Security for SOHO in IPv6 Networks

Srinivas Naik, Rajesh Adepu

Abstract*— *Small Office and Home Office (SOHO) distinguishes from large organizations where there exists minimal security or protection mechanisms. This paper investigates and presents different threats that a network can be exposed to and the common protection techniques that can be applied, with a focus on the network perimeter – specifically the router/firewall between the local area network and the Internet. All Internet connected devices and networks are exposed to and affected by security threats to some degree, hence security is important in almost every type of network. With the constant growth of the Internet the 32-bit addressing scheme ipv4 is proving to be inadequate, and therefore the transition to the 128-bit addressing scheme ipv6 is becoming critical. With ipv6 comes new security threats (while still old threats remain) that requires an understanding of perimeter security. In this paper we secure a home router and describe these steps to enable home and small business owners to secure their IPv6 network.

Index Terms*—*Security, IPv6 Attacks, SOHO threats, Intrusion detection system, Firewall.

I. INTRODUCTION

There is a need to implement new IPv6 networks in homes and small and medium sized enterprises (SOHOs). Following this overview from a security perspective we will examine in home and SME networks, along with a description of the importance of this paper and how it will improve network security in these IPv6 networks.

II. THE SCALE OF PROBLEMS IN IPV6 NETWORKS

The security demands are increasing as IPv6 deployment expands over the globe. The fundamental problem is that every single network will be more or less forced to implement IPv6 at some point if they want to maintain their connectivity. Furthermore, all these new IPv6 networks need to consider their security against both new and old threats. Today ordinary IPv4 routers and firewalls simply cannot protect against IPv6 specific traffic.

Popular client operating systems (such as Microsoft’s Windows, MAC OS, and Linux) all ship with IPv6 enabled by default which contributes to the increased preparedness of these systems to adopt IPv6, but also increases the impact of IPv6 related security problems. Because in most cases

IPv6 security is not a high priority or even a concern, thus most users are not aware of using IPv6 or that they even have it enabled. Unfortunately in reality this means that these hosts could be wide open for all sorts of attacks and abuse by anyone connected anywhere on the Internet via IPv6.

MalWare, malicious intended code such as virus, worms, and Trojans, often infiltrates and in some cases remotely control network connected devices without the user’s knowledge. Such malware has become a common global security problem because this malware takes advantage of the limited or non-existent security in many networks. One of the most famous examples of malware today is the Zeus Trojan specialized in stealing banking information. This malware now claims to have IPv6 support. Such malware mainly uses IPv6 to tunnel traffic between the compromised host and the attacker (i.e., to provide a secure tunnel for the botnet’s command and control traffic).

One common problem that motivates this paper for home users is that the use of virtual private network (VPN) services has grown in popularity due to concerns about Internet integrity. Many home VPN users are unaware that they have an IPv6 address as part of their IPv4 VPN tunnel service. Thus the VPN can deliver IPv6 traffic that they are unaware of and unprotected from. This particular problem cannot be solved at the router/firewall since the VPN traffic is encrypted before it reaches the router.

The investigation begins with what type of threats target IPv6 networks. Specifically we will examine unfiltered traffic, router break-ins, inside-out attacks, service vulnerabilities, and IPv6 protocol specific vulnerabilities.

III. EXISTING PROBLEMATIC SOLUTION

The need for protection is obvious, but the cost of security can be a concern, along with how to implement the security in an existing network due to a lack of knowledge about relevant threats. Since there are both old and new threats that the IPv6 network will be exposed to, a threat analysis needs to be done in order to gain a better understanding of the threat picture and to ensure that we protect ourselves against the relevant threats to a home or SME IPv6 network. While common pre-built routers and firewalls have received much criticism, they also tend to be an expensive and imperfect solution. However, as will be presented in the paper the security needs for a home or SME network can be solved with simple home networking equipment, thus decreasing cost and providing higher security.

A variety of open source router software offer an opportunity to re-use routers and existing computer’s by giving them increased functionality, potentially providing a better and more cost effective solution to achieve perimeter security. Achieving network security means configuring and implementing known solutions to known threats. Identifying these threats and implementing solutions is non-trivial for the ordinary home or SME network

Manuscript received March 11, 2013.

Srinivas Naik, CSE, Princeton College of Engineering, Hyderabad, INDIA.

Rajesh Adepu, CSE, Princeton College of Engineering, Hyderabad, INDIA.

user, so there is a need for a structured method to implement the appropriate security mechanisms.

IV. THREATS RELATED TO IPV6

A. *Outside attacks*

Threats exposing the router's Internet port from the border router's perspective include many well-known attacks that target the router's application layer regardless of the Internet protocol used. However, there are some attacks and security flaws specific to the implementation of the firewall, along with IPv6 specific threats which are clearly in the scope of this paper. When connecting a network device to the Internet the device will be exposed to different threats, such as botnets with malware and malicious hackers making targeted attacks as below

a. Reconnaissance and information gathering
b. Denial of Service attacks
c. Outside router break-ins

B. *Inside attacks*

There are threats that target the inside LAN by means other than forcing their way through the border router. These attacks include social engineering attacks and Trojans. All of these types of attacks seek to exploit security weaknesses of the network structure in different ways, along with flaws in application's implementations. Attacks originated outside but using the inside LAN to target the router from an inside perspective occur mainly at the application layer. Few inside attacks as mentioned below

a. Inside-out attacks
b. Tunnels and encapsulated traffic

V. IPV6 SPECIFIC THREATS

Attacks and security flaws specific to IPv6 along with a firewall implementation. This is the main focus of this paper.

A. *IPv6 address space*

Since the IPv6 address space is quite large the risk of a global host scan is not a major concern, because it would take years to do even a ping scan, i.e., to identify a live host within a given IP range, across the entire global Internet. However, DNS servers can be used by an attacker to collect addresses; these specific addresses could easily be scanned for vulnerabilities.

B. *ICMPv6*

ICMPv6 can be used to gather information about a specific router in order to learn more about the network's structure. ICMPv6 can be used in DoS attacks by sending a stream of error message to the targeted machine, since the receiving host needs to process these error messages this creates an increased load on the machine's resources. Furthermore, from a multicast perspective a multicast packet can be sent with the unknown destination option marked as mandatory with a spoofed source address of a multicast source host, thus triggering other nodes to send an ICMP parameter problem message to the source address which results in a lot of traffic.

In order to prevent DoS attacks, we can use rate-limiting to determine how much ICMP traffic we want to allow or to limit how much we generate. This limiting function is a part of ip6tables which is easy to implement via ICMPv6 rules

C. *Type 0 Routing Header (RH0)*

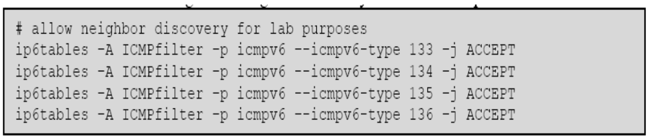
There is a method that may allow scanning by using the Type 0 Routing Header. In this method the outside attacker already knows one internal host and specifies more than one destination IP address which causes the receiving host to forward the packet to the next LAN client in the RH0 IP address list. When the final destination node is reached it can directly respond back to the attacker's source address, and another LAN node is discovered. For example, a host that would have been out of reached for direct communication, due to firewall access control lists, might be accessed via a transit node, such as a public web server connected to the LAN. When the final destination node is reached it can simply respond directly back to the attacker's source.

Ingress filtering in firewalls should block packets containing Type 0, but not disable other types of routing headers. Furthermore, routing headers of Type 0 are no longer required for IPv6 implementations in any way.

VI. COUNTERMEASURES FOR THE THREATS

A. *Clean up from the test session*

Remove the unnecessary icmpv6 rules in the ip6tables that was used for the network test session only, which are the neighbor discovery messages

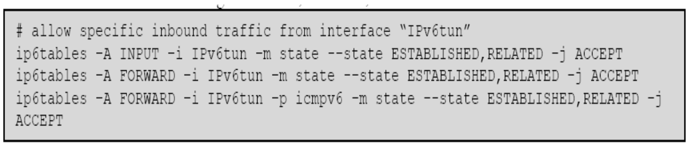


```
# allow neighbor discovery for lab purposes
ip6tables -A ICMPfilter -p icmpv6 --icmpv6-type 133 -j ACCEPT
ip6tables -A ICMPfilter -p icmpv6 --icmpv6-type 134 -j ACCEPT
ip6tables -A ICMPfilter -p icmpv6 --icmpv6-type 135 -j ACCEPT
ip6tables -A ICMPfilter -p icmpv6 --icmpv6-type 136 -j ACCEPT
```

B. *Tunnel or native IPv6 connection*

If there is access to native IPv6 connectivity directly to the router, then there is no need of any additional configuration.

However, if we use a tunnel broker both the INPUT and the FORWARD chain must be modified to support the IPv6 tunnel. Tthe tunnel interface is not the WAN port interface "vlan", but rather the newly created tunnel interface ("IPv6tun") between the tunnel broker and your device. Another even better solution would be to replace the "vlan" rules to instead "IPv6tun" rules. In that case, the firewall is more precise to allow tunnel traffic only, instead of allowing both pure WAN port traffic that is not tunneled along with tunnel traffic



```
# allow specific inbound traffic from interface "IPv6tun"
ip6tables -A INPUT -i IPv6tun -m state --state ESTABLISHED,RELATED -j ACCEPT
ip6tables -A FORWARD -i IPv6tun -m state --state ESTABLISHED,RELATED -j ACCEPT
ip6tables -A FORWARD -i IPv6tun -p icmpv6 -m state --state ESTABLISHED,RELATED -j
ACCEPT
```

VII. CONCLUSION

Providing suitable IPv6 security is a global issue. The need for this security is growing with the expanding IPv6 deployment.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

Unfortunately, it is easy to attack IPv6 these days due to the lack of security knowledge by most users regarding this protocol, but fortunately it is harder to discover targets via global scanning. There are some new threats to the IPv6 protocol itself, such as new DoS possibilities and the increasing difficulty of ingress filtering (as ICMPv6 plays a bigger part in IPv6 than ICMP plays in IPv4).

The usual packet filtering IPv4 firewall does not protect against attacks carried out over IPv6, such as brute force attacks against application layer services. Secondly, this paper has shown that an ordinary home router bought to support IPv4, can be used to support IPv6 in a more secure manner if the reconfiguration is done correctly.

We have seen that on the perimeter, there is a great need for finer granularly filters for ICMPv6 messages (along with rate-limiting), and that we must filter ports to secure services over IPv6 in order to provide security for IPv6 that is comparable with the existing IPv4 security. Furthermore, basic performance analysis has shown that the IPv6 security implementation used in this concept does not affect the overall throughput on the IPv6 protected router.

Finally, security solutions such as implementing a host version of the ip6tables directly on the host is another approach that also gives IPv6 protection if the perimeter router does not have any running services that needs to be protected, such as an SSH service.

REFERENCES

1. ‘IP Address Pools’. American Registry for Internet Numbers, Available at https://www.arin.net/knowledge/ip_address_pools.pdf,
2. Jan Hedström, ‘6 brandväggar för ipv6’, TechWorld, p. 6, 13-February-2012, Available at
3. http://techworld.idg.se/2.15821/1.431895/6-brandvaggar-for-ipv6,
4. Carolyn Duffy Marsan, ‘Five of the biggest IPv6-based threats facing CIOs’, Network World, p. 2, 13-July-2009, Available at http://www.networkworld.com/news/2009/071309-ipv6-network-threat.html
5. E. Karamanos, ‘Investigation of home router security’, Masters Thesis, KTH Royal Institute of Technology, Stockholm, Sweden, Available at http://urn.kb.se/resolve?urn=urn:nbn:se:kth:diva-91107, 2010.
6. ‘Malware Tunneling in IPv6’. US-CERT, 26-May-2005, Available at http://www.uscert.gov/reading_room/IPv6Malware-Tunneling.pdf

AUTHORS PROFILE

Srinivas Naik, MTech (CSE) from Princeton College of Engineering, Hyderabad. His expertise lies across Network Security Assessment, Web Application Security Assessments, Malware Analysis and Network Packet Security Testing. He is internationally certified in CEH, CHFI and ECSA.

Rajesh Adepu, MTech (CSE) from Princeton College of Engineering, Hyderabad. His expertise in UNIX Administration and Management also has well hands-on with Solaris Administration. His interests include Network Security and Data Mining.