A brief analysis of IPv6 security

“Poor security is an inherited vulnerability of the Internet, regardless of whether IPv6 is used or not,” says Wei Leping, Director of China Telecom Science and Technology Committee. “In practice, IPv6 has not introduced any new security threats. On the contrary, introduction of IPSec and the approach of transmission devices using permanent IP addresses enable tracking back to sources at the network layer, and thereby provide an end-to-end solution for network security.”

By Zhang Dong

Security design of IPv6

As a transmission protocol intended for the network layer, IPv6 is the generation following IPv4. The 32-bit address space of IPv4 was expanded to 128-bit for IPv6, which is the fundamental driving force behind IPv6’s selection as the bearer protocol for new networks and increasing commercialization.

On IPv4 networks, addresses are randomly assigned and even multiple hosts share an address. Unlike IPv4, IPv6 provides a unique address for each object, like an ID for a person or a license-plate number for a vehicle. And tracking of source is made feasible and easy, as IPv6 addresses are assigned level by level.

IPv6 also provides a new kind of addresses, among others, called cryptographically generated addresses (CGA). Each IPv6 address thus created is bound with a pair of public and private keys, like a fingerprint on a vehicle plate, making the address unique and unable to be forged.

As originally designed, an authentication header (AH) and the encapsulation security payload (ESP) in the IP security (IPSec) protocol family are built in the IPv6 protocol stack. In an IP packet, the AH and ESP are used as an extension header, ensuring packet integrity, confidentiality, and source authentication, and thereby significantly improving communication security.

In stark contrast, the IPv4 was not designed with such security considerations and its vulnerability to IP-address spoofing makes it hard to monitor the network effectively. When IPv4 networks are facing attacks or security threats, no efficient technical solutions are available to beat attacks from hackers head on, except prevention.
In IPv6, addresses cryptographically generated are a new kind of addresses which are bound with a pair of public and private keys, making a source IPv6 address unique and hard to forge. With this new security mechanism, any attack or malicious action can be traced back to the host.

**IPv6 helps mitigating attacks**

Scanning is always the first step before any attack, as hackers use that to locate the target hosts or devices by pinging IP addresses and collecting data of target networks. Based on analysis of collected data, hackers can derive valuable information about target networks, such as network topology, services opened, and port information as a basis for attacks.

As each IPv6 address has 128 bits and a network prefix of 64 bits, it is much more difficult for hackers to do the scanning, and incurs heavy costs. It will take up to 50,000 years for an attacker to finish the scanning of a network segment that contains 2^64 addresses, even at a scanning rate of 10Mbps. The high cost that attackers have to pay to invade the zombie hosts, to a certain extent reduces the possibility of Distributed Denial of Service (DDoS) attacks.

In addition, IPv6 defines multicast addresses to replace the broadcast addresses that are used in IPv4. This effectively prevents broadcast storm attacks and DDoS attacks initiated via broadcast addresses. Moreover, IPv6 does not allow ICMPv6 response to packets with multicast addresses, preventing amplification attacks by ICMPv6.

In IPv6, cryptographically generated addresses are a new kind of addresses which are bound with a pair of public and private keys, making a source IPv6 address unique and hard to forge. Each packet transmitted on an IPv6 network with this new security mechanism is bound to a host and therefore any attack or malicious action can be traced back to the host.

**Security challenges for IPv6**

Compared with IPv4, radical changes to IPv6 are with the IP layer. Therefore, packet headers and extension headers could easily become targets for security attacks, and preparations need to be made in this regard. The common attacks against extension headers include DDoS attacks, and amplification attacks on networks by using type 0 routing headers in addition to fragmentation attacks by using fragmentation extension headers to escape the detection of firewalls or the intrusion detection system (IDS).

In the transition from IPv4 to IPv6, hidden security issues of transition technologies and transition schemes have to be taken into consideration. In the period when IPv4 and IPv6 coexist and interconnect with each other, security threats must not be passed over from one to the other. So far, various transition technologies adopted by operators are yet to be proven in practice and potential risks are still there.

Specifically, the tunneling technology, as one of the options, is designed to encapsulate packets. When packets using that technology go through network security devices for checking or filtering, the network security device must support various new tunnel protocols and thus be able to de-capitalize tunnels and process the encapsulated packets. It is also very important to authenticate tunnels section by section when setting up tunnels. Otherwise, unauthenticated tunnels can easily be used by hackers or attackers as paths into target networks.

When interconnecting IPv6 networks with IPv4 networks via network address translation (NAT), the
related information about packets at the IP layer and transport layer needs to be changed. This will adversely affect end-to-end security, and IPSec 3-layer tunnels will experience break points when going through address conversion devices. Key to the interconnection, translation devices could easily become the main targets for DDoS attacks.

In summary, the root causes of latent security issues are network protocol design defects, network device bugs, or deployment or usage issues of network protocols. It is highly recommended that we first resolve the similar known threats to IPv4 by using the security features of IPv6 at the very beginning of its commercial use. With expansion of IPv6 networks and the migration and increase of applications, IPv6 may face more new threats.

Security mechanisms and policies of IPv6

Full use of built-in address security features

In certain scenarios, use of the CGA helps detect spoofing and forgery for the Neighbor Discovery (ND) protocol and Dynamic Host Configuration Protocol IPv6 (DHCPv6). With pairs of public and private keys, CGA can also be used for IPSEC negotiation and can simplify the negotiation process in some scenarios to improve IPSEC performance.

The other security mechanism is privacy extension. Due to there being no need for address translation, network address translation devices are not involved in IPv6 networks and therefore internal network topology is vulnerable to exposure. With the privacy extension mechanism, addresses will be changed periodically and this helps prevent information exposure.

Accurate filtering policies

Given the changes in address structures and protocols for IPv6, accurate filtering policies need to be set on firewalls or network edge devices to prevent source address spoofing.

Firewalls need to reject the packets to access frequently-used internal multicast addresses, disable unnecessary service ports, and filter the addresses used by internal networks. IPv6 has much stronger dependence on ICMPv6 than IPv4 does. In addition to ping and error messaging functions, ICMPv6 has more new functions like address assignment, address resolution, multicast management, and usage of mobile IPv6. Therefore, filtering policies for ICMPv6 packets need to carefully set up, preventing interruption of services and applications.

To protect extension headers, firewalls need to verify the validity of IPv6 extension headers. For fragmented packets, firewalls must be able to reject fragmentation packets that are sent to the intermediate network device, support fragmentation reassembly, prevent DDoS attacks, and identify and filter type 0 routing headers. An entrance filtering mechanism is also necessary for firewalls and network edge devices, so as to alleviate threats caused by source address forgery between networks.

Proper deployment policies

During the period that IPv6 and IPv4 coexist, secure deployment of transition technologies is very important. Each type of network security devices must be capable of fighting against IPv4 and IPv6 security threats. It is recommended that static tunnels be used to reduce illegal access or forgery threats brought by dynamic tunnels. Firewalls need to filter packets from unauthorized tunnels, identify various tunnel protocols, and control the access to encapsulated packets in tunnels. And address translation devices must be capable of defending themselves against DDoS attacks.

2010 saw the beginning of commercial use for IPv6 networks, with many mainstream operators developing transition schemes, announcing evolution plans, and deploying IPv6 networks in pilot cities. Huawei has long been fully ready for the commercial use of IPv6. In 2009, it received the IPv6 Ready logo and was the first company with its IPv6 firewalls passing the enhanced certification of IPv6 Ready phase 2 in China. In addition, Huawei is capable of integrating various mainstream transition technologies and solutions on the same device, fully satisfying the requirements of IPv6 commercial use.

Editor: Xu Peng xupeng@huawei.com

Thanks for your reading, the electronic version and subscription information are available at www.huawei.com/communicate. Questions and suggestions may be directed to the editor concerned.