Security in IPv6

Mohammad Ali Badamchizadeh   Ali Akbari Chianeh

University College of Nabi Akram (UCNA), Tabriz, Iran

Abstract - The deployment of the next generation Internet Protocol (IPv6) has already started. There were great expectations about the features of the new protocol, one of which was better network security. IPv6 provides network level security via IPSec. While this is an obvious improvement in security, its universal usability is still questionable. This paper examines the security aspects of IPv6, whether it will change the security of the Internet.

1. Introduction

TCP/IP is the protocol that runs the Internet. It was designed in the 70's, and it was introduced in 1983. Since then, it has served the Internet from a small research network to become a multi-million node global network, while TCP/IP has become the dominant networking protocol.

While the current version 4 of the Internet Protocol (IPv4) has scaled incredibly, several shortcomings have surfaced. Initially, the lack of IP addresses seemed to be the most urgent problem. The IETF has initiated the development of a next generation Internet protocol [1].The main goal was to create a protocol that solves the address space problem. Because of the fundamental changes it had meant, there was an opportunity to make other improvements to IPv4. The new protocol became known as IPv6.

It has become clear, that security is top priority in today's networks, thus with the introduction of IPv6 there is an opportunity to introduce new security features to the Internet Protocol. Besides the new functions, the protocol indirectly influences security also. It is still debated whether this influence increases overall security.

2. IPv6 overview

2.1. Problems with IPv4

The address space depletion first became a serious problem at the beginning of the 1990's with the rapid expansion of corporate networks, and it was the main driving force behind the development of the new protocol. The initial method that was used to allocate the address (the class based scheme) resulted in a very inefficient use of the address space. New techniques were introduced (NAT – Network Address Translation) that have more or less solved the address space issue without the need for new protocol and corporate networks were free to expand. NAT also have the desirable security byproduct of hiding the internal network from outside view.

2.2. IPv6 improvements

The IPv6 protocol [4-5] provides several new features, compared to IPv4:

- *New addressing architecture with 128 bit addresses.* New address types, such as linklocal, multicast, compatibility and global addresses are defined.
- *Security framework.* The IPSec security framework provides network level authentication and encryption. IPSec includes AH (Authentication Header) to authenticate (digitally sign) network packets. ESP (Encapsulated Security Payload) encrypts network traffic. It also includes Routing extension and Fragmentation header. IPSec is a flexible framework, various cryptography algorithms and key-exchange mechanisms may be used. IPSec is also available for IPv4, but it is not mandatory.
- *Autoconfiguration.* The IPv6 autoconfiguration enables hosts to acquire IP addresses either autonomously or in a controlled way [4]. This is performed in a robust way; duplicate addresses are detected and rejected, even when using manual configuration. A running network can also be reconfigured to use other addresses. This is most useful for corporate nets. From the home user's point of view IPv6 needs no manual configuration. Networks can also use DHCPv6 to manually control configuration.
- *Performance improvements.* IPv6 has improved performance. Packet fragmenting,

hierarchical addressing and header chaining makes IPv6 suitable for high-performance operation.

- *Mobility*. IPv6 contains framework form mobile-IP [8]. A host may move (roam) to a foreign network, keeping it original IPv6 address. Host agents arrange initial traffic to be moved the mobile host, while the home address option header provides direct communication between the mobile host and its communicating partners.

3. Security impact of new IPv6 functions

Direct and indirect impact on system security can be identified in all of the above functions, with the exception of QoS. Let us examine these in detail.

3.1. Addressing

The new addressing architecture [4] is radically different from IPv4's. First of all, the size of the available address range is enormous. This can have a direct impact on current "break-in" techniques. Security incidents are usually prepared with prior reconnaissance, such as scanning the network for suitable targets. Viruses use the same method for infecting nearby computers. This is feasible in IPv4, where the range to be scanned is usually in the number of hundreds or thousands. The address range is easily scanned by using brute-force to try all addresses in the host portion of the IP address. An attacker can very quickly survey every on-link address.

What is the case with IPv6? IPv6 uses several address types. Usually for unicast communication the link-local and the aggregatable global unicast address [4] is used.

The link-local address is used for local communication on one link. It is mandatory and its address is always automatically and autonomously configured for the interface. The aggregatable global unicast address is used for global communication. This address may be automatically configured autonomously or by methods such as DHCP. Both address formats are made of two parts: the prefix (with the hierarchical network part in the case of the global address) and the interface identifier part. The interface ID has a length of 64 bits, and is in the EUI-64 format. This means, that the smallest possible local network has 2^{64} available addresses. A brute force scanning in this case is impossible [9]. While this seems to be good news, an attacker will not always have to scan all possibilities. The EUI-64 format is based on the interface token (such as the MAC address of the Ethernet interface). As the Ethernet addresses are allocated on a manufacturer base, knowing the manufacturer of the interfaces, the range of the address space to be scanned may be drastically reduced (but it is still considerably large). This information can be gathered from several sources (such as intercepting network traffic), or even by just trying the most popular values.

However, there are other methods to enumerate the IPv6 addresses used in a network, such as eavesdropping. Thus while the large address space can prevent some kinds of attacks, it is more of security trough obscurity, and thus, should not be treated as effective prevention. While the large address space can make the work of an intruder hard, it may interfere with countermeasures. Security scanners and IDS[1] tools can suffer from this problem. Large address range may also make detection of rogue hosts difficult.

IPv6 does not support NAT (network address translation), which is widely used in IPv4 to provide enough addresses for the internal network. NAT break end-to-end connectivity, so it has drawbacks, but for "workstation-like" connectivity, NAT is sufficient. The operation of NAT has the byproduct of hiding the internal network and preventing connection attempts from outside. Some view this is as an advantage of NAT, and the lack of NAT as a disadvantage of IPv6. Yet this function can be performed by firewalling, without the drawbacks of NAT. Proper IPv6 firewalling is still under development [10].

3.2. IPSec

IPSec is the obvious security enhancement in IPv6. IPSec new features are as fallows:

- *Authentication Header:* Using IPv6 authentication headers, hosts can verify the authentication and integrity of the IPv6 payload data. The authentication header makes use of an established security association, that may, for

[1] Intrusion Detection System

instance, be based on the exchange of algorithm-independent secret keys. In client/server session for instance, both the client and the server need to have knowledge of the key. Before each packet is sent, IPv6 authentication creates a Message Integrity Code (MIC) (using e.g., MD5[1] or SHA-1[2]) based on the key convolved with the entire contents of the packet including data within the Authentication Extension to eliminate replay attacks. The MIC is then recomputed on the receiving side and compared. This approach provides authentication of the sender and guarantees that data within the packet has not been modified or replayed by an intervening party.

- *Routing Extension header:* IPv6 routing extension header replaces the Loose Source Route (LSR) option supported currently by IPv4. This optional header allows a source node to specify a list of IP addresses that determine which routing path a packet will traverse. The source routing feature works in conjunction with another routing header field that contains a value equal to the total number of segments remaining in the source route. Each tome a hop is made, this “segment left” field is decremented.
- *Fragmentation header:* IPv4 has the ability to fragment packets at any point in the path, depending on the transmission capabilities of the links involved. This feature has been dropped in IPv6 in favor of end-to-end fragmentation/reassembly, which is executed only by IPv6 source and destination nodes. Packet fragmentation is not permitted in intermediate IPv6 nodes. The elimination of the fragmentation field allows a simplified packet header design and better router performance for the great majority of cases where fragmentation is not required.
- *Encapsulating Security Payload (ESP):* Authentication headers eliminate a number of host spoofing and packet modification attacks, but they do not prevent passively reading of data traversing the internet and corporate networks. This protection is offered by the ESP service of IPv6. Packets protected by ESP encryption techniques can have very high levels of privacy and integrity, something that is not widely available with the current internet, except with certain secure applications (e.g., private electronic mail and secure HTTP Web servers). ESP provides encryption at the network layer, making it available to all applications in a standardized fasion.

IPv6 corrects another deficiency in the specification of IPv4 source routing options, by relaxing the requirement that destination nodes reverse the source route for transmitting packets back to the node that IPv4 source routing has almost entirely fallen out of use, because it opens up a big security hole [7].

While IPSec is useful for tasks such as creating VPNs, in our view it will not be used as a general purpose security solution. The reasons for this are the followings:

- Practically every application already have their own security measures, such as ssh for remote login, ssl for secure http and other protocols, DNSSec for DNS, etc. IPSec in this case is not necessary, and usually applications wanting high security will want to implement it themselves, without trusting the environment. Moreover, APIs for IPSec are still not standardized.
- Current IPSec implementations are better suited for tunnel mode operation (such as VPN) than for arbitrary end-to-end communication. The main reason behind this is the problem of key management.

Because of these, IPSec will remain as a tool for VPN and similar applications, and will probably not be used in its full potential. IPSec is also implemented for IPv4 and similar observations can be taken in this case.

3.3. Autoconfiguration and Neighbor Discovery

Autoconfiguration is the mechanism that enables nodes to acquire configuration information using several methods. First of all, at system start a node creates the link-local (LL) address for its interface(s). This is a completely autonomous act, and is performed by appending the interface’s EUI-64 identifier to the linklocal
prefix (fe80::/64). The LL address is guaranteed to be unique on the given link only and may be used for communicating on the link only. All further configurations are done over IP, using the LL address.

IPv6 autoconfiguration may be stateful or stateless. Stateless autoconfiguration is used in

[1] Massage-Digest Algorithm
[2] Secure Hash Algorithm

simple cases. It lets nodes to configure the minimal information needed for global communication. It is done in a “stateless” manner, that is outside entities do not hold states on the configured node, configuration is done autonomously. Information, such as prefix for the network is gathered from router advertisements.

Stateless configuration – if enabled – assigns address to any interface, connected to the network. Naturally, a well managed network should not allow arbitrary (possibly illegal) hosts to connect, but stateless autoconfiguration has no features to selectively enable for only chosen nodes.

As a consequence, secure networks will want to use stateful autoconfiguration. Stateful configuration is usually done via DHCPv6; it is not really different from IPv4. However it is still debated, whether DHCP should supply general information (gateway, DNS server, etc.) only, and addresses should be autoconfigured, or DHCP should supply all, including address information. While the relevant RFC describes the later case, there is still no complete implementation.

The Neighbor Discovery (ND) Protocol [11] is responsible for router and prefix discovery, duplicate address detection, neighbor reach ability and link-layer address determination. ND’s function is similar to IPv4’s ARP and some ICMP functions. The autoconfiguration mechanisms depend on ND. The greatest advantage of ND and IPv6 autoconfiguration on IPv4 is that they are entirely IP based, as opposed to IPv4 ARP or DHCP that are link-layer protocol dependent. As a consequence IPSec AH or ESP could be used to authenticate or secure these protocols. While it is possible, currently this is not the practice. The reason is that it requires manual keying of IPSec, which is a tedious job.

Despite this, autoconfiguration and ND can still be considered more secure than their IPv4 counterparts. The reason is, that while they are not cryptographically secure (without IPSec), they contain some added measures (for example TTL value of 255, against outside sourcing of ND packets or Duplicate Address Detection [DAD]) to counteract some kinds of attacks.

ND can be attacked in various ways, by forging ND packets. These packets can interfere with neighbor discovery, resulting in causing unreachability for certain nodes. Fake reply to duplicate address detection can result in failed DAD, and as a result, failed autoconfiguration. Spoofed router advertisements can divert traffic to the attacker to perform man-in-the-middle, etc, attacks, or to another host, resulting in denial of service by flooding with traffic.

However, the way ND operates, these attacks may only be performed by nodes on the same network segment, which mitigates their effect. Operators of such networks, where nodes are not trusted, should apply some kind of protection against these attacks.

3.4. Performance improvements

Performance improvements indirectly affect IPv6 security. These improvements are comprised of several measures: hierarchical addressing, simplification of the header, option headers and lack if in-transit fragmentation.

From security point of view, the header changes are important. The IPv6 header is much simpler than the IPv4 header, and has a fixed size. This simplifies header processing. All optional parts have been moved to option headers, which are chained after the each other. There are different option headers, those that are relevant to end nodes only, and those that should be processed by every node (routers). The order of the option headers is such that endpoint options are at the end of the chain, thus routers do not have to inspect them, while processing the packets.

3.5. Mobility

Mobility is a complex function of IPv6, involving several entities (mobile host, home agent etc.). The benefits for mobile computing are apparent in quiet a number of aspect of the IPv6 protocol design, and go beyond merely providing dial-up support for road worries. The improvements in option processing for destination option, autoconfiguration, routing headers, encapsulation, security, and any cast addresses all contribute to the natural design of mobility for IPv6. In fact, some satellite work in Europe is already starting to become IPv6 based. The IPv6 mobility advantages my be further emphasized by combining flow label management to provide better Quality of Service to mobile node.

Even the normal operation of mobility raises several security questions, such as authentication and authorization of the mobile host in a foreign network. Because mobility uses option headers to store the “real” address of a mobile host, while using the “mobile” address in the IPv6 header, it may be involved in address spoofing attacks. By supplying false information to the home agent, legitimate traffic may be diverted. Mobility is not generally employed, and usually not by default, so should not affect normal networking. When using mobility, network operators have to be very careful to properly apply filtering and monitoring.

Transition issues

When IPv4 was introduced, it happened virtually overnight. Because of the enormous number of hosts, IPv6 can only be introduced gradually. During the design of the new protocol, considerable care was given to the transition from IPv4.

There are many transition scenarios, and many mechanisms to use in these scenarios. There are 3 main types of transition mechanisms:

- *Dual stack methods* – dual-stack nodes “speak” both protocols and use the appropriate one for communication. Dual stack can not be used to communicate between at IPv6 only and an IPv4 only node.
- *Translation methods* – protocols or packets are translated to an other protocol.
- *Proxy* – application level proxies translate from one protocol to the other.

Transition presents many security challenges either directly by themselves the methods, or indirectly in connection with the networking environment.

Dual stack methods employ the two protocols, depending on the protocol used by the communicating nodes. This basically means of heaving – at least partly – parallel infrastructure, with the added security problems of both protocols. Because in most dual stack methods the two protocols are independent, it may lead to confusion, and possible attack, when supplying different information on different protocols. For example having a web page or DNS server that differs depending on the protocol used may trick users into trusting information that they should not otherwise trust. This problem usually occurs on that implementation, that has IPv6 enabled by default, or when an upgrade enables it. For examples Service Packs 1, when installed on Microsoft Windows XP, will list IPv6 amongst the available protocols [4], where users may enable it even by accident. Network operators should watch for these cases and educate users.

The tunneling methods in general present problems, since one protocol is encapsulated in another. This can not only prevent the easy inspection of the tunneled traffic (firewalls, IDS tools), but is susceptible to traffic injection attack.

At the network border ingress filtering is usually performed. For example, packets originating from outside network should not have source address from the inside address range (address spoofing). Spoofed addresses can lead to various attacks to nodes that trust the packet as originating from the inside network.

In the case of tunneled traffic, an attacker can create an IPv4 packet containing an IPv6 packet with spoofed address. The gateway accepts the IPv4 packet, because it does not have to have a spoofed address. After decapsulation, the IPv6 packet is inserted into the internal network. The attack is possible, if the gateway does not perform filtering on the IPv6 packet also. This is a common configuration mistake. There are several tunneling methods, which may be vulnerable to traffic injection attack, if not configured properly.

Some tunnel methods, most notably Teredo has impact on IPv4 security infrastructure. Teredo (formally known as Shipworm) proposes a mechanism that tunnels packets over user datagram protocol (UDP) to bring IPv6 connectivity to IPv6 nodes located behind IPv4 NATs. To run the services, a network needs Teredo services, which are stateless and manage only a function of the traffic between Teredo and the Teredo relays that act as IPv6 routers between the service and the native IPv6 internet. Teredo will likely be used only as a last resort, where IPv4 NATs prevent other mechanisms from working.

Translation methods, because they employ address, header or protocol transformation, may be sensitive to using spoofed addresses or malformed packets. Networks that employ these methods, should take proper precautions to filter traffic. These methods usually create some kind of bottleneck in networks, which may be affected by denial of service attack, or degradation of performance from overload.

Proxy methods work on the application level, and thus do not usually have problems associated with lower level protocols. Because they are, by their nature, limited to specific applications, they are rarely used alone, rather in conjunction with other translation methods.

Implementations and applications

The majority of security incidents are caused by Implementation and not design errors. For example buffer overflow, off-by-one, etc. problems are created by programming errors. Thus it is crucial for IPv6 to not only have secure design, but secure implementations also.

Every major vendor has IPv6 implementation, many of which are in daily use in research and in production networks. Several ISPs (many of them in Japan and Korea) offer IPv6 services. Even though not every implementation is mature, and it will take time while they are debugged and optimized. This means that initially IPv6 will, in fact cause more problems, because of implementation errors, and later on will the more secure design balance and then override them.

The case is the similar with the applications. Initial introduction can present buggy applications, but as application transition usually means revising the application, it may lead to better quality code.

Some important security applications are yet to be developed, namely IPv6 firewalls, IDS tools, network management tools are still in an infant stage.

Probably, the increasing number of IPv6 enabled networks will lead to increased number of security incidents (which have already happened) and it will force vendors to create the necessary tools.

4. Conclusion

To summarize, IPv6 has several new features, which have effect on network security. IPv6 does not provide radically new security measures, but there are small improvements, that, if used appropriately, can change the security in a positive way.

Probably the most crucial part in IPv6 security is the transition, were the old and the new protocol have to exist side-by-side sometimes supported by very complex transition mechanisms.

Because IPv6 is still at the very early stages on introduction, it is still too early to tell, if IPv6, just by itself will enhance IP security. However, it is clear, that one can expect several problems and vulnerabilities to surface, which, given a suddenly accelerating rate of introduction may lead to critical situations. On the long term we expect IPv6 to have an overall better security then IPv4 has.

7. References

[1] S. Bradner, A. Mankin, "IP: Next Generation (IPng) White Paper Solicitation", RFC 1550, December 1993.,

[2] Wang Jilong, Ni chunsheng, Wu Jianping “Next Generation Internet” 2004 IEEE proceedings of the 7th International Symposium on Parallel Architecture, Algorithms and Networks(ISPAN’04). IEEE comp. society press.

[3] Szabolcs Szigsti, Dr.Peter Risztics ”Will IPv6 bring better security?” Proceedings of 30th EUROMICRO Conference (EUROMICRO’04), [4] Joseph Davies “Understanding IPv6” Microsoft press.

[5] Deering, S., and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, December 1998.,

[7] Steve King, Ruth Fax, Dimitry Hasking, Wen Ken Ling, Tom Meehan, Robert Fink, Charles E.Perkins “ DEC 1999. The case for IPv6”

[8] D. Johnson, C. Perkins, J. Arkko, "Mobility Support in IPv6", RFC 3775, June 2004.,

[9] T. Chown, "IPv6 Implications for TCP/UDP Port Scanning" Internet Draft, draft-chown-6ops-port-scanning-implications-00. October 2003., Work in progress.

[10] P. Savola, "Firewalling Considerations for IPv6" Internet Draft, draft-savola-v6ops-firewalling-02.txt October 2003., Work in progress.

[11] T. Narten, E. Normark, W. Simpson, "Neighbor Discovery for IP Version 6", RFC 2461, December 1998.,