



Insights on IPv6 Security

Bilal Al Sabbagh, MSc, CISSP, CCSP

Senior Information & Network Security Consultant - NXme

Information Security Researcher – Stockholm University

NIXU Middle East / NXME

- New company name NXME
- Operations in Gulf region since 1998, in Finland since 1988
- **Trusted and skilled company focusing on information security and network integration**
- GEOGRAPHIC FOCUS: Middle East and Africa
- TECHNOLOGY AREAS: Internet security, Financial IT security, Penetration testing and Forensics, Security Audit, IP network design, operation and integration
- INDUSTRY SPECIALISATION: Banking and finance, telecommunications, government, military

Talk Topics

- IPv6 Addressing Security
- IPv6 Access Control
- IPv6 Border Filters
- IPv6 Neighbour Discovery Protocol Security
- IPv6 And IPv4 Common Security Practices
- IPv6 coexistence with IPv4 security considerations
- IPv6 additional considerations
- IPv6 security deployment conclusion

IPv6 Addressing Security

- The BIG address space make it harder for network reconnaissance using ping sweeps and hosts scans
 - No security scanners are yet capable to scan the default IPv6 /64 subnets.
 - 2^{64} space needs around 5 Billions years to probe every service (RFC 5157, 2008)
 - Implementing stateless EUI-64 addresses make it easier for attackers to scan your IPV6 network
 - The already stuffed 16 bits “fffe”
 - and if they know/guess the vendor of the IEEE 802 network card 24 bits
 - The space will drop to 2^{24} which will need 194 days

IPv6 Addressing Security

- Issues with EUI-64 Addresses
 - Privacy issues because the address is derived from host MAC addresses
 - Trackable hosts
 - Hosts hardware brand could be exposed
 - make it easier for attackers to scan your IPV6 network if they know/guess the vendor of the IEEE 802 network card
- Privacy enhanced EUI-64 (RFC 4941, 2007) addresses use temporarily random addresses based on global interface identifiers for outgoing connections

IPv6 Addressing Security

- Problems with using privacy extended EUI-64
 - Complicated troubleshooting
 - Required frequent DNS records update
 - Still an issue for host require unique IPv6 address
- Recommended Addressing Practices
 - Use static IPv6 Addresses for critical and public services.
 - Avoid using obvious and easy distinguished and memorable addresses
 - Cryptographically Generated Addresses – CGA (RFC 3972, 2005)
 - Random interface identifiers based on user public key
 - Prevent spoofing and stealing
 - Limitations since addresses are not certified

IPv6 Access Control

- IPv6 Capable firewalls that support
 - IPv6 access lists
 - IPv6 routes
 - ICMPv6 including neighbor discovery protocol
 - Plan carefully what ICMPv6 messages type to allow
 - Aggressive filtering of ICMPv6 could have negative impact on the network
 - You need to give special attention to the following ICMPv6 messages
 - Type 133/134 – Router solicitation and advertisement
 - Type 135/136 – Neighbor solicitation and neighbor advertisement

IPv6 Access Control

- Fragmentations controls
 - Mitigate DOS Attacks
 - Configure your firewall not to allow IPv6 packets whose MTU is less than 1280 Octets (RFC 2460, 1998)
 - Mitigations are still being tested
- Spoofing Controls
 - Block spoofed packets according to (RFC 2827, 2000)
 - Block special use and non expected addresses (RFC 5156, 2008)
- Broadcast Amplification Controls
 - IPv6 is designed to mitigate against such attacks
 - IPv6 nodes should not react to Broadcast or multicast addresses (RFC 4443, 2006)
 - Filter multicast packets as well

IPv6 Border Filters

- Filter packets whose source/destination address should not be routable and does not exist in the internet routing table
 - Martians Prefixes
 - Prefixes should not exist in the public IPv6 routing table
 - Look at (RFC 5156, 2008) for special use IPv6 addresses
 - Bogons Prefixes
 - Prefixes Not yet allocated by IANA to RIR
 - Look at this dynamic live list <http://www.bgpmon.net/showbogons.php?inet=6&global>
 - Selective prefixes
 - According to your own policies e.g. your IPv6 prefix
 - Ingress / egress filtering

Bogons Prefixes

update type	seen by #peers	Date (UTC)	Bogon network	announced prefix	Origin AS	transit AS	ASpath
Update (Bogon Prefix)	7	2010-10-06	2a00:0000::/12	2a02:2528::/32	AS25091	AS3549	13030 3549 25091
Update (Bogon Prefix)	14	2010-10-05	2001:0400::/23	2001:498::/32	AS6342	AS278	12859 3257 2497 2914 278 6342
Update (Bogon Prefix)	30	2010-10-05	2a00:0000::/12	2a02:2528::/32	AS25091	AS3549	12859 3549 25091
Update (Bogon Prefix)	14	2010-10-02	2001:0400::/23	2001:498::/32	AS6342	AS278	1103 3257 2497 701 12702 286 2914 278 6342
Update (Bogon Prefix)	27	2010-10-01	2400:0000::/12	2402:ec0c::/32	AS7575	AS6939	2497 1257 6939 7575
Update (Bogon Prefix)	15	2010-10-01	2600:0000::/12	2607:f0b8::/32	AS13490	AS6939	12859 3257 6175 6939 13490
Update (Bogon Prefix)	11	2010-09-30	2620:0000::/23	2620:0:1900::/41	AS40335	AS2828	8426 3549 2828 40335
Update (Bogon Prefix)	14	2010-09-29	2001:0400::/23	2001:498::/32	AS6342	AS278	12859 3257 2497 2914 278 6342
Update (Bogon Prefix)	14	2010-09-28	2001:0400::/23	2001:498::/32	AS6342	AS278	12859 2914 278 6342
Update (Bogon Prefix)	8	2010-09-28	2400:0000::/12	2402:ec0c::/32	AS7575	AS2914	6762 2914 7575
Update (Bogon Prefix)	22	2010-09-24	2600:0000::/12	2607:f0b8::/32	AS13490	AS6939	13030 6939 13490
Update (Bogon Prefix)	4	2010-09-22	2001:0400::/23	2001:5c0:1000::/39	AS6453	AS6939	34695 6939 6453
Update (Bogon Prefix)	4	2010-09-22	2002:0000::/16	2002:c058:6301::/128	AS30975	AS34695	34695 30975

<http://www.bgppmon.net/showbogons.php?inet=6&global>

IPv6 Neighbor Discovery Protocol

- IPv4 ARP replacement
- IPv6 auto configuration
- Neighbor Solicitation
- Router Solicitation
- Neighbor Advertisement
- Router Advertisement
- Duplicate address detection
- Redirections

Securing IPv6 Neighbor discovery protocol

- Neighbor discovery protocol Threats (RFC 3756, 2004)
 - Fake router advertisement
 - False neighbor advertisement messages
 - DOS against duplicate address detection
- Countermeasure
 - Access controls
 - Deploy Secure neighbor discovery SEND (RFC 3971, 2005)
 - Proofing address ownership
 - Protecting message integrity
 - Authorizing router advertisement messages
 - Configure Static neighbor entries for critical systems

Common Security issues in IPv4 and IPv6

- Packet Capturing
 - Implement IPSEC
- Routing Protocols
 - Implement MD5 keyed digest for BGP, IS-IS and EIGRP
 - Implement IPSEC to secure OSPF and RIP in IPv6
- Hijacking
 - Implement IPSEC
- Denial of service
 - Limited protection similar to IPv4. IPSEC can also help
- Malware and Worms
 - Deploy Antivirus, Patching, IDSes and access control

Security Considerations when running IPv6 with IPv4

- Dual Stack implementations requires different access policies for IPv6 networks
 - Surface of attack is doubled
 - Configure separate IPv6 access policies along existing IPv4 ones
- IPv6 tunnels usually bypass IPv4 policies
 - Originate/terminate tunnels on the perimeter where you can configure the required policies
 - Restrict dynamic tunnels by restricting unauthorized outgoing tunnels
 - Security considerations for 6to4 tunnels (RFC 3964, 2004)
 - 6to4 routers have to accept and decapsulate IPv4 packets from other 6to4 routers and relays
 - Spoofing
 - DOS

Further recommendations

- Subnet your network with foresight - Consider (RFC 3531, 2003)
 - Easier to manage your assignments
 - Make routing and aggregation efficient
 - Your link subnet is better to be /64 ?
- Plan addressing strategy
 - You will still need both IPv4 and IPv6
 - Decide on transition approach
 - Dual stack IPv6/IPv4
 - Tunneling: 6in4, 6to4, TEREDO, ISATAP, etc..
 - Translation: Address family translation - AFT

Further Recommendations

- Why /64 prefix length – Not to break at least the following:
 - Neighbor discover including SEND (RFC 3971, 2005)
 - Privacy extensions (RFC 4941, 2007)
 - Other technologies e.g. Mobile IPv6 route optimization (RFC 4866, 2007)

Conclusion

- Develop and define the requirements
- Develop a transition plan
- Develop security policies and control mechanisms
- Develop awareness
- Adopt a transition approach
- Monitor and enhance

Questions?

References

- <http://www.faqs.org/rfcs/rfc3964.html>
- <http://tools.ietf.org/html/rfc4941>
- <http://www.faqs.org/rfcs/rfc3971.html>
- <http://www.ietf.org/rfc/rfc3972.txt>
- <http://www.ietf.org/rfc/rfc3756.txt>
- <http://tools.ietf.org/html/rfc5156>
- <http://www.ietf.org/rfc/rfc5157.txt>
- <http://www.faqs.org/rfcs/rfc2827.html>
- <http://www.faqs.org/rfcs/rfc4443.html>

References

- <http://documents.iss.net/whitepapers/IPv6.pdf>
- <http://www.bgpmon.net/showbogons.php?inet=6&global>
- <http://www.6net.org/events/workshop-2003/marin.pdf>
- <http://www.6net.org/events/workshop-2003/marin.pdf>
- http://www.infosecwriters.com/text_resources/pdf/IPv6_SSotillo.pdf
- <http://6session.wordpress.com/2009/04/08/ipv6-martian-and-bogon-filters/>

References

- <http://www.ipv6.com>
- <http://seanconvery.com/v6-v4-threats.pdf>