A Comprehensive Study on Various Security Attacks against IPv6

[1]Vikram P. Solanki, [2]Prof. Mitesh Thakkar
[1]ME Scholar, [2]Assistant Professor
LJIET, Ahmedabad
[1]cevikram.2010@gmail.com, [2]mitesh.thakkar11@gmail.com

Abstract: **This paper is about the security attacks in relation to the dispersing Internet Protocol version 6 (IPv6). Since it isn't the default network protocol established nowadays. There are no best practices from the issue of network administrators. There are no assurances that applied IPv6 protocol stacks and security techniques without any bugs. Thus this paper interprets almost all IPv6 security attacks.**

Keywords: IPv6, ICMPv6, Security, Firewall, Intrusion Detection, Attack, Man-in-the-Middle, Denial of Service

I. Introduction

The internet protocol version 6 (IPv6), specified in 1998, is intended to replace IPv4 in the worldwide Internet mostly due to the address exhaustion of IPv4. IPv6 exceedingly enhances the address space from 32 bits to 128 bits. But today, 15 years after its issue, the usage of IPv6 in the Internet is still only about 1 % compared to the usage of IPv4. Likewise, IPv6 implementations in all types of hardware and programs are not that mature than IPv4 implementations in relation to, e.g., functioning characteristics and its steadiness, firewall features, localized network defense mechanisms, application support, etc. Although, due to the exhaustion of accessible IPv4 addresses by the Internet Assigned Numbers Authority (IANA) on February 03, 2011, the necessity for utilizing IPv6 becomes more and more conspicuous.

II. ATTACKS AGAINST IPv6

2.1 Multicast

By certain multicast messages an attacker can very very quick do a reconnaissance attack on a local network. Simply pinging the all-nodes multicast address ff02::1 displays several appliances that are living. Additionally, some NMAP scripts can be utilized to disclose nearly all IPv6 clients on the network by forcing them to develop new (temporary) IPv6 addresses by SLAAC. The corresponding Multicast Listener breakthrough messages from the purchasers, which are sent by multicast, reveal their interface IDs,[1].

2.2. Extension Headers

Interior extension headers an attacker can drive data that remain undetected if the intermediary firewalls do not fully ascertain the options of these headers. This kind of attack is called "covert channel". For example, interior the Hop-by-Hop extension header, the PadN option which according to the standard should comprise zeros can be filled with any characters. That means, hidden data can be dispatched by the network without moving the upper layer protocols,[1].

III. ATTACKS AGAINST ICMPv6

ICMPv6 performances a key function in the proper usage of IPv6. Particularly the Neighbor Discovery messages such as Router Advertisements (RAs) and Neighbor Solicitation/ Advertisements (NS/NA) are needed for the clear-cut usage of the new Internet Protocol.

3.1. Router Advertisement Spoofing

If an attacker sends spoofed Router Advertisements interior a subnet, all IPv6 nodes will directly change their routing tables and store the attacker as one of the default routers. If they drive traffic to the Internet, this new default router will be used. This directs to a position in which the attacker can completely see (and even modify) all outgoing traffic from the IPv6 nodes to the Internet. This is called a Man-in-the-Middle (MITM) attack . Meantime the attacker can't see the coming back traffic from the Internet since he is not able to spoof the genuine default router on the network. See Figure 1 underneath for an illustration of this attack,[1].

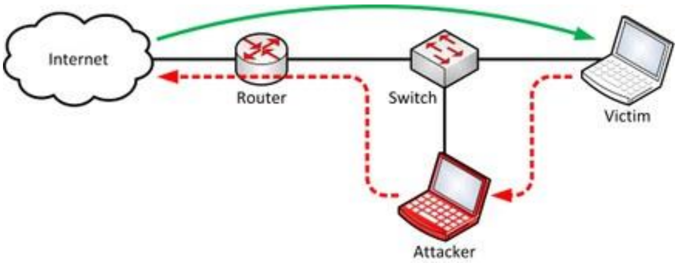

Figure 1: Router Advertisement "Half" Man-in-the-Middle Attack,[2]

3.2. Router Advertisement Flooding

The attacker can flood many thousand RAs which immediately freezes all Microsoft Windows computers since they are completely overloaded with that numerous SLAAC processes. This bug is renowned for numerous years but still exploitable. That means: If an attacker has get access to a localized network and is not stopped by the intermediary switch while sending spoofed RAs, the complete Windows natural environment will be frozen,[1]!

3.3. Neighbor Discovery Spoofing

When the attacker spoofs certain Neighbor Advertisements, he can execute a MITM attack. By answering falsified Neighbor Advertisements to the handed out Neighbor Solicitations from the victims, he redirects all IPv6 traffic over his "routing instance" in the identical subnet,[1].

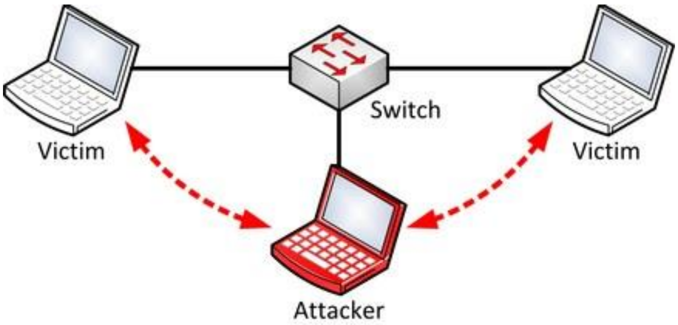

Figure 2: Neighbor Discovery Spoofing "Half" Man-in-the-Middle Attack,[2]

3.4. Duplicate Address Detection

A DoS attack is executed if the attacker responses to all Duplicate Address Detection messages (DADs) from a new IPv6 node (with a not yet assigned IPv6 address). The node habitually believes that this address is currently in use and will not ever get an access to available IPv6 address and is thus unable to get access to the network. This situation remains until the attacker halts the attack,[1].

IV. ATTACKS AGAINST DHCPv6

4.1. Address Space Exhaustion

If the notion of stateful DHCPv6 is utilized, an attacker can consume the IPv6 address pool on the server, alike to a DHCPv4 server. Even though the DHCPv6 server could supply sufficient IPv6 addresses, it has to store a little binding for each address and the corresponding DUID from the purchaser which will at least consume the memory of the server if it is flooded with numerous requests,[1].

4.2. Rogue DHCPv6 Server

An attacker can also place his own DHCPv6 server interior a network and circulate falsified standards, e.g. a spoofed DNSv6 server address. If the clients accept this DNS server, they will get falsified DNS responses from now on if the attacker also owns the spoofed DNS server. With this attack, interior IPv6 users can be redirected to other (web-) servers than they proposed to access. The image underneath shows the basic attack in the local network,[1].

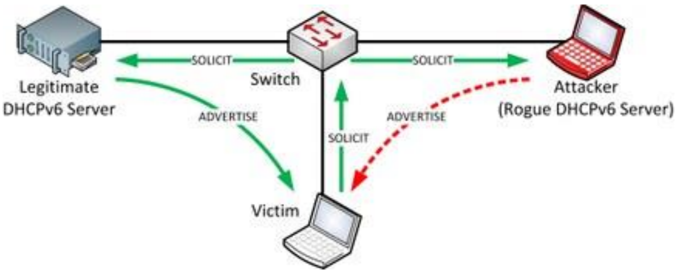

Figure 3: Rogue DHCPv6 Server,[2]

V. Related Work

Johannes Weber proposes that the security matters in relation to the dispersing Internet Protocol version 6 (IPv6). Since it is not the default network protocol deployed nowadays there are no best practices from the point of network administrators and there are no any guarantees that applied IPv6 protocol stacks and security methods are without any bugs. Thus this thesis explains nearly all IPv6 security attacks in details and covers the construction of a test laboratory in which three firewalls disclose their protecting against capabilities against IPv6 security vulnerabilities. Comprehensive benches throughout this thesis register the known attacks with their attacking tools as well as the concrete tests in the lab. Recommendations for IPv6 nodes and firewalls are presented after each attack section,[2].

Savvas Chozos introduces IPv6, the successor of IPv4, the stateless autoconfiguration characteristic as a convenient alternate to the Dynamic Host Configuration Protocol (DHCP). However, the security implications of this new approach have only been discussed at the conceptual grade. This thesis study evolves software founded on the open-source packet capture library Jpcap to capture and construct appropriate ICMPv6 autoconfiguration messages. The evolved Java software is utilized to implement two DoS risks to the IPv6 autoconfiguration procedure in a laboratory IPv6 network. The outcomes indicate that these risks are genuine and farther investigations are required to identify apt countermeasures. Throughout this work compliance defects are also recognized for the Linux Operating System's IPv6 implementation,[3].

Fredrik Folke investigates and presents distinct risks that a network can be revealed to and the common defense methods that can be applied, with a aim on the network perimeter – specifically the router/firewall between the local area network and the Internet. All Internet attached devices and networks are revealed to and influenced by security threats to some degree, therefore security is significant in nearly every type of network. With the constant development of the Internet the 32-bit addressing design ipv4 is proving to be insufficient, and thus the transition to the 128-bit addressing design ipv6 is evolving critical. With ipv6 comes a new security risk (while still old threats remain) that needs an comprehending of perimeter security. In this thesis we protected a home router and recount these steps to enable home and small enterprise owners to protected their IPv6 network at a somewhat reduced cost,[4].

Keith A. Gehrke suggests that With DoD networks gradually adopting and transitioning to the next generation Internet Protocol, IPv6, very cautious concern must be given to IPv6-specific significances on network protection. While network Intrusion Detection schemes (NIDS) aid in defending present IPv4 DoD systems, NIDS performance in operational DoD IPv6 environments is mostly unknown. As a step in the direction of more rigorous NIDS evaluation, we enquire the extent to which known IPv4 attacks are able to evade detection when converted to equivalent IPv6 attacks. Utilizing 13 general attack classes, we test the IPv6 readiness of two well liked open source NIDSs: SNORT and BRO. Attacks in each class are assessed in a virtual check bed that forms both "native" and "Transitional" systems. In the native IPv6 natural environment, we accomplish a 95% detection rate for SNORT as contrasted to 8% with BRO. In addition, we find out a bug in SNORT where a carefully crafted IPv6 package determinants the NIDS to fail open, permitting full circumvention. Our outcome propose that, with esteem to IPv6, both NIDS signatures and NIDS programs need additional checking and evaluation to be operationally ready,[5].

Kazuyuki Nishida alterations the customary paradigm completely and suggest a new solution called *Unified Multiplex Communication Architecture*. The most distinction from the present Internet is that an IP address is not utilized for node identifier, but for service identifier. In the Unified Multiplex connection Architecture, we change IP addresses session-by-session, and the allotted address is invalid directly after the session terminates. This architecture easily changes the direction for use of IP address but enhances the security significantly. However, there is a major topic on Unified Multiplex how to work out the IP address to connect the server, since IP address is assigned to session one-by-one. Former to communication, the client should know the IP address of the server which is utilized for awaiting the connection from the client,[6].

Fred Wieringa reconsiders some of the risks and vulnerabilities affiliated with the new Internet Protocol version 6, with an focus on the vulnerabilities that exist because of the need of utilizing secure methods and protocols in combination with IPv6. At the end, it concludes summarizing some of the most widespread security concerns in the use as a weapon, goal or means,[7].

Muhammad Taqi Raza H. M., Syed Rehan Afzal, Hamid Mukhtar, Seung-wha Yoo, Dong-Kyu Kim and Ki-Hyung Kim concludes that unlike Mobile IPv4, where wireless node communicates with its peer through a longer path, via Home Agent, in Mobile IPv6 a mobile node directly communicates with its peers even though it moves to the new location and alternates its IP address, this mechanism is called Route Optimization. In Route Optimization, the mobile node drives the binding message to its peer node, the message comprises the new address of the mobile node, called as Care of Address, which confirms that the mobile node is infect moved to the new position from its Home Network. After obtaining the binding message, the peer node drives all packets which are destined to the Mobile's Home Address to the Care of Address. But there are numerous security risks involved, when a malicious node might be able to establish a attachment with the mobile node by sending the false binding messages. By doing so malicious node can redirect the traffic, can launch the DOS Attacks and can furthermore Replay the authenticated messages, etc. So considering theses security matters, we have proposed a protected protocol which stops the attacker to set up false attachments and guarantees the secrecy and integrity of the mobile node and its peers,[8].

Ali Emre Yildirim investigates the IPv6 protocol by carrying out some measurements over longer distances. One of the investigations will give an indication of the rate the IPv6 is being taken up in the world, by monitoring over seven thousand University webservers over a period of two weeks. Another study compares the TCP throughput presentation of WWW protocol on five University webservers for both IPv6 and IPv4 networks over a time span of two weeks. The results demonstrated that the TCP throughput present differences between the two Internet protocols were nearly the identical. The IPv6 adoption rate study did not outcome in a conclusive way, although an indication of an boost was observed and by additionally surveying preceding work, and discerning IPv6 monitoring websites on the IPv4 Internet, one can state that it is most likely that the IPv6 are being taken up continuously,[9].

VI. Conclusion

In this paper, it has been surveyed that the living works on the security attacks against IPv6 protocol. Those attacks are studied and investigated deeply to promote the security of IPv6 and furthermore to ensure the solution of attacks. In this thesis we explained the IPv6 protocol and its security vulnerabilities. We displayed the distinct scopes of security matters which we categorized in attacks against the protocol itself, ICMPv6 attacks that are nearly driven from the local connection (layer 2), and DHCPv6 attacks. We farther showed that vulnerabilities can originate from insufficient implementations and enclosed the problems that are relevant throughout the transition from IPv4 to IPv6.

References

[1] Johannes Weber, “IPv6 Security – An Overview”, *https://labs.ripe.net/Members/johannes_weber/ipv6-security-an-overview*, June 18, 2013.

[2] Johannes Weber, “IPv6 Security Test Laboratory”, *http://blog.webernetz.net/2013/05/06/ipv6-security-master-thesis/*, May 6, 2013.

[3] Chozos, Savvas. *Implementation and analysis of a threat model for IPv6 host autoconfiguration*. Diss. Monterey, California. Naval Postgraduate School, 2006.

[4] Folke, Fredrik. *Security for home, small & medium sized enterprises IPv6 networks: Security using simple network equipment*. Diss. KTH, 2012.

[5] Gehrke, Keith A. *The unexplored impact of IPv6 on intrusion detection systems*. NAVAL POSTGRADUATE SCHOOL MONTEREY CA DEPT OF COMPUTER SCIENCE, 2012.

[6] Murata, Masayuki, and Kazuyuki Nishida. "Design and Implementation of Secure IPv6 Communication Architecture using Non-negotiated Specific Service Addresses." (2011).

[7] Wieringa, Fred, C. de Laat, and Mr R. Visser. "IPV6 risks and vulnerabilities Project Report." (2012).

[8] HM, Muhammad Taqi Raza, et al. "Mobile IPv6 (MIPv6) Route Optimization Security Design Protocol."

[9] Yildirim, Ali Emre. "Measuring IPv6 adoption rate and performance in the Internet." (2011).