Possible Attacks by Manipulating IPv6 Tunneling Traffic on 6to4 Network

Nazrulazhar Bahaman[1], Rizki Munawir[1],Aslinda Hassan[1], Erman Hamid[1]

[1]INSFORNET Research Group, Centre for Advanced Computing (C-ACT), Fakulti Teknologi Maklumat dan Komunikasi, Universiti Teknikal Malaysia Melaka, Hang Tuah Jaya, 76100 Durian Tunggal, Melaka, Malaysia

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

Keywords: Transition Mechanism, Neighbor Discovery Protocol, Protocol-41

ABSTRACT – Tunneling mechanism becomes the most delicate transition mechanism compared to others because its offers easier way to start migrating from IPv4 to IPv6. 6to4 tunneling is automatic tunneling to conquer migration issues. In fact, it is believed to be susceptible from several type of attacks. Neighbor Discovery Protocol (NDP) message becomes a potential media to exploit by attacker. As a concern, this paper thoroughly describes on potential of attack reach through the automatic tunneling. It starts with deploying a controlled testbed network environment and running several scenario attack by manipulating NDP in tunneling traffic through 6to4 network. The expected result is to prove that attacking methods is feasible and effective.

1. INTRODUCTION

Internet Engineering Task Force (IETF) was entrusted to develop and replace the existing Internet Protocol (IP). As a result they have successfully introduced the new IP structure more efficient and proficient to accommodate the current weaknesses. This new IP known as Internet Protocol version 6 (IPv6) was first introduced to the public in December 1998. To date, most of deployments by previous researches were to identify constraints that may occur in IPv6. Since it takes prolonged period to full implementation, Transition Mechanism (TM) has been inspired in order to catalyze a successful integration of IPv6 into an existing network. As referred to [1], TMs are identified into three main categories based on their operation and the way of their implementation: dual stack, Tunnelling, and Translation. Among of these mechanisms, tunneling is preferred implemented nowadays.

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 the network is on the same protocol which is IPv6 Protocol (IPsec). [2] 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 occurred on IPv6 environment and vice versa are quite high. [3] stated that a few IPv4 threats are found on IPv6 environment. Theoretical information about security consideration on transition mechanism was already define by RFC2460.

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.

2. METHODOLOGY

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 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 broadcast crafted packet through 6to4 tunneling network. Then, a sequence of schematic flow has been designed as initiate the attack as in Figure 1.

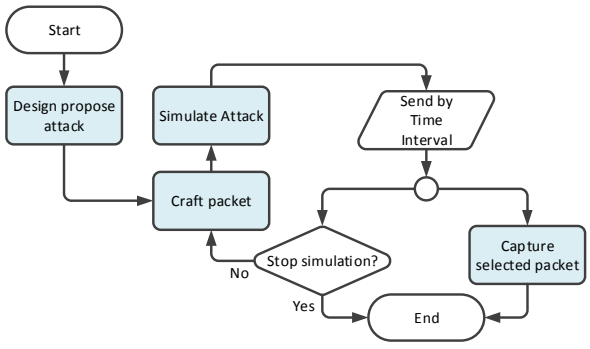

Figure 1 Process of initiating the attack

Figure-2 show the testbed of 6to4 network tunneling that adapted from [4]. Tunneling communication between nodeA and nodeB will be used as media to deliver the packet from nodeX (IPv6) to nodeY (IPv6). 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 as follow:

AJ=A:[A4 J4 payload4]≫[A4 J4 payload4]:J

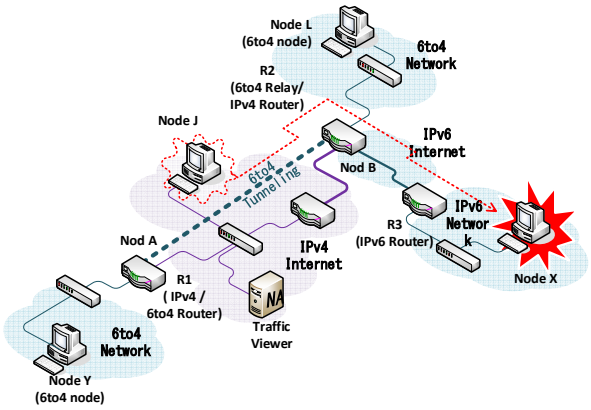

Figure-2. Testbed of 6to4 Tunneling

In this situation node J starts to build crafted packet by manipulating the content of payload$_4$ before broadcasting it to its subnet. The manipulation can be done by changing the source and destination of IPv6 which also changing the payload. 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 payload$_6$ 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]] ≫[A4 B4 [X6 Y6 payload6]]:B

3. EXPERIMENTAL RESULT

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.

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

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*). One part that must be consider at crafted packet 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 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.

4. 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.

ACKNOWLEDGMENT

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/2018/FTMK(4B)/S01631.

REFERENCES

[1] Waddington, D. G., & Fangzhe, Chang. (2002). *Realizing the transition to IPv6*. Communications Magazine, IEEE, 40(6), 138-147.

[2] 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

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

[4] 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.