[21] R. Bonica, "The IPv6 Unrecognized Option", [online]. Available: https://tools.ietf.org/id/draft-bonica-6man-unrecognized-opt-01.html Tools.ietf.org, 2018.
[22] F. Le Faucheur, "IP Router Alert Considerations and Usage," *IETF Request for Comments: 6398*, 2011.
[23] K. Chowdhury and A. Yegin, "Mobile IPv6 (MIPv6) Bootstrapping for the Integrated Scenario," *IETF Request for Comments: 6611*, pp. 1-12, 2012.
[24] J. Crichigno, E. Bou-Harb and N. Ghani, "A Comprehensive Tutorial on Science DMZ," in *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 2041-2078, 2019.
[25] R. M. A. Saad, S. Ramadass and S. Manickam, "A Study on Detecting ICMPv6 Flooding Attack based on IDS," *Australian Journal of Basic and Applied Sciences*, vol. 7, no. 2, pp. 175-181, 2013.
[26] A. H. Bdair, R. Abdullah, S. Manickam and A. K. Al-Ani, "Brief of Intrusion Detection Systems in Detecting ICMPv6 Attacks," *Computational Science and Technology*, vol 603, pp. 199-213, 2020.
[27] E. Davies and J. Mohacsi, "Recommendations for Filtering ICMPv6 Messages in Firewalls", *IETF Request for Comments: 4890*, 2007.

BIOGRAPHIES OF AUTHORS

Marlon A. Naagas is an Assistant Professor, former Department Chairman of Information Technology Department of Central Luzon State University. He is also a former Network Engineer in CLSU, former Network Consultant of DOST PCIEERD- CLSU Bayanihanets Project. He is a CISCO Cyber Security Scholarship Awardee, CISCO Certified Network Associate in Cyber Security Operations (CCNA - CyberOps).

Alvin R. Malicdem. received his Doctorate Degree in Information Technology (DIT) from the University of the Cordilleras, Baguio City, Philippines. He is currently a Dean of College of Information Technology of Don Mariano Marcos Memorial State University (DMMSU).

Thelma D. Palaoag received her Doctorate Degree in Information Technology (DIT) from the University of the Cordilleras, Baguio City, Philippines. She is a Professor and Research Coordinator of the College of Information Technology and Computer Science, University of the Cordilleras.