Volume 3, Issue 5, May 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Outline of Ipv6 Topology and Best-Practice Security Rules

Abdul Raheem Syed
Asst Professor,
Dept of CSE
SNIST, Hyderabad, India.

Kumar Gillela
Asst Professor
Dept of CSE
MRITS, Hyderabad, India.

Phani Kumar.P
Pursuing M.tech(CS)
Dept of CSE
Mannan IST, Chevella, India.

Dr. C. Venugopal
Professor, PhD (C.S)
Dept of CSE
SNIST, Hyderabad, India.

Abstract*— Because of the transition from IPv4 to IPv6 and certain differences between both IP versions, there are quite some possible security issues. In this paper we try to find how the security of networks is affected by this transition. For this purpose we made a questionnaire to inquire about the general status of the transition in companies which provide services connected to networks (ISPs, security providers, etcetera). Secondly we used practical tests on production networks in order to get an idea about the IPv6 networks in the wild. The questionnaire shows that IPsec is not used more with IPv6 than with IPv4. Furthermore it shows that IPv6 and IPv4 are considered to be equally secure, while the IPv6 appliances used still handle IPv6 in software a lot. The practical tests supported the hypothesis that IPv6 networks are less secure than IPv4 networks. Even though the scale of this study is limited, the results are important because they show that the security of IPv6 still has a long way to go.

Keywords: IPv6, transition, security, network, IPv4 security of IPv6 still has a long way to go.

I. INTRODUCTION

Current networks are mostly based on the IP protocol: the entire internet relies on it for the propagation of information. The currently most used version is IPv4, but this version only allows for approximately 4.3 billion addresses. More than a decade ago, the conclusion was drawn that we would eventually run out of addresses because with allocating addresses, a lot of them were wasted: a block of 65 thousand addresses would be assigned to one company with far less computers. Consequently, in December 1995 the new version was specified: IPv6 [6]. However, back then no one was interested in the new version of the Internet Protocol because most people did not see an immediate need for it. Only in the last few years the IPv6 usage started to grow more rapidly. With the rapidly growing number of machines connected to the Internet, the total number of IPv4 addresses is starting to look a bit bleak. Now that also the worldwide IPv4 address pool is depleted [8], network providers are urged more and more to find solutions for the shrinking amount of addresses, of which one is to migrate to IPv6. Some of the Dutch ISPs have already moved to IPv6 like SURFnet [11] and XS4ALL. Some major other service providers, like Google and Facebook, are integrating IPv6 into their networks and will be testing this worldwide on World IPv6 Day[7]. On that day major organizations will offer their content to world over IPv6 for 24 hours as a test flight.

1.1 Focus of This Paper

When migrating to a different technology certain security issues may arise. The mandatory implementation of IPsec in IPv6 makes some parties think it will be more secure [9]. But this is not necessarily the case: implementing it does not mean using it. Even when using IPsec, there are still attacks possible against such networks [13]. Aside from the mandatory implementation of IPsec, there are other differences between both protocols. An example of this is that the larger address space makes it harder for someone to do reconnaissance attacks [1, 12]. It would take quite some time to scan 2^{64} addresses per network. Another difference between both IP versions is that IPv6 heavily relies on ICMPv6 [1] which makes it harder to setup firewalls to be safe without removing functionality from IPv6, but allowing everything through the firewall can pose a threat. All of these differences might have an impact on security, because they might not be known or fully understood by network administrators or they do not see the immediate threat because IPv6 is not widely used yet. Something else that might have an impact on the security of IPv6 might be that network security devices are not capable of handling IPv6 properly yet, resulting in only partially secured networks. With all those possibilities to have a less secure network, the question which arises is whether IPv6 is more or less secure than IPv4, in practice. This paper will try to answer the question "How does the transition from IPv4 to IPv6 affect the security of networks?" To answer this question, first the following questions will be answered:

- What is the state of the transition towards IPv6 in networks?
- What is the state of the transition towards IPv6 in security products?
- What is the security state of the IPv6 enabled networks and how does this differ from IPv4?

The results will consist of an overview of the current state of the transition to IPv6 'in the wild'. It will be used to test the following hypothesis: "IPv6 is in practice not a more secure protocol than IPv4." In order to answer the above mentioned questions first an analysis of the available literature is made to get an overview of differences between the IP versions and possible security problems. This is discussed in the next section. Secondly a survey was conducted among

companies which work a lot with networks, such as ISPs and hosting providers. This should give an idea about how IPv6 is used and implemented in practice. Lastly the network of the University of Twente has been tested in order to find differences in security between IPv4 and IPv6. The questionnaire and the practical tests are described in section 3 after which the results are described. Finally there will be some discussion about the results and a conclusion will be drawn.

II. STATE OF THE ART

First some functions of IPv6 that are mentioned throughout this paper will be explained and then some research into IPv6 will be discussed.

2.1 IPv6 Functions :

IPv6 makes use of State-Less Address Auto Configuration (SLAAC) to obtain an address if there is no DHCPv6 server on the network. This configuration normally takes the linklocal prefix fe80::/64 as network prefix while the lower 64 bits are populated by expanding the MAC address from 48 bits to 64 bits using modified EUI-64. The reason for taking the MAC address is that they should be unique and thus there should not be collisions. However this is not always the case, so in order to be sure there is no collision it uses ICMPv6's Duplicate Address Detection, which asks to the nodes on the network if this address already exists using a Neighbor Solicitation packet. If it does exist, it stops the autoconfiguration and needs manual configuration, otherwise it uses this address. For global addresses it uses the network prefix the router advertised to the machine instead of the linklocal prefix. This process has been depicted in figure 1.

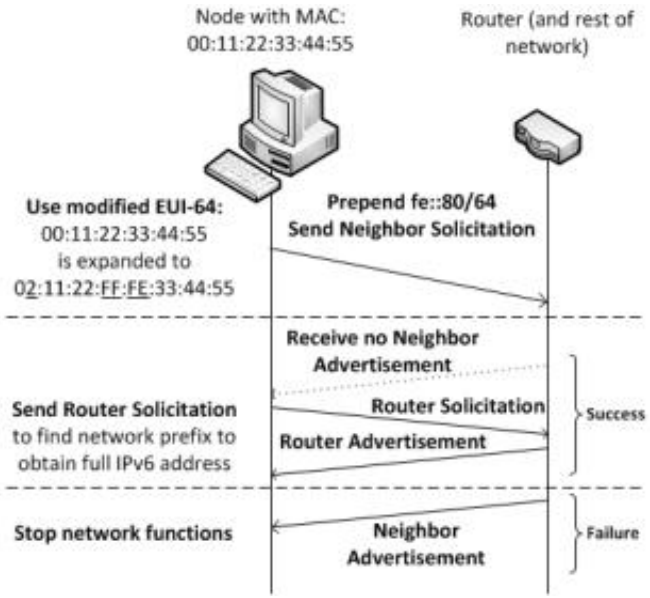

Figure 1. Stateless Address Auto Configuration

Since the MAC address is used, it would be easy to follow a roaming client since the last 64bits will always be the same (assuming there are no collisions and the user does not change the MAC address). To prevent this, there are Privacy Extensions which randomize the IPv6 address each time the machine needs a new one. However, it makes it hard to trace back certain traffic on a network to a specific client since the last 64 bits cannot be reversed to a MAC address and thus a certain computer (assuming the MAC is not changed temporarily). In order to find a router, a node can send a Router Solicitation to which a router will reply with a Router Advertisement (RA). In addition to answering solicitations, the router also can send this advertisement periodically, for example to update certain information. This Router Advertisement contains among other information the network prefix which the nodes must use for their IPv6 addresses, the lifetime of the router which indicates the period in which the nodes may consider the router valid and a preference level, which can be used to order the preference of the router in the nodes. This information is used by the nodes in the network to create an address and to build the routing table.

2.2 Related Works

There has already been a lot of research into the theoretical differences between IPv4 and IPv6. For example, Caicedo and Joshi [1] show some of the security challenges IPv6 poses such as potential problems with the State-Less Address Auto Configuration feature of IPv6, which could facilitate a denial of service attack. This could happen for example if the attacker prevents the target from obtaining an address through SLAAC by pretending the pending address is already in use. Other problems which are discussed are attacks using routing headers which could help an attacker reach a node which would normally drop such traffic and multicast-based attacks which might use the All Router address. Furthermore, they discuss that filtering IPv6 packets will be burdensome due to the amount of possible IPv6 headers and that the place ICMPv6 takes in IPv6 makes it hard to define firewall rules for that as well. They conclude with a short discussion about transition issues. In [3] Choudhary elaborates on [1] and discusses another attack against IPv6 nodes: a denial of service attack against security devices which need the whole packet for deep

packet inspection. By not sending the last fragment their buffers will be fully allocated after a while. IPv6 fixed this issue for routers by not allowing them to reconstruct the packet, but nodes that do are still vulnerable. Also a way of evading detection of attacks is suggested: one could use chains of routing headers to make it hard for firewalls to assess the traffic. Those chains are compliant with the IPv6 specification and thus cannot be dropped as a precaution. Some types of attacks using SLAAC and ICMPv6 are mentioned including: an attacker might insert himself as router and sniff all the traffic or just drop it, an attacker can send out router advertisements pretending to be the real router with lifetime set to zero causing a denial of service, an attacker can send messages to nonexistent nodes causing the routers to neighbor detect them which will fail and the router therefore wastes resources. In addition it is possible to send bad network prefixes which can cause nodes to be unreachable. Carp et al. [2] implemented and evaluated different attacks against IPv6 in local area networks and discuss mitigation of such attacks. They test active and passive reconnaissance attacks respectively using Neighbor Solicitation and sniffing for ICMPv6 traffic. In order to reduce the number of addresses to scan, a few bits were 'frozen'. This is possible when the addresses are obtained by SLAAC and a part of the MAC address is known (e.g. the manufacturer specific part). Also some reconnaissance attack optimizations are proposed, tested and evaluated. These include overflowing the MAC table of a switch so it becomes a hub and pretending to be a router or root bridge so nodes contact the attacker themselves. Furthermore they successfully test a denial of service attack which prevents a node from assigning an IPv6 address to itself by spoofing messages from potential IPv6 addresses of the target and thus preventing the target from auto configuring an address. Yang et al. [13] describe that IPsec is still vulnerable to some attacks like attacks against passwords and the Internet Key Exchange infrastructure. It also introduces a possible new problem: since encrypting uses quite some resources IPsec might open up new opportunities for denial of service attacks.

III. APPROACH

3.1 Questionnaire

In order to get an understanding of the status of IPv6 in the wild, it is necessary to get in contact with companies and organizations that use IPv6. There were two possibilities, either a questionnaire or interviews. The questionnaire was chosen in this case for several reasons. It is more distant and quicker than interviews which might make it easier for companies to cooperate. Furthermore a questionnaire makes it easier and faster to analyze data if most of the questions are closed ended. The questionnaire consists of 34 questions in total; divided in such a way that not all questions will be reached. The reason for this setup is that not all of the questions are needed for all the respondents. Some of the questions also are not necessary if the respondent answers a certain question in a certain way. The questions are made up of 26 closed questions, of which 25 questions are made to find actual information. These questions include rating scales (How secure do you consider your IPv6 network compared to your IPv4 network?), multiple choice questions with both multiple answers (What type of security measures do you employ for IPv6?) and with only one possible answer (When did you introduce IPv6?). The first question is a demographic question in order to find out how much the respondent might know of the network. The other 8 questions, which are open ended questions, are used to find the motivation of a previously given answer, or to let the respondent add extra information to a given answer. As targets for the questionnaire different companies were chose which all have some business with the internet. There were mainly three types: internet service providers (mostly Dutch) such as XS4ALL, UPC and KPN and some hosting providers, big companies which provide their services through the internet such as Google, Hyves etcetera. and fina lly companies which sell network security appliances, such as Cisco, Symantec and Checkpoint. Aside from those companies, the questionnaire was also send to the Dutch IPv6 Taskforce mailing list, because a lot of companies are subscribed to it and the people reading it are mostly technical so it is a good point of contact.

3.2 Practical Test

Aside from a questionnaire a practical test was carried out on the network of the University of Twente, because this can be used to describe how IPv6 is used in practice, as opposed to theory, and in a real environment, not a lab environment. The tests consist of three parts: testing IPsec in the network, testing different ways of identifying nodes on an IPv6 network and lastly testing the consistency of the security settings of the network between IPv4 and IPv6 and testing some other security related issues.

3.2.1 Testing IPsec

With the compulsory implementation of IPsec in IPv6, one might wonder if this is actually used throughout the networks, since there are quite some alternatives available, for example SSL. Beforehand the network administrators already noted that the services of the university were not using IPsec, consequently this test is meant to see if the routers and firewalls can properly handle the IPsec traffic. The environment of this experiment is as follows: two computers running Linux, both wired to the network. Both computers have IPsec-Tools installed, which is a port of KAME's IPsec utilities to Linux-2.6. One of the computers is running Wireshark as well, in order to capture the data that is send between them. This machine was also running a basic Apache server as a means of testing the connectivity between the two computers. The IPsec settings were set to require a connection with Encapsulating Security Payload using 3DESCBC encryption. Once these settings were in place on both machines, the webpage was loaded to see if the IPsec traffic was routed and this traffic was logged with Wireshark.

3.2.2 Identifying nodes on IPv6 network

IPv6 comes with 128-bit addresses, of which usually 64 are the network prefix and the other 64 bits are left to identify a node in the network. Due to this enormous increase in possible addresses, a ping scan to map a network will not work as well with IPv6 as it did with IPv4. Scanning one network would require probing 2^{64} addresses, which would take too

long. Even if one would optimize this scanning (e.g. focusing on a specific network card manufacturer as described in [2]) and thus restricting the scan a lot, this would be an address space of 2^{64} addresses. In order to find nodes attackers will eventually find other ways, e.g. using Neighbor Detection for this, using multicast addresses for this (e.g. FF05::1 for all nodes on a site) or querying the local DNS servers for information about the network. The goal of this experiment is to test other methods of gaining knowledge about the network. The experiment consists of two separate tests, the first one being trying to use DNS servers to find information, the second being using multicast addresses to find nodes on the network. The environment for this experiment consisted of a computer running Linux wired to the network. For the first experiment the program dig was used to query the DNS servers. First the IPv6 address prefix of the machine used was inverted and given as parameter to the dig program yielding the result below. dig AXFR 8.0.9.1.0.1.6.0.1.0.0.2.ip6.arpa

AXFR is the transaction type which is mostly used by administrators to replicate the contents of a DNS, in order to move it to a slave DNS. For the second experiment the ping program was used to send a ping to the Link-Local All-Nodes multicast address FF02::1.

The ping program was also used to receive all the responses.
In order to secure a network against unwanted reconnaissance attacks, networks should be segmented properly and DNS servers and routers should be properly secured to prevent easy access to information about the network. Allowing anyone to extract all the information from the DNS might give an attacker a good idea about where the interesting machines are.

3.2.3 Testing security settings

In the transition period a lot of networks will have both IPv4 and IPv6 enabled, whether it be dual-stack, tunneling or translation. However, using both protocols also requires securing both protocols. Problems may occur when IPv6 is enabled but only IPv4 is protected, since this would allow an attacker to still attack a node in the network if he manages to map the IPv4 address to an IPv6 address which he might do using for example DNS records. This experiment is used to get an idea about how well secured a network which operates on both IP versions in practice is. It consists of testing firewall settings by port scanning a certain machine from inside the network as well from outside the network and testing an aimed denial of service attack using the ICMPv6 Router Advertisement packet. The environment of these experiments consists of two computers wired to the university's network and one machine outside of the university's network (see figure 2).

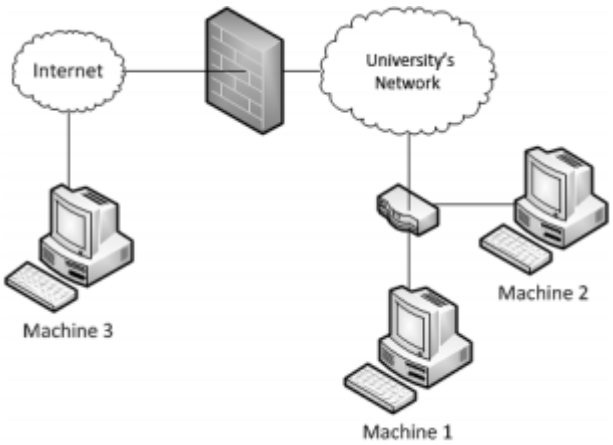

Figure 2. Security Settings Experiment Setup

The reason for this setup is that usually only traffic crossing the border routers is matched against an Access Control List (ACL). The first computer was actively used for the tests within the network and was running Nmap and Scapy. Nmap was used to scan the open ports on the second machine. Scapy was used to test the denial of service attack using RA packets. The second machine was running an Apache server, SSH and had ports 25, 12345 and 31337 open using the netcat program. These ports were chosen because according to [10] they should be blocked on the university's routers. The third machine was only running Nmap to do the port scan from outside the university's network. The first experiment, the port scans, was set up as stated above. First machine 1 scanned all ports of machine 2 over IPv4, then over IPv6. Secondly machine 3 scanned all ports of machine 2 over IPv4 and then over IPv6. The testing of the DoS attack was carried out by machine 1, in Scapy an IPv6 packet was made with the IPv6 address of machine 2 as destination encapsulating an ICMPv6 Router Advertisement packet with the router lifetime option set to zero. This should result in the node dropping routes to that router because the router is not valid anymore. Consequently this machine cannot connect to the internet anymore because it thinks there is no router. For this part of the experiment machine 2 was also running Wireshark in order to find out if the packets were actually received. After testing with only the address of machine 2 as destination, the usual destination was also used: ff02::1, the well-known link-local all nodes address.

IV. RESULTS

In this section the results of the survey and the experiments will be given subsequently. The results will be evaluated and discussed in section 5.

4.1 QUESTIONNAIRE

Of the 25 companies contacted (excluding the IPv6 Taskforce mailing list) roughly 11 responses were useful, the others were only partially filled in or just skipped through. Only the more interesting answers are discussed here. In the first question of the questionnaire, the respondents were asked to indicate their function within the company they work for. Half the respondents indicated they were somehow involved with the company's network. The other half of the respondents indicated they occupied a management function. The second question inquired about what type of company the respondent works for. Here 55% responded that their company provided internet services (i.e. ISPs and hosting providers etc.). The other 45% answered Other which was defined to be a university and a consultancy agency among others. The option that the company provided security services was not used. The next question asked which protocols were supported by the services their company provided. All the respondents indicated that IPv4 was supported while 91% responded IPv6 is also supported by their services and 82% responded that also the backbone of their network supports IP version 6. One reason given for not using IPv6 was that it is too expensive. When asked what the reason is to employ IPv6 in their networks 80% of the people who stated to use IPv6, answered it was out of anticipation of future need. The rest has a different reason for using IPv6. The following question inquired about when IPv6 was introduced, the results can be found in figure 3.

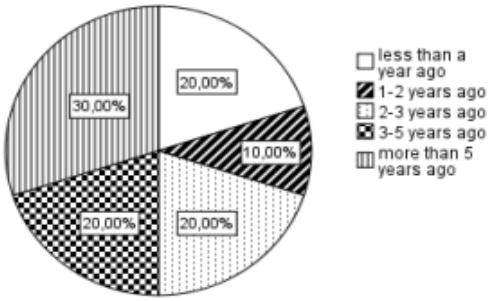

Figure 3. Chart on when IPv6 was introduced in the respondents networks.

In the tenth question in the questionnaire, the respondents were asked what the status is of IPv6 in their services. Of the respondents who answered to use IPv6, 60% answered IPv6 was deployment ready, i.e. it is already deployed or it is ready to be deployed. The remaining 40% answered their IPv6 was still in a testing stage. All the respondents answered they used security measures in their network both in IPv4 and in IPv6. When asked how secure they considered their network, 82% answered they considered their IPv4 network secure, while 18% answered they considered it not secure nor unsecure. For IPv6 the percentages are respectively 80% and 20%. Table 1. Results of questionnaire question: 'What security is used in your network?'

V. DISCUSSION

In this section the previous described results will be interpreted. First some general remarks regarding the research will be given in order to identify certain weak points. The first of those remarks is that this research only gives information about what the status of IPv6 is at the moment of the research: it is a snapshot. However, it might for example be the start of a periodical research which strives to map the progress of the deployment of IPv6.

5.1 QUESTIONNAIRE

Due to time and resource constraints, the number of respondents of the questionnaire it not really high and therefore the results do not have any statistical significance. This does not mean there are no trends to find in the results. First of all, the number of people who responded to support IPv6 seems to be quite high. There are different ways in which IPv6 connectivity can be measured. One of them is the amount of users actually using IPv6 to connect to the internet. Google for one is measuring the amount of people that use IPv6 to use their services [4]. According to these measurements currently about 0.33% of the people using Google use IPv6 to do so. However, since Google's IPv6 is only enables for certain whitelisted networks, this may not be totally representative. A different kind of measure is the amount of Autonomous Systems (AS) that announce IPv6 address blocks compared to the amount announcing IPv4 blocks. Since ASs are roughly speaking the same as an ISP this would indicate how many networks are IPv6 capable. According to the numbers collected by [5] this means that 2.93% of the networks are IPv6 capable. However, this too might not be representative because some networks might announce IPv6 while not the whole network is IPv6 capable. Reasons for this enormous difference between our results and above mentioned numbers might be that people whose company does not support IPv6 do not think their contribution is of any worth, or the group of companies (including the IPv6 taskforce) is not really representative. This number of IPv6 capable respondents is however useful when analyzing IPv6 security.

According to the results, most people think their networks are quite safe, and when asked what types of security measures they use something interesting shows: in order to secure IPv6 less measures are taken, while most respondents

consider both 'parts' of the network to be equally secure. The amount of people who stated to use IPsec in IPv6 is remarkable as well, it was supposed to be the security feature of IPv6 but it's usage is not significantly higher than with IPv4. Most respondents believe that they do not need it, albeit for different reasons. In addition most respondents seem to think IPv4 and IPv6 are generally equally safe while the respondent who answered IPv6 was less secure, also did not use IPv6 in the network. Something also noteworthy is that the security appliances the respondents use, mostly support IPv6 in software. A problem might occur when the firewall has so much traffic to process; it cannot handle it and might end up exhibiting unwanted behavior.

5.2 PRACTICAL TESTS

The results of these tests show that the University of Twente does not use IPsec itself, but that the hardware can route it without problem, as expected. As for the experiment regarding the identification of nodes on an IPv6 network, there is one thing that should be noted: a ping scan using Neighbor Detection was not experimented with, because this would flood the routers neighbor tables which might cause them to crash and consequently disrupt the network as described in [3]. It can be observed from the results that aside from a tedious ping sweep, there are other ways to find online machines in a network. One conclusion might be that network administrators need to secure the network better against such reconnaissance attacks, because they might become a lot more common. The results from the security settings experiment show that there is quite a difference between the security of IPv4 and IPv6. The IPv4 network is protected from the outside world using an Access Control List, but the IPv6 network is not protected at all according to the results. The ports with a dash in Table 2 were not listed by nmap because they are not filtered (as with IPv4) nor open on the target machine and can therefore be considered open. Two things are interesting to note: the samba port is not filtered either, leaving it open to the world and the list in [10] does not match the list of filtered ports.

Even when taking into account that according to ICTS there are no services from the university available over IPv6, it is a remarkable result because it still leaves open regular nodes on the network. Indirectly this can still cause harm. It should be noted however that IPv6 it not totally forgotten. Getting an IPv6 address using SLAAC with privacy extensions would make it nearly impossible to trace anything back as described in section 2.1. However, by making backups of the neighbor tables of the routers they manage to create a link from an IPv6 address back to a MAC address.

This allows them to trace everything back to a certain person if this should be necessary. We could not trace why the DoS attack failed since the packets did arrive at the target machine. Even when copying nearly all the fields from the Router Advertisements of the actual routers on the network, the results stayed the same. The theory makes for a good addition to the DoS attacks described in [1-3].

VI. CONCLUSIONS

The results of the questionnaire showed that a lot of networks have already started to migrate to IPv6. This is only the start, slowly more and more networks will reach the state were IPv6 is usable because there is a lot of pressure due to the limited amount size of the IPv4 address space. The security products do support IPv6 as well, but not optimally yet. The questionnaire shows that IPv6 is handled mostly in software which might cause problems. Furthermore, most respondents answered they do not use IPsec, which was very important in the early protocol specification. It also shows that IPv6 networks are under attack, and thus must be secured. Results of the practical tests show that the security of IPv6 networks is not optimal compared to IPv4, which might be caused by the lack of enthusiasm for IPv6. For now we can conclude that networks running IPv6 are at least not safer than networks running IPv4. The security of networks mainly depends on their deployment, and since IPv6 is still young, networks running IPv6 will most likely more robust over time.

References

[1] Caicedo, C. E., Joshi, J. B. D. and Tuladhar, S. R. IPv6 Security Challenges. Computer, 42, 2 (Feb. 2009), 36-42.
[2] Carp, A., Soare, A. and Rughiniş, R. Practical analysis of IPv6 security auditing methods. In Proceedings of the 9th RoEduNet IEEE International Conference, RoEduNet 2010 (Sibiu, Romania, June 24-26, 2010). IEEE, 2010.
[3] Choudhary, A. R. In-depth analysis of IPv6 security posture. In CollaboarteCom 2009 (Washington, DC, USA, Nov. 11-14, 2009). IEEE, 2009.
[4] Google. IPv6 Statistics. http://www.google.com/intl/en/ipv6/statistics/. Visited on June 1st, 2011.
[5] Huston, G. IPv6: IPv6 / IPv4 Comparative Statistics. http://bgp.potaroo.net/v6/v6rpt.html. Visited on June 1st, 2011.
[6] IETF. RFC 1883 Internet Protocol, Version 6 (IPv6) Specification. December 1995.
[7] ISOC World IPv6 Day. http://isoc.org/wp/worldipv6day/. Visited on Febuary 28th 2011.
[8] NRO. Free Pool of IPv4 Address Space Depleted. http://www.nro.net/news/ipv4-free-pool-depleted. Number Resource Organization, Febuary 2011.
[9] Rowe, B. and Gallaher, M. Could IPv6 Improve Network Security-And, If So, at What Cost. Cybersecurity, 2, 2 (2006).
[10] SNT. Frequently Asked Questions. http://www.snt.utwente.nl/helpdesk/newfaq. Visited on May 5th 2011.
[11] SURFnet. (not so) new IP features: IPv6. http://www.ipv6.surfnet.nl/. Visited on Febuary 28th 2011.
[12] Warfield, M. H. Security Implications of IPv6. Internet Security Systems, 2003.
[13] Yang, D., Song, X. and Guo, Q. Security on IPv6. In Proceedings of the 2nd IEEE International Conference on Advanced Computer Control (Shenyang, China, March 27-29, 2010). ICACC-2010. IEEE, 2010

