International Journal of Soft Computing 9 (2): 79-84, 2014
ISSN: 1816-9503

Security Attacks on IPv4-IPv6 Transitions-Possible Mitagation Techniques

[1]P. Shanmugaraja, [1]D. Balamurgan and [2]S. Chandrasekar
[1]Anna University, 600 025 Chennai, Tamil Nadu, India
[2]Gnanamani College of Technology, Namakkal, Tamil Nadu, India

Abstract: Internet protocol is the widely deployed protocol used for communication. The internet engineering task force is the organization responsible for defining the internet protocol standards. When the IETF developed IPv4, the wide growth of the internet and the security issues were not expected. Due to internet's rapid growth IPv6 was designed. IPv6 is designed to achieve simplicity, increased routing speed, improved QOS and inbuilt security. Due to the massive growth in internet users and technology deployment of IPv6 is mandatory. Because the successor of IPv4 is not compatible, transition technologies play a key role in establishing the communication between IPv4 and IPv6. Currently, both protocol suites are needed for communication so the involvement of transition technology is also mandatory. IETF Next Generation Transition working group (NGTrans) has developed many transition technologies to enable the integration of IPv6 facilities into current infrastructure that uses IPv4. This study discusses Internet Protocol ver4 security issues, internet protocol ver6 issues and compares both the internet communication protocols. Because the transition phase involves both internet protocols, the transition phase is vulnerable to major security issues. This study synthesizes different security threats that are involved in the transition phase. Some of the Mitigation techniques for the threats are also synthesized.

Key words: Dos, IPv6, IPv4, IPSec, tunneling, transition mechanisms

INTRODUCTION

The Internet Protocol Version 4 (IPv4) is approximately 30 years old and it is a foundation of internet. It has been the backbone of the internet's rapid growth. The size of the IPv4 address is 32 bits which can address only 4 billion unique machines. The enormous growth of internet users over the last two decades made the exhaustion of IPv4 address space. The rapid explosion of technology in almost all communication devices demands a new supply of IP address space. IPv4 protocol has no in built security. Keeping these factors in mind the network working group of the internet engineering task force proposed a new suite of protocols called the Internet Protocol Version IPv6. IPv6 also called as IP next generation IPv6 has a vast address space and it can generate 2^{128} addresses. It also eliminates the use of network address translation that IPv4 uses to ease IPv4 address exhaustion. The major drawback of IPv6 is it is not backward compatible with IPv4, i.e., an IPv6 node cannot communicate directly with another IPv4 only node and vice versa due to the following constraints: size of a IPv4 address and IPv6 addresses are different and ize of an IPv4 header is 20 bytes and an IPv6 header size is 40 bytes double that of IPv4.

Because of these constraints, conversion from IPv4 to IPv6 protocol requires changing the existing network infrastructure completely. Therefore, IPv4 network cannot be migrated to IPv6 overnight. The hardware and software used to route packets across networks and that performs security analysis will not work with IPv6 protocol unless they are upgraded to versions that support IPv6 protocol. It will take years to change completely from IPv4 network to IPv6 network. Until then both IPv4 and IPv6 should be interoperated together.

In this study, reseachers focus on existing transition technologies, discussed various security issues related to transition techniques, analyzed the current mitigation techniques for the security issues related to transition techniques, deals with IPSec and its support for mitigating transition related security issues and the limitations of existing accessible methods for mitigating security attacks.

TECHNIQUES FOR TRANSITION

Interoperability between IPv4 and IPv6 is accomplished by integrating both the protocols using various transition techniques. The existing transition techniques (Waddington and Chang, 2002) are as:

Corresponding Author: P. Shanmugaraja, Anna University, 600 025 Chennai, Tamil Nadu, India

- Dual stack systems
- Protocol translation
- Tunneling

IPV6/IPV4 DUAL STACK SYSTEMS

It provides support for both the network layer protocols IPv4 and IPv6. Both protocols suites work independently in this system. All the hardware and software components of this network system should support both IPv4 and IPv6 protocols. It requires current infrastructure to be compatible with IPv6 however, if the current network is not ready then it must be upgrade. It is important to understand that having a device being able to communicate over both IPv4 or IPv6 does not necessarily means that all applications operating within this device are capable of utilizing both IPv4 and Ipv6.

PROTOCOL TRANSLATION

Translator is a device capable of translating traffic from IPv4 to IPv6 or vice and versa. This mechanism intends to eliminate the need for dual-stack network operation by translating traffic from IPv4 only devices to operate within an IPv6 infrastructure. It performs header and address translation between the two protocols. The advantage of this technique is IPv4 users can use this translation technology with no or little change in the existing infrastructure to connect with IPv6 network and vice versa. Some of the feature of IPv6 are lost when translation techniques and it does not solve the problem of IPv4 address space depletion. It works at different layers as:

- Network layer translations
- Transport layer translations
- Application layer translations

The selection of the transition methods is site specific. There is no single best solution. Generally ISP's use Tunnel Broker, 6 to 4 relay and manual tunnels. The best practice is to deploy Dual Stack Systems.

TUNNELS

The term "tunneling" refers to a means of encapsulating one version of IP in another so that the packets travel over a backbone network that does not support the encapsulated IP version. The tunneling protocol carries the tunneled protocol. Tunneling can be either IPv6 over IPv4 or Ipv4 over IPv6 networks. Using this technique an IPv4 user can communicate with IPv6 network using the existing IPv4 network. Tunnels are either configured tunnels or automatic tunnels. Configured tunnels require manual administration. Figure 1 shows IPv6 over IPv4 tunneling. Automatic tunneling is of different types as:

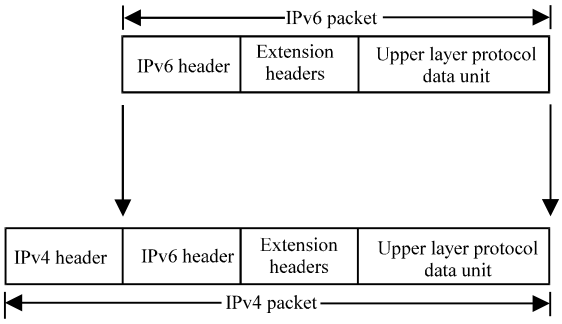

Fig. 1: IPv6 over IPv4 tunneling

- 6 over 4
- 6-4
- ISAT
- Teredo
- DST
- Tunnel Brokers

SECURITY THREATS

Security is a major concern in any network that uses IPv6 or IPv4. All the above existing transition techniques are vulnerable to attacks and poses major security threats. Since, both IPv6 and IPv4 operate parallel in the transition, it leads to major security threats. The transition threats can be divided in terms of issues due to IPv4 protocol itself, issues due to IPv6 itself and issues due to transition techniques (Zagar *et al*., 2007).

SECURITY THREATS IN IPV4 NETWORKS

When IPv4 was developed, security was not a major concern. Therefore, IPv4 has no built in security. IPv4 expects that end nodes should provide the needed security (Bradner, 2006). Internet is completely transparent and no security framework is available for most of the threats.

Denial of Service attacks (DOS): This attack floods the target host with the intention to revent the valid traffic from reaching the host. Because of DOS attacks, the intended users cannot communicate in the network. Example of DOS attacks is broadcast flooding attack or smurf attack (Baker and Savola, 2004). Because of many

types of extension headers in IPv6, various ICMPv6 messages and multicast dependency in IPv6 opens door for many flooding attacks.

Worms's distribution: Malicious codes or programs can propagate from one network to another network and can infect all the hosts in the network. IPv4 network space is small when compared to IPv6 that makes this distribution easier (Baker and Savola, 2004).

Packet fragmentation attacks: This attack sends many fragmented ICMP packets to the destination which when reassembled at the destination can make the destination host to crash or reboot because it exceeds the maximum allowable size for an IP datagram (Baker and Savola, 2004).

Man in the middle attacks: Ipv4 protocol has no built in authentication mechanisms. An attacker can read, insert and modify all the messages that are transferred between two hosts sitting in the middle of the transmission.

Address resolution protocol poison: Address Resolution Protocol (ARP) poison attack makes forged ARP responses broadcasted with incorrect mapping information that could drive the packets to attacker's destination or wrong destination (Caicedo *et al*., 2009).

Port scanning and reconnaissance attacks: This attack scans for multiple listening ports on a single, multiple or an entire network hosts (Caicedo *et al*., 2009).

IPV6 SECURITY THREATS

The protocol specification is different from IPv4 which results in new security problems unknown in IPv4 networks. Although, IPv6 has built in security, it poses several significant security challenges. IPSec is mandatory in IPv6 but its use is not. Managing and deploying IPSec is difficult which reduces the IPSec usage. The following list contains some of the areas of IPv6 where security is an important issue.

Reconnaissance attacks: It is the unauthorized discovery and mapping of systems, services or vulnerabilities. Huge size of IPv6 makes reconnaissance attacks more difficult but there are other ways to identify target hosts. If Administrator uses sequential numbering scheme to assign addresses then scanning becomes easy (Convery and Miller, 2004).

With the help of this attack intruder can gather information about the victim network that can be used to attack the victim network in future. Reconnaissance attacks are common in both IPv4 and IPv6 networks. However, due to huge subnet size of IPv6 it becomes impossible.

Attacks using routing headers: All IPv6 nodes are capable of processing headers. Routing headers are allowed in IPv6 packet structure which can list the addresses of one or more intermediate nodes that the packets will pass through. If an end node accepts these headers and follows their routing suggestion, trusted nodes could forward malicious packets or the flow of packets could lead to resource exhaustion at the routers resulting in denial of service attack.

Auto configuration and associated attacks: Using the auto configuration feature of IPv6, a node can automatically generate an address for each of its network interfaces. An IPv6 node can configure its address through either stateless or stateful configuration. This eliminates the need for DHCP server. It uses ICMPv6 message for auto configuration. This leads to attacks such as flooding and DoS (Nikander *et al*., 2004) because any malicious node that generates ICMPv6 packets can easily fool other nodes on a network segment to follow the packet's instruction resulting in a subversion attack. The performance of the victim node decreases if the attacker generates a flood of ICMPv6 messages.

Multicast based attacks: IPv6 has standard multicast addresses for routers and DHCP server groups. A malicious user can modify messages directed to these addresses on a network and receive information that helps identify systems on which to target attacks (Caicedo *et al*., 2009). ICMPv6 allows an error notification response to be sent to multicast address. Attackers can use this information to attack the victim network.

Bogus router implantation attack: Routers in IPv6 can use the ND protocol to discover each other's presence and determine their data link layer addresses and subnet information. This also lets a malicious node impersonate a network segment's default gateway (Convery and Miller, 2004). A malicious node can propagate bogus address prefix information to reroute legitimate traffic to prevent the victim from accessing the desired network resources.

THREATS WITH IPV4 AND IPV6 SIMILARITIES

Some types of attacks in IPv4 networks does not change their nature even with IPv6. They cause the same effect on both the protocols. The below said attacks come under this category.

Sniffing: This attack involves capturing data while transmitting data across a network. An example of this is tcpdump. An intruder using this attack can determine the sensitive information carried in a plain text protocol.

Rogue devices: Unauthorized devices in the network are rogue devices. It can be a wireless access point, domain name server, switch or a router.

Application layer attacks: Most of the attack in the internet is based on layer 7 of the OSI model. This attack includes buffer overflows, web application attacks, viruses and worms. Both the version of network layer protocols are neutral to application layer attacks.

Man in the middle attacks: Both IPv4 and IPv6 headers do not have in built security mechanisms. Both protocols rely on IPSec that is the key technology for security. However, IPSec strength relies on Internet Key Exchange (IKE). While exchanging the public key it may fall prey to man in the middle attacks.

Flooding: This attack floods a network device or host with more traffic to make the host or device to crash or to take a resource out of service. Flooding in IPv4 easy when compared with IPv6 due to the size of the network. However, the core principle does not change in IPv6.

THREATS DUE TO TRANSITION MECHANISMS

The transition from IPv4-IPv6 will take some time and will not happen immediately. Till then both protocols should interoperate to move the network traffic. The transition mechanisms open the path for many unknown security threats. This study examines the attacks possible with different mechanisms.

Tunneling can be used to evade security measures: The tunneling protocol allows the encapsulation of IPv6 data inside an IPv4 packet for passing the traffic through dissenting devices. It is vulnerable to Denial of Service (DoS) attacks, Reflection Denial of Service (DoS) and service theft in which a malicious node or site or malicious user may make unauthorized use of the service. These attacks are possible because of no preconfigured association between tunneling end points. Tunnel sniffing and eavesdropping on traffic going through tunnel is also possible. If automatic tunneling (6-4, Teredo and ISATAP) is used all receiving nodes must allow decapsulation of packets that can be sourced from anywhere. The problem becomes more serious when IPv6 tunneled over IPv4 encapsulation in UDP as UDP usually allowed passing through NAT's and firewalls (Convery and Miller, 2004). Tunnels encapsulating IPv6 in SSL/TLS or IPSec are more dangerous if the datagram payload is encrypted because there is no technique to examine the payload. The 6-4 is the most widely used tunneling mechanism in the world for transition between IPv4 and IPv6. The 6-4 routers cannot identify whether relays are legitimate (Savola and Patel, 2004). The 6-4 is vulnerable to packet laundering. It is subject to administrative abuse, e.g., service theft (Savola and Patel, 2004). Some Operating System (Windows Vista or Windows 7) enables tunneling by default. The end users may not be aware of this auto configuration which may enable the intruders by bypassing firewalls, IDS and other security mechanisms.

Translation technology is affected by threats similar to circumventing ingress filtering or improper use. It is also vulnerable to buffer overflow attack however, this issue depends on the implementation. IPSec cannot be used in transport relay translator because translation works above the network layer and IPSec in network layer that makes IPv6 vulnerable. The translation system intersects TCP connection between sending and receiving hosts. This is an illegitimate behavior for a communicating node. The transport relay translator must retain state, so it is vulnerable to various DOS attacks (Hagino and Yamamoto, 2001). Protocols that base authentication on IP address do not work across TRT (Hagino and Yamamoto, 2001).

Dual stack technologies drawback is all processes applied for IPv4 duplicates in IPv6 also. The dual stack node has two separate protocol stacks (IPv4 and IPv6). A dual stack host will have to face the vulnerabilities of both Ipv4 and Ipv6. In most cases, dual stack technology relies on tunneling and translation mechanisms for interoperability for networks that are not dual stack (Nordmark and Gilligan, 2005). Unexpected tunneling between the hosts may occur which may violate security policies.

EXISTING SOLUTIONS

Existing techniques can eliminate the vulnerabilities faced by the transition technologies to some extent. The following are the mitigation methods for the above discussed transition technologies.

TUNNELING TECHNOLOGY

Manual tunneling is less vulnerable when compared to automatic tunneling mechanisms. This allows the administrator to establish an association between tunnel

endpoints. The tunnel endpoint must be configured to allow the encapsulated packets to get through any of the security policy enforcement such as IDS, ALgateways and Packet filters (Davies *et al*., 2007). IPSec may be used to protect the ongoing traffic. But still additional security controls such as authorization should be used at tunnel endpoints. Unicast reverse path forwarding filtering (Baker and Savola, 2004) must be used on the tunnel endpoints to avoid traffic injection or reflection. Sending the forged packets toward a tunnel endpoint router that will forward the packet toward the tunnel destination. The router may forward the packet assuming that the packet is legitimate. IPSec provides data confidentiality (Kent and Atkinson, 1998a-c), i.e., the sender can encrypt packets before sending over the network. IPSec can eliminate sniffing and eavesdropping. Most of the Tunneling mechanisms can be secured by blocking an IP packet which contains 41 as protocol field value in the IPv4 header (i.e., IPv6 encapsulated in IPv4 (Convery and Miller, 2004)). UDP packets with specific port no can also be blocked for some tunneling protocols (Convery and Miller, 2004). However, these methods can in turn prevent legitimate traffic.

MULTI STACK TECHNOLOGY

The threat faced by this technology is mitigated to some extend by using Distributed Firewalls and Intrusion Detection System (IDS) and by applying appropriate filtering and detection rules. The rules should be applied for both IPv4 and IPv6 protocol suites. Administrators should audit router and neighbor solicitations to detect the insertion of rogue routers and devices on the network (Davies *et al*., 2007). Consistent security policies must be implemented for both IPv4 and IPv6. Because of the dual protocol suites, unexpected tunneling between the hosts may takes place which results in violation of security. To detect the insertion of rogue routers and devices a periodic audit should be applied for routers and neighbor solicitation messages.

TRANSLATION TECHNOLOGY

The administrator can set a policy in IPv6 enabled firewall to drop all multicast packets to avoid ingress filtering related attacks and improper usage. The rsh/rlogin protocols should not use translation technology because they authenticate based on source IP address (Davies *et al*., 2007). The host which sits in the middle of IPv6, performs translation from IPv4 and IPv6 hosts. There is a possibility that the translator can itself pose as source host (Davies *et al*., 2007). Attackers may use the translator to hide the true source of traffic. If authentication is not used, application layer translation may face vulnerabilities like DOS, address spoofing and open relay attacks.

IP SECURITY-CONSTRAINTS

IPSec is a security framework that has been formally defined and standardized by IETF IP security protocol working group in RFC 2401 for secure communication in a network. IPv4 offers IPSec support but it is optional whereas in IPv6 it is mandatory. IPSec does place an additional burden to the network. CPU needs to work extra cycles to perform encryption and decryption processes. IPSec cannot eliminate application layer attacks. IPSec makes CPU to work additional cycles for encryption and decryption process. The IPSec encryption process increases the network traffic. IPSec's mathematically intensive cryptographic algorithms require a significant amount of computing power which can prevent your computer from making use of all of the available bandwidth (Kent and Atkinson, 1998a-c). A bootstrapping problem makes IPSec not always a valid option (Taib and Budiarto, 2007). IPSec is helpless with application layer attacks.

If configured properly then IPSec can protect most of the attacks discussed above. IPSec still has several security issues such as scanning, head of susceptibility, routing, multicast attack and DoS attack (Zagar *et al*., 2007). In addition, it can not mitigate TCP-flood attack, UDP-flood attack, ICMP-flood attack without spoofed address, i.e., attacking with original IP address (Yang *et al*., 2007). However, IPSec will prevent all these attacks if the attackers use spoofed source address. If fragmentation takes place then IPSec cannot prevent attacks on fragment related attacks. Authentication is done prior to fragmenting the packets thus making the attacker to launch DoS attacks by constructing the packets which could not be reassembled thus legitimate packets not accepted (Davies *et al*., 2007). Tunnels can be secured using Access Control Lists (ACL) in the router along with IPSec. Traffic can be limited by defining the correct ACL that prevents packets with spoofed source address. With the help of ACL and IPSec most of the above said threats can be prevented. Still DoS attacks make a major threat to IPv6 transition. Two major solutions can be used to prevent DoS attack. One is strengthening the end host using various algorithms and a data structure, another one is strengthening the network. To prevent DoS one solution is not enough a combination of mitigation techniques should be used.

CONCLUSION

After few years, IPv6 will replace IPv4 completely and IPv4 protocols will only be in the history of networks. Until those years, we need to have mediators to make, communication between IPv4 and IPv6 and this role is done by the translation technologies. Almost all the attacks in IPv4 remain common in IPv6 but different in the way they are applied. Even though IPv6 solves most of the problems of IPv4, it also introduces more new network security threats. It also discusses security issues on these transition techniques. Existing mitigation techniques are surveyed with all the transition techniques. IPSec is discussed as a solution for security issues in transition techniques with its limitations. A proposed methodology is to be framed for overcoming these limitations in future. The current internet is very large and complex to manage which leads to newer security threats every moment.

REFERENCES

Baker, F. and P. Savola, 2004. Ingress filtering for multihomed networks. IETF RFC 3704, March 2004. http://www.ietf.org/rfc/rfc3704.txt.

Bradner, S., 2006. The end of end to end security? [Internet security]. IEEE Secur. Privacy, 4: 76-79.

Caicedo, C.E., J.B.D. Joshi and S.R. Tuladhar, 2009. Ipv6 security challenges. Computer, 42: 36-42.

Convery, S. and D. Miller, 2004. IPv6 and IPv4 threat comparison and Best-practice evaluation (v1.0). http://www.seanconvery.com/v6-v4-threats.pdf.

Davies, E., S. Krishnan and P. Savola, 2007. IPv6 Transition/coexistence security considerations. RFC 4942, September 2007. http://www.ietf.org/rfc/rfc4942.txt.

Hagino, J. and K. Yamamoto, 2001. An IPv6-to-IPv4 transport relay translator. R.f.C. 3142. Internet Engineering Task Force.

Kent, S. and R. Atkinson, 1998a. Security architecture for the internet protocol. RFC 2401, IETF, November 1998. http://www.ietf.org/rfc/rfc2401.txt.

Kent, S. and R. Atkinson, 1998b. IP encapsulating security payload. RFC 2406, (Proposed Standard), November 1998. http://tools.ietf.org/html/rfc2406.

Kent, S. and R. Atkinson, 1998c. IP authentication header. RFC 2402 (Proposed Standard), Internet Engineering Task Force, November 1998.

Nikander, P., J. Kempf and E. Nordmark, 2004. IPv6 Neighbor Discovery (ND) trust models and threats. Internet Engineering Task Force, RFC 3756, Editor 2004.. http://www.hjp.at/doc/rfc/rfc3756.html.

Nordmark, E. and R. Gilligan, 2005. Basic transition mechanisms for IPv6 hosts and routers. RFC 4213, October 2005. http://tools.ietf.org/html/rfc4213.

Savola, P. and C. Patel, 2004. Security considerations for 6to4. RFC 3964, Internet Engineering Task Force. http://www.ietf.org/rfc/rfc3964.txt.

Taib, A.H.M. and R. Budiarto, 2007. Security mechanisms for the IPv4 to IPv6 transition. Proceedings of the 5th Student Conference on Research and Development, December 12-11, 2007, Selangor, Malaysia, pp: 1-6.

Waddington, D.G. and F. Chang, 2002. Realizing the transition to Ipv6. IEEE Commun. Magazine, 40: 138-147.

Yang, X., T. Ma and Y. Shi, 2007. Typical DoS/DDoS threats under IPv6. Proceedings of the International Multi-Conference on Computing in the Global Information Technology, March 4-9, 2007, Gosier, Guadaloupe, pp: 55.

Zagar, D., K. Grgic and S. Rimac-Drlje, 2007. Security aspects in IPv6 networks-implementation and testing. Comput. Electr. Eng., 33: 425-437.