Denial of service attack: an analysis to IPv6 extension headers security nightmares

Marlon A. Naagas, Anazel P. Gamilla
Department of Information Technology-College of Engineering, Central Luzon State University, Science City of Munoz, Philippines

Article Info

Article history:

Received Apr 29, 2021
Revised Jan 1, 2022
Accepted Jan 19, 2022

Keywords:

Covert channel
Denial of service threats
Extension headers threats
Fragmentation header attack
IPv6 security
Routing header 0 attack

ABSTRACT

Dealing with scarcity issues of internet protocol version 4 (IPv4), internet engineering task force (IETF) developed internet protocol version 6 (IPv6) to support the needs of IP addresses for future use of the internet, however, one challenge that must be faced while transitioning to IPv6 is in the area of security. IPv6 is a new protocol that has many new probabilities for attackers to exploit the protocol stack and one of them is through IPv6 extension headers. Mishandling of extension headers are the security nightmares for network administrators, allowing for new security threats that will cause denial of service (DoS). As a result, the mishandling of IPv6 extension Headers creates new attack vectors that could lead to DoS–which can be exploited for different purposes, such as creating covert channels, fragmentation attacks, and routing header 0 attacks. Furthermore, this paper becomes proof of concepts that even to this day our well-known network devices are still exploitable by these attack vectors.

Corresponding Author:

Anazel P. Gamilla
Department, of Information Technology, Central Luzon State University
Science City of Munoz, Philippines
Email: apgamilla@clsu.edu.ph

1. INTRODUCTION

The internet community was threatened by the fundamental resource scarcity issue of IPv4. As of January 2020, three out of five Regional Internet Registries (RIRs) of Internet Assigned Numbers Authority (IANA) have already depleted the assigned block of IPv4 addresses. American Registry for Internet Numbers (ARIN), Latin America and Caribbean Network Information Centre (LACNIC), and Réseaux IP Européens (RIPE) already reached address depletion while the depletion of African Network Information Centre (AFRINIC) and Asia Pacific Network Information Centre (APNIC) were projected by the mid-2020 and late 2021 [1]. To address the issue, the Internet Engineering Task Force (IETF) developed internet protocol version 6 (IPv6) to address these limitations, along with several protocol improvements like network performances, ease-of-configuration, address length, and network management issues [2].

One challenge that must be faced while transitioning to IPv6 is in the area of security. While IPv6 does not have backward compatibility with its predecessor, it poses many of the same vulnerabilities related to internet protocol version 4 (IPv4). However, IPv6 is a completely new protocol, and it offers several new capabilities that could potentially offer additional vulnerabilities and threats to agencies. APNIC conducted a 2016 APNIC survey report [3] that runs every two years to gather feedback from members and other key stakeholders about their services, including the challenges that are being faced by the Internet community. The conducted survey report last 2016 has shown major challenges that have been experienced upon facing the shortage of IPv4 addresses, and security issues have become the number one challenge reported by APNIC members, followed by transitioning to IPv6. In almost all of the focus groups, dealing with issues of the network, security was cited as the next biggest challenge they faced after IPv4 and IPv6. In the APNIC survey report (2018), again, similar to the 2016 survey, security threats were regarded as the biggest challenge encountered by members and non-members. All forms of threats were bundled together, including end-user vulnerabilities, network security, malware, cyber-security, and more [4]. Security threats are increasing in quantity, sophistication, and impact, demanding more financial resources and personnel to manage them. On the other hand, the survey report stated above also found out that among the security challenges which were encountered during the IPv6 transition, 61% of the respondents identified the denial of service (DoS) threats as one of the top concerns.

Internet Engineering Task Force (IETF) defined new RFC 8200 [5] and it obsoletes RFC 2460 [6], which specified the characteristics of IPv6 protocol but, 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. As mentioned, IPv6 was defined as a completely new protocol and it was not directly compatible with IPv4, however, it poses some security vulnerabilities that are similar to IPv4, these security liabilities include: Eavesdropping, replay packet insertion, packet deletion, packet modification, and man-in-the-middle (MITM) threats. IETF addresses the aforementioned threats by the use of the “security architecture for the internet protocol” and it was published in RFC 4301 [7]. RFC 8200 [5] also cited that among all these threats, DoS attacks remained unresolved. As cited in RFC 8200 “There is no other mechanism to protect against DoS attacks”.

On the other hand, with IPv6 as a new protocol, there are many new probabilities for the attackers which allow for new attack surfaces and attack vectors. One of the security nightmares that we have to consider is the mishandling/abusing of extension headers. One serious threat that extension headers poses was the DoS attacks. Even though there is no mechanism to protect against DoS, the network administrator should always stay one step ahead of the attackers by knowing the characteristics of the new protocol that are vulnerable to DoS and should find a solution to alleviate these vulnerabilities before migration [8].

IPv6 extension headers have additional information that was utilized by network devices such as routers, switches, and endpoint hosts, to determine how to process or manage an IPv6 packet [9]. However, there were one or more classifications of security vulnerabilities of an IPv6 extension headers and these were: Hop-by-Hop options header and destination options headers covert channel threats, fragmentation attacks, router header 0-source routing and router alert threats [8]. These vulnerabilities could cause evasion of security controls, DoS due to processing requirements, and DoS due to implementation errors. 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 attack that can be performed is through sending a large amount of IPv6 traffic that uses IPv6 extension headers with the intention of performing DoS attack [10]. Negative performances mentioned previously may affect devices such as routers, firewalls, and Network Intrusion Detection Systems (NIDS) [11].

Several pieces of research have been made wherein the researchers performed evasion testing against the well-known vulnerabilities of extension headers [12]–[17]. The recent research showed that even well-known security devices have no inherent capability to stop the DoS attack in full capability because this attack vector uses open ports and protocols [18]. However, most of the research was dated from the year 2010-2015 and one of the questions to ask was, are the popular intermediary devices today still vulnerable to the extension headers security flaws?

The study will give you a solid understanding about the protocol design issues of IPv6 extension headers that if handled incorrectly will cause DoS threats. This will also expose the limitations of well-known intermediary devices such as routers and firewalls on protecting your network against this adversary. The results will become proof of concepts that even to this day, our well-known network devices are still exploitable by this attack.

2. METHOD

The experiment was conducted at Central Luzon State University Network-network operation center (NOC). Several ways of abusing extension headers were tested, and the behavior of the victim’s computer is also examined. To abuse the security vulnerabilities, the researchers crafted new and modified IPv6 packets with chaining extension headers and inject some malicious payloads on them. Python-Scapy and Chiron are the tools used in crafting IPv6 packets. The following presents the sample script of a crafted packet with unlimited extension headers.

Python-Scapy:

```
IPv6Packet=IPv6 (src=<source ip>dst=<dest ip>) for x in range (0,100):
IPv6Packet=IPv6Packet/IPv6ExtHdrDestOpt()
                    /IPv6ExtHdrRouting()
```

```
                         /IPv6ExtHdrHopByHop()
                         /ICMPv6EchoRequest()
 send(IPv6Packet)
```

Chiron advanced IPv6 scanning techniques:

```
‟python chiron_scanner.py <interface> -s <source IPv6 address> -d <destination IPv6
address>
-sn -luE <list of headers remains unfragmented> -lfE <list of headers to be fragmented> -nf
<number of fragments> -l4_data" <layer 4 payload>"
```

Where, *-sn* is defines a destination ping scan, *-lfE* is defines an arbitrary list of extension headers which will be included in the fragmentable part, *-luE* is defines an arbitrary list of extension headers which will be included in the unfragmentable part, *-l4_data* is defines the layer 4 protocol data payload.

Three popular routers were chosen and evaluated: CISCO, mikrotik routerboard, and pfSense were chosen and evaluated because of their availability in the host university. The tests happened under the existing network configuration of the host university. Two-gigabit interfaces are assigned for attacker and victim. Eleven (11) malformed packets were used and crafted to test the behavior of network infrastructure against extension header attacks, see Table 1. To simplify the tests, the researchers use the ICMPv6 echo request as attacking payloads. By using this upper-layer protocol, it provides a clear indication that the attacker reaches the target by getting an ICMPv6 echo reply message. To test further, other attack vectors were also used to confirm that this technique can be used for other attacking purposes. Figures 1, 2, and 3 show the presentation of the attack topology used in this study.

Table 1. IPv6 extension headers attack vectors

Threat-Id	Attack Vectors
EH. A1	Hop-by-Hop options extension header with multiple large arbitrary payloads in PadN option data at the IP level-covert channel
EH. A2	Hop-by-Hop options extension header mixing with multiple fragmentation header and destination options header with large arbitrary data at the IP-level covert channel
EH. A3	Destination options extension header with multiple large arbitrary payloads in PadN option data at the IP level-covert channel
EH. A4	Mixing of multiple fragmentation header and destination options header with large arbitrary payload at the IP level-covert channel
EH. A5	Mixing multiple and various extension headers per datagram in atomic fragments
EH. A6	Mixing of multiple extension headers at the 1st fragment combining with upper-layer protocol header at the 2nd fragment
EH. A7	Mixing of different extension headers in fragmented and unfragmented part with a layer 4 payload
EH. A8	Fragmentation overlapping using paxson/shankar model
EH. A9	Router alert within the Hop-by-Hop options header
EH. A10	Type-0 Routing header (RH0)-CISCO model
EH. A11	Type-0 Routing header within Hop-by-Hop extension options header and a fragmented destination options header.

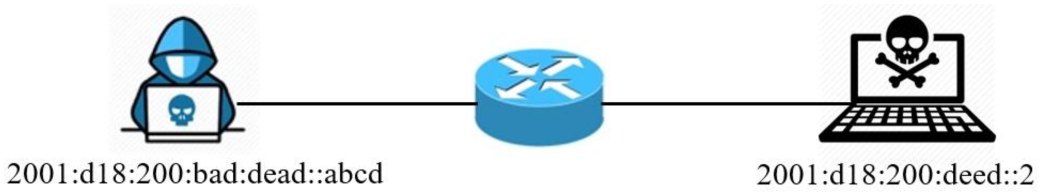


Figure 1. CISCO

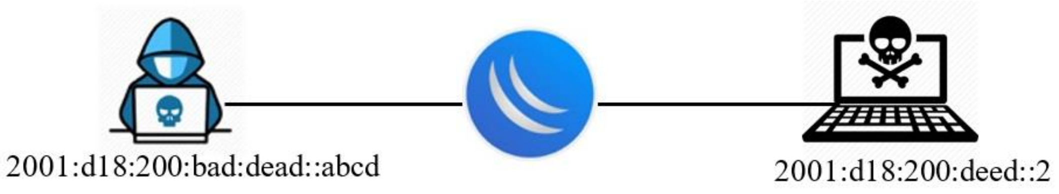


Figure 2. Mikrotik

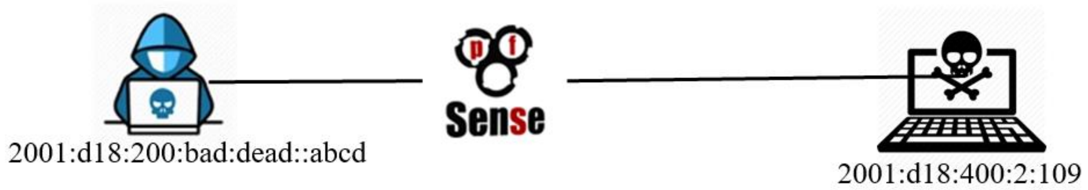


Figure 3. pfSense

3. RESULTS AND DISCUSSION

3.1. Attacking Hop-by-Hop and destination option extension headers

In the first attack scenario as shown in Table 1, EH. A1, malformed packets were created and combined the Hop-by-Hop extension header with multiple large arbitrary payloads in PadN option data at the IP level to create a covert channel attack. This attack method injected a large arbitrary payload in the "Options field" of the Hop-by-Hop options header. The malformed packet is created with 120 "A", 150 "B", and 15 "A" as covert channels injected in PadN option data and sends the packet along the network path to a target destination host. Results have shown that the victim's operating system (OS) responded to the attacker's request with an ICMPv6 echo reply message. This was the indication that the malformed packets with a payload of multiple padN received by the victim operating system and that all routers allowed them to be passed as shown in Tables 2, 3 and 4, EH.A1.

Table 2. Complete list of CISCO router tests summary

Threat-Id	Results	Remarks
EH. A1	With ICMPv6	Multiple PadN of 120 "A", 150 "B" and 15 "A" as covert channels in the Hop-by-Hop options header
EH. A2	With ICMPv6	3 IP Fragments + Multiple PadN of 120 "A", 150 "B" and 15 "A" as covert channels in the Hop-by-Hop options header
EH. A3	With ICMPv6	Multiple PadN of 120 "A", 150 "B" and 15 "A" as covert channels in the destination options header
EH. A4	With ICMPv6	3 IP Fragments + Multiple PadN of 120 "A", 150 "B" and 15 "A" as covert channels in the destination options header
EH. A5	With ICMPv6	multiple Hop-by-Hop options header+destination options header in one atomic fragment
EH. A6	No ICMPv6	received fragmented packets
EH. A7	With ICMPv6	Multiple Hop-by-Hop options header+destination options header with PadN of "XXXXYYYYZZZZ" payload in fragment and unfragmented part
EH. A8	No ICMPv6	No response
EH. A9	With ICMPv6	Router Alert () received
EH. A10	No ICMPv6	Type: Source router (0) Segment Left: 1
EH. A11	With ICMPv6	Type: Source router (0) Segment Left: 0

New attack variations were also crafted, the researcher modified the IPv6 packet of EH.A1 script by mixing multiple fragmentation headers and destination headers at the IP level as show in Table 1, EH.A2. The victim's operating system received and responded with ICMPv6 echo reply message and accepted the four rouge packets with the addition of fragments and multiple destination headers loaded with 120 "A", 150 "B" and 15 "A" injected in PadN option data as shown in EH.A2 of Table 2, 3 and 4. All routers did nothing to secure the network and let the rouge packets pass to infiltrate the target host. The same test was repeated in EH.A3, but this time instead of Hop-by-Hop extension header, destination option extension header was used and combined with multiple large arbitrary payloads in PadN option data at the IP level to create a covert channel attack. The packet captured obtained the same result and behaved as the same as EH.A1. The victim's OS response to the attacker's request with ICMPv6 echo reply message. This served as evidence that the crafted packet with a covert channel was accepted and treated as a normal packet by the victim's operating system. The middle router allowed them to pass, and no security measures were done.

Further, mixing of multiple fragmentation header and destination header with large arbitrary payload at the IP level to create a covert channel was also crafted, as shown in Table 1, EH.A4. This attack vector contains payloads of multiple IPv6 fragments with a total of 848 bytes and multiple destination options header with embedded multiple PadN's of 120 "A", 150 "B" and 15 "A" injected to IPv6 packet. The test obtained the same results wherein, the malformed packet was received and accepted as a regular packet by the victim's operating system to which the victim replied back with an ICMPv6 echo reply message to the attacker. CISCO router allowed the rouge packets to pass on the network as shown in Tables 2, 3 and 4, EH.A4.

Table 3. Complete list of mikrotik router tests summary

Threat-Id	Results	Remarks
EH. A1	With ICMPv6	Multiple PadN of 120 "A", 150 "B" and 15 "A" as covert channels in the Hop-by-Hop options header
EH. A2	With ICMPv6	3 IP Fragments + Multiple PadN of 120 "A", 150 "B" and 15 "A" as covert channels in the Hop-by-Hop options header
EH. A3	With ICMPv6	Multiple PadN of 120 "A", 150 "B" and 15 "A" as covert channels in the destination options header
EH. A4	With ICMPv6	3 IP Fragments + Multiple PadN of 120 "A", 150 "B" and 15 "A" as covert channels in the destination options header
EH. A5	With ICMPv6	Multiple Hop-by-Hop options header+destination options header in one atomic fragment
EH. A6	No ICMPv6	No Payload
EH. A7	With ICMPv6	Multiple Hop-by-Hop options header+destination options header with PadN of "XXXXYYYYZZZZ" payload in fragment and unfragmented part
EH. A8	No ICMPv6	No Response
EH. A9	With ICMPv6	Router Alert () Received
EH. A10	No ICMPv6	Type: Source router (0) Segment Left: 1
EH. A11	With ICMPv6	Type: Source router (0) Segment Left: 0

Table 4. Complete list of pfsense router tests summary

Threat-Id	Results	Remarks
EH. A1	With ICMPv6	Multiple PadN of 120 "A", 150 "B" and 15 "A" as covert channels in the Hop-by-Hop options header
EH. A2	With ICMPv6	3 IP Fragments + Multiple PadN of 120 "A", 150 "B" and 15 "A" as covert channels in the Hop-by-Hop options header
EH. A3	With ICMPv6	Multiple PadN of 120 "A", 150 "B" and 15 "A" as covert channels in the destination options header
EH. A4	With ICMPv6	3 IP Fragments + Multiple PadN of 120 "A", 150 "B" and 15 "A" as covert channels in the destination options header
EH. A5	With ICMPv6	Multiple Hop-by-Hop options header+destination options header in one atomic fragment
EH. A6	With ICMPv6	Multiple destination options header in first fragment+upper protocol (icmpv6) in second fragment
EH. A7	With ICMPv6	Multiple Hop-by-Hop options header+destination options header with PadN of "XXXXYYYYZZZZ" payload in fragment and unfragmented part
EH. A8	With ICMPv6	Paxson/Shankar model payloads were successfully transmitted and received
EH. A9	No ICMPv6	No Router Alert Received
EH. A10	No ICMPv6	No Router Header 0 Received
EH. A11	No ICMPv6	No Router Header 0 Received

3.2. Fragmentation header security attack

The above-mentioned IP fragmentation vulnerabilities that were identified in Table 1 were examined in this scenario. Four attack vectors (EH-A5 to EH-A8) that were associated with fragmentation were utilized to analyze the behavior of the network during the attack sequence. Threat EH.A5 was examined first. The attack was composed of mixing multiple and various extension headers per datagram crafted in one atomic fragment such as a combination of multiple destination options header and fragmentation header. Again, this atomic fragmentation packet manipulation technique successfully penetrated the default security of all routers. As seen in Tables 2, 3, and 4 (EH-A5), the victim received and accepted the atomic payload of chaining various extension headers and replied back with ICMPv6 echo reply message to the attacker and all routers allowed the malformed packet to be passed in the edge network.

We also mixed various headers in 1st and 2nd fragments and combined the upper protocol header (EH.A6). However, the said attack vector produced different results in three routers. CISCO and Mikrotik worked properly in this scenario, no ICMPv6 echo reply message responds to the target OS and both routers did not allow the rouge packet, while pfSense was the most vulnerable amongst the three in this case because pfSence did nothing and allowed the rouge packet to bypass the network edge.

New attack variations were also added by mixing of different extension headers in fragmented and unfragmented parts with a layer 4 payload as shown in Table 1, EH.7. The packet created has one Hop-by-Hop extension header located in the unfragmentable part of the IPv6 including three destination options header, while the fragmentable part comprises of 3 destination options header with an ICMPv6 echo request header and an “XXXXXXYYYYYYZZZZZZZZZ” data payload. Also, 3 fragments were created in fragmented parts. As an attacker transmits this packet, our results show that the receiving end OS (victim) received a Hop-by-Hop packet with multiple destination options header on both unfragmented and fragmented parts of IPv6 datagram with layer 4 data payload. Therefore, the test results signified that all routers allowed the packets to bypass the security.

Finally, Paxson/Shankar model also adapts to evaluate the overlapping fragments. This attack describes how a malicious packet can bypass a firewall using overlapping fragments [19], however, some research found out that this fragmentation attack technique is obsolete nowadays [13] and handled properly by some operating system. However, in our testing, we analyze the behavior of CISCO and Mikrotik first and we obtain different responses in the attack. The CISCO device handles the attack with “no response” in the victim OS, as shown in Table 2 EH.8, but the OS received the complete fragmented packets with layer 4 data payload. Mikrotik handles with no response and drops all the overlapping packets, as shown in Table 3 EH.8, because no traces are found in the captured packets on the receiving end. In this case, both devices are compliant with the said attack, however, Mikrotik handled the attack correctly and has a slight advantage against CISCO. For further analysis, pfSense captures different behavior in fragmentation overlapping using Paxson/Shankar model attack. The results show that Pfsense allows to pass the Paxson/Shankar packet and the victim OS accepts the attacker payload and response with ICMPv6 echo reply message, as shown in Table 4 EH.8, however, if you inspect deeply the captured packet, Pfsense removed the overlapping fragments, unlike CISCO where no overlapping fragments removal was done. CISCO’s advantage here is that there is no response on the victim OS however, Mikrotik handles the issue correctly versus CISCO and pfsense because Mikrotik rejects the fragmented payload and has no response to attacker requests.

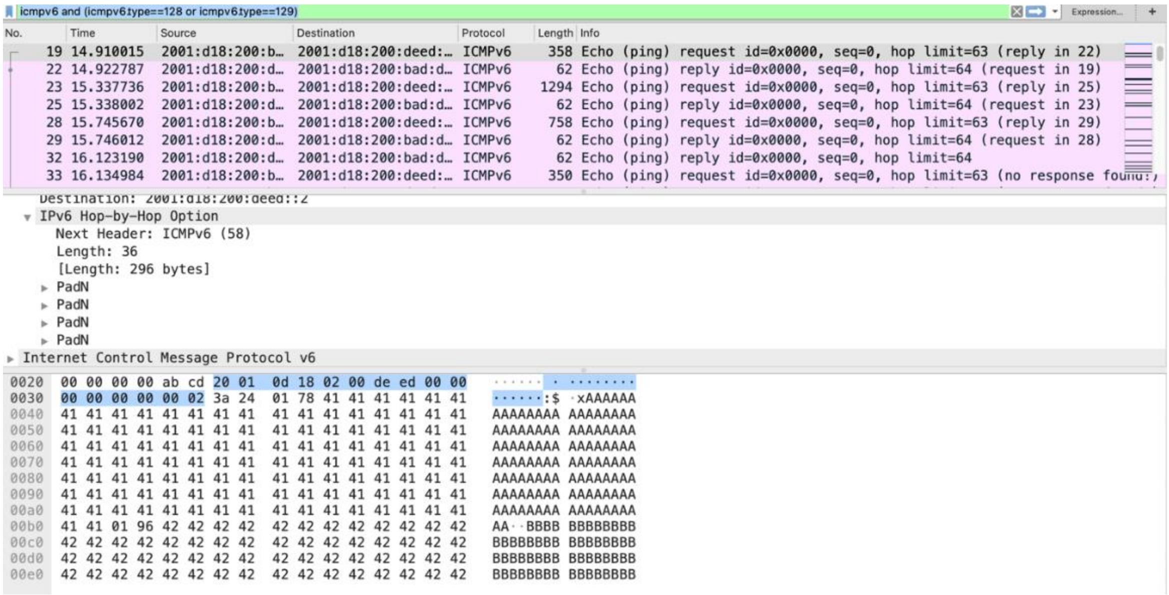
3.3. Mixing router alert option into various extension headers attack

Router alert option was also tested in this scenario. In this attack, the attacker generates a malicious packet with router alert option in Hop-by-Hop options extension header including upper-layer protocol and layer 4 data payload [20]. Evidently, the test results showed that the attack was successfully penetrated CISCO and Mikrotik and accepted the packet with a router alert option inserted in the upper layer protocol while the receiving OS establishes 3-way handshaking in TCP layer 4 as shown in Tables 2 and 3, EH.A9. If the attacker uses this method frequently and floods the router with an alert message, there’s a possibility that the router memory will be exhausted and that will cause a denial of service. Surprisingly, pfSense worked much better than CISCO and Mikrotik in this case, because no router alert option traces were found, and remove/drop the router alert option malformed packet before it arrives in the destination host, as shown in Tables 2, 3, and 4 (EH.9).

3.4. Routing header 0 (RH0) attack

Finally, two attacks were used to test the vulnerability of two intermediary devices using routing header 0 (RH0). First, we used the traditional RH0 routing header attack. The RH0 packet was crafted and could be used by the attacker to bounce traffic from the midpoint node on the way to the target destination end-system [12]. However, this kind of attack is obsolete nowadays. The results showed all intermediary devices handle this attack correctly by deprecating or disapproving the use of RH0 extension header. The result also showed that the segment left field in the destination OS was marked as 1 instead of 0, and there are no responses on all victim OS, as shown in Tables 2, 3, and 4 (EH.10). However, we modified the attack method by combining the Type-0 routing header into Hop-by-Hop options extension header and a fragmented destination options header. As a result, the left segment field of the two captured packets are equal to 0, this value indicates that the RH0 packet bypassed the security mechanism of both CISCO and Mikrotik and the target OS response to the attacker by ICMPv6 echo reply, as shown in Tables 2 and 3 (EH.11). This signifies that the RH 0 attack is still possible today if the attacker uses different kinds of attack variations. However, the results also showed that pfSense has an advantage amongst the three in containing the RH0 attack because no traces of RH0 were found in the pfSense packet captured, as shown in Table 4 (EH.11).

To summarize, the corresponding network behaviors and responses are presented in Tables 2 to 4, Figures 4 to 6. The overall results have shown that eight out of eleven (8/11) attack vectors using extension headers are successfully penetrated on CISCO, Mikrotik, and pfSense. Three routers by default did nothing to stop or reject most of the malformed packets sent by the attackers. The results have also shown that it is possible that IPv6 traffic with a large amount of extension headers are sent into the target network with the malicious intention of exhausting the hardware resources of network devices, regardless of the hardware device platform is subjected to DoS or DDOS type of attack vectors. Therefore, this is also an indication that the three popular routers were prone to extension header vulnerabilities [21] up to now and the network administrator needs to address these vulnerabilities [22] and fix them before these malformed packets reach their targeted destinations [23]. Security features mitigating this kind of adversary must be implemented during the deployment of IPv6 network [24], [25].

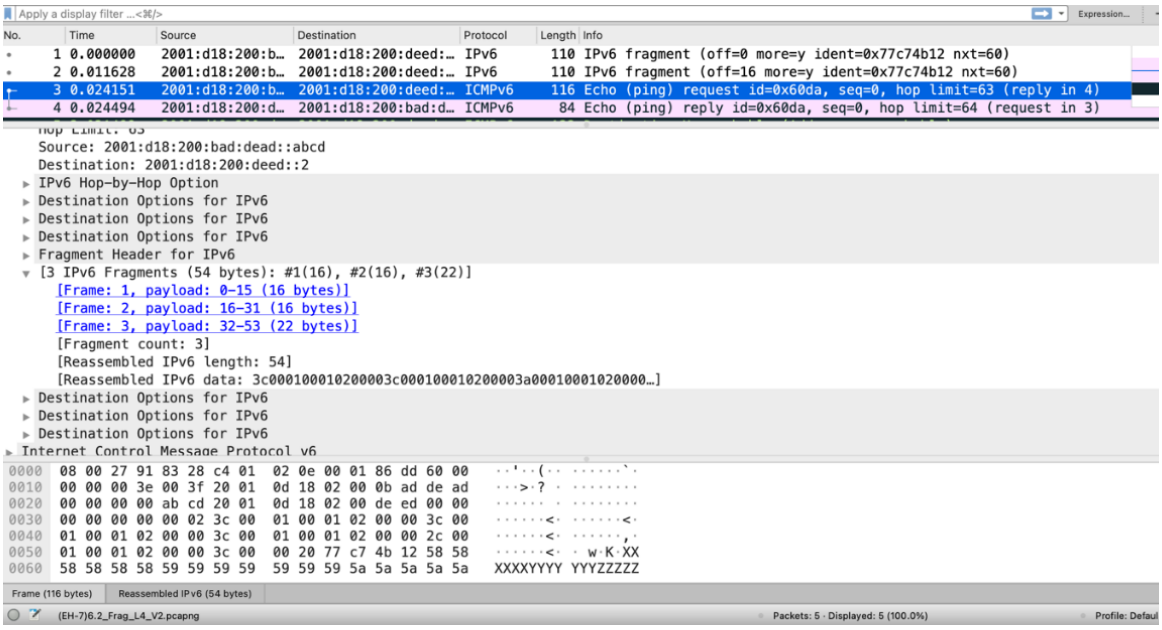


```
No.   Time       Source             Destination          Protocol  Length Info
   19 14.910015  2001:d18:200:b…   2001:d18:200:deed:…  ICMPv6     358 Echo (ping) request id=0x0000, seq=0, hop limit=63 (reply in 22)
   22 14.922787  2001:d18:200:d…   2001:d18:200:bad:d…  ICMPv6      62 Echo (ping) reply id=0x0000, seq=0, hop limit=64 (request in 19)
   23 15.337736  2001:d18:200:b…   2001:d18:200:deed:…  ICMPv6    1294 Echo (ping) request id=0x0000, seq=0, hop limit=63 (reply in 25)
   25 15.338002  2001:d18:200:d…   2001:d18:200:bad:d…  ICMPv6      62 Echo (ping) reply id=0x0000, seq=0, hop limit=64 (request in 23)
   28 15.745670  2001:d18:200:b…   2001:d18:200:deed:…  ICMPv6     758 Echo (ping) request id=0x0000, seq=0, hop limit=63 (reply in 29)
   29 15.746012  2001:d18:200:d…   2001:d18:200:bad:d…  ICMPv6      62 Echo (ping) reply id=0x0000, seq=0, hop limit=64 (request in 28)
   32 16.123190  2001:d18:200:d…   2001:d18:200:bad:d…  ICMPv6      62 Echo (ping) reply id=0x0000, seq=0, hop limit=64
   33 16.134984  2001:d18:200:b…   2001:d18:200:deed:…  ICMPv6     350 Echo (ping) request id=0x0000, seq=0, hop limit=63 (no response found!)

    Destination: 2001:d18:200:deed::2
  ▼ IPv6 Hop-by-Hop Option
      Next Header: ICMPv6 (58)
      Length: 36
      [Length: 296 bytes]
    ▶ PadN
    ▶ PadN
    ▶ PadN
    ▶ PadN
▶ Internet Control Message Protocol v6

0020  00 00 00 00 ab cd 20 01  0d 18 02 00 de ed 00 00   ······ · ········
0030  00 00 00 00 00 02 3a 24  01 78 41 41 41 41 41 41   ······:$ ·xAAAAAA
0040  41 41 41 41 41 41 41 41  41 41 41 41 41 41 41 41   AAAAAAAA AAAAAAAA
0050  41 41 41 41 41 41 41 41  41 41 41 41 41 41 41 41   AAAAAAAA AAAAAAAA
0060  41 41 41 41 41 41 41 41  41 41 41 41 41 41 41 41   AAAAAAAA AAAAAAAA
0070  41 41 41 41 41 41 41 41  41 41 41 41 41 41 41 41   AAAAAAAA AAAAAAAA
0080  41 41 41 41 41 41 41 41  41 41 41 41 41 41 41 41   AAAAAAAA AAAAAAAA
0090  41 41 41 41 41 41 41 41  41 41 41 41 41 41 41 41   AAAAAAAA AAAAAAAA
00a0  41 41 41 41 41 41 41 41  41 41 41 41 41 41 41 41   AAAAAAAA AAAAAAAA
00b0  41 41 01 96 42 42 42 42  42 42 42 42 42 42 42 42   AA··BBBB BBBBBBBB
00c0  42 42 42 42 42 42 42 42  42 42 42 42 42 42 42 42   BBBBBBBB BBBBBBBB
00d0  42 42 42 42 42 42 42 42  42 42 42 42 42 42 42 42   BBBBBBBB BBBBBBBB
00e0  42 42 42 42 42 42 42 42  42 42 42 42 42 42 42 42   BBBBBBBB BBBBBBBB
```

Figure 4. Covert-channel attack packet captured


Apply a display filter ...<⌘/>
Expression...
Frame (116 bytes)
Reassembled IPv6 (54 bytes)
Packets: 5 · Displayed: 5 (100.0%)
Profile: Defaul

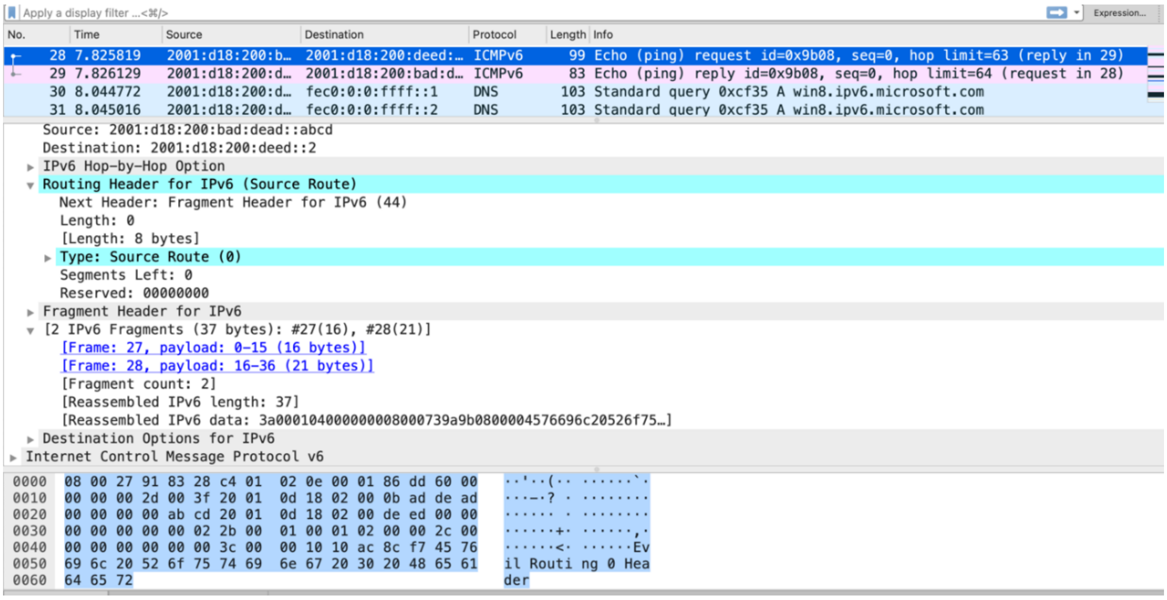
```
No.   Time       Source             Destination          Protocol  Length Info
    1 0.000000   2001:d18:200:b…   2001:d18:200:deed:…  IPv6       110 IPv6 fragment (off=0 more=y ident=0x77c74b12 nxt=60)
    2 0.011628   2001:d18:200:b…   2001:d18:200:deed:…  IPv6       110 IPv6 fragment (off=16 more=y ident=0x77c74b12 nxt=60)
    3 0.024151   2001:d18:200:b…   2001:d18:200:deed:…  ICMPv6     116 Echo (ping) request id=0x60da, seq=0, hop limit=63 (reply in 4)
    4 0.024494   2001:d18:200:d…   2001:d18:200:bad:d…  ICMPv6      84 Echo (ping) reply id=0x60da, seq=0, hop limit=64 (request in 3)

    Hop Limit: 63
    Source: 2001:d18:200:bad:dead::abcd
    Destination: 2001:d18:200:deed::2
  ▶ IPv6 Hop-by-Hop Option
  ▶ Destination Options for IPv6
  ▶ Destination Options for IPv6
  ▶ Destination Options for IPv6
  ▶ Fragment Header for IPv6
  ▼ [3 IPv6 Fragments (54 bytes): #1(16), #2(16), #3(22)]
      [Frame: 1, payload: 0-15 (16 bytes)]
      [Frame: 2, payload: 16-31 (16 bytes)]
      [Frame: 3, payload: 32-53 (22 bytes)]
      [Fragment count: 3]
      [Reassembled IPv6 length: 54]
      [Reassembled IPv6 data: 3c000100010200003c000100010200003a00010001020000…]
  ▶ Destination Options for IPv6
  ▶ Destination Options for IPv6
  ▶ Destination Options for IPv6
▶ Internet Control Message Protocol v6

0000  08 00 27 91 83 28 c4 01  02 0e 00 01 86 dd 60 00   ··'··(·· ······`·
0010  00 00 00 3e 00 3f 20 01  0d 18 02 00 0b ad de ad   ···>·? · ········
0020  00 00 00 00 ab cd 20 01  0d 18 02 00 de ed 00 00   ······ · ········
0030  00 00 00 00 00 02 3c 00  01 00 01 02 00 00 3c 00   ······<· ······<·
0040  01 00 01 02 00 00 3c 00  01 00 01 02 00 00 2c 00   ······<· ······,·
0050  01 00 01 02 00 00 3c 00  00 20 77 c7 4b 12 58 58   ······<· · w·K·XX
0060  58 58 58 58 59 59 59 59  59 59 59 5a 5a 5a 5a 5a   XXXXYYYY YYYZZZZZ

(EH-7)6.2_Frag_L4_V2.pcapng
```

Figure 5. Fragmentation attack packet captured



```
No.  Time      Source             Destination          Protocol  Length Info
  28 7.825819  2001:d18:200:b…    2001:d18:200:deed:…  ICMPv6        99 Echo (ping) request id=0x9b08, seq=0, hop limit=63 (reply in 29)
  29 7.826129  2001:d18:200:d…    2001:d18:200:bad:d…  ICMPv6        83 Echo (ping) reply id=0x9b08, seq=0, hop limit=64 (request in 28)
  30 8.044772  2001:d18:200:d…    fec0:0:0:ffff::1     DNS          103 Standard query 0xcf35 A win8.ipv6.microsoft.com
  31 8.045016  2001:d18:200:d…    fec0:0:0:ffff::2     DNS          103 Standard query 0xcf35 A win8.ipv6.microsoft.com
```

```
    Source: 2001:d18:200:bad:dead::abcd
    Destination: 2001:d18:200:deed::2
  ▸ IPv6 Hop-by-Hop Option
  ▾ Routing Header for IPv6 (Source Route)
      Next Header: Fragment Header for IPv6 (44)
      Length: 0
      [Length: 8 bytes]
    ▸ Type: Source Route (0)
      Segments Left: 0
      Reserved: 00000000
  ▸ Fragment Header for IPv6
  ▾ [2 IPv6 Fragments (37 bytes): #27(16), #28(21)]
      [Frame: 27, payload: 0-15 (16 bytes)]
      [Frame: 28, payload: 16-36 (21 bytes)]
      [Fragment count: 2]
      [Reassembled IPv6 length: 37]
      [Reassembled IPv6 data: 3a0001040000000008000739a9b0800004576696c20526f75…]
  ▸ Destination Options for IPv6
▸ Internet Control Message Protocol v6
```

```
0000  08 00 27 91 83 28 c4 01  02 0e 00 01 86 dd 60 00   ··'··(·· ······`·
0010  00 00 00 2d 00 3f 20 01  0d 18 02 00 0b ad de ad   ···-·? · ········
0020  00 00 00 00 ab cd 20 01  0d 18 02 00 de ed 00 00   ······ · ········
0030  00 00 00 00 00 02 2b 00  01 00 01 02 00 00 2c 00   ······+· ······,·
0040  00 00 00 00 00 00 3c 00  00 10 10 ac 8c f7 45 76   ······<· ······Ev
0050  69 6c 20 52 6f 75 74 69  6e 67 20 30 20 48 65 61   il Routi ng 0 Hea
0060  64 65 72                                           der
```

Figure 6. Router header attack packet captured

4. CONCLUSION

IPv6 protocol is not a perfect protocol but it is our gateway of dealing with the scarcity issue of IPv4 addresses. However, security issues are now the number one challenge reported by APNIC, followed by transitioning to IPv6. Denial of service (DoS) security threat is one of the top security nightmares faced by the IPv6 early adopter, and the extension headers are new features introduced in IPv6 specification which creates new attack vectors if attackers could use this characteristic maliciously and the network becomes vulnerable to a DoS attack. The result of this study also shows that up to date, the popular routers and firewalls were at immature stage to handle IPv6 extension headers vulnerabilities such as Hop-by-Hop options header and destination options header-covert channel, fragmentation and routing header 0 security threats, and even if devices have the capability to handle IPv6 extension headers threats, there is a lack of knowledge in the network administrator's side to address the issues. It should be also concluded that this is not a vendors' issue, but rather a protocol design issue in particular. We also note that proper knowledge and training are a must before you plan to migrate to IPv6 because IPv6 is a new entity. Finally, the analysis of the security implications will allow us to reach our future direction: to propose a defendable architecture that can work in the existing infrastructure and mitigates the aforementioned attack vectors.

REFERENCES

[1] M. A. Naagas, N. A. Macabale 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, pp. 1167–1175, Jun. 2020, doi: 10.11591/eei.v9i3.2173.

[2] F. Gont and W. Liu, "Security implications of IPv6 on IPv4 networks," {RFC} Editor, Feb. 2014. doi: 10.17487/rfc7123.

[3] B. Mainland, "2016 APNIC survey report," Asia Pacific Network Information Centre, 2016.

[4] R. Sullivan and B. Mainland, "2018 APNIC survey report," Asia Pacific Network Information Centre, 2018.

[5] S. Deering and R. Hinden, "Internet protocol, version 6 (IPv6) specification," {RFC} Editor, Jul. 2017. doi: 10.17487/RFC8200.

[6] S. Deering and R. Hinden, "Internet protocol, version 6 (IPv6) specification," {RFC} Editor, Dec. 1998. doi: 10.17487/rfc2460.

[7] S. Kent and K. Seo, "Security architecture for the internet protocol," {RFC} Editor, Dec. 2005. doi: 10.17487/rfc4301.

[8] M. A. Naagas, A. R. Malicdem, and T. D. Palaoag, "DEH-DoSv6: A defendable security model against IPv6 extension headers denial of service attack," *Bulletin of Electrical Engineering and Informatics*, vol. 10, no. 1, pp. 274–282, Feb. 2021, doi: 10.11591/eei.v10i1.2670.

[9] Juniper Networks, "IPv6 flow-based processing overview," *Juniper Networks, Inc*, 2021. https://www.juniper.net/documentation/us/en/software/junos/flow-packet-processing/flow-packet-processing.pdf (accessed Jul. 18, 2021).

[10] F. Gont, N. Hilliard, G. Doering, W. Kumari, G. Huston, and W. Liu, "Operational implications of IPv6 packets with extension headers," *IETF*, Sep. 2016.

[11] European Advanced Networking Test Center Aktiengesellschaf, "IPv6 security assessment and benchmarking abstract test suite." 1st ed. Salzufer 14 D–10587 Berlin Germany: EANTC European Advanced Networking Test Center Aktiengesellschaft, 2013.

[12] S. Hogg and E. Vyncke, *IPv6 security*. Cisco Press, 2008.

[13] A. Atlasis, "Fragmentation (overlapping) attacks one year later," *Troopers 13 – IPv6 Security Summit 2013*, 2013. https://troopers.de/wp-content/uploads/2013/01/TROOPERS13-Fragmentation_Overlapping_Attacks_Against_IPv6_One_Year_Later-Antonios_Atlasis.pdf (accessed Jul. 21, 2021).

[14] M. Wadhwa and M. Khari, "Prevention algorithm against the vulnerability of type 0 routing header in Ipv6," in *2011*

International Conference on Computational Intelligence and Communication Networks, Oct. 2011, pp. 616–620, doi: 10.1109/CICN.2011.133.

[15] A. Atlasis, "Security impacts of abusing IPv6 extension headers," *Centre for Strategic Cyberspace + Security Science*, 2012. https://pdfs.semanticscholar.org/0d55/e5ccf45091b44ac41a5b71a4c18f183cb869.pdf (accessed Jul. 21, 2021).

[16] M. Mavani and L. Ragha, "Security implication and detection of threats due to manipulating IPv6 extension headers," in *2013 Annual IEEE India Conference (INDICON)*, Dec. 2013, pp. 1–6, doi: 10.1109/INDCON.2013.6726061.

[17] A. Atlasis, "The impact of extension headers on IPv6 access control lists real-life use cases," *IPv6 Security Summit*, 2016. https://troopers.de/events/ipv6-security-summit-2016/687_the_impact_of_extension_headers_on_ipv6_access_control_lists_-_real_life_use_cases__/ (accessed Jul. 21, 2021).

[18] M. A. Naagas, E. L. Mique Jr, T. D. Palaoag, and J. S. Dela Cruz, "Defense-through-deception network security model: securing university campus network from DOS/DDOS attack," *Bulletin of Electrical Engineering and Informatics (BEEI)*, vol. 7, no. 4, pp. 593–600, Dec. 2018, doi: 10.11591/eei.v7i4.1349.

[19] A. Atlasis and E. Rey, "Evasion of high-end IPS devices in the age of IPv6," *Blackhat.com*. 2014. Accessed: Jul 23, 2021. [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.

[20] F. Le Faucheur, "IP router alert considerations and usage," Rfc 6398, Oct. 2011. doi: 10.17487/rfc6398.

[21] R. A. Hansen, L. Gino, and D. Savio, "Covert6: a tool to corroborate the existence of IPv6 covert channels," *Annual ADFSL Conference on Digital Forensics*, pp. 100–112, 2016.

[22] K. Barker, "The security implications of IPv6," *Network Security*, vol. 2013, no. 6, pp. 5–9, Jun. 2013, doi: 10.1016/S1353-4858(13)70068-0.

[23] O. E. Elejla, M. Anbar, and B. Belaton, "ICMPv6-based DoS and DDoS attacks and defense mechanisms: review," *IETE Technical Review*, vol. 34, no. 4, pp. 390–407, Jul. 2017, doi: 10.1080/02564602.2016.1192964.

[24] S. E. Frankel, R. Graveman, J. Pearce, and M. Rooks, "Guidelines for the secure deployment of IPv6," Gaithersburg, MD, 2010. doi: 10.6028/NIST.SP.800-119.

[25] A. Al-Ani, M. Anbar, S. A. Laghari, and A. K. Al-Ani, "Mechanism to prevent the abuse of IPv6 fragmentation in OpenFlow networks," *PLOS ONE*, vol. 15, no. 5, May 2020, doi: 10.1371/journal.pone.0232574.

BIOGRAPHIES OF AUTHORS

Marlon A. Naagas holds a Doctorate degree in Information Technology (DIT) from the University of the Cordilleras as a CHED Scholar. He is a CHIEF of Management Information System Office (MISO) and also an Assistant Professor IV of Department of Information Technology, College of Engineering at Central Luzon State University. He is a CISCO CyberSecurity Scholarship Awardee, passed CISCO Certified Network Associate in Cyber Security Operations (CCNA-CyberOps) and CISCO Certified CyberOperation Associate. He is associated to DICT-ILCDB as a trainer. Also, he is heavily Involved in collaborative projects of DOST-ASTI, UPEEEI and CLSU such as Bayanihanets, ASI@Connect-Scimix and CHED PCARI-Prime as a Network and technical consultant.He can be contacted at email: manaagas@clsu.edu.ph.

Anazel P. Gamilla holds a master's degree in Information Technology (MIT) from Tarlac State University (TSU), Philippines. An Instructor of the Information Technology Department, College of Engineering, former Chief of Management Information Systems Office at Central Luzon State University (CLSU) and a Department of Information Technology and Communications Technology (DICT-ILCDB) trainer. Her current research interests include Computer Networks, SDN and Cyber Security. She can be contacted at email: apgamilla@clsu.edu.ph.