International Journal of Network Security & Its Applications (IJNSA), Vol.4, No.6, November 2012

REVIEW ON IPv6 SECURITY VULNERABILITY ISSUES AND MITIGATION METHODS

Supriyanto[1], Raja Kumar Murugesan[2], and Sureswaran Ramadass[3]

[1]Universitas Sultan Ageng Tirtayasa (UNTIRTA), Banten, Indonesia
supriyanto@ft-untirta.ac.id
[2]Taylor's University, Kuala Lumpur, Malaysia
Rajakmar.murugesan@taylors.edu.my
[3]National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia
sures@nav6.org

ABSTRACT

One of the main purposes of Internet Protocol version 6 (IPv6) developments was to solve the IP address depletion concern due to the burgeoning growth of the Internet users. The new Internet protocol provides end-to-end communication, enhanced security and extensibility apart from the other features such as address auto-configuration or plug-and-play and faster packet processing in the routers. However, as a new technology, it is also reported that the protocol introduces some security vulnerabilities both in the header format and in the other protocols associated to it. This paper reviews IPv6 security vulnerabilities that have large potential exploitation in terms of denial of service attacks. The IPv6 security vulnerabilities are classified under three categories that include the IPv6 main header field, IPv6 extension header and Neighbour Discovery Protocol (NDP). This paper also summarizes the current mitigation methods proposed by researchers and practitioners to secure from these IPv6 security vulnerabilities.

KEYWORDS

*IPv6 security vulnerability, flow-label, fragment header, NDP***,** *DoS attacks*

1. INTRODUCTION

IPv6 as the Next Generation Internet protocol and considered as the future Internet or technology has infinite possibilities in terms of connecting the entire world through communication. It is an enabler for the Internet of Things making it possible to throw everything and anything over the Internet. It has insurmountable number of IP addresses that can be used to identify and connect possibly everything in the world over the Internet. Though, the IPv6 was developed and introduced in the 90s [1], it is still a new technology to most Internet users. As a new technology, the users need to understand, learn and adapt to it. The study conducted by Maarten Botterman from the European Commission in IPv6 shows that even though 84% of the survey respondents indicated to have or consider having an IPv6 allocation, the biggest problem with IPv6 penetration is lack of user demand [2]. This is the fact that from a user point view, they don't care what the version of Internet protocol is used. They just wish to have a good Internet connectivity so that their business can continue and grow. Today, most users are connected to the Internet through IPv4. However, the reality also shows that on April 15, 2011 the Asia Pacific Network Information Centre (APNIC), the Regional Internet Registry (RIR) that manages IP address allocation in the Asia Pacific region has already given their last /8 of IPv4 addresses [3]. The rest of the other RIRs have very little /8 of IPv4 address to be released. As known the IPv4 address is said to be depleted when each RIR received its last /8 address [4].

DOI : 10.5121/ijnsa.2012.4613

It is imminent from the above that IPv6 is the only working technology that can assist Internet users to stay connected. IPv6 is necessary not only for Internet connectivity, and Internet continuity but also for business continuity. Today, Internet is perceived as the greatest economy in the world. We need to be prepared to embrace this new technology of IPv6. IPv6 was developed to meet the end to end communication with fast and secure data exchange. With all the big benefits of IPv6, it is believed that in the near future Internet will grow to become more omnipresent in the world.

However, implementation of a new technology such as IPv6 needs to ensure that it would not affect the health of the Internet. The most in consideration is to the security aspect that has got more attention of the researchers [5-7]. Taking this into consideration the IPv6 protocol was developed making IPsec [8] mandatory of IPv6 [9] that was an option in IPv4. IPsec is a set of protocol suite that can be added to IP packets to provide confidentiality and integrity [10] of the message being communicated over the Internet. To do this, IPsec combines two extension headers namely, Authentication Header (AH) [11] and Encapsulation Security Payload (ESP) [12]. Even though the protocol is mandatory, the use of IPsec is optional that is included through general extension header usage. The Internet standards defined by IEEE through Request For Comments (RFCs) also does not mandate that IPsec be used for all IPv6 communications [10]. In addition, IPsec does not cover the entire IPv6 packet header such as flow label field [13]. Thus, security in IPv6 is an important concern that challenges researchers to find out the mitigation techniques against any possible attacks in an IPv6 network.

Despite of the above effort, incidence on compromising IP network and/or the Internet is still in rise. Cisco Annual Report that provided comparison of the rise of vulnerabilities and threat by category reports that since 2008 there is a slight increase in terms of vulnerabilities and threat [14]. CSI survey made in 2010 shows that 45.6% of the respondents have been the subject of at least one targeted attack [15]. Cisco Global Threat Report 2Q11 finds that the rate of unique instances of malware more than doubled in the second quarter of 2011, from 105,536 in March 2011 to 287,298 unique instances in June 2011 [16].

These reports confirm that security is the current and future challenge faced in the Internet communications. Therefore, understanding of IPv6 protocol security vulnerability is very important and critical. Identifying and understanding the security vulnerabilities in Internet communication would help to explore and find possible methods or solutions to mitigate it. This paper reviews on the IPv6 protocol security vulnerabilities and mitigation methods.

2. OVERVIEW OF IPV6 PROTOCOL

It is assumed that the reader has familiarity with the basics of IPv6. This section gives an overview of the three important elements of IPv6 that are also its advantages include the main header field and its format, extension header, and auto configuration mechanism using neighbor discovery protocol (NDP). In principle, the IPv6 header format when compared to IPv4 help to improve the performance of IP packets transmission over current network technology. Fields in IPv4 that are not used has been removed, while fields that are frequently used have been retained with the addition of a new field to improve Quality of Service (QoS) such as flow label [17]. Taking this into consideration, the IPv6 developers have defined the IPv6 header to be simpler than IPv4 to reduce router task. On the other hand they have added optional extension headers to offer additional services needed. Fortunately, the extension headers were included in the packets payload that is not required to be processed in every router along the packets journey to its destination.

2.1. IPv6 Packet Format

The format of IPv6 packet was standardized in RFC 2460 [1] as shown in Figure 1 that consists of fixed main header, optional extension header and data from upper layer. IPv6 main header is fixed 40 bytes that consists of 8 fields instead of 12 fields in IPv4 header. The simpler header was intended to reduce the router task including no header checksum as well as fragmentation in routers. While the extension header is flexible that it is open to add new extension headers in the future. Use of extension header is optional to a source that it can carry either no or one or more extension header in a packet header.

VER is version field that indicates the protocol version. The field is 4 bits that has a value of 06. The second field is an 8 bits *traffic class* field that describes packet priority or its enlistment into a certain traffic class. The following 20 bits is *flow label* that contains information that helps a router to determine the handling of each packet in the flow quickly. This flow label is the only new field introduced in the IPv6 header. The 16 bits *payload length* carries the information on packet size including extension header. With 16 bits, it can identify the maximum length of a packet, 2^{16} or 65,535 bytes. The next 8 bits field is *next header* that defines either header or data type that follows the IPv6 main header. The 8 bits *hop limit* is defined in units of seconds that defines the time limit within which the packet would be discarded. The value of this field decreases by one each time a router forwards the packet. The last two fields of Figure 1 are *IPv6 source and destination address* field that are before the extension header field. These fields are the largest field in the IPv6 header, and each field address is 128 bits long. Source address identifies the address of the source of the IPv6 packet while destination address is the address of the recipient of the IPv6 packet [1].

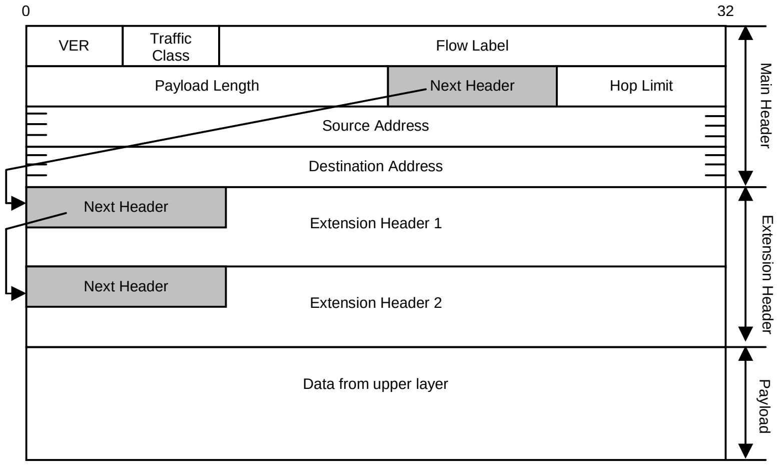


Figure 1. IPv6 Packet Format

Some fields in IPv6 main header are immutable that have fixed value such as version, payload length, next header, source address and destination address (packet without routing header). There are also fields that are not fixed or mutable, they are traffic class, flow label and hop limit. The mutable field especially flow label is a subject of concern to the Internet research community. Even though, IPv6 flow label specification is already standardized [13], it is not used in practice [18]. The number of discussions on implementation of this field is still in rise. RFC 6294 documented proposals on use cases for the IPv6 Flow Label [18].

2.2. IPv6 Extension Header

As shown in Figure 1, IPv6 has an optional field called extension header. The difference with the former is the optional place inclusion of the Next Header field, while the status is still the same. IPv6 extension header is placed after destination address field before upper layer data and they are counted as part of IPv6 payload. In general, most extension headers are not required of processing in routers except for hop by hop option header [1]. This is a benefit of IPv6 extension header. Sender may use more than one extension header to get some services without any additional work or load to the router. Every extension header has next header field that connect any other following extension header in the extension header chain.

By the extension headers, IPv6 opens up the possibility of future growth of Internet services. The hop by hop option header allows the exchange of packet with payload up to 4 GB [19]. This is accordance with the improved link layer technology that supports transmission of jumbo frames [20]. If the Maximum Transmission Unit (MTU) of the link does not support large IPv6 packets, a sender could use path MTU (PMTU) mechanism [21] and perform fragmentation [1] that is also provided in IPv6 extension header. The most important feature of IPv6 extension header is the mandatory support of IPsec that is provided by the authentication header and encapsulated security payload header.

2.3. Neighbour Discovery Protocol

The third advantage of IPv6 is the auto-configuration mechanism that uses Neighbour Discovery Protocol (NDP). It is also called plug-and-play networking for an IPv6 host. An IPv6 host can get an IPv6 address automatically using two types of auto configuration mechanism, stateful address auto-configuration that uses Dynamic Host Configuration Protocol version 6 (DHCPv6) to generate IPv6 address for host [22] and stateless address auto-configuration that includes generating a link local address and generating global addresses [23]. The NDP protocol for IPv6 nodes including router as well as host is specified in RFC 4861 [24].

The NDP protocol regulates the interaction between nodes (router and host) attached to the same link. It defines five different Internet Control Message Protocol version 6 (ICMPv6) packet types that include a pair of Router Solicitation (RS) and Router Advertisement (RA) messages, a pair of Neighbour Solicitation (NS) and Neighbour Advertisements (NA) messages, and a redirect message. Using the five ICMPv6 messages, IPv6 nodes on the same link discover other’s presence, determine each other link layer addresses, find routers and maintain reachability information about the path to active neighbours. The first pair is used to locate and obtain information from routers. The second pair function is to determine the link layer addresses of neighbours as well as to verify that a neighbour is reachable.

This protocol is very important on host initialization and defining network parameter. Host initialization is the process on an IPv6 node to get ready for communication. It includes deriving IPv6 address both local and global scope. It is also used to make sure the address is not in use by duplicate address detection. Failure to do the process, the node may not be able to communicate locally as well as globally. Router discovery that is also done by NDP enable IPv6 nodes to get information on both Internet parameter (hop limit) and link parameter (MTU). These two parameters are essential for sending IPv6 packets externally.

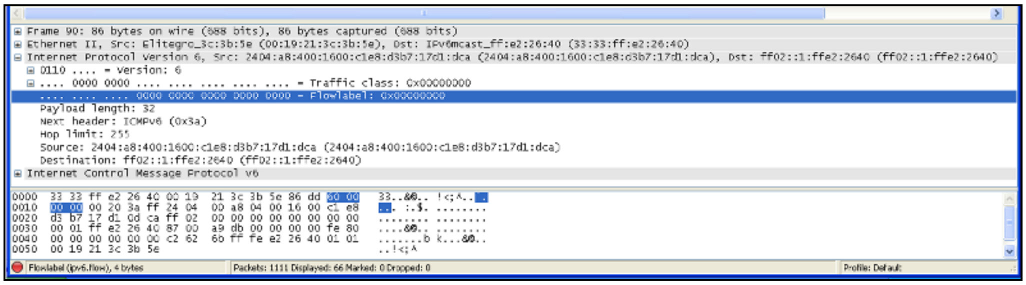
3. IPv6 Security Vulnerability and Mitigation Methods

There is no doubt that the IPv6 protocol has many advantages and the arrival of the new technology in the real world is immediately available in reality. However, IPv6 as a new technology may be bound to incorrect configuration that could open vulnerabilities to be exploited by others. The exploitation of IPv6 security vulnerabilities could make the advantages of IPv6 to become suboptimal. This section surveys IPv6 protocol vulnerabilities as well as their impact on IPv6 packet transmissions. RFC 4942 classified the vulnerability related to IPv6 in to three categories: vulnerability due to the IPv6 protocol itself, vulnerability of IPv6 transition, and vulnerability on IPv6 deployment. This paper focuses on the first and categorizes the vulnerability of the IPv6 protocol in to three groups. The three groups are identified based on the three main features of IPv6 that are also its advantages. They are IPv6 main header, IPv6 extension header and IPv6 associated protocols such as NDP and ICMPv6.

3.1 IPv6 Main Header

The IPv6 main header is fixed in size of 40 bytes. However, the size is not optimally used nowadays. Most of the fields in IPv6 header are available in IPv4, may be the field name are different. The only new field is flow label. It is part of IPv6 main header and intended to label an IPv6 packet flow. However, as a new field it also invited lot of discussion among researchers to define the flow label's functionality. A number of proposals were submitted to IPv6 working group as noted in RFC 6294 [18]. The specification of the field also was always changing. Firstly, the flow label was specified in the IPv6 specification standard RFC 2460. It was updated by two standards RFC 3697 and RFC 6437. In the security point of view, this field has several vulnerabilities as identified below:

a. The flow label is hardly used in practice in most widespread IPv6 implementation. Currently, most host implementations are simply set to zero [25], pass the field unchanged or this field is ignored when forwarding packets [1]. Figure 2 shows the zero in the flow label field (highlight part) in real IPv6 traffic captured in National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia.



```
⊞ Frame 90: 86 bytes on wire (688 bits), 86 bytes captured (688 bits)
⊞ Ethernet II, Src: Elitegro_3c:3b:5e (00:19:21:3c:3b:5e), Dst: IPv6mcast_ff:e2:26:40 (33:33:ff:e2:26:40)
⊟ Internet Protocol Version 6, Src: 2404:a8:400:1600:c1e8:d3b7:17d1:dca (2404:a8:400:1600:c1e8:d3b7:17d1:dca), Dst: ff02::1:ffe2:2640 (ff02::1:ffe2:2640)
  ⊞ 0110 .... = Version: 6
  ⊞ .... 0000 0000 .... .... .... .... .... = Traffic class: 0x00000000
    .... .... .... 0000 0000 0000 0000 0000 = Flowlabel: 0x00000000
    Payload length: 32
    Next header: ICMPv6 (0x3a)
    Hop limit: 255
    Source: 2404:a8:400:1600:c1e8:d3b7:17d1:dca (2404:a8:400:1600:c1e8:d3b7:17d1:dca)
    Destination: ff02::1:ffe2:2640 (ff02::1:ffe2:2640)
⊞ Internet Control Message Protocol v6

0000  33 33 ff e2 26 40 00 19  21 3c 3b 5e 86 dd 60 00   33..&@.. !<;^....
0010  00 00 00 20 3a ff 24 04  00 a8 04 00 16 00 c1 e8   ... :.$. ........
0020  d3 b7 17 d1 0d ca ff 02  00 00 00 00 00 00 00 00   ........ ........
0030  00 01 ff e2 26 40 87 00  a9 db 00 00 00 00 fe 80   ....&@.. ........
0040  00 00 00 00 00 00 c2 62  60 ff fe e2 26 40 01 01   .......b `...&@..
0050  00 19 21 3c 3b 5e                                  ..!<;^

Flowlabel (ipv6.flow), 4 bytes | Packets: 1111 Displayed: 66 Marked: 0 Dropped: 0 | Profile: Default
```

Figure 2. Flow Label Value in the Current IPv6 Traffic

This would open the door for two kinds of Denial of Service (DoS) attacks [7]. Firstly, an attacker could forge large number of IPv6 packets with different values of flow label. This makes the victim's memory to be exhausted leading to system crash and causing denial of services to legitimate flows [26]. Secondly, an attacker could send forged packets to make the victim record the packet header resulting in future packets being discarded from legitimate host due to not including the same extension header as the forged packet.

b. Flow label is not protected in any way [25]. There is no header checksum in IPv6 main header. The flow label is also not included in transport pseudo-header checksums. As a result intentional and malicious changes to its value cannot be detected.

c. The zero value of flow label in Figure 2 could also be used as a covert channel implementation. Attacker is able to set a false value of flow label that impact on intermediate devices to perform wrong services [27]. An attacker also could forge an IPv6 packet with specific value of flow label to request specific services such as 'do not modify the flow label value'. Packet delivery may get in to a problem as the intermediate nodes will assume this as default behaviour.

d. If the value of flow label is predictable, this could result in an information leakage [7]. A third party could inject traffic directly to the flow label field and set another flow label value to make the router busy and deny performing services.

To mitigate the above flow label vulnerability, the value of the field must not be easily predictable by other parties. To do this, authors of [28] have proposed the use of a Pseudo Random Number Generator (PRNG) to generate the value of flow label. PRNG is an algorithm for generating a sequence of numbers that approximates the properties of random numbers. This method is a general random number generator including security implementation. The generator usually uses a short random seed as an input and produces output as a long stream which is indistinguishable from truly random bits. The authors of [7] proposed an alternative algorithm of Flow Label value generation using a mathematical formula as follows:

$$\text{Flow Label} = F\,(SA, DA, SK2) + \text{table}\,[G\,(SA, DA, SK1)]$$

F ( ) and G ( ) is a hash function that uses Source Address (SA), Destination Address (DA) and a Secret Key (SK) as input. Result of the functions should not be computable without the knowledge of all parameters in the hash functions. Table on the second function is an array of counters that are initialized to random value. The secret key is any secret number that has 128 bits length and should change after some time or automatically to produce better random data.

3.2 IPv6 Extension Header

IPv6 extension header is an optional header in IPv6 that offers protocol extensibility. There are six extension headers specified in RFC 2460. Several advantages of IPv6 protocol is supported by these extension headers such as security, jumbo gram and mobility. However, the flexibility of IPv6 extension header is reported to also introduce some security vulnerabilities. Possibility to define new extension header without specific limitation will affect the security mechanism. Every new extension header definition that is deployed needs to change security policy [29]. It provides opportunity for attackers to craft an IPv6 packet with extension header manipulation for the purpose of denying a network service [10]. In addition, each type of IPv6 extension header also has vulnerability. This section provides details of some IPv6 extension header vulnerabilities based on current standardized extension headers.

3.2.1 Hop by hop Option Header

Hop by hop option header is the only extension header that will be processed by routers along the packet journey to destination. This extension header is placed in the first order of IPv6 extension header chain. It may contain more options and each option could appear multiple times with various sizes as shown in Figure 3. This could be exploited by an attacker to make DoS attack by manipulating inconsistent options [29]. The DoS attack could be launched by forming IPv6 packets with large number of options. As every router has to look at each option carried by the header, it will be difficult to control [30]. In addition, if all routers along the path get affected by this attack, packet transmission will be in problem. Potential security issue is present within the option field, where one of the options is the Router Alert option. Misuse of this option could degrade the CPU performance of router [10]. Another vulnerability of this extension header is the use of padding option Pad1 and PadN to ensure the size is 8 octet boundaries. These options are the same with destination option header that is only processed in the destination node. Normally, these padding are zero values. However, attacker could deliberate to craft non-zero value of padding option that will cause a covert channel communication.

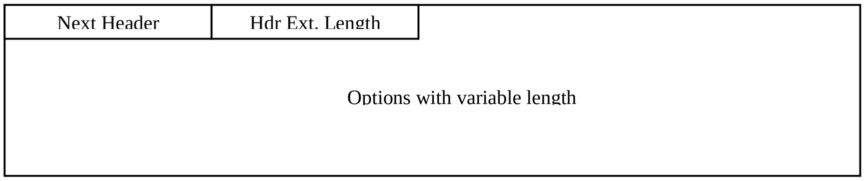


Figure 3. Format of Hop by Hop Option Header

Due to the hop by hop option header has to be present in the first order of extension header chain, exploitation of this extension header will impact overall data transmission. Therefore, mitigating this extension header from any threat is important. Several mechanisms have been proposed to solve this problem such as [10] and [30]. However, until now no appropriate solution has been found. Instead, the author of [30] proposed to deprecate this extension header from IPv6 specification or stopping new option definition. IPv6 nodes have to skip the header without processing this option within the extension header. It also suggests using other method which is to limit the rate of packet with hop by hop extension header and randomly dropping the packets when the CPU load is very high.

3.2.2 Type 0 Routing Header

One type of extension header in IPv6 is routing header that has value 43 identified by next header field [1]. It is used by an IPv6 host to list one or more intermediate nodes to be visited along the journey until the destination is reached. There are two types of routing header, type 0 (RH0) for source routing indication and type 2 (RH2) for mobile IPv6. A single RH0 may contain multiple addresses of intermediate nodes. Therefore the destination of the IPv6 packet will be replaced at every network layer hop that is processing the routing header. The final destination node will receive the packet with intermediate node as the source. This is a vulnerability of the routing header. It may invite attacker to exploit them by rebounding an IPv6 packet to a potential victim. The attacker also could bypass firewall that do not check for the presence of the routing header extension [10] [31] [32].

If the packet filtering does not have capability to process routing header, attacker could access the filtering system to gather secret information. The information may be used to generate malicious packet with routing header to perform attacks on the IPv6 network. If an IPv6 packet has single RH0 that contain more intermediate nodes addresses, same address may appear more than once. This is also a vulnerability that allows attacker to construct such packet that will be processed many times between two RH0 inside the packet. Attacker may also launch a packet to be amplified along the path between two remote routers. This will lead to network congestion. Thus, a legitimate packet is difficult to be transmitted in this way. Experiment of this vulnerability exploitation was presented by Biondi and Ebalard [33]. This presentation was one of the considerations of IETF to deprecate the usage of RH0 in IPv6 packet transmission [34].

3.2.3 Fragmentation Header

The principle of IP packet transmission is to deliver an IP packet from source to destination. Sending a few large packets is better than many small packets to carry large amount of data. This is because the cost needed for packetized communication of data is based on packets rather than bytes [35]. This reality has encouraged researchers to find suitable size of packets to be sent efficiently such as jumbo frame [20] and super jumbo frame [36] over the gigabit Ethernet. However, the network infrastructure of current IP packet transmission varies in their capability to send packets that is defined by a Maximum Transmission Unit (MTU). Some of them have small capability to transmit packets such as the common Ethernet that has a MTU of 1500 bytes. Sending a large packet through the small MTU media is possible by breaking the packet into smaller fragments and sent individually. This concept then called fragmentation that were used in IPv4 is also used in IPv6 as extension header.

Fragmentation is a dilemma due to its negative impact on IP packet transmission. The authors in [35] have presented three arguments against fragmentation; it causes inefficient use of resources, loss of fragments leads to degraded performance, and making efficient fragmentation is hard. The author recommended avoiding fragmentation by sending small packet and guessing the media MTU. In IPv4, the fragmentation done in every router caused additional task to the router. IPv6 development has accommodated the recommendation by introducing path MTU discovery. However, the new protocol also opens the possibility to use fragmentation using fragmentation header. If the extension header is used in IPv6 packet transmission, the problem of fragmentation may also appear.

In addition, the usage of fragmentation header in IPv6 also introduces security vulnerability that does not appear in IPv4. The first security hole is when the fragments overlap that is not specified in RFC 2460. It could be used by attackers to bypass the filtering system in the receiver. Attackers can form the following fragment by changing the TCP header such as, change the ACK = 0. By doing this, the receiver will think that the packet received in a connection is a request instead of response. RFC 5722 stated that this security hole is more dangerous in IPv6 than in IPv4. This is because a fragment in IPv6 may contain source and destination port that are exploitable by attackers [37]. To avoid the negative impact of fragment overlapping, it is important to consider the packet fragmentation. If the fragmentation is required by sender, it must not create overlapping. When the packets reach the destination that needs to reassemble, the receiver has to discard the datagram with fragment overlapping indication.

The second security hole is the predictable value of fragment identification field. The usage of a global counter for setting the fragment identification field may generate predictable values. If this happens, it may potentially result in information leakage that can be exploited by a malicious node [38]. This can be done by determining the packet rate at which a given system is transmitting information. It also can be used to perform a DoS attack by sending *packet too big* report from a third party. The victim then replies a packet with fragmentation header to the third party. Identification value inside the packet can be used to forge IPv6 packets resulting in sending malicious fragment from attacker. Identification field on fragmented packets is very important. Thus, the value has to be unpredictable. This can be done by performing destination cache entry look up before sending an IPv6 packet. In the cache if the last fragment identification value exists, the next value should be incremented. Otherwise, a new identification value using random number could be created [38].

3.3 Neighbour Discovery Vulnerability

Neighbour Discovery Protocol (NDP) is one of the important protocols associated with IPv6 used by a node to discover its neighbour in the same link. However, it has certain vulnerability that is prone to attackers to be exploited. Threat and vulnerabilities on NDP are specified in RFC 3756 [39]. The authors of RFC 3756 categorized the threats and vulnerabilities in to three types. Firstly, threats related to non router/routing that exploits the NDP messages includes NS/NA spoofing, Neighbour Unreachability Detection (NUD) failure and Duplicate Address Detection (DAD) DoS attack. Secondly, threats related to router/routing such as malicious last hop router, default router is ‘killed’, good router goes bad, redirect message spoofing, bogus on-link prefix and parameter spoofing. The third is remotely exploitable attacks that consist of replay attack and NDP DoS attack. All the attack types caused a denial of service on the IPv6 network.

One of the benefits of NDP implementation is stateless IPv6 auto-configuration [23]. There are three ways to get IPv6 address using this stateless mechanism. Firstly, EUI-64 mechanism that generates interface id of IPv6 address from 48 bits of node's MAC address [40]. Secondly, privacy extensions address mechanism that generates the interface id randomly [41]. Thirdly, Cryptographically Generated Addresses (CGA) mechanism that generates the interface id using cryptography [42].

However, before an IPv6 node gets an IPv6 address, it will process the duplicate address detection as explained in [23]. The process begins by sending multicast NS message that contains a temporary IPv6 address to all neighbours. The DAD process will end by receiving a NA message from the neighbouring nodes. An attacker could send a forged NA message repeatedly that causes DAD to fail. If the DAD process failed, the new host is unable to get an IPv6 address and cannot do communication with other nodes. NDP also does the router discovery by sending RS messages to multicast group of routers in the same link. An attacker may send forged RA message as response to the RS sent by a new host. By receiving the forged RA message, the host will get wrong information on network prefix, default router and network parameters. Hence, network services will not be received by this node.

NS/NA messages may also overwrite neighbour cache information on an IPv6 node. Exploitation of NDP messages may cause the neighbour cache overflow in an IPv6 node. As known, IPv6 has a default subnet of /64 that makes possible to have 2^{64} addresses in a network [43, 44]. However, in reality the number of machines in a network is very small compared to the default subnet number. This attracts attackers to spoof the network by sending more NS/NA messages that makes the neighbour cache full. Therefore, a new IPv6 node cannot attach to the network. The old node also finds difficult to communicate with others due to overwriting address in the cache. As known, a node has neighbour cache entry that contains default router list, prefix list, link layer address and neighbour reachability state. The last information is used to perform NUD. However, RFC 4861 specifies that the timeout of default router list in a neighbour cache is too short (a second for three transmission probe).

Mitigating NDP vulnerability from attacker is very important because most of the benefits of IPv6 implementation will not be used if the NDP messages are in wrong condition. The benefits of IPv6 that depending on the NDP are PMTU discovery, router discovery, neighbour discovery, prefix discovery and address auto configuration. Therefore, an IETF working group standardized SEND [45] to secure the NDP process. SEND is an enhancement of the NDP by adding several options on the ICMPv6 messages used in NDP. The options include CGA (Cryptographically Generated Address), RSA signature, Nonce and Timestamp. It also offered two ICMPv6 messages on router authorization process: CPS (Certificate Path Solicitation) and CPA (Certificate Path Advertisement). However, implementation of this security protocol faced several limitations as studied in [46]. The limitations include non-guarantee that NDP communication is confidential, computation exhaustion and bandwidth consumption. Several proposals were proposed to enhance the SEND protocol deployment.

In [47], the authors defined a new NDP option called RSA encryption option field. The new option results in an encryption process using Advanced Encryption Standard (AES). Both NS and NA messages provide RSA algorithm [48] using a public key. Due to the CGA verification, which consumes large amount of computing resources, attacker could launch DoS attack by forging large number of packets to the machine such that it runs out of resources [49]. They proposed a mitigation method to prevent SEND from DoS attack by adding a set of message interaction before CGA verification without any security infrastructure. Regarding the neighbour cache entry of an IPv6 node, there are three Internet draft proposed to manage the cache and handle the reachability time. In [43] and [44], the authors recommended to prioritize the NDP activities, manage the entry queue and refresh the neighbour cache entry. While [50] suggested timing on the status of neighbour reachability. They proposed to give longer time rather than 3 seconds for the case where there is no alternative for the host to switch the status on Neighbour Unreachability Detection.

4. CONCLUSIONS

IPv6 as the next generation protocol comes with a host of advantages that many are yet to be realized. However, as a new protocol it also has security vulnerability apart from its benefits. There are three parts of the IPv6 protocol that are vulnerable to network attacks. The first is in the IPv6 main header that is the flow label field whose specification is still in discussion today. The zero value of the flow label in the current implementation could be exploited by an attacker to cause network disturbance. The second is the extension header that includes hop by hop option header, type 0 routing header and fragmentation header. Hop by hop options has to be placed in the first order, thus all node has to process the extension header. The Type 0 Routing header (RH0) has already been deprecated as defined in RFC 5905. The fragmentation header is currently still in discussion. The third vulnerability is in the protocol associated with IPv6. The most important protocol is the ICMPv6 that is used by NDP to discover router, network prefix, neighbours and also network parameters. In order to secure NDP, IETF standardized SEND to ensure that the NDP process is safe. However, the SEND is also reported to have constraints in its implementation

ACKNOWLEDGEMENTS

This research was supported by the Directorate General of Higher Education, Ministry of Education and Culture, the Republic of Indonesia, and in collaboration with National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia, and Taylor's University, Malaysia.

REFERENCES

[1] Request for Comments: 2460, Internet Protocol Version 6 (IPv6) Specification, December 1998: Internet Engineering Task Force. http://www.ietf.org/rfc/rfc2460.txt.

[2] Botterman, M., *IPv6 Deployment Survey*, 2010, The European IPv6. Available from: http://www.nro.net/wp-content/uploads/ipv6_deployment_survey.pdf

[3] IPv4 Exhaustion Counter. [cited 2012 February 20]; Available from: www.ipv6forum.org.

[4] Deploying IPv6: The Time Is Now. [cited 2012 February 20]; Available from: http://www.nro.net/ipv6.

[5] Arkko, J. and P. Nikander, *Limitations of IPsec policy mechanisms*, in Proceedings of the 11th international conference on Security Protocols 2005, Springer-Verlag: Cambridge, UK.

[6] Atay, S. and M. Masera, *Challenges for the security analysis of Next Generation Networks. Information Security Technical Report*, 2011. 16(1): p. 3-11.

[7] Gont, F., Security Assessment of the IPv6 Flow Label, Internet Draft 2012 work in progrres. http://tools.ietf.org/html/draft-gont-6man-flowlabel-security-03

[8] Request for Comments: 4301, Security Architecture for the Internet Protocol, 2005. Internet Engineering Task Force. http://www.ietf.org/rfc/rfc4301.txt.

[9] Request for Comment 4294, IPv6 Node Requirements, 2006. Internet Engineering Task Force http://www.ietf.org/rfc/rfc4294.txt.

[10] Hogg, S. and E. Vyncke, *IPv6 Security* 2009: Cisco Press.

[11] Request for Comment 4302, IP Authentication Header, 2005, Internet Engineering Task Force. http://www.ietf.org/rfc/rfc4302.txt.

[12] Request for Comments: 4303, IP Encapsulating Security Payload (ESP), 2005, Internet Engineering Task Force. http://www.ietf.org/rfc/rfc4303.txt.

[13] Request for Comment 6437, IPv6 Flow Label Specification, in 2011, Internet Engineering Task Force. http://www.ietf.org/rfc/rfc6437.txt.

[14] Cisco 2011 Annual Security Report, 2011. Available from: http://www.cisco.com/en/US/prod/collateral/vpndevc/security_annual_report_2011.pdf

[15] CSI, 2010/2011 Computer Crime and Security Survey, 2011. Available from: http://gocsi.com/survey/

[16] Cisco 2Q11 Global Threat Report 2011. Available from: http://www.cisco.com/en/US/prod/collateral/vpndevc/cisco_global_threat_report_2q2011.pdf

[17] Blanchet, M., *Migrating to IPv6 : A Practical Guide to Implementing IPv6 in Mobile and Fixed Networks* 2006, Québec, Canada: John Wiley & Sons Ltd.

[18] Request for Comments: 6294, Survey of Proposed Use Cases for the IPv6 Flow Label, 2011, Internet Engineering Task Force. http://www.ietf.org/rfc/rfc6294.txt.

[19] Request for Comments: 2675, IPv6 Jumbograms, in 1999, Internet Engineering Task Force. http://www.ietf.org/rfc/rfc2675.txt.

[20] Garcia, N.M., M.M. Freire, and P.P. Monteiro. *The Ethernet Frame Payload Size and Its Effect on IPv4 and IPv6 Traffic*. International Conference on Information Networking (ICOIN), 2008.

[21] Request for Comments 1981, Path MTU Discovery for IP version 6, in 1996, Internet Engineering Task Force. http://www.ietf.org/rfc/rfc1981.txt.

[22] Request for Comments 3315, Dynamic Host Configuration Protocol for IPv6 (DHCPv6), in 2003, Internet Engineering Task Force. http://www.ietf.org/rfc/rfc3315.txt.

[23] Request for Comments 4862, IPv6 Stateless Address Autoconfiguration, in 2007, Internet Engineering Task Force. http://www.ietf.org/rfc/rfc4862.txt.

[24] Request for Comments 4861, Neighbor Discovery for IP version 6 (IPv6), in 2007, Internet Engineering Task Force. http://www.ietf.org/rfc/rfc4862.txt.

[25] Request for Comments 6436, Rationale for Update to the IPv6 Flow Label Specification, in 2011, Internet Engineering Task Force. http://www.ietf.org/rfc/rfc6436.txt.

[26] Prasad, K.M., A.R.M. Reddy, and V. Jyothsna, *IP Traceback for Flooding Attacks on Internet Threat Monitors (ITM) Using Honeypots*. International Journal of Network Security & Its Applications (IJNSA), 2012. **Vol. 4**(No. 1): p. pp. 13 - 27.

[27] Lucena, N., et al., Covert Channels in IPv6. Privacy Enhancing Technologies (Vol. 3856, pp. 147-166): Springer Berlin / Heidelberg.

[28] Dorrendorf, L., Z. Gutterman, and B. Pinkas, *Cryptanalysis of the random number generator of the Windows operating system*. ACM Trans. Inf. Syst. Secur., 2009. 13(1): p. 1-32.

[29] Choudhary, A.R. and A. Sekelsky. *Securing IPv6 network infrastructure: A new security model.* 2010 IEEE International Conference on Technologies for Homeland Security (HST). 2010.

[30] Krishnan, S., The case against Hop-by-Hop options, Internet Draft 2010 work in progress. Internet Engineering Task Force. http://tools.ietf.org/html/draft-krishnan-ipv6-hopbyhop-05

[31] Jeong-Wook, K., et al. *Experiments and Countermeasures of Security Vulnerabilities on Next Generation Network*. Future Generation Communication and Networking (FGCN 2007). 2007.

[32] Wadhwa, M. and M. Khari, V*ulnerability Of IPv6 Type 0 Routing Header And It's Prevention Algorithm*. International Journal of Advanced Engineering Sciences and Technologies 2011. Vol. 5(No. 1): p. 056 - 061.

[33] Biondi, P. and A. Ebalard, *IPv6 Routing Header Security,* in CanSecWest 2007: Canada. Available from: www.secdev.org/conf/IPv6_RH_security-csw07.pdf

[34] Request for Comments 5095, Deprecation of Type 0 Routing Headers in IPv6, 2007, Internet Engineering Task Force. http://www.ietf.org/rfc/rfc5095.txt.

[35] Kent, C.A. and J.C. Mogul, *Fragmentation considered harmful*. SIGCOMM Comput. Commun. Rev., 1995. 25(1): p. 75-87.

[36] Rutherford, W., et al., *16 000-64 000 B pMTU experiments with simulation: The case for super jumbo frames at Supercomputing '05*. Optical Switching and Networking, 2007. 4(2): p. 121-130.

[37] Request for Comment 5722, Handling of Overlapping IPv6 Fragments, in, Internet Engineering Task Force. http://www.ietf.org/rfc/rfc5722.txt.

[38] Gont, F., Security Implications of Predictable Fragment Identification Values, Internet Draft work in progress 2011, Internet Engineering Task Force. http://tools.ietf.org/id/draft-gont-6man-predictable-fragment-id-00.txt

[39] Request for Comments 3756, IPv6 Neighbor Discovery (ND) Trust Models and Threats, 2004, Internet Engineering Task Force. http://www.ietf.org/rfc/rfc3756.txt.

[40] Request for Comments 5342, IANA Considerations and IETF Protocol Usage for IEEE 802 Parameters, 2008, Internet Engineering Task Force. http://www.ietf.org/rfc/rfc5342.txt.

[41] Request for Comments 4941, Privacy Extensions for Stateless Address Autoconfiguration in IPv6, 2007, Internet Engineering Task Force. http://www.ietf.org/rfc/rfc4941.txt.

[42] Request for Comments 4581. Cryptographically Generated Addresses (CGA), 2005, Internet Engineering Task Force. http://www.ietf.org/rfc/rfc4581.txt.

[43] Request for Comment 6583. Operational Neighbor Discovery Problems, Internet Engineering Task Force. http://www.ietf.org/rfc/rfc6583.txt.

[44] Kumari, W., I. Gashinsky, and J. Jaeggli, Neighbor Discovery Enhancements for DOS mititgation, Internet Draft work in progress 2012, Internet Engineering Task Force. http://tools.ietf.org/html/draft-gashinsky-6man-v6nd-enhance-00

[45] Request for Comments 3971, SEcure Neighbor Discovery (SEND), 2005, Internet Engineering Task Force. http://www.ietf.org/rfc/rfc3971.txt

[46] Alsa'deh, A. and C. Meinel, *SEcure Neighbor Discovery: Review, Challenges, Perspectives and Recommendations*. Security & Privacy, IEEE, 2012. PP(99): p. 1-1.

[47] ByungGoo, C., et al. *Enhanced SEND Protocol for Secure Data Transmission in Mobile IPv6 Environment*. International Conference in Computational Sciences and Its Applications, 2008. ICCSA '08.

[48] Sainia, H., T.C. Panda, and M. Panda, *Prediction of Malicious Objects in Computer Network and Defense.* International Journal of Network Security & Its Applications (IJNSA), 2011. **Vol. 3**(No. 6): p. pp. 161 - 171.

[49] Meigen, H., L. Jianrong, and Z. Yunjie. *An improved SEND protocol against DoS attacks in Mobile IPv6 environment*. IEEE International Conference in Network Infrastructure and Digital Content, 2009. IC-NIDC 2009.

[50] Nordmark, E. and I. Gashinsky, Neighbor Unreachability Detection is too impatient, Internet Draft work in progress2012, Internet Engineering Task Force. http://tools.ietf.org/html/draft-ietf-6man-impatient-nud-01

Authors

Supriyanto received his B.Eng. degree in Electrical Engineering from Brawijaya University Malang, Indonesia in 1999, and M.Sc in Computer Sciences from Universiti Sains Malaysia (USM) in 2010. He is lecturer in the Electrical Engineering Department at the Universitas Sultan Ageng Tirtayasa (UNTIRTA) Indonesia. Currently, he is pursuing his PhD at the National Advanced IPv6 Centre in USM, Malaysia. His research interest includes computer networks, IPv6 security, IPTV over overlay network and wireless communication.

Raja Kumar Murugesan is a Senior Lecturer, and Heads Research at the School of Computing in Taylor’s University, Malaysia. He holds a PhD in the area of Advanced Computer Networks, M.Phil in Computer Science, M.Sc in Computer Electronics, Post Graduate Diploma in Computer Science & Applications (PGDCA), and a B.Sc. in Physics. His research interest includes Internet Communication Protocols especially IPv6 (Internet Protocol version 6), Internet Addressing Architecture, Network Architecture, Internet Governance, Future Internet, and Microprocessor based systems.

Prof Dr Sureswaran Ramadass is the Director of the National Advanced IPv6 Centre of Excellence (NAv6) at Universiti Sains Malaysia. He obtained his BsEE/CE (Magna Cum Laude) and Masters in Electrical and Computer Engineering from the University of Miami in 1987 and 1990 respectively. He graduated as the top student in the College of Engineering for his Bachelors Degree. He obtained his PhD from Universiti Sains Malaysia (USM) in 2000 while serving as a full time faculty in the School of Computer Sciences. His research interest includes IPv6, Network Monitoring and Security and Multimedia Conferencing System.