IPv6 SECURITY THREATS AND POSSIBLE SOLUTIONS

DRAGO ŽAGAR, FACULTY OF ELECTRICAL ENGINEERING OSIJEK, CROATIA
drago.zagar@etfos.hr
KREŠIMIR GRGIĆ, FACULTY OF ELECTRICAL ENGINEERING OSIJEK, CROATIA
kresimir.grgic@etfos.hr

ABSTRACT

In comparison to IPv4, IPv6 provides many improvements considering simplicity, routing speed, quality of service and security. IPv6 brings significant improvements in mechanisms for assuring a higher level of security and confidentiality of the transmitted information. Nevertheless, it is still necessary to take care of network security. This paper analyzes how actual security threats and different types of attacks affect IPv6 networks. IPv6 specific security issues and issues due to different transition mechanisms are also analyzed. Certain security tests have been done and their comments have been given. Finally, some possible solutions for a number of security threats in IPv6 networks have been given.

KEYWORDS: IPv6, Network security, Firewall, Intrusion detection

1. INTRODUCTION

It could be expected that a new version of the Internet protocol, IPv6, will replace an old IPv4 during the next few years. IPv6 brings many new features, possibilities and improvements, especially considering simplicity, routing speed, quality of service and security [1]. Although IPv6 security mechanisms are much improved comparing to IPv4, their evasion and misuse is unfortunately still possible.

Considering security issues, especially problematic is the transition period of coexistence of both IPv4 and IPv6. It is because transition mechanisms provide new, previously unknown, possibilities of intrusion and misuse of computer systems. Security threats due to transition mechanisms should be seriously taken into consideration, because it is expected that IPv4 to IPv6 transition will not be quick (it could last for years).

Presence of the IPv6 protocol brings new demands for typical network protecting mechanisms such as firewalls and intrusion detection systems that need to be upgraded to support IPv6 correctly. Some security threats against IPv4 networks might also affect an IPv6 network. Fortunately, IPv6 is more resistant to some threats than IPv4. But, there are some new threats specific to IPv6.

IPv6 security issues can be observed from different standpoints: issues due to the IPv6 protocol and its deployment and issues due to transition mechanisms.

2. SECURITY THREATS SIMILAR IN IPv4 AND IPv6 NETWORKS

Some types of attacks have not fundamentally changed by appearance of the IPv6 protocol. A typical example is a sniffing attack. The sniffing attack refers to an attack that involves capturing data being transmitted through the network. The sniffing attack can easily compromise confidential data if they are transmitted in a plaintext protocol. Sniffing attacks can be avoided by a proper use of security architecture, which is used in IPv4 as an option and in IPv6 as an obligation.

Most common attacks today are application layer attacks. To this group of attacks belong buffer overflow attacks, web application attacks (e.g. CGI attacks), different types of viruses and worms. These types of attacks are actually performed at the application layer of the ISO/OSI

network model (layer 7). Since IPv4 and IPv6 are protocols of the network layer, transition to IPv6 does not have influence on these types of attacks.

A flooding attack is a very frequent type of attack in current networks. The flooding attack means flooding a network device (e.g. a router) or a host with large amounts of network traffic, much larger than it is able to process. It can be a local or a distributed DoS (Denial of Service) attack and it can cause unavailability of network resources. Arrival of IPv6 did not change basic principles of a flooding attack. New types of extension headers in IPv6, new types of ICMPv6 messages and dependence on multicast addresses in IPv6 (e.g. all routers must have site-specific multicast addresses) may provide new ways of misuse in flooding attacks.

3. IPv6 SPECIFIC SECURITY ISSUES

IPv6 protocol brings many differences and new features in comparison to IPv4. Some of changes in protocol specifications may potentially result in security problems.

3.1 Reconnaissance attacks

An intruder uses reconnaissance attacks to gather essential data about the victim network that are used later in further attacks. An intruder can use active methods, such as scanning, or passive data mining. As a result of a reconnaissance attack an intruder gets information about hosts and network devices and their interconnections in the targeted network. To gather these information an intruder uses ping probes in order to determine which IP addresses are in use. After that a port scan of the accessible system is performed. There are software tools (such as Nmap) that can perform all these actions together.

The port scan procedure is identical for both IPv4 and IPv6, but there is a major difference in identification of valid address. Reconnaissance techniques are the same for IPv4 and IPv6, but the subnet size in the IPv6 network is much larger than in the IPv4 network (the default size is 64 bits). To perform a scan of the whole subnet it is necessary to make 2^{64} probes – so that makes it impossible.

Unfortunately, some types of multicast addresses used in IPv6 networks can help an intruder to identify and attack some resources in the targeted network. RFC 2375 [2] defines a node, a link and site-specific use of multicast addresses (e.g. all routers have a site-specific address FF05::2). Also, it is crucial to ensure that these internal-use addresses are unreachable from the outside. It can be performed by filtering on network's border routers.

3.2 Misuse of routing headers

According to [1], all IPv6 nodes have to be capable of processing routing headers. This behavior produces some security problems, because routing headers can be used to avoid access controls based on destination addresses. It is possible that an intruder sends a packet to a publicly accessible address with a routing header containing a "forbidden" address (address on the victim network). Then the publicly accessible host will forward the packet to a destination address stated in the routing header ("forbidden" address) even though that destination address is filtered. By spoofing packet source addresses an intruder can initiate a denial-of-service attack by using any publicly accessible host for redirecting attack packets.

3.3 Fragmentation related attacks

IPv6 protocol specification [1] does not allow packet fragmentation by intermediary devices. Fragmentation is possible only at the source node meaning that usage of the path MTU discovery method (based on ICMP messages) is an obligation. The minimum recommended MTU size for IPv6 is 1280 octets. It is recommended security practice to drop all fragments with less than 1280 octets unless the packet is the last in the flow. Using fragmentation an intruder can achieve that port numbers are not found in the first fragment and in that way bypass security monitoring devices (which do not reassemble fragments) expecting to find transport layer protocol data in the first fragment. By sending a large number of small fragments an attacker can cause an overload of reconstruction buffers on the target system potentially implying a system to

crash (a type of a Denial of Service attack). This can be avoided by limiting the total number of fragments and their arrival rate.

3.4 Misuse of ICMPv6 and multicast

Some important mechanisms in IPv6 networks, such as neighbor discovery and path maximum-transmission-unit discovery, are dependent on some types of ICMPv6 messages [3]. Therefore it is a must to permit some ICMPv6 messages in order to have the IPv6 network operate properly (e.g. a “packet too big” message is required for the path MTU-discovery procedure, or a “parameter problem” message is necessary if there is an unrecognized option in the packet header). ICMPv6 specification also allows an error notification response to be sent to multicast addresses (if a packet was targeted to a multicast address). That fact can be misused by an attacker. By sending a suitable packet to a multicast address an attacker can cause multiple responses targeted at the victim (the spoofed source of the multicast packet).

4. SECURITY ISSUES DUE TO TRANSITION MECHANISMS

Transition from the IPv4 to the IPv6 protocol will not be rapid and for a certain period of time both protocols will coexist. There are several transition mechanisms, such as tunneling and dual-stack configurations (supporting both IPv4 and IPv6) [4]. It is very important for network designers and administrators to understand security implications of the transition mechanisms in order to apply proper security mechanisms, such as firewalls and intrusion detection systems.

On dual-stack configuration hosts applications can be targeted by both IPv4 and IPv6 attacks. Accordingly, firewalls and intrusion detection systems on such hosts must support both IPv4 and IPv6 and must have proper filtering/detection rules for both protocols.

Tunneling mechanisms may also bring new danger and misuse possibilities. Tunneling can facilitate an intruder to avoid ingress filtering checks. Special attention must be paid to automatic tunneling mechanisms. Two methods of automatic tunneling are specified. The first method is called “6to4” and it connotes encapsulation of the IPv6 packet directly into an IPv4 packet. The “Teredo” tunneling mechanism connotes encapsulation of the IPv6 packet into an IPv4 UDP packet. If these tunneling methods are in use, all receiving nodes must allow decapsulation of packets that can be sourced from anywhere. This can be a serious security problem.

The 6to4 mechanism uses automatic IPv6-over-IPv4 tunneling for interconnecting IPv6 networks. The 6to4 architecture includes 6to4 routers and 6to4 relay routers. The 6to4 router accepts and decapsulates IPv4 packets from other 6to4 router, and the 6to4 relay router accepts packets from native IPv6 nodes.

Addresses within the IPv4 and IPv6 headers may be spoofed, meaning this mechanism can be used for Denial of Service (DoS) attacks. By misusing a 6to4 transition mechanism a DoS attack can be targeted to the IPv6 node, the IPv4 node or other 6to4 node [5].

5. IPv6 FIREWALLS

Firewalls represent one of the most important network security mechanisms. They act as network traffic filters filtering all traffic that enters or leaves the local network. Firewalls are usually positioned between a LAN and the Internet (or other insecure network), but it is also possible to place firewalls on LAN segments, even on every single host in the local network. Every packet is being analyzed and results are compared with a predefined set of rules. According to predefined rules, the packet can be accepted, discarded or sent to an additional check.

Filtering rules must be defined separately for IPv4 and IPv6 traffic meaning that firewalls for IPv6 networks must have support for the IPv6 protocol. On the Linux platform exists an “ip6tables” tool for configuring IPv6 firewall (i.e. writing filtering rules for IPv6 traffic). “ip6tables” is included in all recent Linux distributions and it is very similar to the “iptables” tool (a tool for setting an IPv4 firewall).

MS Windows platform uses a “Windows Firewall” tool (formerly called ICF – Internet Connection Firewall) with support for the IPv6 protocol. It is included in Service Pack 2 for MS Windows XP and it is not available as a single product. Filtering rules for Windows Firewall can be set in graphical user environment or using the Command Prompt (net shell).

6. INTRUSION DETECTION IN IPv6 NETWORKS

Intrusion Detection System (IDS) is a hardware or software system for supervision and analysis of different events occurring in the network or on the particular host. The purpose of the IDS system is to find potential security problems and to detect an unauthorized intrusion and misuse of network resources.

There are two main types of IDS systems: Host-Based IDS systems (HIDS) and Network-Based IDS systems (NIDS). The NIDS system captures and analyzes network traffic on a whole local network or a network segment protecting many hosts simultaneously. The HIDS system protects a single host. For achieving maximum level of protection it is recommended to install the HIDS system at every host in LAN. The NIDS system should be implemented on every segment (subnet) of LAN or at least between LAN and the Internet. Such placement of HIDS and NIDS systems enables detection of outside attacks such as unauthorized activities of local users.

Unfortunately, the situation considering IPv6 support by non-commercial IDS systems is not so good. There are several commercial IDS systems with IPv6 support, but no freeware known to authors (November 2005).

IPv6 supporting the IDS system must consider some new things typical of the IPv6 protocol. IPv6 defines a new header format that the IDS system must properly recognize. In order to simplify the main header, IPv6 introduces extension headers (such as Hop-by-hop, Routing, Fragment, Destination Options, Authentication, Encapsulation Security Payload). A Next Header format also allows new types of IPv6 extension headers to be defined and implemented. The IDS system must implement support for these types of headers. A proper header order is also defined, thus it is desirable for IDS to check the order of extension headers. It is recommended for IDS to discard a packet with an undefined “Next Header” value and to record this as incident.

A Hop-by-hop options header is the only header examined at each hop along the path from the source to the destination node. Since it may have multiple or repeated options an IDS system should be capable of detecting irregular or duplicate options. A Destination options header is processed by the destination node. This header should also be checked by IDS due to a possibility of irregular or duplicate options. A Bad destination option or a hop-by-hop option can be set up intentionally by an attacker. If the node is set to send an ICMP error message in case of bad options, it can be misused for a smurf-like attack. An attack will be targeted back to the spoofed source address via the remote network.

Intrusion Detection System with IPv6 support should also be able to recognize and analyze IPv6 traffic tunneled in IPv4. That implies support for both automatic and manual tunnels. Proper deployment of IDS is also very important. If a node or a network has separate connections for IPv4 and IPv6, it is necessary to deploy a proper IDS for every connection. For a dual-stack node with a single connection deployed IDS must recognize and support both protocols. If IPv6 traffic is tunneled, a tunnel should be terminated outside the IPv6 firewall and IDS deployed at the ingress point of a network, behind firewall.

7. TESTING OF SECURITY ISSUES IN EXPERIMENTAL IPv6 NETWORK

For experimenting purposes at the Faculty of Electrical Engineering, University of Osijek, a small IPv6 network has been established. The network consists of three computers, two desktop PCs (based on Intel Celeron and Intel P4 CPUs) and one notebook (Gericom Hummer, based on Intel Celeron CPU). All computers have been configured as dual-boot configurations driven by MS Windows XP (with SP2 included) and Mandrake Linux 10 operating systems. Also, all computers in the experimental network have been configured as dual-stack devices

supporting both IPv4 and IPv6 protocols. A local IPv6 network was connected to the CAR6Net network (CAR6Net – experimental IPv6 network established by CARNet, Croatian Academic and Research Network).

In the described experimental network some IPv6 firewall tests have been done. Different types of reconnaissance attacks have been performed and some possibilities for their successful detection have been analyzed.

All tests have been performed both on Windows XP and Linux platform. Command-line applications Netshell (on Windows XP) and ip6tables (on Linux) have been used for setting of the filtering rules. Settings of Windows and Linux firewall were identical for the purpose of better comparison.

Nmap application [6] has been used for testing purposes (scanning for security vulnerabilities). The official version of Nmap supports the IPv6 protocol, but there is an adapted version of Nmap based on an older official version (ver. 2.54BETA36) with an improved support for IPv6. This Nmap version is recommended for use in IPv6 networks by authors of the original Nmap. It supports more scanning techniques such as *TCP connect scan, SYN scan, ACK scan, FIN scan, Xmas Tree scan* and *UDP scan*.

A TCP connect scan technique connotes attempts to establish a TCP connection on different ports on the targeted host. If the port is listening, the connection will be established, otherwise the port will be unreachable. This type of scan can be performed by any user (without administrative privileges), but it is also easiest to detect. By a SYN scan technique a SYN packet is sent to a targeted host, similarly to the procedure of establishing a full TCP connection. A SYN/ACK response indicates that the targeted port is listening, while RST response designates a non-listening port. The ACK scan method sends an ACK packet with random looking acknowledgement/sequence numbers to the specified port. A RST response on the ACK scan denotes an unfiltered port. The Xmas Tree scan method sets flags FIN, URG and PUSH. A closed port should reply with RST, while the open port ignores the probe packet. By the UDP scan method 0 byte UDP packets are sent to targeted ports. A received ICMP port unreachable message denotes a closed port.

For the testing purpose we have performed all described scanning methods. On the Linux platform none of the scanning methods could bypass the firewall and discover port settings on the targeted host. On the Windows XP platform some scanning techniques (TCP connect scan and SYN scan) successfully discovered port settings through the firewall. Therefore, the Linux firewall currently provides a higher security level than the Windows firewall. Consequently, in networks requiring a higher security level the usage of the Linux firewall is recommended.

Possibility of intrusion detection is very important in networks that require a high level of security and protection. Since currently there are no non-commercial Intrusion Detection Systems, we have been considered some other available approaches and methods for successful detection of an unauthorized intrusion.

Historically, prior to the appearance of different software tools which automated the procedure of intrusion detection (i.e. Intrusion Detection Systems), different packet dumping tools have been used for that purpose. Thus, in absence of an IPv6 supporting IDS tool, for purpose of intrusion detection we have been used Ethereal, network capture and analysis tool [7].

Ethereal is a network packet analyzer with a very good support for decoding many network protocols and application layer traffic, including full support for the IPv6 protocol. It is often used for troubleshooting network problems, examining security problems, debugging protocol implementations and learning purposes. Ethereal can be used to actively monitor network traffic or to analyze previously captured traffic. It implements powerful and fully adjustable filtering options and is available on both MS Windows and Linux/UNIX platforms.

Ethereal can be successfully used for intrusion detection in IPv6 networks. For the testing purposes we have been performed different types of reconnaissance attacks by using Nmap application. All attack-related IPv6 traffic was successfully recognized and logged by Ethereal.

Owing to this fact we could detect all attack attempts by analysis of captured traffic. Table 1 shows an example of a reconnaissance attack logged by Ethereal.

No.	Source	Destination	Protocol	Info
1	2001:b68:8001::2	2001:b68:8001::3	TCP	34405 > epmap [SYN] Seq=0 Ack=0 Win=5760 Len=0
2	2001:b68:8001::3	2001:b68:8001::2	TCP	epmap > 34405 [SYN; ACK] Seq=0 Ack=1 Win=17280 Len=0
3	2001:b68:8001::2	2001:b68:8001::3	TCP	34406 > 136 [SYN] Seq=0 Ack=0 Win=5760 Len=0
4	2001:b68:8001::3	2001:b68:8001::2	TCP	136 > 34406 [RST; ACK] Seq=0 Ack=0 Win=0 Len=0
5	2001:b68:8001::2	2001:b68:8001::3	TCP	34407 > 134 [SYN] Seq=0 Ack=0 Win=5760 Len=0
6	2001:b68:8001::3	2001:b68:8001::2	TCP	134 > 34407 [RST; ACK] Seq=0 Ack=0 Win=0 Len=0
7	2001:b68:8001::2	2001:b68:8001::3	TCP	34405 > epmap [ACK] Seq=1 Ack=1 Win=5760 Len=0
8	2001:b68:8001::2	2001:b68:8001::3	TCP	34405 > epmap [RST; ACK] Seq=1 Ack=1 Win=5760 Len=0

Table 1. Reconnaissance attack pattern captured by Ethereal

In this example we recognize a reconnaissance attack as a sequence of connection attempts to different ports on the targeted host during a very short period (Table 1. shows only one fragment of captured traffic). A big disadvantage of the described method of intrusion detection is a necessity of constant monitoring by a well-educated administrator, since there is no possibility in Ethereal for an automatic alert or response to an attack.

The described example shows a situation where an attack was efficiently detected, but it also represents a situation where an attacker successfully collected the desired information about port configuration on the targeted host. Namely, an attacker got a SYN/ACK response from port 135 and concluded that the port is listening.

8. CONCLUSIONS

After a certain period of coexistence the IPv6 protocol will replace IPv4. Every day IPv6 becomes more and more accepted and used throughout the global network. Although IPv6 brings numerous improvements, there are still some potential security problems that require consideration. Certain misuse possibilities known in IPv4 persist, and some new transition-related and IPv6 specific emerge.

Therefore, it is necessary to undertake all possible steps for achieving the highest possible security level. For an improved protection in IPv6 networks it is recommended to implement security mechanisms for packet filtering and intrusion detection. It is recommended to filter internal-use IPv6 addresses at border routers in order to avoid some reconnaissance attacks. All unneeded services should be filtered at the firewall. To avoid certain types of fragmentation attacks it is advisable to discard all fragments smaller than 1280 octets (except the last one) and to limit the fragment arrival rate. Selective filtering of ICMPv6 messages is also a recommended practice. During a transition period it is advisable to use dual-stack configurations rather than tunneling. If tunneling is in use, it is more secure to use static tunnels rather than dynamic.

Considering security, the IPv6 protocol can still be improved, but this fact should not be an obstacle to its wide acceptance and usage.

9. REFERENCES

[1] RFC 2460: Internet Protocol, Version 6 (IPv6) Specification
[2] RFC 2375: IPv6 Multicast Address Assignments
[3] RFC 2463: Internet Control Message Protocol (ICMPv6) for the IPv6 Specification
[4] RFC 2893: Transition Mechanisms for IPv6 Hosts and Routers
[5] RFC 3964: Security Considerations for 6to4
[6] http://www.insecure.org/nmap (Nmap)
[7] http://www.ethereal.com (Ethereal)