Missouri S&T's Peer to Peer

Volume 1 | Issue 2 Article 3

May 2017

Network Security: Internet Protocol Version Six Security

Hannah Reinbolt

Hannah Reinbolt
Computer Science at Missouri University of Science and Technology

NETWORK SECURITY:
INTERNET PROTOCOL VERSION SIX SECURITY

Abstract

It is no secret that the pool of public internet addresses available with Internet Protocol version Four (IPv4) is gone. (Morphy, 2011) Thus the migration to the more roomy Internet Protocol version Six (IPv6) has begun. This migration is a complex process including different security procedures and updates that require time and knowledge. This paper will dive into scientific writings, with databases like Scopus and IEEE, about various security risks in the IPv6 protocol such as tunneling practices, router issues and issues with Internet Protocol Security (IPsec). This paper will overview security practices to better clarify common vulnerabilities in IPv6. While some configurations cause issues with host safety, it is commonly noted that due to user error most of the attacks escalate more than they should. Network professionals should be informed about IPv6 security issues in order to best protect a system. Information on IPv6 security risks is crucial to protecting against an attack before it happens and minimizing damage when real time attacks take place.

Network Security:

Internet Protocol Version Six Security

The transfer of information online allows many of systems of today to operate and Internet Protocol version Four (IPv4) does a great job working like a post office to organize digital traffic. IPv4 provides public internet addresses to communicate with networks but after its release in the 1970s and the rapid growth of the internet, the current demand for public internet addresses has reached its physical limit. By 1998 the Engineering Task Force deemed the new Internet Protocol version Six (IPv6) to be the successor to IPv4 and solve the address problem. The transfer to IPv6 allows a lot more flexibility, address space and security due to better architecture and physical space but unfortunately these two protocols were not meant to be interoperable. This makes the transfer complex and some vulnerabilities from IPv4 are implemented into IPv6.

Unfortunately many entities have not switched to IPv6 because of price and compatibility. Even with this barrier, Carlos Caicedo, James Joshi, and Summit Tuladhar explain in their journal titled 'IPv6 Security Challenges' that many Asian countries such as China, Korea and Japan have made the upgrade a priority by limiting IPv4 address space (2009). Nevertheless, due to physical address limits, the switch will have to be made in the coming years because IPv6 is the only infrastructure that can support the internet (Amutha, Albert Rabara, Meenakshi Sundaram, 2016.). Caicedo, Joshi and Tuladhar go on to explain one of the main security challenges being a lack of understanding IPv6 security infrastructures (2009). Since the internet is beginning to merge into IPv6, the hacker community has begun to exploit weaknesses. (Hauser, 2017) As more of the internet converts we will have greater knowledge and experience dealing with newly formed attacks. Network professionals need to be informed of as many security risks as possible to help protect this new IPv6 system and prevent common user error.

As the number of attacks continue to grow and IPv6 becomes more ingrained with the majority of Internet users, understanding how IPv6 infrastructure and security issues work become crucial. This paper takes scholarly writings from Google, Scopus and IEEE databases, then reviews them for information regarding IPv6 security practices and issues. Priority is focused on common security risks many users face. Results include findings on tunneling, packet issues IPsec vulnerabilities, and information of potential risks.

Internet Protocol Security Issues

Old features of IPv4 now being used as add ons for IPv6 may give rise to previous security issues. Amutha, Albert, and, Meenakshi remark in their paper about IPv4 and IPv6 transitions, "IPv6 is enmeshed with various issues: its global interoperability is limited due to the weakness of the encryption algorithm; IPSec [Internet Protocol Security] has not yet been fully standardized; there is no protection against Denial of Service/Flooding attacks." (2016). This paper explained that certain old vulnerabilities with IPv4 could be brought over with IPv6, such as Denial of Service or Flooding attacks. IPsec works like a lock on a package about to be mailed. It encrypts the data making it more secure for travel and protects the data until delivery. Features like IPsec are now being implemented as a requirement which is something to consider when planning to make the switch to IPv6. Denial of Service or Flooding attacks happen when the bandwidth of multiple servers are flooded with information in such a way that it disrupts the services the host provides. This can momentarily or permanently take that host down depending on the nature and intensity of the attack (McDowell, 2009).

There is also concern as to how IPsec can be secure in encryption. Zamani and Zubair state that strength of the encryption algorithms to ensure global interoperability is limited (2014). The complexity of the IPsec security algorithms is simplified due to export laws that regulate

who has access to US developments. While these laws help global workability they also make boundaries easier to break compared to more complicated algorithms.

The usage of a stronger encryption is looked down upon because the National Security Agency (NSA) fears it will make the intelligence gathering more difficult and possibly threaten national security (Tidball, Best, 1998). It is tricky to propose a stronger algorithm but still on the mind of experts when it comes to IPsec management. While Denial of Service attacks are more common than deficiency in algorithm strength, both papers bring up some concerning vulnerabilities in IPsec encryption. These papers suggest that a factor in helping increase security would be for "Security practitioners"(Amutha, Albert, Meenakshi, 2016) to educate themselves on IPv6 technology and workings in order to understand how to keep networks secure and decrease the chance of simple human errors letting the attacks escalate.

Tunneling Challenges

In the older protocol, IPv4, rogue traffic slipping by via tunneling is a challenge but with IPv6 having sixteen different tunnel and transition methods, it makes filtering more difficult. Going back on our post office examples, tunneling is like the route from the post office to a house. The post office truck carries all the packages safely to a house but has several paths to take in order to get there. Tunneling is like the path to the package destination with IPv6 having many more paths. Sharma notes in a study on IPv4 and IPv6 best security practices that, "As noted in many of the transition studies done, automatic tunneling mechanisms are susceptible to packet forgery and DOS (denial of service) attacks (2010). These risks are the same as in IPv4, but increase the number of paths of exploitation for adversaries." Information is being streamed through these IPv4 and IPv6 tunnels but these tunnels are set to filter out bad information and packets. In IPv4 it is possible to overflow the tunnels with information in Denial of Service attacks in hopes of

shutting down the host but is manageable by setting up the tunnels to be filtered. In IPv6 it would be harder to filter out the bad packets due to there being larger amounts of tunnels and transition methods. The damage that can be done by having a mass of unfiltered traffic flow through the IPv6 protocol could lead to damage to your host, exposure to bugs and other risks. Sharma goes on to say that if the network structure is dual stacked that it would need to heavily rely on these filtering methods. Static tunneling proves to be a lot more stable because it can secure a trust relationship between both ends of the tunnel. Proper tunneling management is important in protecting against mass attacks like Denial of Service or other bad packets in order to save time and information. While tunneling mechanisms should be a concern to all administrators it is not always considered since most traffic is blocked by default.

Tunneling methods should be reviewed in order to have optimal security. Gont & Liu (2014) seem to stress that, "Tunneling mechanisms should be a concern not only to network administrators that have consciously deployed them, but also to those who have not deployed them, as these mechanisms might be leveraged to bypass their security policies." It is discussed that tunneling mechanisms have been standardized and called 'automatic tunneling' mechanisms which might be put in place without the user or network administrators consent. Checking the setup to make sure there are no loopholes packets can slip through is a good way to prevent attacks from common user error. In most cases IPv6 will have traffic blocked but as Gont & Liu remark, it is important to check and make sure what is configured. If not managed properly these implications could lead to host exposure, evasion of security protocols, protocol-based vulnerabilities and others. In the case of what Sharma, and Gont & Liu said, one of the main concerns is making sure the current IPv6 configuration is known for each setup. In perspective,

attacks like Denial of Service are less likely to happen if careful consideration is taken to set up any tunnels and to be aware of current tunneling mechanics.

Routing and Packet Vulnerabilities

In addition to tunneling, routing headers being hijacked is a concern. Chasser (2010) warns about routing headers being manipulated to carry a blocked packet to a host processing header. A header is like a destination address on a package as it is on the way to be mailed while a packet is like a package to be mailed, carrying digital information. The destination of the packet would be manipulated and once it is headed towards the destination, the host must accept this address with a packet. Because the packet is linked to a good address, it is not properly dropped like it would have been before. This would be a way to sneak dangerous packets into your host through the levels of security already implanted. Chasser suggests verifying the waypoint of the router addresses so they appear only once for a destination. This is only a countermeasure to prevent suspicious activities but not guaranteed. However, this is not the only threat meant to derail the router process.

Supriyanto, Hasbullah, Murugesan, and Ramadass (2013) argue that a ‘hop’(bridge or gateway) router pretends to be a default router and then an attacker can send packets wherever desired, with the option of disturbing packet transmission. In detail this hop router will send a false transmission to the inform the host of the best way to send the packet. The host will think it is the default router and send the packet. Unfortunately rogue transmissions like this can cause false parameters and the packet to not arrive at its destination. Between Chasser, Supriyanto, Hasbullah, Murugesan, and Ramadass, they all bring to mind the importance of security and how it can affect IPv6. From big features like IPsec to small packets of corrupted information, all of these can cause major issues with the functionality of the host.

Discussion

IPv6 security is a complicated issue and many authors have a different approach on the subject. Here it was discussed that many different issues can lead to Denial of Service attacks, such as some current problems with the IPsec feature and proper tunneling techniques proving to be difficult. Here is is discussed that tunnel filtering is more challenging to accomplish with IPv6 due to more tunnels and more physical space. Algorithm strength was discussed, topics such as limits to the complexity and how those limits are fixed based on the national concerns of NSA. One of the main issues suggested by many of the articles reviewed was the notion of IPv6 administrators not being knowledgeable on IPv6 security and risks. Much of the IP usage is done with the old IPv4 protocol while IPv6 is still very new in the network society. It is encouraged for information about IPv6 security to be reviewed since it is slowly taking over IPv4. Many of these security flaws can be stopped and prevented if the correct procedures are taken in a timely manner.

Internet routing issues were also discussed, including spoofing and address header manipulation. Header manipulation can be prevented in most cases if the host checks makes sure the destination address did not change. Many of these issues are not fully developed and tested due to IPv6 only being used to a fraction of its full potential. As time goes on more threats will be unveiled, and the need for new preventive practices will emerge. More research is needed to properly investigate these security holes as this document only covers a small quantity of issues with IPv6 security. Many attacks and fixes are still theoretical at this stage since IPv6 is still small but because of the imminent switch from IPv4, these threats will only be put into play and even more research will be required.

References

Amutha J., Albert Rabara S., Meenakshi Sundaram R. (2016) *An Integrated Secure Architecture for IPv4/IPv6 Address Translation Between IPv4 and IPv6 Networks*. In: Satapathy S., Raju K., Mandal J., Bhateja V. (eds) Proceedings of the Second International Conference on Computer and Communication Technologies. Advances in Intelligent Systems and Computing, vol 380. Springer, New Delhi

Caicedo, C., Joshi, J., Tuladhar, S. (2009). *IPv6 Security Challenges*. IEEE. Vol. 42. No. 2. (p. 36-42). Retrieved on March 12 2017 from http://ieeexplore.ieee.org.libproxy.mst.edu/document/4781968/.

Chasser, J. M. (2010). Security Concerns in IPv6 and Transition Networks. *Information Security Journal: A Global Perspective*, *19*(5), 282-293. doi:10.1080/19393555.2010.514653

Gont, F., Liu, W. (2014). Security Implications of IPv6 on IPv4 Networks. Internet Engineering Task Force. Retrieved on April 14, 2017 from https://www.ietf.org/rfc/rfc7123.txt.

Hauser, Van. (2017). THC-IPV6. The Hacker's Choice. Retrieved on April 14, 2017 from https://www.thc.org/thc-ipv6/.

McDowell, M. (2009). *Understanding Denial-Of-Service Attacks*. Retrieved on April 14, 2017 from https://www.us-cert.gov/ncas/tips/ST04-015.

Morphy, E. (2011). *No Room At The Internet: IPv4 Addresses All Gone*. Tech News World. Retrieved on April 14, 2017 from http://www.technewsworld.com/story/71793.html

Sharma, V. (2010). *IPv6 and IPv4 Security Challenge Analysis and Best-Practice Scenario.* Int.J. of Advanced of Networking and Applications. Vol. 1. No. 4. (p. 258-269). Retrieved on February 2, 2017 from http://www.ijana.in/papers/4.9.pdf.

Supriyanto, Hasbullah, I., Murugesan, R., & Ramadass, S. (2013). Survey of internet protocol version 6 link local communication security vulnerability and mitigation methods. *IETE Technical Review, 30*(1), 64-71. doi:http://dx.doi.org.libproxy.mst.edu/10.4103/0256-4602.107341

Tinbal, K., Best, R. (1998). *The Encryption Debate: Intelligence Aspects*. The Library of Congress. Retreived on April 14, 2017 from http://www.sci-links.com/files/CRS-_Encryption_Intelligence-_11-98.pdf.

Zamani, A., Zubair, S. (2014). Deploying IPv6: Security and Future. International Journal of Advanced Studies in Computer Science and Engineering. Vol. 3. No. 4. (p. 1-9). Retrieved on April 14, 2017 from http://www.ijascse.org/volume-3-issue-4/Deploying_Ipv6_Security.pdf.