Journal of Engineering and Applied Sciences 14 (11): 3674-3678, 2019
ISSN: 1816-949X

Building a Security System Based on Internet Protocol Version 6 Routing Header

[1]Ahmed Khaleel Ibrahim Saihab and [2]Nazhat Saeed Abdulrazaq
[1]Iraqi Commission for Computer and Informatics, Information Institute for Postgraduate Studies, Baghdad, Iraq
[2]Department of Electromechanical Engineering, University of Technology, Baghdad, Iraq

Abstract: Internet Protocol Version 6 was introduced by the Internet Engineering Task Force (IETF) to replace the Internet Protocol Version 4 and introduce features like a significantly larger address space, flow labelling and additional security features but the new IPv6 bring new challenges with it. The routing header which is an extension header type that is used in the IPv6 has some vulnerabilities in it, a vulner ability allows a potential attacker to by pass firewall systems or access control lists by using the routing header to access internal protected networks and can also use the routing header to generate an attack called Reflective Denial of Service (RDOS) to overload the network bandwidth and stop network operation. This study suggests a protection system to protect against vulnerabilities that reside within the IPv6 routing header, the results show that the proposed protection system provides a secure communication without blocking normal traffic.

Key words: Routing header, packet filtering, protection system, IPv6, IPv4, network security

INTRODUCTION

The current internet protocol generation IPv4 was designed back in the 1980's, it has since been used for over 30 years in the vast majority of networking devices, IPv4 has proven to be very useful, however, the IPv4 has some issues like the lack of integrated security and the insufficient address space which is expected to be depleted in the near feature for these reasons it appeared necessary to develop a new version of the internet protocol to replace the Internet Protocol Version 4. To solve the problems mentioned above with the IPv4. In 1998 the IETF (Internet Engineering Task Force) Network working group introduced a new internet protocol that is called Internet Protocol Version 6 (IPv6) (Deering and Hinden, 1998). The IPv6 is defined with 128 bit address space which is a big improvement compared to the IPv4 address space which supported only 32 bit address, furthermore, IPv6 support IPsec as part of the header, IPv6 also includes simple routing header format, flow labelling capabilities, Quality of services (QoS) and security at IP level. In addition, through auto configuration and mobility feature of IPv6, nodes on the internet can communicate in simpler way IPv6 was developed based on the vast experience obtained from the development and use of IPv4. reliable and established mechanisms have been attained and the limits of the IPv4 were disposed of and scalability have been widely extended. IPv6 was designed to handle the incremental internet growth and to handle the necessities on its services like mobility, end-to-end security (Hagen, 2004). Extension header is an important feature defined in the IPv6 the extension header can be used with the IPv6 header whenever it is required. This way packet became flexible and transmitting of packets is more effective, however, there are multiple attack types on this extension header. Routing header is an extension header defined with the IPv6 and it's used by an IPv6 source devices to choose a path for the packet to take on the way to a the destination (Deering and Hinden, 1998).

Several researchers made a study to the security threats in IPv4 and IPv6 and pointed that the IPv6 has a security issue in its routing header that allow some packets to access forbidden address by inserting the forbidden address to the routing header (Lim and Kim, 2006; Durdagi and Buldu, 2010).

Proposed an algorithm to counter the security issues with IPv6 routing header type 0 that allows packets to by pass security mechanisms like firewall or access control lists (Wadhwa and Khari, 2001), other researcher proposed an algorithm to protect from IPv6 routing header redirect exploit, the researcher provided experimental results with high success (Shenify, 2014), however, the need still exist for a security system to protect against the denial of service exploit as well as the redirect exploits.

MATERIALS AND METHODS

Exploits within the routing header: The adoption of any new protocol brings new attack possibilities to the

Corresponding Author: Ahmed Khaleel Ibrahim Saihab, Iraqi Commission for Computer and Informatics, Information Institute for Postgraduate Studies, Baghdad, Iraq

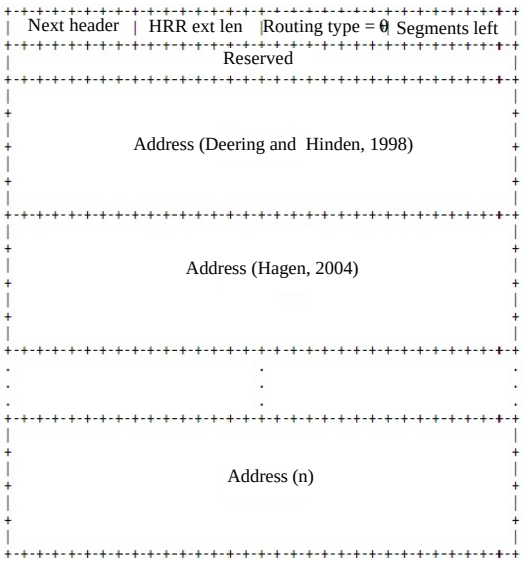

Fig. 1: The routing header format (Shenify, 2014)

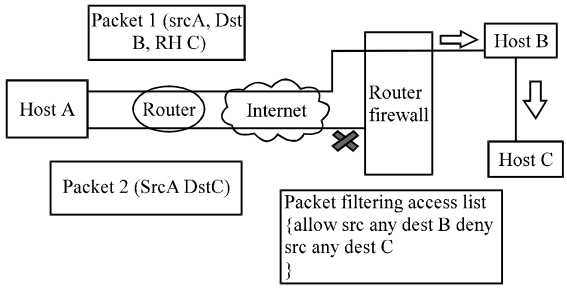

Fig. 2: Routing header vulnerability

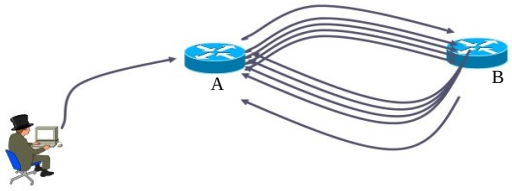

Fig. 3: Reflective DOS attack

attackers. The structure of Ipv6 packets allows the existence of routing headers (Fig. 1) which list addresses of one or multiple transitional nodes the packets will traverse on its way to the destination. The attacker can create packets with routing headers that allows it reach hosts that usually does not accept traffic from the attacker. Furthermore, if an end point accepts malicious routing headers and follows their routing instructions, trusted nodes could forward malicious packets or the flow of packets could overload the routers, ensuing a denial of service attack (Caicedo *et al*., 2009).

A weakness can be exploited due to abuse of the IPv6 RH feature was established and examined in a number of recent studies. All IPv6 compliant nodes must have the ability to process routing headers. Similarly that weakness can be exploited by malitious users to evade network security mechanisms through avoiding network firewall on the destination addresses. The firewall rule can block the packet forwarding to packets that use type 0 routing header and allow other types of the routing header like type 2 to pass. However, blocking all the packets employing routing headers is not a good solution to the problem as this could have grave consequences to the future development of IPv6. Lately, the majority of firewall and access control list rules block every packet that employ RH0. Furthermore, the default configuration in the firewall and access control list stops the forwarding of IPv6 packets that contain RH0. The functionality of the routing header which originally is delivered by IPv6 can be used to list one or many transitional nodes to be traversed on the way to the destination of the packet.

Also, it can be exploited by the malicious users to create a Denial of Service attack (DoS). The attacker can abuse the RH to create malicious packets that are achieved by stating the victim's IP address in the routing header and repeating addresses in way that will make packets continually bouncing between nods and consuming the bandwidth. These packets will be routed by a network server and some midway network nodes to be delivered to the host of the victim. Definitely, the malicious packets will be checked in a procedure at the server in the network. Then the server sends the packets by using the IP addresses stated in the routing header then the malicious packets will be able to reach the victim's host machine without violating any security rules. Consequently, all the network packets that pass through and into the network must be subjected to a checking process. Figure 1 shows the layout of the routing header. A variety of possible security concerns associated with the routing header of IPv6 both IPv6 routing header types can be exploited to bypass access control mechanisms based on the address of the destination that could be accomplished through sending the malicious packets seemingly to an openly accessible host address but with the routing header encompassing a forbidden address of the host being targeted as shown in Fig. 2 and 3.

The source address of the packet can be spoofed by using the type 0 routing header, the mechanism explained

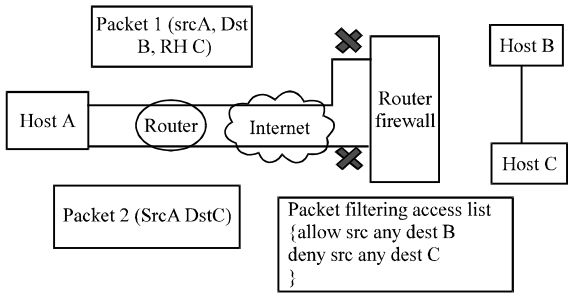

Fig. 4: Prevented attack by using the protection system

earlier could be abused with any host to mediate a reflective DOS attack by employing an openly accessible host address to redirect the packets being used in the attack (Davies *et al*., 2007) (Fig. 3).

RESULTS AND DISCUSSION

The proposed protection system: The goal of the proposed protection system is to enable a secure network operation throughout all connections on networks that use IPv6 and to thwart any attack attempts made using IPv6 routing header exploits.

The system also will allow network users to use all types of network applications without any restriction to network flow or the type of application used.

In addition, the system will allow network administrators to protect critical hosts from external network access and will also allow the network administrators to protect the network from attacks that aim to disrupt the network operations through routing header based DOS attacks.

The proposed protection system will be scanning incoming IPv6 packets and will strip the headers of the packets and will check for the existence of the IPv6 routing header if the IPv6 routing header is not found the security system will make a decision only based on source and destination IPv6 address from the packet that will be done by checking the packet source and destination address with a list of addresses specified by the system.

If the IPv6 routing header is found inside the packed the protection system will remove the header from the packet and will open the header to check the type of the header weather it is type 0 routing header or type 2 routing header and will check the packet source and destination addresses before examining the routing header itself.

If type 2 routing header is found the protection system will read the address from the header and then the protection system will compare the address in the type 2 routing header with a list of protected address that are stored in a file and if one of the addresses in the list of protected addresses is found in the type 2 routing header addresses the protection system will make a decision to drop the packet other If type 0 routing header is found inside the packet, first similarly to the case with type 2 routing header the protection system will first read the addresses from the routing header and will check them against the list that are containing protected addresses of the system if no protected addresses are found inside the type 0 routing header the protection system will move to checking the routing header if it is being used for amplification attack (Fig. 4) and checking amplification attack or any attempted waste of bandwidth will be done by checking the addresses inside type 0 routing header for any loops (which is a repeated sequence of addresses), so, the protection system will check if an address is present more than once inside the routing header, the protection system is described in Fig. 5.

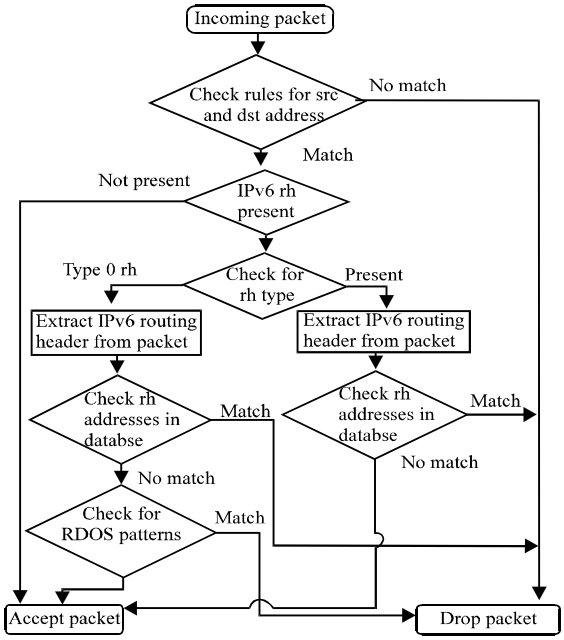

Fig. 5: Flowchart for the proposed security system

Table 1: Software used

Specifications	Details
Simulation software	GNS3
Platform for simulation software	Windows 10
Platform to run protection system	Ubuntu Linux
Programming language	Python, scapy
Routers	Cisco c7200

Implementation and testing: The protection system will be implemented and tested in a simulation environment using Gns3 (graphical network simulator 3) and the network devices used are operated and connected in Virtual Machine environment using VM ware work station in Table 1 is a list of the all the software and tools used to implement the protection system.

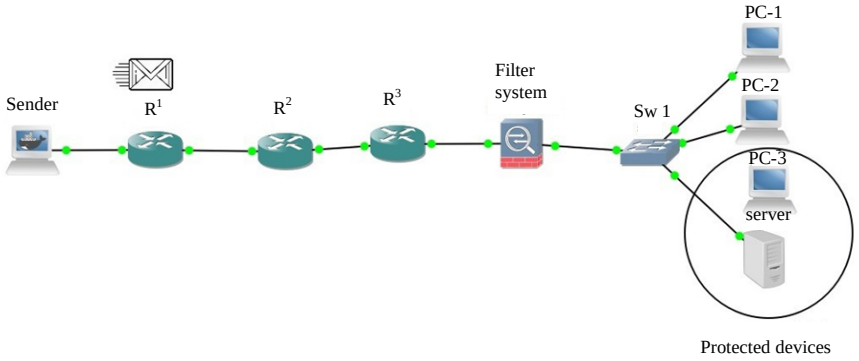

Fig. 6: The testbed network

Table 2: Host names and addresses

Device name	IPv6 address
PC1	2a11::2050:79ff:fe66:6801
PC2	2a11::2050:79ff:fe66:6802
Server	2a11::2050:79ff:fe66:6803
PC3	2a11::2050:79ff:fe66:6804
End hosts	Virtual PCs

Table 3: Stream packet types and count

Packet types	RH type	Counts
Normal packets	No RH	300
Packets with routing header type 0 (safe)	RH0	200
Packets with routing header type 0 (access violation)	RH0	200
Packet with blocked source address (blocked source)	RH0	200
Packet with routing header type 2 (safe)	RH2	200
Packet with routing header type 2 (access violation)	RH2	200
Packets with routing header type 0 (RDOS attack)	RH0	200

In order to analyze the efficiency of the proposed protection system a Testbed network has been created to simulate four deices in a network of which two of them to be assigned as protected devices meaning they must not be accessed from devices from outside the network, then these devices where interconnected to a network via. a switch to establish connectivity between them as shown in Fig. 6. Furthermore, the deices where assigned an IPv6 address to each of them as shown in Table 2.

A stream of packets will be sent to test the protection system the stream will be containing a total of 1500 packets that contain several kinds of packets that the protection system might encounter during its time of operation the details of the stream are listed in Table 3.

After the testing packet stream is sent Wireshark will help with the analysis of the efficiency of the protection system by capturing and analyzing all packets on the link selected in this case it will be the link between the protection system and the network being protected, so, Wireshark Software will capture all packets forwarded by the protection system and then when all the packets from the testing packet stream are sent and processed by the protection system Wireshark will be able to provide a detailed statistics about the packets that passed in the link. The statistics obtained from Wireshark indicating the efficiency of the protection system are illustrated in Table 4.

The statistics obtained by using Wireshark indicating that from 1500 packets of the testing packet stream sent that a total 700 packets where accepted by the protection system and a total of 800 packets were dropped thus the percentage of packets accepted by the protection system is counted by the following equation:

$$\frac{\text{Packets forwarded}}{\text{Total No. of packets}} \times 100\%$$

And similarly, the percentage of packets dropped by the protection system is calculated by the following equation:

$$\frac{700}{500} \times 100\% = 4636\% \text{packets accepted}$$

Out of the 700 packets accepted 700 of them where designated as safe packets and from the 800 packets dropped by the protection system 800 of them where designated as malicious packets or forbidden packets. The percentage of accepted packets in this test packet stream:

$$\frac{\text{Safe packets forwarded}}{\text{Toal safe packets}}$$

The percentage of accepted packets in this test packet stream:

$$\frac{700}{700} \times 100\% = 100\% \text{ of safe packets forwarded}$$

Table 4: Protection system statistics

Packet types	RH types	Count sent	Count accepted	Count dropped
Normal packets	No RH	300	300	0
Packets with routing header type 0 (Safe)	RH0	200	200	0
Packets with routing header type 0 (Access violation)	RH0	200	0	200
Packet with blocked source address (Blocked source)	RH0	200	0	200
Packet with routing header type 2 (Safe)	RH2	200	200	0
Packet with routing header type 2 (Access violation)	RH2	200	0	200
Packets with routing header type 0 (RDOS attack)	RH0	200	0	200

CONCLUSION

This study identified vulnerabilities in the IPv6 routing header that allows attackers to abuse mechanisms within the routing header to bypass security systems like firewalls and access control lists in addition to perform a kind of denial of service attack mostly referred to as reflective denial of service attack. The research proposed and detailed the implementation of a protection system that successfully intercepted network attacks that aims to abuse vulnerabilities within the IPv6 routing header. The proposed protection system applies protection to the network without impacting the flow of normal packets.

The results of the protection system testing show that the proposed protection system was successful to stop all malicious attempts that aim use the vulnerabilities within the IPv6 routing header without impacting normal packets from accessing the network.

RECOMMENDATIONS

For future development the protection system can be implemented to existing firewall devices without any considerable change to the systems, furthermore, it supports easy configuration for network engineers or administrators, since.

ACKNOWLEDGEMENT

This research was supported by Iraqi Commission for Computer and Informatics. I would like to thank my colleagues from Iraqi Commission for Computer and Informatics. who provided insight that assisted the research.

REFERENCES

Caicedo, C.E., J.B.D. Joshi and S.R. Tuladhar, 2009. IPv6 security challenges. Comput., 42: 36-42.

Davies, E., S. Krishnan and P. Savola, 2007. IPv6 transition/co-existence security considerations. Internet Engineering Task Force, Fremont, California, USA. http://www.rfc-editor.org/info/rfc4942

Deering, S. and R. Hinden, 1998. Internet protocol version 6 (Ipv6) specification. Internet Protoc., Vol. 6, 10.17487/RFC2460.

Durdagi, E. and A. Buldu, 2010. IPv4/IPV6 security and threat comparisons. Procedia-Social Behav. Sci., 2: 5285-5291.

Hagen, S., 2004. IPv6 Essentials. 3rd Edn., O'Reilly Media, Inc., Sebastopol, California, USA., ISBN:978-1-4493-1921-2, Pages: 391.

Lim, J. and Y. Kim, 2006. Protection algorithm against security holes of IPv6 routing header. Proceedings of the 8th International Conference on Advanced Communication Technology (ICACT 2006), February 20-22, 2006, IEEE, Phoenix Park, South Korea, pp: 2004-2007.

Shenify, M., 2014. Trusted node-based algorithm to secure home agent nated IPv4 network from IPv6 routing header attacks. TELKOMNIKA. Telecommunication Comput. Electron. Control, 12: 969-976.

Wadhwa, M. and M. Khari, 2001. Prevention algorithm against the vulnerability of type 0 routing header in Ipv6. Proceedings of the 2011 International Conference on Computational Intelligence and Communication Networks, October 7-9, 2011, IEEE, Gwalior, India, ISBN:978-1-4577-2033-8, pp: 616-620.January 28, 2019.