In-depth Analysis of IPv6 Security Posture

Abdur Rahim Choudhary
Scientist, Serco North America
12012 Sunset Hills Rd, Suite 600
Reston, VA 20190, USA
01-301-262-3224
rahim.choudhary@serco-na.com

ABSTRACT

The version 6 of Internet Protocol (IPv6) is being gradually deployed worldwide. This paper analyzes the security of IPv6 protocol. is the analysis concludes that serious security vulnerabilities exist that are IPv6 specific. Therefore additional security measures are needed and more capable security management tools are required in IPv6 networks in order to achieve a security posture at parity with that of the IPv4 networks.

1. INTRODUCTION

The version 6 of Internet Protocol (IPv6) is the next generation protocol that is gradually being deployed worldwide. Hence the understanding and mitigating the IPv6 security challenges has become a pressing need [1]. This paper provides an in depth analysis of the IPv6 security posture, i.e. the security enhancements and vulnerabilities that are present in IPv6 networks that arise specifically from the changes that were made in IPv6 specification compared to IPv4.

The version 4 of IP (IPv4) was specified in 1981 via the Internet Engineering Task Force (IETF) Request For Comments (RFC) number 791. It was designed on an experimental basis to connect computers in a way resilient to faults in the connecting links. There was no expectation that it would be used world-wide with hundreds of millions of installations. However the protocol was designed with simplicity and foresight and it served extremely well for nearly thirty years. IPv4 uses a 32 bit field for the IP address, thus allowing 2^{32} addresses, i.e. 4,294,967,296 different addresses. This was considered large enough to allow all users to have IP addresses if they wished. Even today there are not four billion installations of IPv4 addresses. However, there is an explosion of ideas where IP networks might be used, such as net-centric operations concept [2], sensor networks, technologies like the Radio Frequency Identifiers (RFID), home appliances like televisions, personal digital assistants, mobile phones and automobiles. Therefore a very large number of addresses will be needed in the future and under the present allocation schemes the IPv4 addresses available for allocation will deplete by 2012 [3]. Hence IPv6 was specified in 1995 via the RFC 1883 which was soon superseded by RFC 2460 [4] in 1998. It provides a 128 bit address field resulting in 3.4×10^{38} addresses.

This paper takes a critical look at the security posture of this IPv6 specification and the associated specifications that are needed for its operations. The paper identifies the new IPv6 specific security vulnerabilities and also suggests mitigation steps for them. The purpose of this analysis is: (a) to warn the users of the new security challenges posed by the IPv6 protocol and to suggest the minimal mitigation steps; (b) to emphasize the need for the users to test the IPv6 products for correct implementation and the inclusion of the suggested mitigations for the identified vulnerabilities; (c) and for the vendors to ensure that they implement the needed security features including the identified mitigations for the vulnerabilities discussed in this paper.

2. Changes in IPv6 compared with IPv4

The analysis of the IPv6 security posture is based on the changes that were made in IPv6 specification compared with the IPv4 specification. The main reason for the introduction of IPv6 was the expansion of the available address space, so that a 128 bit address field was specified allowing 2^{128} different addresses. In addition, some IPv4 operational lessons learned were also incorporated into the specification of IPv6. Following are the major changes made in defining IPv6 with respect to IPv4.

1. IPv6 uses a 128 bit address space versus a 32 bit address space in IPv4. The large address space makes it impractical to perform brute force scanning for IPv6 addresses. This stops the attackers from performing port scanning and finding out vulnerabilities in a network node. On the flip side, it also disallows the administrators to perform topology mapping using similar scans.
2. IPv6 requires that all packet fragmentation and reassembly be performed by the sender and receiver hosts. Three of the fields in the IPv4 packet header dealt with the packet fragments, namely fragment offset, (fragment) flags, and (fragment) identification. These fields were removed. The IPv6 routers no longer

Digital Object Identifier: 10.4108/ICST.COLLABORATECOM2009.8393
http://dx.doi.org/10.4108/ICST.COLLABORATECOM2009.8393

perform packet fragmentation and reassembly., which enhances the router performance. It also eliminates fragmentation related attacks on the routers. However, the fragmentation related attacks are still possible against the receiving hosts, as well as the security devices (firewalls, IDS/IPS) which still must perform packet reassembly for deep packet inspection.

3. A new capability was introduced in IPv6 to automatically configure IP addresses on new nodes, which reduces the administrative burden of manually configuring them. A set of new protocols, called the Neighbor Discovery (ND) protocols, were defined for this purpose. The new capability is referred to as Autoconfiguration capability which lets IPv6 appliances behave in a plug-and-play fashion. This capability was deemed necessary also for the future IPv6 applications with a large number and variety of IPv6 devices. However, the trust model used by Autodiscovery is too trusting to be secure. Therefore new protocols called the Secure Neighbor Discovery (SEND) was defined to avoid spoofing related and other attacks.
4. The above two changes meant that the use of Internet Control Message Protocol (ICMP) was now required, versus its optional use in IPv4. Because the use of ICMPv4 in IPv4 was not necessary for the basic IPv4 functions, network administrators often could block all ICMPv4 messages to secure the networks. The same blanket blockage is however not possible for IPv6 networks because IPv6 operations like Path MTU discovery and Autoconfiguration do not work without the use of ICMPv6 messages.
5. Support for extension headers is required in IPv6 networks. According to the IPv6 specification [4] a full implementation must include support for the following six extension headers: hop-by-hop options header, destination options header, routing header, fragment header, authentication header (AH), and encapsulating security payload (ESP) header. The last two headers are the components of IP security (IPsec) the support for which is therefore required under IPv6 specification. Subsequently this support was somewhat weakened when, the IPv6 security architecture [6] downgraded the requirement for the support of AH from MUST to MAY.

3. Security Posture of IPv6

The changes described above form the basis for security advantages and disadvantages of IPv6.

The support for IPsec in IPv6 at the specification level has sometimes been interpreted, though incorrectly, to mean that IPv6 is more secure than IPv4. In reality the use of IPsec is equally available for both protocols. The practical difficulties in both cases stem from the need for a key management infrastructure (KMI) that is necessary for the use of IPsec. However KMI requires complicated trust relationships and key management operations which are not adequately supported in most implementations. Today a consensus view is that IPv6 is neither more secure nor less secure than IPv4 [7]. This view also is rather cursory. The in-depth analysis in this paper will clarify the security posture of IPv6 compared to the same for IPv4.

As has been analyzed in references [8, 9] most of the vulnerabilities are common between IPv4 and IPv6. Vulnerabilities specific to IPv4 and IPv6 do exist and these are further analyzed in sections 4 and 5. The purpose of this analysis is to go beyond the broad consensus view and present a detailed picture of the relative security postures of the two protocols. The results will show that:

- The emerging IPv6 networks should be protected against all attacks for which IPv4 networks are currently protected.
- The IPv6 networks should additionally be protected against new attacks that are specific to new features of IPv6 such as the Path MTU discovery, Neighbor Discovery, and the required use of ICMPv6, etc.

This situation implies two things. If the same security model is used for both IPv6 and IPv4 networks, namely the perimeter-based security model, then IPv6 networks require additional security measures and security tools with additional capabilities in order to achieve a security posture at parity with IPv4. Alternately a different security model may be used for IPv6, for example the end-to-end security model that uses host based security and policy based management. Such a model will be presented in future [10].

4. Vulnerabilities specific to IPv4

There are three areas where IPv6 offers security enhancements, namely dropping the requirement on the IPv6 routers to perform packet fragmentation and reassembly, a large address space that makes the brute force scanning impractical, and an end-to-end addressability that makes the use of Network Address Translation (NAT) unnecessary. These three areas also correspond to three vulnerabilities that are IPv4 specific.

4.1 Fragmentation and Reassembly Vulnerabilities

Fragmentation and reassembly of packets is required for IPv4 routers while the IPv6 routers do not performed this function. The vulnerabilities due to this requirement on the routers are therefore unique to IPv4. These vulnerabilities have been analyzed in literature and filtering guidance is provided for their mitigation [11]

The fragmentation related DoS attacks are, however, still possible against the IPv6 end hosts which are now required

Digital Object Identifier: 10.4108/ICST.COLLABORATECOM2009.8393
http://dx.doi.org/10.4108/ICST.COLLABORATECOM2009.8393

to perform all packet fragmentation and reassembly. The form of these attacks is the same for both protocols. An example of the DoS attack in IPv6 is by sending a large number of fragmented packets to the end host without including a terminating last fragment packet. Such DoS attacks are also possible against IPv6 security devices, e.g. the firewalls and intrusion detection and prevention systems. These devices need to reassemble the fragmented packets in order to perform deep packet inspection to apply packet filtering security policy and to perform signature analysis.

The conclusion is that, while the IPv6 routers do not suffer from the fragmentation attacks, the IPv6 end hosts and intermediate IPv6 security devices do suffer from these attacks. Mitigation measures therefore still need to be deployed in IPv6 networks.

4.2 Ease of Port Scanning

IPv4 addresses and ports can be scanned using brute force methods because all the 2^8 addresses in a class C IPv4 subnet can be scanned in a reasonable amount of time, say of the order of 5 minutes,. This ease of port scanning in IPv4 is another vulnerability that is specific to IPv4. A corresponding vulnerability does not exist in IPv6 because the number of possible addresses (64 bit interface IDs allows 2^{64} distinct addresses) in a subnet is too large to be scanned in a reasonable length of time. The flip side to this advantage of IPv6 is that the administrators can also not do a brute force scan for topology mapping.

This advantage is only possible if the IPv6 interface IDs and subnet IDs are randomized. This advantage is lost if an administrator chooses interface IDs in a non randomized deterministic manner, for example using 01 interface ID values for routers. Further, while the brute force methods are not available to discover IPv6 addresses for the purpose of device profiling, alternate methods do exist such as querying the router neighbor discovery cache in poorly secured routers [12]. More methods will likely be discovered by the hackers as the IPv6 networks are deployed. Therefore reliance on the IPv6 address space as a main security measure against device scanning is not recommended.

4.3 Lack of end-to-end connectivity

Because of the IPv4 address depletion, NAT schemes are deployed [13]. The use of NATs breaks the end-to-end addressability and connectivity. This causes problems in deploying IPsec in IPv4 networks with NAT, and security problems with UDP traffic. Please see the reference [14] for a detailed discussion of applications that break because of NAT.

Another security limitation of NATs is in the application of enterprise wide security policies. These policies can not be pushed to the nodes that are behind a NAT by a centrally controlled policy server located outside the NAT. This is because, in general, only that traffic can reach a node behind NAT that was originated by the node.

The NAT mechanisms provide 'security through obscurity' as a side benefit to its main purpose. There are IPv6 mechanisms that would enable the same security benefits without the use of NAT [16].

5. Vulnerabilities specific to IPv6

Security vulnerabilities that exist for IPv4 also generally apply to IPv6 [17, 18]. This section analyzes additional vulnerabilities that exist for IPv6 but do not apply to IPv4. These fall in three major categories: vulnerabilities due to basic protocols for IPv6, vulnerabilities for the protocols that facilitate the transition of an IPv4 network to IPv6 network, and protocol related vulnerabilities in IPv6 operations. Each of these categories is analyzed in the following subsections, in the light of the discussion in reference [20]. Well known IPv6 vulnerability for routing header of type zero [21] is not included, because the type zero routing header has since been deprecated [22].

5.1 IPv6 Basic Protocol Vulnerabilities

The changes made from IPv4 header to IPv6 header that were discussed in section 2 can potentially cause security issues. Some features that cause significant security issues are discussed below.

5.1.1 Extension Headers

Extension headers in IPv6 can be chained, meaning one extension header points to another resulting in a chain of extension headers between the main IPv6 header and the transport header. This chain of extension headers can be long for multifold reasons. One reason is the ambiguity in the specification [4] itself. There are six extension headers currently defined, with more possibly defined in the future. The specification *recommends* that "Each extension header **should** occur at most once, except for the Destination Options header which should occur at most twice (once before a Routing header and once before the upper-layer header)". But the specification *requires* that "IPv6 nodes **must** accept and attempt to process extension headers in any order and occurring any number of times in the same packet, except for the Hop-by-Hop Options header which is restricted to appear immediately after an IPv6 header only".

The chain of the extension headers can repeat when an IPv6 packet is encapsulated in another IPv6 packet which can then have its own chain of extension headers.

An attacker can use a long chain of headers to make it difficult for the security devices to get to the transport layer header for deep packet inspection. The difficulty increases considerably if a malicious node also uses packet fragmentation, thus forcing the security devices to reassemble them before deep packet inspection and

Digital Object Identifier: 10.4108/ICST.COLLABORATECOM2009.8393
http://dx.doi.org/10.4108/ICST.COLLABORATECOM2009.8393

security signature and anomaly analysis can be performed. Such packets can potentially evade inspection by the perimeter security devices, depending on the level of sophistication of these devices.

Such techniques by the attackers are compliant with IPv6 specification so that the routers can not stop them. Well deliberated security policies are needed to mitigate such vulnerabilities through special filtering and anomaly analysis. Following mitigation measures should minimally be applied: (a) unusual headers order, (b) unusual header repetition, (c) fragmented packets, (d) small packet sizes (especially smaller than 1280 bytes), (e) IPv6 in IPv6 encapsulation, (f) excessively large number of options in a hop-by-hop option header, (g) invalid options, and (h) monitoring non zero-filled padding bytes (see section 5.3).

In addition, there are security issues in the individual extension headers. For example, the specification does not limit the hop-by-hop extension header with respect to the number of hop-by-hop options. Further, any option can appear multiple times. An attacker can use the situation by employing inconsistent option values, or by inserting invalid options. 'Parameter Problem' ICMPv6 error messages are issued to the sender in such situations. An attacker can burden the routers by flooding with such maliciously crafted packets, causing a DoS attack. In order to mitigate these vulnerabilities, security policies are needed to handle packets with inconsistent parameter values, invalid parameters, or repeated options and unusual option values in hop-by-hop options header.

5.1.2 Packet reassembly by security devices

The security devices must by necessity reassemble the fragmented packets and parse the extension headers in order to perform deep packet inspections. For example, a firewall must reach the transport layer header to apply the transport layer protocol and port number filtering rules. However both these functions are inconsistent with the IPv6 specification [4]. The specification asserts that (a) the intermediate nodes not perform packet reassembly, and (b) the intermediate nodes not process the extension headers except the hop by hop extension header. Thus the protocol does not attend to the needs of the perimeter security devices that are deployed as intermediate nodes. Further, the need to reassemble fragmented packets exposes the security devices to the same type of attacks as are known for IPv4 [23].

There is also a legitimacy issue here. The security devices may decide to drop or redirect suspicious packets, but the legitimacy of such actions by the intermediate nodes is unclear because the specification states that only the hop-by-hop header is processed by the intermediate nodes and packet reassembly is performed only by the end hosts.

5.1.3 Autoconfiguration

State-Less Address Auto Configuration (SLAAC) [24] is a distinguishing feature of IPv6. However, SLAAC also raises serious security concerns.

One of the concerns about SLAAC is its trust model with respect to the network trusting the node [25]. A node can acquire a link-local address without any approval or control. The new node is therefore allowed an unchecked access to the link. This unchecked access is not limited to the local link because a node can acquire a global prefix using node solicitation and router advertisement ICMPv6 messages for Neighbor Discovery (ND) [26]. Combining the global prefix with the link local address, the node can construct a globally routable address and start using it without any approval or control. This trust model introduces serious security vulnerabilities and possibilities of attacks. Following are the examples [25] of the types of attacks that are possible on the autoconfiguration feature of IPv6.

- *Malicious router*: A node can maliciously decide to serve as a router on the link. That means it will start sending router advertisements and start responding to node solicitations. An unsuspecting node can select the malicious router as its on-link router. The malicious router can then siphon traffic from the host, mount a man in the middle attack, and issue redirect messages.
- *Attack on legitimate router*: A malicious node can attack the legitimate on-link router. It can spoof the address of the legitimate router and issue a router advertisement with a zero router lifetime. That will make the legitimate router unavailable. Alternately the malicious node can attack the legitimate router to reconfigure it.
- *Bad prefixes*: A malicious router can advertise bad prefixes, that is prefixes that are not on the link. Hosts that autoconfigure themselves with that prefix will have an invalid address. Alternately the rogue router can announce an external address to be on-link, thus making that external address unreachable by the hosts on the link. That is because a host will think the address is on link and it will not send the packet to the router, rather it will try to perform address resolution by sending neighbor solicitations which will not be responded to.
- *Failure of DAD and NUD processes*: A malicious node can falsely respond to DAD requests and prevent a new node from joining the link. That is because the malicious node can respond to all DAD requests by claiming that it is already using the requested address, and thus prevent the node from acquiring a link local address. Similarly, a malicious node can falsely

Digital Object Identifier: 10.4108/ICST.COLLABORATECOM2009.8393
http://dx.doi.org/10.4108/ICST.COLLABORATECOM2009.8393

respond to neighbor unreachability detection (NUD) messages, thus causing the failure of the NUD process.

- *A non existent address*: An external host can send traffic to legitimate looking addresses but with invalid interface ID. The router will try to resolve these addresses and fail. The router will therefore spend resources on resolving invalid addresses, and possibly be the victim of a DoS attack. Given the vastness of the address space in IPv6, it is not difficult to guess the non existent addresses for this type of DoS attack.

A variety of approaches are required to mitigate these risks. The on-link ND messages should be filtered at the boundary [25]; the SEND protocol [27] should be used to avoid attacks that use address spoofing; and link layer filtering [28] should be applied. The cryptographically generated addresses (CGA) used by the SEND protocol don't provide authentication, however. An authentication method is needed in the mobile ad-hoc networks (MANet) that are one of the most promising applications of the autodiscovery feature of IPv6. Further, the nodes in MANet networks are often battery and compute power limited so that cryptographically intense calculations may not be feasible. This security issue remains unmitigated.

5.1.4 DNS updates

Once the address is acquired, a corresponding DNS entry may need updating. This update can use Dynamic DNS (DDNS) which has its own security issues though they are common to both IPv4 and IPv6. However, SLAAC operation requires that the individual nodes, not just the DHCP servers, be able to update the DNS entry which introduces a scaling problem for the DDNS security mechanisms. For example, if IPsec security associations are used between the node and the DNS, the number of security associations needed for securing communications from all autoconfiguring IPv6 nodes may be too large to manage. The scaling problem is made worse if the nodes use privacy addresses that change periodically requiring frequent updates to DNS entries, especially if the rate of address change needed for privacy is rapid.

5.1.5 Multiple Addresses

IPv6 allows the assignment of multiple addresses to an interface. However this feature complicates the filtering rules, for example in the firewalls and access control lists. This is because, unlike IPv4, address based filtering is no longer very feasible because all addresses assigned to all interfaces on a node will need to be included to block a node: and this is not feasible when these addresses are autoconfigured and for privacy reasons they change at some desired rate. In such cases, a firewall will need to learn all the addresses dynamically and the filtering rules will need to be automatically generate-able using sophisticated policy rule-sets. Such capabilities are not currently available. Therefore simpler formalisms must be employed that use some kind of identification tokens instead of addresses in order to identify a host or an interface. No standard identification mechanisms currently exist at OSI layer 3. This makes the implementation of a security policy difficult. It also adds to the complexity of the firewall requirements that the vendors need to incorporate. Multicast and anycast addresses also make the address based filtering more difficult to configure.

5.1.6 ICMPv6 Filtering

ICMP use in IPv4 is optional and not required for normal network operation. Many IPv4 network administrators therefore may block ICMPv4 messages for security reasons. This blanket blocking is not possible for IPv6 networks because IPv6 network operation require the use of ICMPv6 messages as illustrated by the following examples:

- The discovery of Path Maximum Transmission Unit (PMTU) requires a "Packet Too Big" response in an ICMPv6 message. This helps the sender to either send smaller packets or to fragment them.
- An invalid option in the hop-by-hop options header requires the routers to send a "Parameter Problem" response to the sender in an ICMPv6 message. The sender can then either correct the option in the retransmission or not use it if the router generated the "Parameter Problem" message because of an unrecognized option.
- SLAAC requires ICMPv6 solicitation and advertisement messages for its operation.
- SEND requires ICMPv6 for solicitation and advertisement messages as well as for authentication and certification path messages.

Because of the essential role of ICMPv6 in IPv6 networks a blanket filtering of ICMPv6 messages is no longer possible in IPv6. The firewalls must allow specific ICMPv6 traffic, complicating the filtering policies and mechanisms [29].

IPv6 sends the ICMPv6 messages to unicast as well as multicast addresses, thus presenting a potential for DoS attack through packet amplification. Using a deliberately malformed packet an attacker can cause error responses that spuriously utilize network resources, especially when the error response is sent to a multicast address. The attacker can in addition use a spoofed address, directing the amplified error messages to the victim of a DoS attack. Thus a node can be attacked by spoofing its address on a crafted packet that is sent to a multicast destination.

Digital Object Identifier: 10.4108/ICST.COLLABORATECOM2009.8393
http://dx.doi.org/10.4108/ICST.COLLABORATECOM2009.8393

5.2 Vulnerabilities in IPv6 Transition Mechanism Protocols

The discussion above will show that IPv6 networks substantially have all the security vulnerabilities that exist for IPv4 networks; in addition, the IPv6 protocol presents serious security vulnerabilities of its own which are not present in IPv4.

However, IPv6 and IPv4 networks need to coexist for the duration of the transition from IPv4 to IPv6. This requires transition specific protocols that bring into the networks their own security vulnerabilities. Two basic transition mechanisms that are widely adopted are the dual-stack mechanism and the tunneling mechanism [30]. The latter encapsulates IPv6 packets within IPv4 packets.

Security analysis of the dual stack at the protocol level has not been done because dual stack specific protocols are few. However, dual stack transition shares all the vulnerabilities of a native IPv6 or IPv4 network. In particular, it is vulnerable to the security weaknesses of the IPv6 protocol that were discussed in this section. There is a potential for additional vulnerabilities because of a security sensitive interaction between the two protocols. Recently there has been a protocol for dual stack mobile IPv4 [31] but its security vulnerabilities are not yet analyzed. However, this protocol uses tunneling of IPv6 in IPv4 and can be susceptible to security risks associated with tunneling, which are discussed below.

The specification for tunneling IPv6 via IPv4 [32] has been analyzed for security issues [33]. These attacks are made possible because all 6to4 capable routers regard other 6to4 routers and relays as "on-link". Therefore a 6to4 router must accept traffic from all other 6to4 routers and relays, and a 6to4 relay must accept traffic from all 6to4 routers. This assumed trust between the 6to4 routers and relays leads to DoS attacks that can be directed at the 6to4 networks, IPv4 networks, or IPv6 networks. In addition, there is a "meta-threat" in which case some other attack is laundered hidden into the 6to4 traffic. The tunneling encapsulation may also provide a way to evade access controls based on destination address. To mitigate these risks it is recommended that 6to4 tunnel traffic be filtered at the edge of the domain with the public Internet and other untrusted domains.

5.3 IPv6 Protocol Related Operational Vulnerabilities

For the purpose of the discussion in this paper, the protocol related operational vulnerabilities refer to situations that occur because of certain operational behavior of the network under the protocol specifications. The discussion does not include vulnerabilities because of the deficiencies in implementation or errors in configuration. That is because the security issues related to the protocol implementation and the device configuration are not inherent to the protocol, and the discussion in this paper is at the level of the protocol specification.

One such issue is with respect to the possibility that the padding options be used to communicate covert channel information. Both protocols use padding to align boundaries. However, IPv6 makes a greater use of them through the currently defined Pad1 and PadN options. The specification requires that these padding bytes be zero filled. However there is no requirement for the receivers or the routers to verify that they are zero filled. Therefore, if the padding bytes are not all zero filled they may serve as a covert communication channel. It can also happen if the padding bytes are zero filled and yet the pattern in which Pad1 and PadN options are used may itself communicate covert channel information.

Another concern is the complexity of IPv6 filtering compared to the same for IPv4. The causes of complexity include the extension header chains, the essential use of ICMPv6, and the need to tunnel IPv6 in IPv4. Though by itself it is not a security vulnerability, the complexity can lead to erroneous operations because it may cause ambiguity is defining and interpreting IPv6 security policies

There is a possibility that new extension headers will be added to the IPv6 specification. The new extension headers will likely have an impact on the security policy of an enterprise. After the security policy has been formulated and deployed, the new extension header will make it necessary to revise the security policy, its deployment, and the selection of the security tools. Such need for periodic revisions can cause security uncertainty in IPv6 operations until the revision analysis is complete and the new security policy is successfully deployed.

6. Conclusions

This paper has presented an in-depth analysis of the IPv6 protocol security posture. It has identified IPv6 specific security vulnerabilities that are not present in IPv4 and has suggested the needed mitigation steps. In order to achieve security parity with IPv4 networks, the emerging IPv6 networks should be protected against all attacks for which IPv4 networks are currently protected; and they should additionally be protected against new attacks that are specific to new features of IPv6 such as the Neighbor Discovery, State-Less Address Auto Configuration, and the essential role of ICMPv6.

These results can be used in three essential ways: (a) to provide a caveat regarding the new security challenges posed by the IPv6 protocol; (b) to stress the need to incorporate the minimal mitigation steps that are suggested

Digital Object Identifier: 10.4108/ICST.COLLABORATECOM2009.8393
http://dx.doi.org/10.4108/ICST.COLLABORATECOM2009.8393

in this paper; (c) to emphasize the need for vendor-independent testing of the IPv6 products for correct implementation and the inclusion of the suggested mitigations for the identified vulnerabilities; and (d) for the vendors of the IP security management tools to ensure that they implement the additional security features.

References

[1] Caecedo, C. E., Joshi, J. B. D., and Tuladhar, S. R., "IPv6 Security Challenges", Computer Vol 42, pp. 36-42, 2009.

[2] M. Fewell and M.G. Hazen Network-Centric Warfare: Its Nature and Modelling, Defence Science and Technology Organisation, Australia. DSTO Research Report 0262, September 2003

[3] Geoff Huston, "IPv4 Address Report", automatically generated report on potaroo.net/tools, June 8, 2009.

[4] IETF RFC 2460, "Internet Protocol, Version 6 (IPv6) Specification", December 1998.

[6] IETF RFC 4301, "Security Architecture for the Internet Protocol", December 2005.

[7] Joseph Klein Sr (moderator) "Securing IPv6 Networks", panelists Ron Broersma, Bob Scott and Dave Rubal, panel discussion at Military Communications (MILCOM) 2008.

[8] Lancaster, Troy, "IPv6 and IPv4 Threat Review with Dual Stack Considerations", COMP6009: Individual Research Project, University of Southampton, Department of Electronics and Computer Science, UK, 2006.

[9] Convery, Sean and Miller, Darrin, "IPv6 and IPv4 Threat Comparision and Best Practices Evaluation (v1.0), Cisco Corporation, 2004.

[10] Choudhary, A. R., "A New Security Model for IPv6 Networks", work in progress for a 2010 publication.

[11] IETF RFC 1858, "Security Considerations for IP Fragment Filtering", October 1995.

[12] C. Zou et al., "Routing Worm: A Fast Selective Attack Worm Based on IP Address", Proceedings of the 19th ACM/IEEE/SCS Workshop on Principals of Advanced and Distributed Simulation (PADS), June 2005.

[13] IETF RFC 2663, "IP Network Address Translator (NAT) Terminology and Considerations", August 1999.

[14] IETF RFC 3027, "Protocol Complications with the IP Network Address Translator", January 2001.

[16] IETF RFC 4864, "Local Network Protection for IPv6", May 2007.

[17] Lancaster, Troy, "IPv6 and IPv4 Threat Review with Dual Stack Considerations", COMP6009: Individual Research Project, University of Southampton, Department of Electronics and Computer Science, UK, 2006.

[18] Convery, Sean and Miller, Darrin, "IPv6 and IPv4 Threat Comparison and Best Practices Evaluation (v1.0), Cisco Corporation, 2004.

[20] IETF RFC 4942, "IPv6 Transition/Coexistence Security Considerations", September 2007.

[21] Biondi, P. and A. Ebalard, "IPv6 Routing Header Security", CanSecWest Security Conference 2007, April 2007. http://www.secdev.org/conf/IPv6_RH_security-csw07.pdf

[22] IETF RFC 5095, "Deprecation of Type 0 Routing Header in IPv6", December 2007.

[23] IETF RFC 1858, "Security Considerations for IP Fragment Filtering", October 1995.

[24] IETF RFC 4862, "IPv6 Stateless Address Autoconfiguration", September 2007.

[25] IETF RFC 3756, "IPv6 Neighbor Discovery (ND) Trust Models and Threats", May 2004.

[26] IETF RFC 4861, "Neighbor Discovery for IP version 6 (IPv6)", September 2007.

[27] IETF RFC 3971, "SEcure Neighbor Discovery (SEND)", March 2005.

[28] IETF Internet Draft draft-nward-ipv6-autoconfig-filtering-ethernet-00, March 4, 2009.

[29] IETF RFC 4890, "Recommendations for Filtering ICMPv6 Messages in Firewalls", May 2007.

[30] IETF RFC 4213, "Basic Transition Mechanisms for IPv6 Hosts and Routers", October 2005.

[31] IETF RFC 5454, "Dual-Stack Mobile IPv4", March 2009.

[32] IETF RFC 3056, "Connection of IPv6 Domains via IPv4 Clouds", February 2001.

[33] IETF RFC 3964, "Security Considerations for 6to4", December 2004.

Digital Object Identifier: 10.4108/ICST.COLLABORATECOM2009.8393
http://dx.doi.org/10.4108/ICST.COLLABORATECOM2009.8393