Applied Computing Journal https://doi.org/10.52098/acj.202112
ISSN: 2788-9688 Volume 1, Issue 1, pp 1-9, January 2021
Received: 22/10/2020 Revised: 3/1/2021 Accepted: 23/1/2021

IPv6 Multicast Vulnerability – An Overview

Shubair Abdullah*[1]
[1]Instructional and Learning Technology Department, Sultan Qaboos University
* Corresponding author: Shubair Abdullah, shubair@squ.edu.om

Abstract

IPv6 is the next Internet Protocol version designed to eventually replace IPv4 as the number of potentially allocated IPv4 addresses is insufficient. The vulnerabilities of the IPv6 protocols and the attacks on them demand more attention be paid. The multicast mechanism is one of the crucial mechanisms related to the IPv6 protocol. Despite its usefulness in performing basic tasks in IPv6 environments, the multicast mechanism is considered a security hole that calls to be understood by the security specialists and IPv6 network administrators. To address the multicast security aspects, this paper presents attacks that use the multicast vulnerability along with the identification of countermeasures for each attack. In particular, this paper analyzes the state-of-the-art attacks and ranks them based on a new severity ranking method to provide significant security guidance for deploying IPv6 networks. The results of the severity calculation show that the DoS attack is the most dangerous attack, getting 4.5 out of 10, followed by the reconnaissance attack and the "smurf" attack which have 2 and 1.5 degree respectively.

***Keywords**:* IPv6; multicast; vulnerability; reconnaissance phase; Smurf attack; DoS attack

1. Introduction

The year 1998 witnessed the development of IPv6 as a successor to IPv4. The main reason for developing IPv6 is that the amount of potentially allocated IPv4 address is insufficient as the Internet is expanding rapidly. IPv6 technology possesses multiple new features. IPv6 address space allows 2128 addresses that mean one IP address for every Internet-capable device on the planet. The IPv6 clients can independently auto-configure their interfaces with plug-and-play IPv6 addresses using a combination of locally-available information and information automatically advertised by IPv6 routers when connected to an IPv6 segment. The new protocol specifies a new packet format that helps achieve fast routing of the packet for networking, reduces the size of routing tables and makes routing more efficient. Moreover, the overhead on routers has been reduced by avoiding the checksum recalculation process, which is a result of eliminating IP-level checksum in IPv6 (Davies, 2012).

The IPv6 technology is fairly new vector to a large group of security specialist. The security holes that might be exploited need to be understood. The security specialist must be trained to understand and avoid all the IPv6 security vulnerabilities. A new feature that can be considered a critical feature in IPv6 is the multicast technology. IPv6 multicast is a mechanism that serves to save the network bandwidth, it transmits a single copy of datagram from one source to a group of receivers. An IPv6 multicast address is a single address identifies a group of IPv6 addresses. A packet sent to that address will be received by all interfaces identified by that address. Since a multicast address is an identifier for a collection of nodes in a network segment, this address can never be the source address of packets. An IPv6 multicast group of addresses usually begins with the prefix FF02. Some examples of groups of IPv6 multicast addresses include the following:

- ff02::1: All IPv6 devices
- ff02::2: All IPv6 routers
- FF05::1:3 All DHCPv6 Servers
- ff02::5: All OSPFv3 routers

One segment could have one or more multicast group and a node can be part of more than one multicast group (Hagen, 2014). When a packet is initiated by a host toward a multicast address, all members of the multicast group receive the packet. Any host regardless of whether it is a member of a multicast group, can send packets to it, but only the group members receive the packet.

IPv6 heavily relies on the multicast messages. It uses them for Neighbor Discovery Protocol (NDP) and Internet Control Messaging Protocol (ICMPv6) (Horley, 2014). Moreover, multicast mechanism reduces the overall network load and minimizes the impact on the source from unnecessary replication of traffic (Hagen, 2014). Examples of applications that take advantage of multicast addresses include video conferencing, news, and distance learning.

Despite its usefulness, the multicast mechanism is considered also as a one of the security holes that are related to the IPv6 protocol specifications (Shubair, 2017). If an attacker succeeds in penetrating a multicast group, he can send anomaly packets to conduct a malicious activity against the network such as reconnaissance, Smurf, and Denial of Services (DoS) against all nodes in a network segment. Since the anomaly packets are not routed, all attacks caused by multicast vulnerability are only applicable if the attacker resides on the local segment (Hinden & Deering, 2006). Therefore, the multicast vulnerability has called the developers of IPv6 as well as the scientists to invent security solutions. The scope of this paper is limited to IPv6 multicast vulnerability. It introduces an overview of the threats to IPv6 networks that are caused by utilizing the multicast vulnerability along with solutions that could be used to counter and prevent IPv6 multicast utilization attacks. Moreover, it analyzes and ranks the attacks based on a new attack severity-ranking method.

The reminder of this paper is organized as follow: Section II provides some background information and refers to the literature of the paper. Section III discusses the attacks and countermeasures. Section IV provides results of discussing the attacks and countermeasures. Finally, Section V concludes the research.

2. Background and Literature Review

IPv6 multicast uses two protocols: Multicast Listener Discovery (MLD) protocol and Protocol Independent Multicast (PIM). The MLD protocol is used by IPv6 switches to discover the nodes ready to receive multicast packets on the directly attached links. All MLD messages are link-local with a hop limit of 1 and are carried by the ICMPv6. Alternatively, the PIM is by IPv6 switches to track which multicast packets to forward to other switches don the directly attached links. According to Cisco, the implementation and customization of IPv6 multicast along with MLD and PIM protocols have no specific instruction to secure the multicasting process. However, they recommend some configurations such as configuring “the timeout value before the switch takes over as the querier for the interface” and configuring “MLD reporting for a specified group and source” in customizing the MLD

Few research papers have been published to identify the attacks on IPv6 and to review the countermeasures (Arjuman & Manickam, 2015; Elejla, Anbar, & Belaton, 2016; R. M. Saad, 2013). However, many approaches have

been introduced to mitigate the DoS attacks on IPv6 networks. (Barbhuiya, Biswas, & Nandi, 2011) and (Bansal, Kumar, Nandi, & Biswas, 2012) proposed Intrusion Detection Systems (IDSs) to detect ICMPv6 DoS attacks. The authors in (An & Kim, 2008) developed an approach that uses routers to classify the IPv6 packet based on their addresses to DoS and normal packets. In the same context, some research attempted to upgrade the published IDS for IPv4 network to work in IPv6 networks. For example (Saad, Anbar, Manickam, & Alomari, 2015) introduced a system of ICMPv6 flooding-attack detection framework using back-propagation neural network in IPv6 networks.

Some researchers have focused on studying the transition mechanisms from IPv4 to IPv6. For example (Lencse & Kadobayashi, 2019) introduced a comprehensive survey of IPv6 transition technologies in their efforts to identify the technologies that will play the most important role in the transition to IPv6 for several years. In the same context, a new methodology has been developed to identify the potential security issues of different IPv6 transition technologies based on the STRIDE approach (Lencse & Kadobayashi, 2018).

Despite these efforts of the scientists, many potential IPv6 multicast security issues are still identified as open issues and need to be addressed. These issues include securing the DHCPv6 servers multicast group (FF05::1:3), and securing the IPv6 routers multicast group (FF05::2). The attacker would be provided with information about the systems that are parts of these two groups that could be used to launch more severe attacks, i.e. reconnaissance, smurf, and DoS, if he can send multicast packets and get responses.

3. Research Methodology

This section first reviews the possible scenarios for three attacks: reconnaissance, smurf, and DoS. Second, it provides the available countermeasures for these attacks. The scope of these scenarios is local network segments and their focuses will be on utilizing the multicast vulnerability.

3.1. Multicast Vulnerability Attacks

The reconnaissance attack is launched by attackers to find vulnerable hosts on the network. In most cases, the reconnaissance attack is an initial phase for a subsequent malicious phase. After the attacker has found vulnerable host, he can perform for example scanning-specific ports to target certain applications or services. A simple reconnaissance phase can be done by sending spoofed packets to the all-nodes multicast address (ff02::1) or to the all-routers multicast address (ff02::2) as depicted in Figure 1.

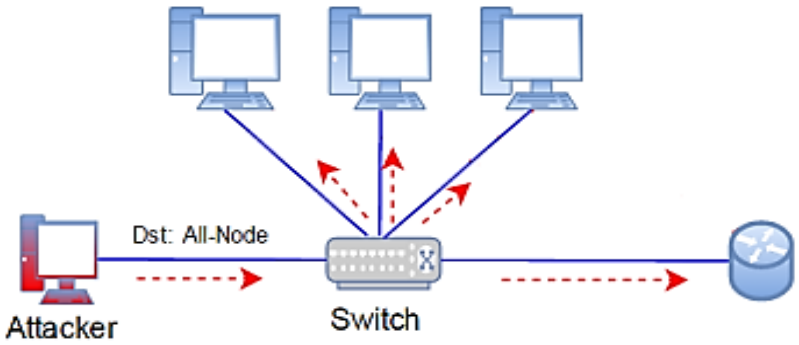

Figure 1: Attacking all-nodes multicast address ff02::1

Figure 2 shows an example of initiating a simple reconnaissance attack using Python and Scapy. The instruction "IPv6(dst=allnodesdst) / ICMPv6MRD_Advertisement (advinter=cusadvinter)" is used to send multicast packet, i.e. Multicast Router Advertisement with a custom advertisement interval (15 second) to all nodes in the local network. A loop is used to generate 5000 packets, which will increase the amount of traffic generated. The start and time along with the packets sent are shown on the screen.

```
From scapy.all import *
n_packets = 5000
start_time = time.time()
allnodedst = "ff02::1"
cusadvinter = 40
for i in range(n_packets):
   IPv6(dst=allnodedst) / ICMPv6MRD_Advertisement(advinter=cusadvinter)

end_time = time.time()
print("sent {n_packets} packets in {end_time - start_time: .3f} seconds")
```

Figure 2: Scapy cope to generate a simple reconnaissance attack on all-nodes multicast address ff02::1

As discussed, the reconnaissance phase aims at revealing potential targets on the network. The next phase is to send spoofing messages to attack all the potential targets at once, i.e. Denial of Service (DoS) or to use all potential targets to attack a single node on the network, i.e. Distributed Denial of Services (DDoS). The later attack is called Smurf attack. A possible scenario of this attack when an attacker sends echo-requests by spoofing the address of a node as source address and all hosts respond by sending echo-replies, the node in will be overwhelmed with traffic of the echo-replies. Figure 3 depicts this scenario (Weber, 2013).

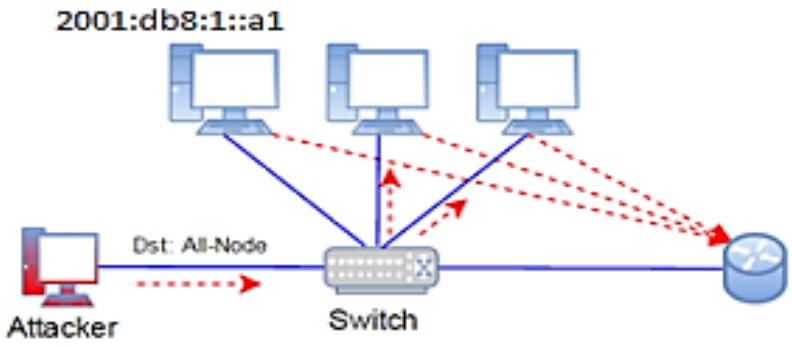

Figure 3: Smurf attack utilizing the all-nodes multicast address ff02::1

Figure 4 shows an example of initiating a simple reconnaissance attack using Python and Scapy. It sends echo-requests by spoofing the address of "2001:db8:1::a1" as source address and all hosts. A for loop is used to generate 5000 packets, which will lead to an increase in the amount of traffic generated. The start and time along with the packets sent are shown on the screen.

```
from scapy.all import *
n_packets = 5000
start_time = time.time()
allnodedst = 'ff02::1'
scr = "2001:db8:1::a1"
for i in range(n_packets):
   IPv6(src=src,dst=allnodedst) / ICMPv6EchoRequest()

end_time = time.time()
print("sent {n_packets} packets in {end_time - start_time: .3f} seconds")
```

Figure 4: Example of initiating a simple reconnaissance attack using Python and Scapy

3.2. Security Solutions

Many solutions have been presented concerning the IPv6 security and several of them could be used to counter and prevent multicast utilization attacks. The first and simplest solution is to block the network echo-request messages from outside the network to the multicast addresses inside the network. The best choice to perform this task is the firewalls. Despite the effectiveness of this solution, it may lead to stop legitimate tasks. For example, it may stop the process of monitoring network traffic on a network. A monitoring tool should ping routers, i.e., sending legitimate echo-request messages and receiving echo-reply messages from the routers confirm their existence. Firewall could block such crucial stage to perform monitoring. A successful alternative to this solution is to implement the rate

limiting for the ICMPv6 echo-replies that can prevent the smurf attacks effectively and could be considered are a built-in protection mechanism. The default value is one ICMPv6 destination unreachable message per 500 milliseconds (0.5 second). The bigger the rate-limit value per packet the less ICMP unreachable messages will be sent.

The lower the rate-limit value per packet, the more unreachable messages will be sent. So it is wise to limit the rate of ICMPv6 echo-replies to a certain level. Another useful countermeasure is the use of Intrusion Detection Systems (IDSs). After detecting massive echo-request floods, the IDSs can be used in two ways: either to block the floods or to produce an alarm only. Several open-source IDS have been active for many years such as Snort, BRO, and Suricata.

In most cases, the multicast DoS attacks are considered the second phase of other attacks as we discussed earlier the reconnaissance attacks. Therefore, the large networking companies started to invent industrial countermeasures to prevent DoS attacks. One of these countermeasures is the unicast Reverse Path Forwarding (uRPF) (Baker & Savola, 2004). uRPF is routers' security feature that prevents anomaly multicast echo-request. When the router receives an IPv6 packet, it will check if it has a matching entry in the routing table for the source IPv6 address. If it does not match, the packet will be discarded. Table 1 summarizes the attacks and countermeasures for each attack.

Table 1: Multicast Attacks and Countermeasures

Attack	Countermeasures
Reconnaissance	1. Firewall 2. Limiting the ICMPv6 echo-replies rate
Smurf	1. Limiting the ICMPv6 echo-replies rate 2. IDS 3. uRPF
DoS	1. Firewall 2. IDS

4. Results and Discussion

This section provides the results of security analysis of multicast attacks. The goal of the analysis done is to establish a severity degree rank for each attack. To generate the list of security ranks, two measures were used in the calculation: (1) the degree of harm and (2) the number of countermeasures for each attack. The individual severity rank is calculated based on the fact that the severity of an attack is directly proportional to the degree of harm and it is inversely proportional to the number of countermeasures for the attack:

$$R = \frac{h}{c} \quad (1)$$

Where:

R: the severity rank of the attack

h: the degree of harm

c: the number of countermeasures

Based on the results of this study and as the history of attacks shown, the degree of harm of each attack is estimated. The range of estimation was from 0-10. The estimated values of harm degrees are listed in Table 2.

Table 2: Harm Degrees

Attack	Harm Degree	# of Countermeasures
Reconnaissance	3	2
Smurf	6	3
DoS	9	2

Figure 5 shows the results of calculating the severity degree of each attack.

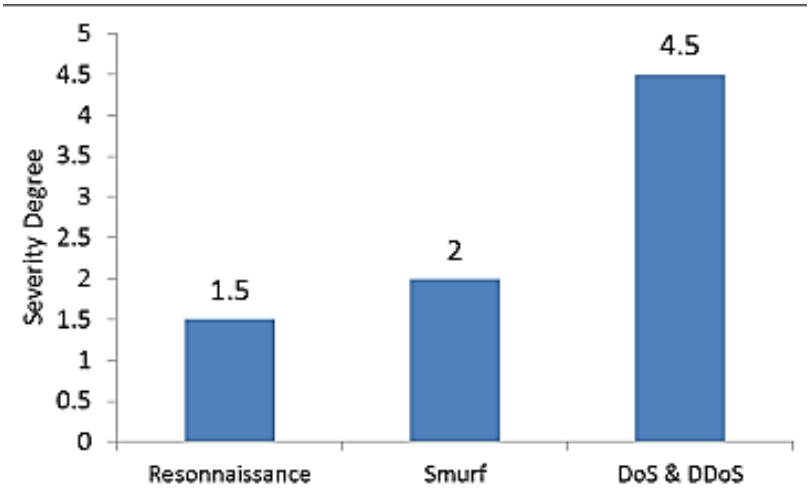

Figure 5: Multicast attack severity degrees

The results have suggested that the DoS and DDoS attacks are marginally more severity than their counterpart attacks, reconnaissance and smurf with 4.5 severity degree. The calculation also suggested that the reconnaissance takes the least severity degree compared to the other attacks.

5. Conclusion

The main concern about the transition from IPv4 to IPv6 environment is data security protection. Although the growth of IPv6 security research has been very rapid and many techniques have emerged, we are still far from 100% securely IPv6 deployment. In this paper, the attacks to IPv6 networks that are caused by utilizing the multicast

vulnerability are introduced, the reconnaissance, the smurf, and the DoS. In addition, four countermeasures to attacks are discussed by simulating the scenarios of applying each one of them. Also, the attacks are ranked on the basis of new attack severity-ranking method. Two factors are considered in producing the attack rank: the degree of harm and the number of counter measures. According to severity-ranking methods, the DoS attack has 4.5 out of 10 degree, which is the most severity degree, followed by the reconnaissance attack and the smurf attack which have 2 and 1.5 degree respectively. However, the overall results showed that the multicast vulnerability call for more investigation. This menace can be prevented to a great extent if a proper method is able to detect the multicast attacks at their first stage.

Acknowledgment

The research leading to these results has no Research Project Grant Funding.

References

[1]. An, G., & Kim, K. (2008). Real-time IP checking and packet marking for preventing ND-DoS attack employing fake source IP in IPv6 LAN. Paper presented at the International Conference on Autonomic and Trusted Computing.
[2]. Arjuman, N. C., & Manickam, S. (2015). A review on ICMPv6 vulnerabilities and its mitigation techniques: Classification and art. Paper presented at the Computer, Communications, and Control Technology (I4CT), 2015 International Conference on.
[3]. Baker, F., & Savola, P. (2004). RFC 3704. Ingress Filtering for Multihomed Networks.
[4]. Bansal, G., Kumar, N., Nandi, S., & Biswas, S. (2012). Detection of NDP based attacks using MLD. Paper presented at the Proceedings of the Fifth International Conference on Security of Information and Networks.
[5]. Barbhuiya, F. A., Biswas, S., & Nandi, S. (2011). Detection of neighbor solicitation and advertisement spoofing in IPv6 neighbor discovery protocol. Paper presented at the Proceedings of the 4th international conference on Security of information and networks.
[6]. Davies, J. (2012). Understanding IPv6: Understanding IPv6 _p3: Pearson Education.
[7]. Elejla, O. E., Anbar, M., & Belaton, B. (2016). ICMPv6-Based DoS and DDoS Attacks and Defense Mechanisms: Review. IETE Technical Review, 1-18.
[8]. Hagen, S. (2014). Pv6 Essentials, 3rd Edition: O'Reilly Media, Inc.
[9]. Hinden, R., & Deering, S. (2006). RFC 4291. IP version, 6, 13-15.
[10]. Horley, E. (2014). Practical IPv6 for Windows Administrators: Apress.
[11]. Lencse, G., & Kadobayashi, Y. (2018). Methodology for the identification of potential security issues of different IPv6 transition technologies: Threat analysis of DNS64 and stateful NAT64. Computers & Security, 77, 397-411.
[12]. Lencse, G., & Kadobayashi, Y. (2019). Comprehensive survey of IPv6 transition technologies: A subjective classification for security analysis. IEICE Transactions on Communications, 102(10), 2021-2035.
[13]. R. M. Saad, S. R., and S. Manickam. (2013). A Study on Detecting ICMPv6 Flooding Attack based on IDS. Australian Journal of Basic and Applied Sciences, 7(2), 175-181.
[14]. Saad, R. M., Anbar, M., Manickam, S., & Alomari, E. (2015). An Intelligent ICMPv6 DDoS Flooding-Attack Detection Framework (v6IIDS) using Back-Propagation Neural Network. IETE Technical Review, 1-12.
[15]. Shubair, A. (2017). Survey of security issues in IPv4 to IPv6 tunnel transition mechanisms. International Journal of Security and Networks, 12(2), 83-102.
[16]. Weber, J. (2013). IPv6 Security Test Laboratory. (Master), Ruhr-University Bochum, Germany.