Volume 7, Issue 5, May 2017 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Review of Security Issues in IPv6 based Networks

Komal
Department of CSE, Amity University, Haryana,
India

DOI: 10.23956/ijarcsse/SV7I5/0139

Abstract— The pace of growing Internet population has resulted in the exponential demand rate of IP addresses. IPv6 came as a solution to the depleting address space and various other problems of IPv4. However, the co-existence of these protocols has created some unpredictable challenges, security being the foremost. IETF developed some transition ways to supply seamless communication in such a varied atmosphere. Since IPv6 is not globally adopted, its co-existence with the IPv4 protocol will be best exploited by the black-hat community. This paper addresses the vulnerabilities of IPv6 based networks in the current Internet scenario and recommends various methods, techniques and security policies to prevent these security threats.

Keywords— IPv4, IPv6, Protocol, IETF, Internet, Security threats.

I. INTRODUCTION

Besides servicing the internet community for years, IPv4 encountered a number of pitfalls. To overcome those difficulties, a new internet protocol (called IPv6) was proposed by the Network Working Group of IETF (Internet Engineering Task Force). From the viewpoint of security, IPv4 and IPv6 differ in the context that the use of IPSec is mandatory in IPv6 and optional in IPv4. IPSec ensures the authentication, privacy and integrity of data. This feature solves out the security issues related to IPv4. However, the features of IPv6 brought newer security challenges [1]. Today, both IPv4 and IPv6 based networks exist together, which makes the security enforcement even more difficult. IETF has suggested a tunneling mechanism [2] for such communication which has its own shortcomings.

This paper is structured as follows. Section 2 highlights the need of having IPv6 enabled network devices and configuration, as a communication way in integrated IPv4-IPv6 environment, specifically in the scenario of Big Data environment [3]. Section 3 puts a light on the weaknesses of current security framework together with the features of IPv6. Section 4 discusses the various attacks and intrusions on IPv6 based networks. Section 5 proposes some mitigation measures to combat the attacks stated in the previous section. Finally, we conclude in section 6.

II. NEED OF IPV6 CONFIGURATION

Internet Protocol version (IPv6) expanded the address-space of network addresses from thirty two bits (in IPv4) to 128 bits, that provides over enough globally distinctive IP addresses for each networked device on the earth. The unlimited address area provided by IPv6 permits networks to deliver additional and newer applications and services with reliability, improved user expertise and increased security. IPv6 is designed intentionally to have minimal impact on upper- and lower-layer protocols. Following features highlights the need of IPv6 over IPv4 [4]:

- *Larger address space*- The most important feature of IPv6 is a much larger address space than in IPv4. The length of an IPv6 address is 128 bits, compared to 32 bits in IPv4. The longer addresses simplify allocation of addresses; enable efficient route aggregation and implementation of special addressing features.
- *New Header Format*- IPv6 provides a new header format that is designed to minimize the header overhead. This optimization is achieved by moving both non-essential fields and optional fields to extension headers that appear after the IPv6 header. Intermediate routes can process the restructured IPv6 header more efficiently. However, IPv6 is not backward compatible with IPv4 and their headers do not interoperate. A host or router must use an implementation of both IPv4 and IPv6 to recognize and process both header formats.
- *Efficient and Hierarchical Addressing and Routing Infrastructure*- IPv6 global addresses that are used on the IPv6 portion of the Internet are designed to create an efficient, hierarchical and summarizable routing infrastructure that is based on the common occurrence of multiple levels of Internet service providers.
- *Stateless and Stateful Address Configuration*-To simplify host configuration, IPv6 supports both stateful address configuration (as in the presence of a DHCP server) and stateless address configuration (as in the absence of a DHCP server). With stateless address configuration, hosts on a link automatically configure themselves with IPv6 addresses for the link (called link-local addresses) and with addresses that they derive from prefixes that local routers advertise. Even in the absence of a router, hosts on the same link can configure themselves with link-local addresses and communicate without manual configuration.
- *Better Support for QoS*- New fields in the IPv6 header define how traffic is handled and identified. In IPv6, a mechanism called flow label has been added to enable special handling of the packet. This mechanism can be used to support traffic such as real- time audio and video.

- *Neighboring Discovery Protocol* - The Neighbor Discovery protocol for IPv6 manages the interaction of nodes on the same link, known as neighboring nodes. Neighbor Discovery replaces the broadcast-based Address Resolution Protocol, ICMPv4 Router Discovery, and ICMPv4 Redirect messages with efficient multicast and unicast Neighbor Discovery messages.
- *Support for Extensibility* -IPv6 can easily be extended by adding extension headers after the IPv6 header. Unlike options in the IPv4 header, which can support only 40 bytes of options, the size of IPv6 extension headers is constrained only by the size of the IPv6 packet. The extension header mechanism provides extensibility to support future services for quality of service, security, mobility, and others, without redesign of the basic protocol.
- *Better Mobility support*-Unlike MIPv4, MIPv6 avoids triangular routing and is therefore as efficient as native IPv6. MIPv6 came with a route optimization feature (to find shortest path between mobile node and correspondent node), which solves out triangle routing problem.IPv6 routers may also support network mobility which allows entire subnets to move to a new router connection point without renumbering.
- *Mandatory support for network layer security*-IPsec is an integral part of the base protocol suite in IPv6. IPsec support is mandatory in IPv6, which enforces security at network layer. However, implementation of IPsec is optional in IPv4.

III. SECURITY LOOPHOLES OF IPV6 BASED NETWORK CONFIGURATIONS

Every intrusion or attack is derived from some loopholes in the security architecture and the technology implementation. Before heading towards the security threats, let's have a look on the factors that makes IPv6 networks more attack-prone [6] [7]:

A. Auto-configured malicious nodes

Stateless auto-configuration feature of IPv6 can be used by attackers to configure malicious nodes and use them as attacking source.

B. Incompetent and compromised Infrastructure

IPv4 based network devices can't handle IPv6 traffic. They pass on the encapsulated packets by simply checking the IPv4 header. IPSec support is also not provided to IPv4 routers. Hence, they cannot deeply inspect the encapsulated IPv6 packet.

C. Automatic and dynamic tunnel configurations

Automatically and dynamically configured host-to-host tunnels are most vulnerable to be used as an attacking tool by adversaries. Dual stack attacking nodes can create malicious tunnels safely with any dual stack victim node. Victim has no prior knowledge and no intervening safeguards or checking is performed.

D. Misconfigured or partially configured nodes

Partially configured or misconfigured hosts, routers, relays and other networking infrastructure can't enforce proper security measures and are more susceptible to any kind of attack.

E. Lacking firewall Rule-set

IPv6 supported firewalls have different rule-sets [6] for IPv4 and IPv6 traffic. For an IPv4 firewall rule-set, 6-to-4 tunnels are nothing but IP protocol 41 on IPv4 and teredo tunnels appear as UDP protocol on IPv4. Moreover, IPv6 firewall rule-set do not identify these tunnels. This seems to be a big security hole.

F. Lack of information about legitimate relays

6-to-4 routers in dual stack environment are not enriched with the knowledge regarding legitimate 6-to-4 relays and 6-to-4 routers. Therefore, they can't differentiate the traffic from illegitimate and legitimate relays.

G. Perimeter security enforcement

Existing security architecture [8] is network-centric. All the security checks being applied on network boundaries (firewall, gateways etc.) make nodes susceptible to insider attacks. Host-to-host tunneling is an additional help for such attacks.

IV. SECURITY ATTACKS IN IPV6 NETWORKS

Tunneling mechanism provides safe pavements for malware down the tunnel. Attackers can never let go such an opportunity. Security threats that deliberately take the advantage of tunneling mechanism and existing security architecture are [7]:

A. Spoofing Attack

Attacker encapsulates a spoofed IPv6 packet using IPv6-over-IPv4 tunnels. Router at the other end of the tunnel simply decapsulates the packet and hand it over to destination node. Spoofing attack has following consequences:

(a) Difficult to trace the source of attack if some malicious code discovered.

(b) Spoofed address might not exist, thus wasting network resources while attempting to reply for spoofed packet.
(c) Attacker might have used address of some victim node to further exercise flooding attack.

B. Denial-of-Service Attack

Denial-of-service attacks are performed in order to prevent legitimate hosts from accessing a service or network resource. Sending infinite tunnel requests to a 6-to-4 router to keep it engage in encapsulating forged packets, hence preventing the processing of legal requests, called Denial-of-Service.

C. Distributed Reflection Denial-of-Service Attack

This is more severe Denial-of-Service attack that uses a victim node as a reflector to attack other victim nodes in the network. A number of malicious nodes perform it together by sending spoofed traffic to victim using same source address.

D. Service Theft

It might be possible that a 6-to-4 relay restrict its service to some specific IPv6 networks. However, some users may breach all control policies and gain access to its service. It can be done in two ways:

(a) Using 6-to-4 routers' headers to reach 6-to-4 relays.
(b) By configuring relay with its IPv4 address instead of 192.88.99.1

E. Neighbour Discovery message Attack

Any malicious node in IPv4 network can attack 6-to-4 routers with a neighbor discovery or router solicitation message, using a link local address (since 6-to-4 routers' security checks apply only to 6-to-4 addresses).

F. Unauthorized access

A network may comprise of some private site (using NAT) to which outside nodes are not allowed to communicate. But teredo tunnels have possibility for NAT traversal allowing unauthorized users to communicate with NAT hosts.

G. Flooding Attack

Flooding attack basically used to exhaust the storage capacity and processing power of a system by overwhelming it with requests. Tunneling can be used to target any dual stack host or router as victim of this attack.

H. Viruses and Trojans

Tunneling mechanism allows encapsulated IPv6 packets to travel to the destination without any scanning or checking being performed. Such a scenario makes it easy for attackers to perform the malicious code (worms, viruses, Trojans) execution on victim node if it doesn't have the capability (antivirus software) to detect that activity.

I. Routing Loop Attack

This attack [9] exploits the assumption that destination address of IPv6 packet is valid and reachable via tunnel. The attacker creates an IPv6 packet with a destination address that doesn't exist. Such a packet is handed over to a border router that sends the packet into a tunnel over IPv4 network, which ultimately reaches another edge router. This router takes the packet out of the tunnel and forwards it to native IPv6 network, from where it is looped back into tunnel and so on. The loop terminates only when hop limit of packet reaches zero. This attack targets the edge routers.

V. SECURITY POLICIES & MEASURES FOR PREVENTING ATTACKS

In order to have a safe and smooth transition to IPv6, organizations need to carefully plan. Since tunneling doesn't require much infrastructure changes, it can be an obvious choice. However, it puts the security of the network on stake. Following mitigation measures help overcome the risk of potential security threats:

A. Using Dual Stack as preferred transition mechanism

Dual Stack mechanism [1] [2] requires hosts, routers and other networking devices to have dual functionality supporting both IPv4 and IPv6 protocols. Dual Stack architecture enables the communication to all other nodes using either of the internet protocols. No spoofing or other tunneling attacks possible.

B. Deploying manually configured and semi-automatic tunnels

Automatically configured tunnels enable attackers to create malicious links with the victim nodes, without their confirmation .Therefore, network administrators should configure tunnels manually by adding tunnel end points and routes info to avoid establishing tunnels with malicious nodes. Another option can be semi-automatic tunnels (e.g. Tunnel Broker).

C. Deeper inspection of tunneled packets at edge routers

Malicious dual stack nodes in IPv4 network can establish host-to-router tunnel to attack some node in IPv6 network. Edge routers simply decapsulates the tunnel traffic and delivers it to intended recipient. Thus, edge routers

should be equipped with additional functionality of checking the encapsulated packets before forwarding it to native network.

D. Handshake mechanism before tunnel establishment

There must be some agreement process prior to tunnel establishment. This will help the nodes to allow or deny the tunnels from other nodes. This will act as a constraint for automatic and dynamic tunnel configurations.

E. Enforcing policies to terminate tunnels outside the firewalls

Since tunnels can break through firewalls, they must be terminated outside the firewall [6]. Hence, proper security checks can be performed on the traffic before letting it into the native network.

F. Advancing Firewall Rule-set and Testing techniques

Firewall rule-sets need to be advanced so that the tunnels can be identified and filtered selectively preventing those carrying malware. Testing of network resources, bandwidth and security specification from users' perspective [5].

G. Imparting knowledge about legitimate relays

There must be some secure way to inform perimeter devices (routers, gateways etc.) about legitimate relays and routers. Edge routers should have rich information-base with blacklist feature to ban the illegitimate relays.

H. Using anycast address for relays

Prevent the use of actual IPv4 addresses of relays [7] and use anycast address 192.88.99.1 instead. This will help prevent two attacks:

(a) Service Theft: Relays can filter out tunneled packets with destination address other than 192.88.99.1
(b) Relay Abuse: Routers can block traffic from relays using other IPv4 addresses.

I. Verifying source and destination existence

Routing loop attack uses a destination address that does not exist. Similarly, spoof attack can use a source address that does not exist. Hence, a router must verify the existence of source and destination nodes [9] before forwarding it further on the tunnel. One way to verify is to check neighbor cache to see if a valid entry exists for that address.

J. Avoiding operation of multiple tunnels

Routing loop attack requires two routers making end points of two different tunnels. There can be a no. of edge routers in a network acting as end-point of various tunnels. The attack can be surely prevented if only one tunnel [9] is allowed to operate in the network.

K. Having single edge router

Allowing only one edge router forces all the traffic (going in and out of the network) to pass through it. Such scenario narrows the attacking area and helps enhance security capability on border. Routing loop attack is not possible with single border router [9].

L. Host-centric security architecture

There is a need to develop host-centric security architecture that will perform intrusion detection and security checks at multiple points in the distributed environment. Such architecture will provide fine-grained security levels. This will prove more efficient for mobile nodes.

VI. CONCLUSIONS

An organization should carefully plan before adopting and implementing a new technology or protocol in existing network infrastructure. Tunneling mechanism can be an easy choice since it doesn't require much infrastructure changes. However, tunneling can be exploited in many ways to execute attacks. This paper suggests some mitigation measures to prevent attacks on IPv6 networks and Dual-Stack networks. The stated measures and techniques can help subvert the ill intentions of the black-hat community.

REFERENCES

[1] S. Convery and D. Miller, *IPv6 and IPv4 Threat Comparison and Best-Practice Evaluation (v 1.0),* Cisco Systems Technical Report, 2014.
[2] Microsoft Corporation, *IPv6 Transition Technologies*, Windows Server 2008 White paper, February 2008.
[3] Preetishree, P. B. Nagpal and S. Chaudhary, *Emerging Clustering Techniques on Big Data*, GE-International Journal of Engineering and Research, vol.3, Issue 6, 2015.
[4] W. Stalllings, *IPv6: The New Internet Protocol,* IEEE Communications Magazine, pp. 96-108, 1996.
[5] S. Kaushal, and J. K. Bajwa, *Analytical Review of User Perceived Testing Techniques*, International Journal of Advanced Research in Computer Science and Software Engineering, vol. 2, issue 10, pp. 213-216, 2012.

[6] M.H.Warfield, X-force, Internet Security Systems, *Security Implications of IPv6*, http://documents.iss.net/whitepapers/IPv6.pdf
[7] P. Savola and C. Patel, *Security Considerations for 6to4*, RFC 3964, December 2004.
[8] R. Atkinson and S. Kent, *Security Architecture for Internet Protocol*, RFC 2401, November 1998.
[9] G. Nakibly and F. Templin, *Routing Loop Attack using IPv6 Automatic Tunnels: Problem Statement and Proposed Mitigations*, Internet-Draft, February 2011.

