Hacking Techniques in IPV6 Networks and Prevention Machanisams

A.M Aslam Sujah, H.M Shadir, M.S.M Shakir, K. Jasandan, S. Kavitha, Dhishan Dhammearatchi

Sri Lankan Institute of Information Technology Computing Pvt. Ltd.

Abstract- Internet protocol version 6, the new version of the Internet Protocol has been developed to provide new services and to provide flexibility to the Internet's growth. An overview of the key security issues outlines the challenges in deploying and transitioning to IPv6. Protecting against threats, viruses, hackers can be regarded as the most difficult problems on the Internet today. One solution for these attacks is to trace the source of the attacks. However, it is not easy to trace since the attackers generally use the spoofed IP source addresses to hide own network location. The current Internet architecture does not provide any means to find the real sources of IP packets. Numerous trace back mechanisms have been proposed to this prevention method to overcome this issue. Most of such works have been focused on addressing the trace back issues based on the Internet protocol version 4 based network. In this paper, the research group analyze IPv6 hacking techniques and propose a combined solution from the existing solutions.

Index Terms- IPv6, Trace back issues, Wimax, Spoofed IP source, IPv4 network

I. Introduction

The number of connected devices is growing vastly where 6.4 Billion connected IoT (Internet of things) will be used in 2016 and it is predicted to go up to 21 Billion IoT devices by 2020. Since IPv4 has a theoretical maximum of about 4 billion addresses, IPv6 was introduced by The Internet Engineering Task Force (IETF) in 1998 to supplement (and eventually replace) IPv4 where IPv6 has an unthinkable theoretical maximum because it is 2128 of total addresses. Figure 01 illustrates the IPv6 packet header. This ultimate growth, the potential expansion of security threats has made a big impact on IPv4 addresses. Therefore, IPv6 addresses were designed with enhanced security. Figure 02 illustrates how a network structure goes as hierarchy way in the proposed research.

Security enhancement was another key component in IPv6 development. Security was not considered when IPv4 was developed. IP Security, a set of protocols were introduced later to provide data integrity, confidentiality and authentication. IPv6 should provide better security because IPsec is mandatory in IPv6.

IPv6 has node auto configuration for devices such as PC, laptop etc. through DHCPv6 which a node can configure its IP address based on the local information without connecting to a server.

IPv6 also provides better methods for generating routing tables and better mobility support [1].

Even if IPv6 was designed for better performance, it faces some security challenges same as IPv4. IPsec is mandatory in IPv6 but its use is not, that makes the network and devices vulnerable to almost all the existing IP related threats. Further, there’s uncertainty in some of the features of the IPv6 security suggestions because they are not yet completely understood by the networking administrators. It holds stakeholders back from making switch to IPv6. In addition to that the already existing threats such as application layer attacks, packet flooding can also affect IPv6 networks and devices [2].

IPv6 traffic is being tunneled over IPv4 connections and appears to be the regular IPv4 packets unless an organization has deployed a security mechanism that inspects tunneled traffic. Firewalls and network management tools which are used for IPv4 do not automatically block IPv6 traffic coming into networks. The typical IPv4 security devices are not tuned to look for IPv6 tunnels [3].

The development of a protocol to replace IPv4 started in 1990s. One major reason for that was the limited maximum number of IPv4 address space. A technology called NAT (Network Address Translation) was introduced to alter this space issue by providing internet access for a huge number of computers using small number of IP address. NAT was operated between the hosts and private network. Due to the increase of the Internet of Things (IoT) devices, NAT comes across vast management challenges to support communication [9].

Mobile Wimax is a broad band access technology which is growing rapidly that allows low-cost mobile Internet applications. Wimax is combined of OFDMA. Some of the main threats to Wimax security are man-in-the middle, privacy compromise, theft of service, Denial of service security attack (DOS)[6][7]. Due to the recent increase in e-crime, DoS/DDoS attacks, victims and security authorities need IP trace back mechanism that could trace back the attack to its source [11]. DDoS is a rapidly growing problem in IPV6. Grouping of DDoS attacks and defenses which gives problem and the current solution space [10].

Intrusion Detection Systems (IDSs) arranged in the virtual machines (VMs) of the cloud Systems with a data fusion methodology in front end and quantitative solution for alert generated by the IDSs. Detection uses the Dempsters combination rule to fuse from multiple evidence sources and solves the problem of analyzing the logs generated by sensors [4]. K-nearest neighbor (k-NN) and classifying the networks status, helps to utilized in the detection stage and to differentiate the network status into each phase [5].

The Router Advertisement (RA) Guard functionality examines the RAs and filters out RA packets sent by unapproved devices. The RA guard feature is deactivated by default. By allowing, the RA packets received on the interface are dropped and the port be able to shutdown based on the interface configuration. The port can be restarted after the constituted time by configuring the auto-recovery option. RA Guard could be compared to the best practice of blocking DHCP server-side traffic from clients [8].

The most popular method of hacking technique is Man in the Middle (MITM). The tool used can be downloaded from THC website. MITM take advantage of spoofed neighbor advertisement and use it to perform sniffing FTP traffic. It is required at least 3 computers in the same IPv6 network to do MITM and sniffing. 1st test is to send the ICMPv6 echo request from client FTP server then take a look at the neighbor cache entry if it testing no anomaly the next test is started by enabling IPv6 forwarding and utilizing parasite on the attacker computer. The goal is to perform man in the middle using spoofed neighbor advertisement, this test is continued by transferring ICMPv6 echo call to FTP server from client by looking at the neighbor cache entry. If there is anomaly on the client neighbor cache attached attacker mac-address. Figure 03, 04 illustrates the Man in the middle. Hence the traffic from client to FTP server through the attacker [12].

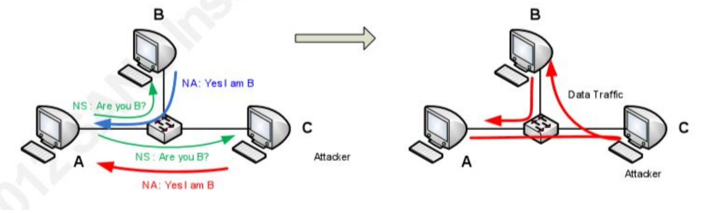


Figure 03: Man In The Middle
(Source: https://www.sans.org/reading-room/whitepapers/detection/complete guide-ipv6-attack-defense-33904)

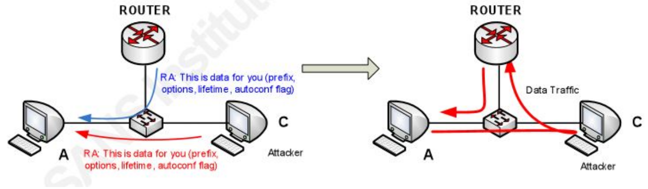

ROUTER
RA: This is data for you (prefix, options, lifetime, autoconf flag)
C
Attacker
A
RA: This is data for you (prefix, options, lifetime, autoconf flag)
ROUTER
Data Traffic
C
A
Attacker

Figure 04: Man In The Middle Data Traffic
(Source: https://www.sans.org/reading-room/whitepapers/detection/complete-guide-ipv6-attack-defense-33904*)*

Another hacking technique which exist in IPv6 is Smurf, a type of DoS attack which aims to flood the target with network traffic so that it cannot be accessed. This can be performed by spoofed ICMP echo request to the broadcast address. Source address of the request is the target of this technique. IPv6 does not have a broadcast address, but it has a multicast address to reach all PCs in the network Figure 05 illustrates the Smurf attack [12].

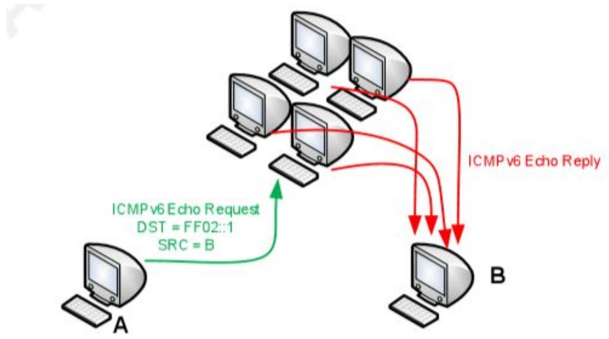


Figure 05: Smurf attack
(Source: https://www.sans.org/reading-room/whitepapers/detection/complete-guide-ipv6-attack-defense-33904*)*

The following sections of the document is as follows: section II describes about existing methods to prevent MITM and Smurf attacks; section III describes the solution, the research group proposed; conclusion, future work and acknowledgement.
Solutions

There are vast number of hacking techniques and protection methods in IPv6. Some of the hacking techniques and methods are already mentioned in this paper in the introduction. To limit the scope of this paper, the research group will propose a solution which can be applied to prevent both MITM and Smurf attacks.

Packet filtering as a solution for Smurf attack

Firewalls can be a software or hardware element that is designed to protect network from one another. They are mainly used for controlling the traffic and filtering it, entering and leaving. They are kept areas between low and high trust like private and public network or between to different networks belonging to the same organization.

Firewalls maintain the traffic using filters. These filters are mostly set of rules which are defined in the order of priority. If the packet match the criteria of the rule then actions of the rule are being applied and if they are not matched then next, no action is kept and next set of rules are practicality checked.
These packet firewalls filters are based on evidence placed in the packet header similar protocols, destination address, source address, port number used etc. These firewalls works at the network layer (layer 3) and transport layer (layer 4). These are commonly called as routers.

How packet filter works

Packet filters work with individual packets, therefore every packet should be decided whether can pass or should undergo some other action. The basic steps of packet filtering are the following:

1. The filter system inspects the packet. It regularly checks the following information in the packet header:
    - Source/destination IP addresses.
    - IP options.
    - TOS/TTL fields.
    - Source/destination port numbers.

- TCP flags.
- Data part of packet.

State full packet filters can check the state of the given packet related to the known connections (whether this packet goes to an already seen connection or it is a different packet or it is a packet connected to an already established connection, like an ICMP control packet), or to other state full information (whether this packet fits in the TCP window of the link). This information provide the base for the decision. Of course, the firewall can test whether the packets checksum and packets in general are adequate.

2. After inspecting the packet and collecting state full information, the packet filter assesses the policy for the given packet. The policy and the demonstration of the policy might be different between various implementations, but usually Access Control Lists (ACL) are used. ACL are checked from the top of the list to the bottom. The list entries are usually called rules and these rules are calculated after one another.

A rule usually contains a match and a decision part. The match part is evaluated based on the information gathered from the packet before the rule check. If a packet matches the rule the rule's decision is taken for that packet. The several implementations change in how they run over the list. One stops evaluating at the first matching, while others might take the last match's decision.

3. After evaluating the ACL the packet filter can work with that packet as reported by to the decision. Usually, every ACL has a default decision which has authority to see what should happen with the packet if no match happens. Based on the main security rule a default reject or default drop approach is a good choice, but as natural it depends on the implementation and on the administrator.

There are many decisions, but usually all implementations support the following basic judgments. The meaning of the decisions though strength differ to some extent.

- Accept

Agreeing the packet to pass.

- Deny/Drop

Denying the packet soundlessly meaning
That no error packet is sent back to the sender.

- Reject

Denying the packet with sending back some caring of error packet (ICMP error message or TCP rearrange packet depending on the situation).

VPN as a solution for MITM

Virtual Private Network (VPN) is a commonly used for secure connections. A VPN extends a private network across internet and allow users to strongly access a private network and share data remotely through public networks. Functionality of VPN is almost same as a firewall that defends data on computer, VPN protect it online. And while a VPN is technically a WAN (Wide Area Network) the front end holds the same functionality, security, and appearance as it would on the private network.

VPN use a combination of dedicated connections and encryption protocols to generate virtual peer to peer (P2P) connections. Attackers might manage to get access to transmitted data, but transmitted data will not be able to be read due to the encryption.

1. The user first connects to the public internet through an Internet Service Provider.
2. Then initiates a VPN linking with the company VPN server using client software.
3. The client software on the server starts the secure connection, contributions the remote user access to the internal network.

Many security protocols for VPN are available. The most common are,

1. IP security (IPSec)
2. Layer 2 Tunneling Protocol (L2TP)/IPsec
3. Secure Sockets Layer (SSL) and Transport Layer Security (TLS)
4. Point-to-Point Tunneling Protocol (PPTP)
5. Secure Shell (SSH)

VPNs are the best solution of securing traffic to protect personal data from an attacker.

II. PROPOSED SOLUTION COMBINING EXISTING SOLUTIONS

To protect personal data and computer networks in IPv6 from the mentioned attack techniques MITM and Smurf, VPN and Packet Filtering are already used separately. Theoretically VPN and Packet Filtering can be implemented together to provide enhanced security, privacy and will be low in cost and have better impact on network performance.

III. CONCLUSION

In this paper briefly defined about hacking techniques such as Man in the Middle, Smurf attacks their functionalities and how to protect each are in individual way. Then this paper gives the solution for this attacks used firewall in middle and used VPN for monitoring the online processing. Used these things together in the internal firewall it is protect network very efficiency.

IV. FUTURE WORK

In future this firewall add trackback mechanism in it purposes, it would be additional secured, because trace back mechanism will be check out the packets and packet filtering mechanism will be filtering the packets carefully so if intruders get into a packet the both mechanism will block the intruder and protects the network. By adapting to high performance packet filtering firewalls the protections gets to the next level. If the packet filtering mechanism try to read tunneling traffic we can reduce hackers getting into the network in future VPN will get more techniques so this firewall become very helpful for protect the IPV6 environment.

Acknowledgement

The authors are very much grateful to Sri Lanka Institute of Information Technology for doing research work in Computer Networking. Authors are also grateful to Mr.Dhishan Dhammearatchi for this content support and inspiration for conducting research work in Computer Network Design and Implementation.

References

[1] G. Velde, "Local Network Protection for IPv6", 2007. [Online]. Available: https://tools.ietf.org/html/rfc4864. [Accessed: 14- Feb- 2016].

[2] S. Convry and D. Miller, "IPv6 and IPv4 Threat Comparison and Best Practice Evaluation (v1.0)". [Online]. Available: http://www.seanconvery.com/v6-v4-threats.pdf. [Accessed: 14- Feb- 2016].

[3] C. Huitema, "RFC 4380 - Teredo: Tunneling IPv6 over UDP through Network Address Translations (NATs)", Tools.ietf.org, 2016. [Online]. Available: https://tools.ietf.org/html/rfc4380. [Accessed: 26- Feb- 2016]..

[4] A. Lonea, D. Popescu and H. Tianfield, "Detecting DDoS Attacks in Cloud Computing Environment", 2016. [Online]. Available: http://trap.ncirl.ie/1543/1/Detecting_DDoS_attacks_in_cloud_computing_environment.pdf. [Accessed: 27- Feb- 2016].

[5] H. Nguyen and Y. Choi, "Proactive Detection of DDoS Attacks Utilizing k-NN Classifier in an Anti-DDos Framework", Waset.org, 2010. [Online]. Available: http://www.waset.org/publications/9510. [Accessed: 14- Feb- 2016].

[6] H. Zhou, H. Zhang and Y. Qin, "An authentication method for proxy mobile IPv6 and performance analysis", Security and Communication Networks, vol. 2, no. 5, pp. 445-454, 2009.

[7] K. Etemad, "Overview of mobile WiMAX technology and evolution", IEEE Commun. Mag., vol. 46, no. 10, pp. 31-40, 2008. [Online]. Available ftp://doc.nit.ac.ir/cee/m.zahabi/Articles/miscellaneous/4644117.pdf [Accessed: 07- Mar- 2016]

[8] F. Gont, "RFC 7113 - Implementation Advice for IPv6 Router Advertisement Guard (RA-Guard)", Tools.ietf.org, 2016. [Online]. Available: https://tools.ietf.org/html/rfc7113. [Accessed: 25- Feb- 2016].

[9] M. Gallagher and W. Jeffrey, "Technical and Economic Assessment of Internet Protocol version 6 (IPv6)", 2006. [Online]. Available: https://www.ntia.doc.gov/files/ntia/publications/ipv6final.pdf. [Accessed: 14- Feb- 2016].

[10] J. Mirkovic and P. Reiher, "A taxonomy of DDoS attack and DDoS defense mechanisms", ACM SIGCOMM Computer Communication Review, vol.34, [Online]. Available: https://www.eecis.udel.edu/~sunshine/publications/ccr.pdf [Accessed: 18- Feb- 2016]. no. 2, p. 39, 2004.

[11] R. KumarSingh, S. Pundir and E. S. Pilli, "IPv6 Packet Traceback: A Survey", International Journal of Computer Applications, vol. 74, [Online]. Available: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.403.1625&rep=rep1&type=pdf [Accessed: 18- Feb- 2016].no. 16, pp. 31-35, 2013

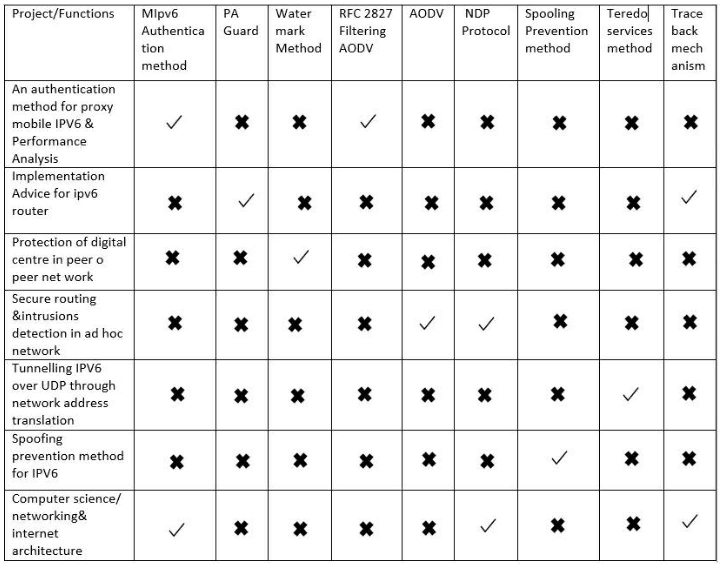
[12] A. Pilihanto, "A Complete Guide on IPv6 Attack and Defense", Sans.org, 2011. [Online]. Available: https://www.sans.org/reading-room/whitepapers/detection/complete-guide-ipv6-attack-defense-33904. [Accessed: 01- Mar- 2016].

Authors

First Author – A.M Aslam Sujah, Sri Lankan Institute of Information Technology Computing Pvt. Ltd.
Second Author – H.M Shadir, Sri Lankan Institute of Information Technology Computing Pvt. Ltd.
Third Author – M.S.M Shakir, Sri Lankan Institute of Information Technology Computing Pvt. Ltd.
Fourth Author – K. Jasandan, Sri Lankan Institute of Information Technology Computing Pvt. Ltd.
Fifth Author – S. Kavitha, Sri Lankan Institute of Information Technology Computing Pvt. Ltd.
Sixth Author – Dhishan Dhammearatchi, Sri Lankan Institute of Information Technology Computing Pvt. Ltd.

Appendix

Table: 01



Project/Functions	MIpv6 Authentication method	PA Guard	Water mark Method	RFC 2827 Filtering AODV	AODV	NDP Protocol	Spooling Prevention method	Teredo services method	Trace back mechanism
An authentication method for proxy mobile IPV6 & Performance Analysis	✓	✖	✖	✓	✖	✖	✖	✖	✖
Implementation Advice for ipv6 router	✖	✓	✖	✖	✖	✖	✖	✖	✓
Protection of digital centre in peer o peer net work	✖	✖	✓	✖	✖	✖	✖	✖	✖
Secure routing &intrusions detection in ad hoc network	✖	✖	✖	✖	✓	✓	✖	✖	✖
Tunnelling IPV6 over UDP through network address translation	✖	✖	✖	✖	✖	✖	✖	✓	✖
Spoofing prevention method for IPV6	✖	✖	✖	✖	✖	✖	✓	✖	✖
Computer science/ networking& internet architecture	✓	✖	✖	✖	✖	✓	✖	✖	✓

Existing Functionalities

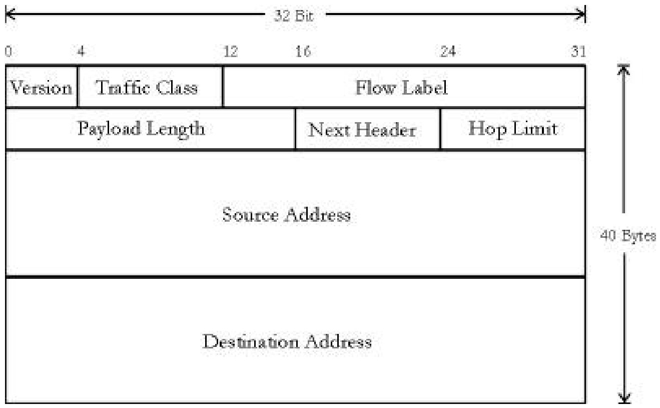


Figure 01: IPv6 packet header.

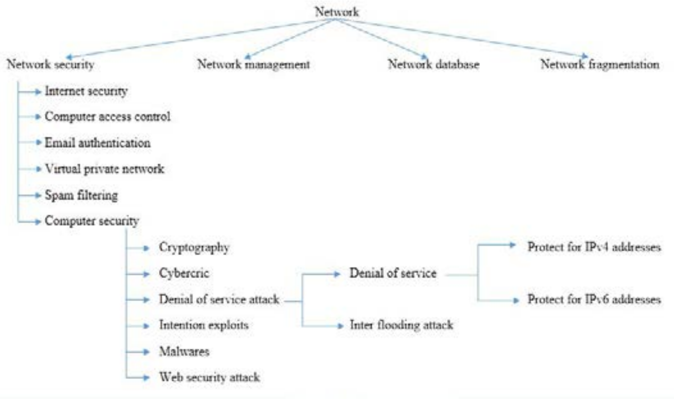


Figure 02: Network Structure.