A manipulated neighbor discovery protocol as attack in hybrid internet environment

Nazrulazhar Bahaman[1*], Erman Hamid[1], Mohd Zaki Mas'ud[1], Nur Azman Mat Ariff[1], Elia Erwani Hassan[2]

[1]Faculty of Information and Communication Technology, Universiti Teknikal Malaysia Melaka, Hang Tuah Jaya, 76100 Durian Tunggal, Melaka, Malaysia
[2]Faculty of Electrical Engineering, Universiti Teknikal Malaysia Melaka, Hang Tuah Jaya, 76100 Durian Tunggal, Melaka, Malaysia

[*]Corresponding e-mail: nazrulazhar@utem.edu.my

Keywords: Transition Mechanism; IPv6; Protocol-41

ABSTRACT – The IPv6 automatic tunneling has established, among other numerous transition mechanisms. It introduced to ensure that IPv6 is applied smoothly in the current infrastructure. Nonetheless, the implementation suspected of having been exploited for many sorts of attacks. As a matter of concern, this study discusses the ability of a Neighbor Discovery-based attack pushed on automatic tunneling. The methods and networking frameworks for preference development set up to execute the suggested attack method in a testbed environment. The result proved that the attack could attempt. The tunnel implemented a profound impact on the accomplishment of the threat on the modern internet.

1. INTRODUCTION

IPv6 mandates Internet Protocol Security (IPsec) inclusion to make it safer than IPv4. Most of the threats from the IPv4 network are no longer successful on IPv6 networks. Therefore, current security issues can mitigate for future implementation. However, after a few years of IPv6 services, [1] found some IPv4 threats in the IPv6 environment. Furthermore, [2] stated that automatic tunneling is among the spreader threats without detected by intrusion detection tools. Although [3] acknowledged this issue, but they are only given theoretical approaches to their proposed steps.

This study proposes possible NDP-based attack [4] methods through 6to4 tunneling. The technique focuses on flooding attacks using Router Advertisement and 6to4 tunneling as manipulated elements. This attack performed by review and identified the possible method. Next, to understand precisely, this method is presented in equation form. After that, the testbed developed for acquiring the desired environment. Then the packet analyzer was assigned to monitor and verify. The proposed attacks were structured and triggered via the testbed.

2. METHODOLOGY

The development of the NDP-based attack model to resolve the 6to4 tunnel security issues addressed here. In the tunneling context 6to4, a router believes all other routers and relays are "on-link." This condition allows attacking any router with ND messages from any node in the IPv4 network. Targeted attacks are a pseudo-interface of 6to4. When an IP address in the source or destination address, the tunneling will make the packet into it. The local link address has the ability to realize this attack. Both 6to4 routers and 6to4 relay routers are expected to be "accessible," and the whole IPv4 internet is a link, the proposed attack can make any node in the IPv4 network. While the victim node can either 6to4 or 6to4 relay router.

The flooding attack with the NA message technique was performed and tested on the testbed environment. Although the flooding triggered disruption, this study did not intend this attack to paralyze network activity, but rather to ensure that the packet of designs reached the destination with the suggested technique. Tunneling flow control developed and applied to show the claim correctly. This threat and monitoring built using a device capable of creating, transmitting, receiving, and analyzing packets. Then a series of schematic flow was planned to start as in Figure 1.

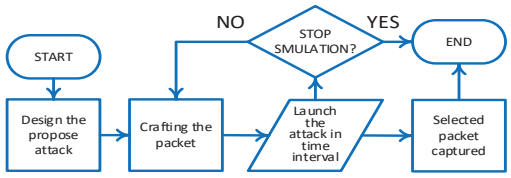

Figure 1 Process of initiating the attack

Design: Manipulating tunneling systems and generating numerous protocol-41 traffic between node X and node Y operates this form of attack. An attacker initiated from node G communicated on the 6to4 network with a 6to4 router. If the above-described equation taken from each traffic flow, the traffic structure across 6to4 tunnels can present as follows:

Node G triggers attacks inside the IPv4 networks and targeted to node X on 6to4 networks. The packet flow is generally interpreted as follows:

$$GX \rightarrow G:[G_4X_4\ [payload_4]]>>[B_6A_6ICMP88]:X \quad (1)$$

Then Eq. 1 modified by manipulating design neighbor discovery packet as follows:

$$T(Y,X) \rightarrow G:[Y_4X_4[B_6A_6ICMP88]]>>[B_6A_6ICMP88]:X \quad (2)$$

Traffic GX is modified to Tunnel (Y, X) or traffic-41 protocol, $payload_4$ is modified to packet NA, ICMPv6 type 136. When Eq. 2 entered the IP address, then:

$$T(G,R1) \rightarrow G:[10.0.3.1\ 10.0.1.1\ [FE80::2\ FE80::1\ ICMP88]]>>\ [FE80::2\ FE80::1\ ICMP88]:X \quad (3)$$

Craft: After deriving an outline of the attack strategy, the process began by constructing the packets, as shown in Figure 2. Development phases began with packet structure design. The IPv4 packet type-41 then created. Ethernet source and destination addresses are then declared and followed with IPv4 source and destination addresses. Lastly, IPv4 payload must contain ICMPv6 packet, source, and destination IPv6 addresses and NDP message IPv6 payload. Table 1 shows an example of instructions for each element of the packet.

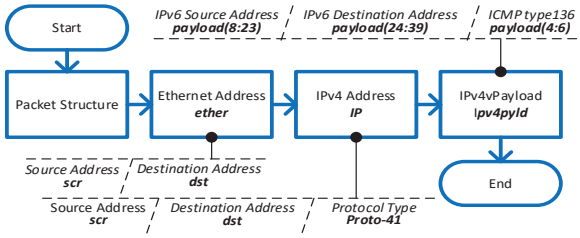

Figure 2 Packet crafting phase flow diagram

Table 1 Element instructions in the crafted packet

Elements involved	Program Commands
Source and destination Ethernet addresses.	>>> ether=(Ether (src='00:00:00:00:00:0e' , dst='00:00:00:00:00:0f' , proto='41'))
Source and destination IPv4 addresses.	>>> ipv4=IP(src='10.0.3.1' , dst='10.0.1.1')
Source and destination IPv6 addressees in IPv4 payload.	>>>ipv4pyld=IP(payload(8:24) = 'fe80::1', payload(24:40)= 'fe80::2')
Neighbor Advertisement in IPv4 payload.	>>>ipv4pyld=IP(payload(4:6)='88')
Send the crafted traffic at regular interval onto tunnel.	>>>send(ether/ipv4/ipv4pyld, iface='' loop='1' inter= 2)

Capture: Overall, the approach selects specific packet types 41 to be used with IPv6 data and keep the preferred information in a log file. It involved several steps, as shown in Figure 3. Briefly, all traffic on tunneling is filtered first. Second, the first payload byte identified in hexadecimal as '6.' The third process is to record IP protocol value and IPv4 address external source and destination. The next step is to select the IPv6 inner source and destination. Lastly, traffic flow remains in a log file. Table 2 shows programming by prescribed levels.

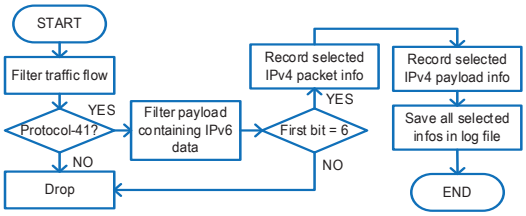

Figure 3 Process flow diagram of the packet capturing process

Table 2 Part of the programming according to the steps implemented

Steps	Program commands
Filtering IPv4 proto-41.	if pkt[IP] and pkt[IP].proto and pkt[IP].proto==41:
Identify IPv4 payload containing IPv6 data.	if pkt[IP].payload and hexlist(pkt[IP].payload)[0][0] == "6":
Record the ip protocol value and the outer source and destination IPv4 address.	v4src = str(pkt[IP].src) v4dst = str(pkt[IP].dst) v4p = str(pkt[IP].proto)
Record inner source and destination IPv6 address inner source and destination IPv6 address.	v6src = v6tostr(hexlist(pkt[IP].payload)[8:24]) v6dst = v6tostr(hexlist(pkt[IP].payload)[24:40])
Save the traffic flow in log file.	logstate(v4src, v4dst, v4p, v6src, v6dst)

Experimental design: Experimental 6to4 tunneling [3] provides a useful testbed for this study. This experiment was conducted under a controlled environment to reduce disturbances that may affect accurate results. Figure 4 shows a Testbed scenario developed with several different networks: 6to4 Network, Internet IPv4, Internet IPv6, and IPv6 Network.

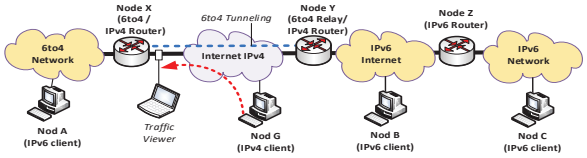

Figure 4 Scenario of 6 to 4 tunneling

3. RESULTS AND DISCUSSION

As expected, no resources are exhausted. On the other hand, the initiator threatens can validate by seeing crafted packets reached the victim's node. Figure 5 shows a part of the output gained from the log file that contained packet information. The records showed that this attack is valid and can execute under an automatic tunneling network.

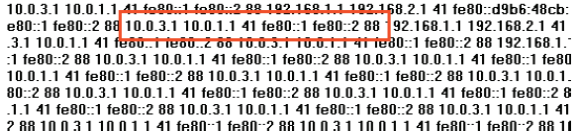

Figure 5 Log file saved by traffic builder

4. CONCLUSIONS

As found throughout the experiment, automatic 6to4 tunneling as an IPv6 transition mechanism may be abused by an intruder to initiate threats to IPv4, IPv6, or 6to4 network during transition periods. Like an NDP-based attack that intercepts various IPv4 or IPv6 traffic protocols, today's threat has shown its successful tunnel traffic protocol-41 capabilities. A previous researcher's proposed solution is not a reason to ignore but to keep it motivated. Therefore, serious action must arrange to develop suitable techniques to improve past work results. The discovery will soon find another appropriate method for their corresponding threats via IPv6 transition mechanism, specifically 6to4 tunneling. The comprehensive work is on protocol-41 traffic.

REFERENCES

[1] M. Tayyab, B. Belaton and M. Anbar, ICMPv6-Based DoS and DDoS Attacks Detection Using Machine Learning Techniques, Open Challenges, and Blockchain Applicability: A Review, *IEEE Access*, vol. 8, pp. 170529-170547, 2020.

[2] Bahaman, N., A.S. Prabuwono and M.Z. Masud, Implementation of IPv6 network testbed: Intrusion detection system on transition mechanism. *J. Applied Sci.,* vol. 11, pp. 118-124, 2011.

[3] Savola, P. and C. Patel, 2004. Security considerations for 6to4. RFC 3964, Internet Engineering Task Force. http://www.ietf.org/rfc/rfc3964.txt.

[4] Tao Zhang and Zhilong Wang, "Research on IPv6 Neighbor Discovery Protocol (NDP) security," *2016 2nd IEEE International Conference on Computer and Communications (ICCC)*, pp. 2032-2035.