Analysis of the Threats abusing IPv6 Fragment Header*

Zhen Zhao, Gyehyeon Gyeong, Kwang Sun Ko, and Young Ik Eom
School of Information and Communication Engineering, Sungkyunkwan University
email: oszzer@gmail.com, {gyehyeon, rilla91, yieom}@ece.skku.ac.kr

Abstract

The security issues related to IPv6 protocol have been focused on by many researchers and engineers. Especially, extension headers of IPv6 protocol provide various functionalities such as IP security, mobile IP, and in principle, it is said to give much more effective network services than the previous protocol, IPv4. In this paper, the cases are surveyed in which fragment header, that is one of many extension headers in IPv6 protocol, is abused and made to be the sources of threats. Prevention mechanisms are also surveyed to countermeasure the threats.

1. Introduction

The advent of IPv6 protocol opens up broad prospects to implement the next generation Internet. The characteristic of IPv6 makes the uses of Internet extend to all areas. Among the various functionalities, fragmentation mechanism is used to fragment and reassembly large IPv6 packets, which makes it possible to transport large IPv6 packets between different types of networks by following concerted length of the fragments.

In the meantime, because of some features of fragmentation itself, Fragment Header is also used as carriers of invasion or means of attacks by attackers frequently. In view of this, the security research on these threats has been extensive widely. Many effective prevention methods have also been developed and applied to the IPv6 networks

This paper discusses three kinds of threats: 'tiny fragment attack', 'overlapping fragment attack', and 'DoS attack'. The prevention mechanisms to these attacks are also discussed.

2. Background

Fragment Header is the extension header that used to fragment large data packets. This section describes Fragment Header structure and fragmentation mechanism in IPv6 protocol.

2.1 Structure of Fragment Header

Fragment Header is used to send IPv6 packets that are larger than the Path Maximum Transmission Unit (PMTU). According to RFC 2460 [1], the format of the Fragment Header is shown in Figure 1.

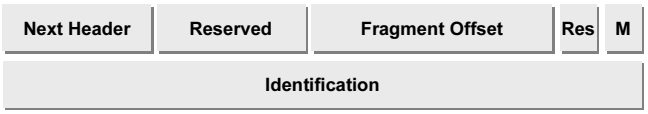

Fig.1. Structure of the Fragment Header in IPv6 protocol

IPv6 standard describes that the fragmentation can only be performed at the source node to remove the burdens of immediate nodes for the efficiency of data transmission. It is suggested that a source node check PMTU to a destination node before sending any length of an IPv6 packet using PMTUD (PMTU discovery) mechanism. IPv6 standard requires a MTU value of at least 1280 bytes and proposes the link path to be able to transmit at least 1500-byte long packages. When an IPv6 packet is larger than the MTU of a current path, the source node must perform the fragment operation to divide the original IPv6 packet into several small fragments. At the destination node, these fragments will be reassembled into original IPv6 packet.

An IPv6 packet can be divided into two parts: an unfragmentable part and a fragmentable part. An unfragmentable part includes the IPv6 header of the original packet and three IPv6 extension headers, which are

* This work was supported by National Center of Excellence in Ubiquitous Computing and Networking (CUCN), Korea.

Hop-By-Hop Header, Destination Options Header, and Routing Header. If these extension headers appear in the original IPv6 packet, then they must be carried by every fragment. A fragmentable part consists of the other possible extension headers, such as Authentication Header and Encapsulation Security Payload Header, and payload which are not included in the unfragmentable part.

A fragmentable part is divided into several parts and contained in all of the fragments. The fragments come from the same IPv6 packet must have the same fragment identification with different offset values. For each fragment, it can be made up of three parts, in order, an unfragmentable part, Fragment Header and a piece of the fragmentable part [1].

2.2 An example of IPv6 fragmentation

In this section, we describe an example of the IPv6 fragmentation mechanism.

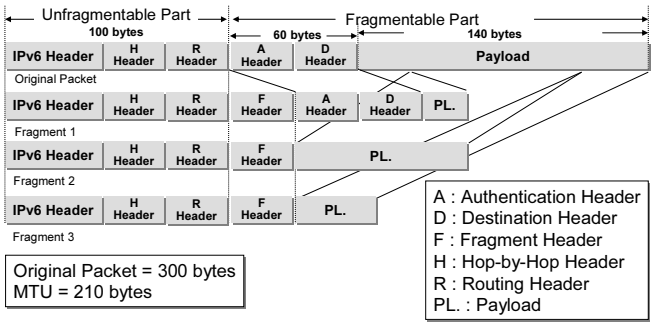

Fig.2. Example of IPv6 fragmentation

As shown in Figure 2, we assume that the original IPv6 packet is 300 bytes in length, including 40 bytes of the IPv6 Header, Four 30-byte IPv6 extension Headers (Hop-by-Hop Header, Routing Header, Authentication Header and Destination Header) and 140 bytes of payload. Assuming that the value of PMTU to be 210 bytes. As the unfragmented part must be included in each fragment, therefore, a total of three fragments need to transmission 140 bytes payload.

<Table 1> Fields of each fragment

Fragment	1	2	3
unfragmentable part	100 bytes	100 bytes	100 bytes
Fragment Header	30 bytes	30 bytes	30 bytes
fragmentable part	60+20 bytes	80 bytes	40 bytes
offset / M flag	0 / 1	20 / 1	100/ 0

The 32 bit unsigned integer value in the three Fragment Headers is the same. It means that the three fragments belong to one original IPv6 packet. When these fragments reach the destination, they can be reassembled [4].

3. Threats of Fragment Header

We discuss three kinds of the most used attack methods based on the IPv6 Fragment Header: ‘tiny fragment attack’, ‘overlapping fragment attack’, and ‘DoS attack’. The concerned areas of these attacks are illustrated in Figure 3.

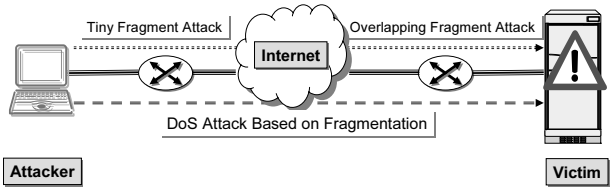

Fig.3. Three kinds of attacks

3.1 Tiny fragment attack

Tiny fragment attack is an attack that imposes an unusually small fragment size on outgoing packets. If a fragment size is made small enough to force some of a TCP packet's TCP header fields into the second fragment, filter rules deployed in security systems that specify patterns for those fields will not match. If the filtering implementation does not enforce a minimum fragment size, a disallowed packet might be passed because it does not hit a match in the filter.

3.1.1 Attack

In this example, the attacker generates a very small IPv6 packet to force the sensitive TCP header fields to be fragmented into the second fragment. As we see, there are two fragments that have been generated. Fragment 1 contains only 8 octets of TCP data, including Source Port, Destination Port and Sequence Number fields, the TCP flag field has been pushed into Fragment 2. So the filter will not find the TCP flags field and will not be able to test the validity of the connection request, it will ignore them in sequence. Because most of the filtering mechanisms only check the first fragment of the IPv6 packet, Fragment 2, which has the other fields of the TCP data including the TCP flags filed, can pass through the filter unhindered. After all

the fragments have arrived at the destination, they will be reassembled, the TCP connection, which ought to be dropped, will be accepted [2].

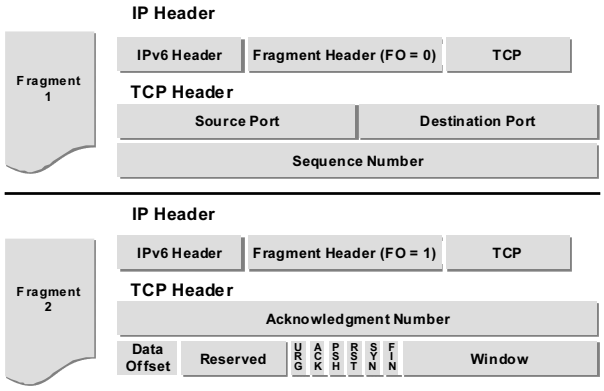

Fig.4. Fragmented packets used by tiny fragment attack

3.1.2 Prevention

As it has been mentioned in RFC 1858 [2] and 3128 [3], the method that used to prevent the attack has been afforded.

```
if FO=0 and NextHeader=TCP
and TRANSPORTLEN<tmin then
DROP PACKET
if FO=1 and NextHeader=TCP then
DROP PACKET
```

Here, FO means the Fragment Offset of the fragment, and tmin is the minimum length of the transport header (i.e. TCP) required containing enough information that should be checked by the filter. The filter will check the fields in Fragment 1 and Fragment 2, and math with the rules, drop illegal fragments. If the original IPv6 packet contains TCP information, then the Fragment 1 should include all the TCP information. So when Fragment 1 contains TCP information but the length is less than the reasonable length, then drop the packet. For these reasons, Fragment 2 should never contain any TCP information, so when TCP information appears in the Fragment 2, drop the fragment [2] [3].

3.2 Overlapping fragment attack

Overlapping fragment attack is also called IP fragmentation attack. In an overlapping fragment attack, the reassembled packet starts in the middle of another packet. As the operating system receives these invalid packets, it allocates memory to hold them. The illegal data in the later-coming fragments will overwrite the legitimate data during the reassembly process. Then the reassembled IPv6 packet can access limited system resource, and invade the system.

3.2.1 Attack

Following the fragment reassembly mechanism, the fragments will be reassembled by following the sequence and data offset when all reach the destination. In this example, Fragment 1 has the harmless TCP flags value, so it can pass through the filter unharmed. Although Fragment 2 contains harmful TCP flags information, it can also pass through the filter because most of the filters do not check the non-zero-offset fragments. During the reassembly process, Fragment 2 will overwrite the specific portion of Fragment 1 with harmful TCP flag data. And then the restricted port connection request of this IPv6 packet will be accept. [2]

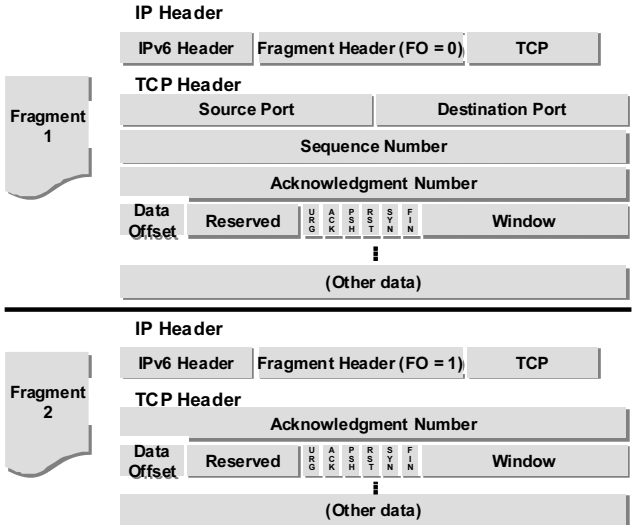

Fig.5. Fragmented packets used by overlapping fragment attack

3.2.2 Prevention

For the overlapping fragment attack, the RFC 3128 document provides a method to prevent this kind of threat. The method considers both the fragment with offset 0 and offset 1. For a common fragment with offset 0, it must contain the whole TCP header information, so if the length of the TCP header is less than tmin, then we can drop this fragment. Because all the TCP header information must be contained in the fragment with offset 0, the TCP flags should never be contained in a non-zero-offset fragment. So if the fragment with offset 1 contains TCP flags information, it

will be dropped [2] [3].

```
if FO=0 and NextHeader=TCP
and TRANSPORTLENTH<tmin then
DROP PACKET
if FO=1 and NextHeader=TCP then
DROP PACKET
```

3.3 DoS attack

A denial-of-service attack (DoS attack) is an attempt to make a computer resource unavailable to its intended users. In IPv6 environment, the attackers attempt to consume the reassembly buffers of the destination system by sending massive large Ipv6 packets, and make the system unable to answer the other service requests [5] [6].

3.3.1 Attack

An IPv6 packet that larger than the MTU will be fragmented at the source and be reassembled at the destination. The attacker sends a great deal of large IPv6 packets to a victim. So the destination has to reassembly these fragments, but the workload of reassembling these fragments is out of the ability of the victim, reflects on that the other normal service requests will not be response, further more the service is interrupted. The attacker can also set the data offset of the non-zero-fragments with abnormal values in order to force the buffer to be overflowed during the reassembly process, this may cause the service to be interrupted or system down [5] [6].

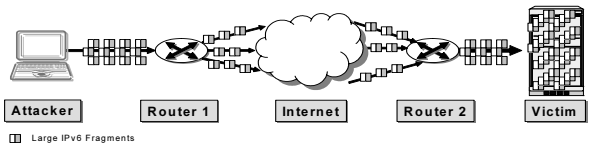

Fig.6. Illustration of DoS attack

3.3.2 Prevention

It seems that the prevention of DoS attack based on fragmentation is a little passive. We are going to implement the prevention by 2 steps. First we have to monitor the network traffic in real-time, analysis the information and decide whether the traffic is abnormal. Then if the traffic is considered to be abnormal, we can apply an access control list to filter and block the malicious IPs. The items in the access control list can be derived from the statistics that we have got in the first step. However, this method still can not completely prevent DoS attacks. New prevention methods are constantly developed [6].

4. Conclusion

By monitoring the NextHeader and setting the value of ***tmin*** (shown in Section 3.1.2), we can prevent most of the 'tiny fragment attack' and 'overlapping fragment attack', but this is of no effect to prevent 'DoS attack based on fragmentation'. Whereas the DoS attacks are diversity, the prevention of 'DoS attack based on fragmentation' can be done by dedicated prevention systems, in order to reduce the workload of fragment filtering system.

We described the IPv6 fragmentation mechanism, brought three kinds of IPv6 Fragment Header aiming attacks and the corresponding prevention methods, and gave an overall view of the Fragment Header security issues. More significantly, by doing research on the content of the above-mentioned, we found that the current prevention method are not enough to stop attack based on Fragment Header, and the complicated prevention methods had affected on the efficiency of the system. Research on more complete and more efficient prevention method is of great significance for the development of IPv6. The research in this area will continue.

Reference

[1] S. Deering and R. Hinden, RFC 2460, *Internet Protocol Version 6 (IPv6) Specification*, Dec. 1998.

[2] G. Ziemba, D. Reed, and P. Traina, RFC 1858, *Security Considerations for IP Fragment Filtering,* Oct. 1995.

[3] I. Miller, RFC 3128, *Protection Against a Variant of the Tiny Fragment Attack,* Jun. 2001.

[4] Z. Hu, Z. Su, X. Zhao, and Y. Ma, "The Implementation of IPv6 Fragment Reassembling in Intruding Detection System," Modern Science & Technology of Telecommunications, Vol.4, pp. 45-49, Apr. 2005.

[5] J. Mirkovic, J. Martin, and P. Reiher, *A Taxonomy of DDoS Attacksand DDoS DefenseMechanisms.* Tech. Report 020018, CSDept, UCLA, Apr. 2004.

[6] C. Kaufman, R. Perlman, and B. Sommerfeld, "DoS Protection for UDP-Based Protocols," Proc. of the 10th ACM Conf. on Computer and Communications Security (CCS '03), Oct. 2003.