FEASIBLE THREATS BY MANIPULATING TUNNELING PACKET ON 6TO4 NETWORK

Rizki Munawir[1], Nazrulazhar Bahaman[2], Aslinda Hassan[3]
Faculty of Information and Communication Technology, Universiti Teknikal Malaysia Melaka, Hang Tuah Jaya, 76100 Durian Tunggal, Melaka, Malaysia.
[1]rizkimunawir@gmail.com, [2]nazrulazhar@utem.edu.my, [3]aslindahassan@utem.edu.my

ABSTRACT

Tunneling mechanism becomes the most delicate transition mechanism compared to other transition mechanism, Dual Stack and Address Translation because tunneling offers easier way to start migrating from IPv4 to IPv6 and offers a smooth transition. 6to4 tunneling is automatic tunneling to conquer migration issues. In fact, tunnel transition mechanism is believed to be susceptible from several type of attacks. On 6to4 tunneling, Neighbor Discovery Protocol message becomes a potential media to exploit by attacker. It starts with deploying a controlled testbed network environment and running several scenario DoS attack by manipulating NDP message through 6to4 tunneling. The expected result is to prove that attacking methods is feasible and effective.

Keywords: 6to4 tunneling, Transition mechanism, IPv6, IPv4, Denial of Service, Neighbor Discovery Protocol, Protocol-41

INTRODUCTION

The expansion of internet usage in recent year has a great impact on availability of global addressing. Internet Protocol version 4 (IPv4) which was already deployed since a decade ago has running out. Therefore to overcome the limit of IPv4 addressing, Internet Engineering Task Force (IETF) started in 1994 has initiated a design and development of a new standard protocol known as Internet Protocol version 6 (IPv6). Compared with the earlier version, there are significant improvements such as expanded addressing capabilities, header format simplification, improved support for extension and options, flow labeling capacity, authentication and privacy capabilities [1, 2].

One of the big problems and challenges in deploying IPv6 environment is how to

IPv6 [3]. In order to achieve this, it needs lots of investment to build pure IPv6 environment and also it cannot straightaway replace IPv4 with IPv6.

IETF has been working with several groups to make strategies and mechanisms to ensure the migration from IPv4 to IPv6 is smooth and success without any interference to existing IPv4 environment [2].

Transition mechanism from IPv4 to IPv6 can be divided into three big categories: Dual stack mechanism [4,5], address translation mechanism [6,7] and tunneling mechanism [8,9]. Dual stack mechanism will enforce element of network to support both IPv4 and IPv6 protocol. Address translation mechanism will place a device to translate address between two different protocols. Tunneling mechanism will encapsulate every IPv6 packet into IPv4 packet and deliver it to another node through IPv4 network infrastructure/environment tunneling mechanism which is the most delicate mechanism to deploy and implement IPv6 network environment to extend and replace IPv4 network environment [10].

As mentioned, IPv6 protocol offers new enhancement on security to protect their network element from malicious activity or threat, but it is only when all traffic across

e protocol which is

[12] and [13] also review a few security threats and scenario for IPV6 transition. Transition from old into the new protocol will involve two different environments, in that case feasibility of threats on IPv4 environment occured on IPv6 environment and vice versa are quite high [14]. [14] and [15] stated that a few IPv4 threats are found on IPv6 environment. Theoretical information about security consideration on transition mechanism was already define by [1] and [16].

This paper in general proposes the feasible method of attacks on 6to4 tunneling transition mechanism. A few methods can be conducted to attack this tunneling however this paper will focus only on silent attack trough 6to4 tunneling which exploit Neighbor Discovery Protocol as vulnerability part. The process involved is by identifying the possible attack and the method is described in some equation. On the controlled network environment the method of attack will be testing and analyzing. Network environment is built on GNS3 software, the attack is performed by Scapy Python and Wireshark is used for monitoring and validating the traffic.

The following section will explain about tunneling transition mechanism and Denial of Service threats followed by explanation of design and testing mechanism. Then we will discuss about testing result. Lastly conclusion of the research will be described.

6TO4 TUNNELING MECHANISM

[17] defined tunneling mechanism as a start-up transition method or tool used during transition period from IPv4 native network into IPv6 native network but it is not a permanent solution because at the end of the result, every network only use one protocol which is IPv6 protocol. Automatic tunneling of IPv6 trough IPv4 can be described as when user wants to reach or access IPv6 network environment service via a network which is not supported by IPv6 Protocol such as IPv4 network environment without any explicit tunneling setup or called by automatic tunneling mechanism. In the transition case, tunneling mechanism will encapsulate every IPv6 packets in IPv4 packets. This packet will use Protocol-41 as their header mark. The 6to4 tunneling consists of two elements: 6to4 Host/Router and 6to4 Router Relay. The 6to4 Host/Router is an element which uses to communicate with another 6to4 host/router while the 6to4 Relay is an element that acts as a bridge to communicate with IPv6 Native network. Figure-1 shows the standard topology of 6to4 tunneling.

Automatic tunneling makes this mechanism has a security vulnerability. When a link on the tunnel defined as "on-link", every traffics passing through 6to4 Router/Relay will be processed as a normal traffic. Problem will occur when traffics already altered or spoof by unauthorized person and it has a possibility to affect node which involved in 6to4 tunneling communication. [16, 18] defined the possibility of traffic manipulation on 6to4 tunneling as Denial of Service Attack. The mechanism of attack almost same with attack or threats on IPv4 network environment, even worse in IPv6 network environment due to lots of new enhancement and mechanism on IPv6 communication.

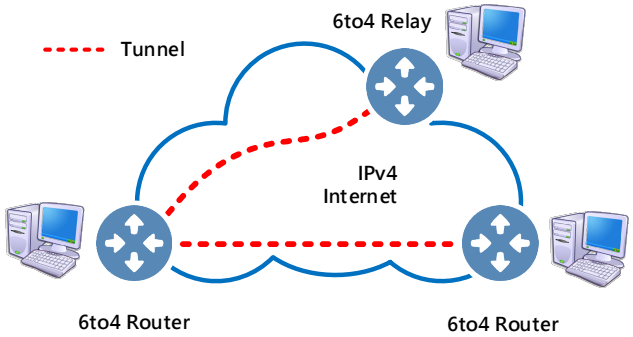

Figure-1. Topology of 6to4 Tunneling

By exploiting this kind of attack method, not only IPv6 native becomes susceptible but all node which involved in 6to4 tunneling (IPv4 native element and 6to4 element) also becomes susceptible.

6TO4 TUNNELING PACKET FLOW

To maintain the understanding of this transition mechanism, traffic or packet flow will be described in equation forms. Flow will describe the detail process and modification of packet from source node until destination node on normal communication and 6to4 tunneling communication. Refers to [19], normal transmission form source node (node_A) to destination node (node_B) in IPv4 (equation 1) and IPv6 (equation 2) network environment can be represented as follows:

$$AB=A:[A_4\ B_4\ payload_4] \gg [A_4\ B_4\ payload_4\ ]:B \quad (1)$$

$$XY=X:[X_6\ Y_6\ payload_6] \gg [X_6\ Y6\ payload_6]:Y \quad (2)$$

Equation 1 shows the transmission is from interface on node A to interface on node B. A_4 is IPv4 source IP, B_4 is destination IP and $payload_4$ is payload of IPv4. Same explanation on equation 2 for IPv6 transmission.

For 6to4 tunneling mechanism which will encapsulate IPv6 in IPv4 payload, the equation may be written as follow:

$$payload_4 = X_6\ Y_6\ payload_6 \quad (3)$$

Tunneling is established from node A and node B, it can be written as follow:

$$Tunnel(AB)=A:[A_4\ B_4\ payload_4] \gg [A_4\ B_4\ payload_4\ ]:B \quad (4)$$

By combining (3) and (4) the IPv6 communication trough 6to4 tunneling can be established.

$$Tunnel(AB)=A:[A_4\ B_4\ [X_6\ Y_6\ payload_6]] \gg [A_4\ B_4\ [X_6\ Y_6\ payload_6]]:B \quad (5)$$

METHOD

This section will discuss about the security issue which could happen on 6to4 tunneling. By developing and initiating a few kind of attacks, the expected security issues could be determined. An experiment will be conducted on controlled network environment [20] which deployed on GNS3 simulator software. The experiment assumes that attacker already know every detail of information of the target network and node so there are no initial activity conducted by attacker to collect network information. Normally, intrusion will try to make the target exhausted however the types of attack used in this paper only ensure that the packet initiated by attacker to reach the target is suitable with the used method. All traffics are monitored to proof the traffic is correct. Attacker will use Python Scapy to build crafted packet and broadcast it through 6to4 tunneling network.

Figure-2 show the testbed of 6to4 network tunneling that adapted from [20] and [21]. Tunneling communication between nodeA and nodeB will be used as media to deliver the packet from nodeX (IPv6) to nodeY (IPv6).

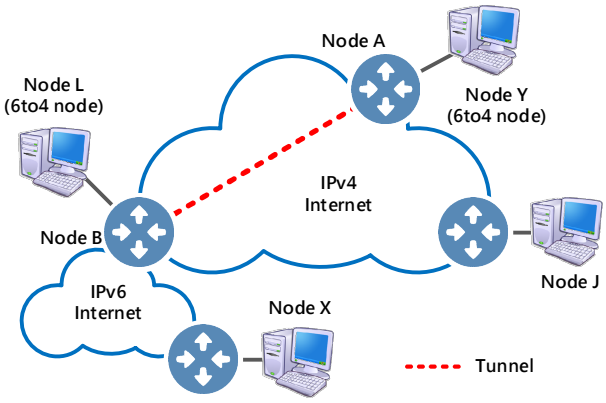

Figure-2. Testbed of 6to4 Tunneling

Initiator of attack is node J which is a member of IPv4 Network. Let node X as a target node. Because of node B and J are using the same IPv4 protocol, the communication between A and J can be represented with equation (1). In this situation node J starts to build crafted packet by manipulating the content of payload4 before broadcasting it to its subnet. The manipulation can be done by changing the source and destination of IPv6 which also changing the payload [6]. The important thing which attacker must consider is he must include protocol 41 header on crafted packet so it can be recognize by 6to4 router/relay. NDP manipulation on payload6 also has an important part. Manipulation conducted in this part can determine what type of attack is used such as packet injection, injected ping, dying packet and *etc*. based on what type NDP is being used when building the crafted packets. Formally the scenario above can be written as follow:

$$Tunnel(AB)=J:[A4\ B4\ [X6\ Y6\ payload6]] \gg [A4\ B4\ [X6\ Y6\ payload6]]:B \quad (6)$$

Table-1. Content of Crafted Packet

INITIATOR	TARGET	SOURCE 4 - VALID / (FAKE)	DESTI 4 - VALID / (FAKE)	SOURCE 6 - VALID / (FAKE)	DESTINATION 6 - VALID / (FAKE)	PAYLOAD (TENTATIVE)
IPV4 Native	6to4 Router	(192.168.2.2)	10.10.10.1	2001::3	2001::1	ICMPv6 Echo Request
		(192.168.2.2)	10.10.10.1	2001::3	2001:1111::a00:27ff:fe13:2455	ICMPv6 Echo Request
IPV4 Native	IPv6 Native	(192.168.2.2)	10.10.10.1	2001:3333::a00:27ff:fe13:2455	2001::1	ICMPv6 Echo Request
		(192.168.2.2)	10.10.10.1	2001:3333::a00:27ff:fe13:2455	2001:1111::a00:27ff:fe13:2455	ICMPv6 Echo Request

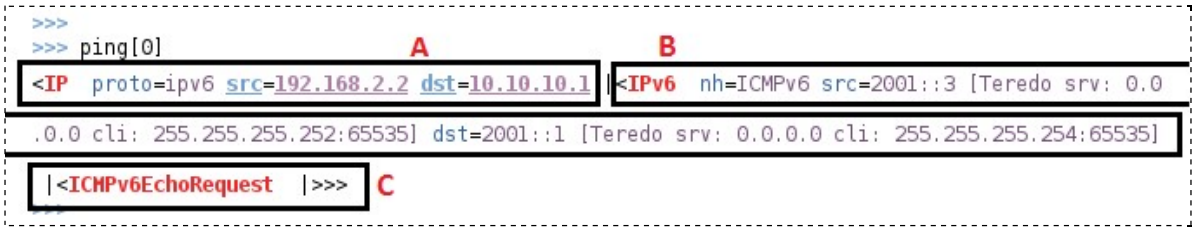

Figure-3. Crafted Packet on Scapy Python

EXPERIMENTAL RESULT

Experimental environment is built on GNS3 Simulator software. It consists of three different network clouds which is IPv4 native, IPv6 Native and 6to4 Dual Stack. Each cloud has a dedicated host. Node A and Node B will be configure as a gateway to 6to4 tunnel called as 6to4 Router/Relay. In this paper all attacks only initiated by IPv4 native node which is node J and the targets are other nodes which are IPv6 nodes and 6to4 Dual Stack nodes. Decision to used IPv4 as initiator is based on a fact that the majority real networks still use this protocol.

Router is built using Cisco 3750 which supports dual stack network. Linux Debian platform will be used for a hosts, Scapy Python plays role as attacker software and wireshark is used as a traffic monitoring and validating system which will be embedded on every link on tesbed network.

Experiment is started by configuring all routers and hosts to run in 6to4 tunneling and ensuring that traffic can be deliver to other node trough 6to4 tunnel. It then activates traffic viewer on corresponding link and initiates attack from node J. Finally tracing and analyzing packet movement and changes on traffic viewers are done.

Table-1 show an example content of crafted packet. NDP manipulation used in this paper is ping injection. The content can be anything depends on type of attacks that wants to launch, but it is not detail discussed here. Based on figure 2 example of crafted packet can be written as follow:

Tunnel(AB)=
J:[192.168.2.2 10.10.10.1[2001::1 2001::3 ICMPv6-128]] ≫
[192.168.2.2 10.10.10.1[2001::1 2001::3 ICMPv6-128]]:B(7)

Equation above shows that node J becomes the initiator interface which is using 192.168.2.2 as a source address. Destination 4 address must be a valid 6to4 router address and match with destination 6. In this case source 6 becomes the main target of attack. First, node J will broadcasts crafted packet to IPv4 network and deliver it to node B. Node B will decapsulate it and send to end destination node. Destination node will process the packet and send reply (ICMPv6EchoReply) to real target (Source 6).

Figure-3 is example of crafted packet which build by scapy, the description of that figure same with equation 7 but one part that must be consider is on part A there is proto which configure as "ipv6". This protocol is synonym of protocol-41 on scapy. Protocol-41 must be included on IPv4 part so 6to4 router/relay will process as 6to4 tunnel packets.

Result of table 1 shows that every packet sent by attacker will be accepted and processed by 6to4 Router like normal packets. Crafted packets will not cause any problem and not causes any exhaustion on the targeted node. In this kind of attack not only NDP message is being manipulated, by spoofing the source and destination address attacker also can using another IPv6 node as a reflection node to attack. From this experiment we can validate that this attack method is one of security issue on 6to4 automatic tunneling.

CONCLUSION

Experiment results show that 6to4 automatic tunneling transition mechanism is susceptible to many kind of intrusions, it can cause havoc not only on 6to4 elements but also on IPv6 and IPv4 elements. Process inside 6to4 tunneling which accept and processing every packet that already considered as "on-link packet" lead this mechanism to many security issues. NDP manipulation attacks prove that method is feasible and effective to produce silent attacks.

There are a few ways to mitigate issue on automatic tunneling. First is by disabling/blocking protocol 41 which still not effective yet because it will deactivate function on 6to4 tunneling. Second is by filtering or blocking NDP message however it

will cut the communication of IPv6. IPSEC and SEND (Secure Neighbor Discovery) are possible solutions but still have high complexity to develop. For future, research and developing a technique to conquer security issues on 6to4 automatic tunneling is indispensable.

ACKNOWLEDGMENTS

The authors would like to thank C-ACT and INSFORNET Research Group of Universiti Teknikal Malaysia Melaka (UTeM) for providing facilities and financial support under the university Short Term Grant with Project No. PJP/2014/FTMK(1B)/S01295.

REFERENCES

[1] S Deering and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification," Internet Engineering Task Force, Request For Comment: 2460 1998.

[2] Peng Wu, Yong Cui, Jianping Wu, Jiangchuan Liu, and Chris Metz, "Transition from IPv4 to IPv6:A State-of-the-Art Survey," IEEE COMMUNICATIONS SURVEYS & TUTORIALS, vol. 15, no. 3, p. 14071424, 2013.

[3] E. Davies, S. Krishnan, and P. Savola, "IPv6 Transition/Co-existence Security Considerations," Internet Engineering Task Force, Request For Comment: 4942 2007.

[4] Jian Chen, Zhiping Jia, and Xin Li, "A New Design of Embedded IPv4/IPv6 Dual-stack Protocol ," in International Conference on Network Computing and Information Security, 2011, pp. 163-167.

[5] Ra'ed AlJa'afreh, John Mellor, and Irfan Awan, "Evaluating BDMS and DSTM Transition Mechanisms," in Second UKSIM European Symposium on Computer Modeling and Simulation, 2008, pp. 488-493.

[6] C. Huitema, "Teredo: Tunneling IPv6 over UDP through Network Address Translations (NATs)," Internet Engineering Task Force, Request for Comments: 4380 2007.

[7] F Baker, X Li, C Bao, and K Yin, "Framework for IPv4/IPv6 Translation," Internet Engineering Task Force, Request for Comments: 6144 2011.

[8] Nazrulazhar Bahaman, Anton S Prabuwono, Raed Alsaqour, and Mohd Zaki Mas`ud, "Network Performance Evaluation of Tunneling Mechanism," Journal of Applied Sciences, vol. 12, no. 5, pp. 459-465, 2012.

[9] Mohammad Aazam, M. Syed Adeel, Hussain Shah Syed Atif, Muhammad Alam, and Imran Khan, "Evaluation of 6to4 and ISATAP on a Test LAN," in IEEE Symposium on Computers & Informatics, 2011.

[10] Dinesh Hadiya, Rohit Save, and Geetu Geetu, "Network Performance Evaluation of 6to4 and Configured Tunnel Transition Mechanisms," in International Conference on Emerging Trends in Engineering and Technology, 2013.

[11] Nazrulazhar Bahaman, Anton S Prabuwono, and Nurul Azma Zakaria, "Neighbor discovery message as threats on 6to4 tunneling", Research Journal of Information Technology, vol. 6, no. 3, pp. 198-206, 2014.

[12] Amjed Sid Ahmed, Rosilah Hassan, and Nur Effendy Othman, "Security Threats for IPv6 Transition Strategies: A Review," in International Conference on Engineering Technology and Technopreneuship (ICE2T), 2014.

[13] Viney Sharma, "IPv6 and IPv4 Security challenge Analysis and Best- Practice Scenario," Int. J. of Advanced of Networking and Applications, vol. 01, no. 04, pp. 258-269, 2010.

[14] Emre Durdagi and Ali Buldu, "IPV4/IPV6 Security and Threat Comparisons," in Procedia Social and Behavioral Science 2 , 2010, pp. 5285-5291.

[15] Harith Dawood, "IPv6 Security Vulnerabilities," International Journal Of Information Security Science, vol. 1, no. 4, pp. 100-105, 2012.

[16] P. Savola and C. Patel, "Security Considerations for 6to4," Internet Engineering Task Force , Request for Comments: 3964, 2004.

[17] B. Carpenter and K. Moore, "Connection of IPv6 Domains via IPv4 Clouds," Internet Engineering Task Force, Request for Comments: 3056, 2001.

[18] Monali Mavani and Leena Ragha, "Security Implication and Detection of Threats due to manipulatingIPv6 Extension Headers," in Annual IEEE India Conference (INDICON), 2013.

[19] L. Colitti, G. Di Battista, and M. Patrignani, "Discovering IPv6-in-IPv4 Tunnels in the Internet," in Network Operations and Management Symposium, Seoul, 2004, pp. 613 - 626.

[20] Nazrulazhar Bahaman, Anton S Prabuwono, and Mohd Zaki Mas`ud, "Implementation of IPv6 Network Testbed- Intrusion Detection System on Transition Mechanism", Journal of Applied Sciences, vol. 11, no. 1, pp. 118-124, 2011.

[21] N. Bahaman, E. Hamid, and A. S. Prabuwono, "Network performance evaluation of 6to4 tunneling," ICIMTR 2012 - 2012 Int. Conf. Innov. Manag. Technol. Res., pp. 263–268, 2012.