Insights on IPv6 Security

Bilal Al Sabbagh, MSc, CISSP, CISA, CCSP

Senior Information & Network Security Consultant – NXme FZ-LLC

Information Security Researcher, PhD Candidate – Stockholm University

bilal@nxme.net

+966 50 440 3124

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

IPv6 Addressing Security

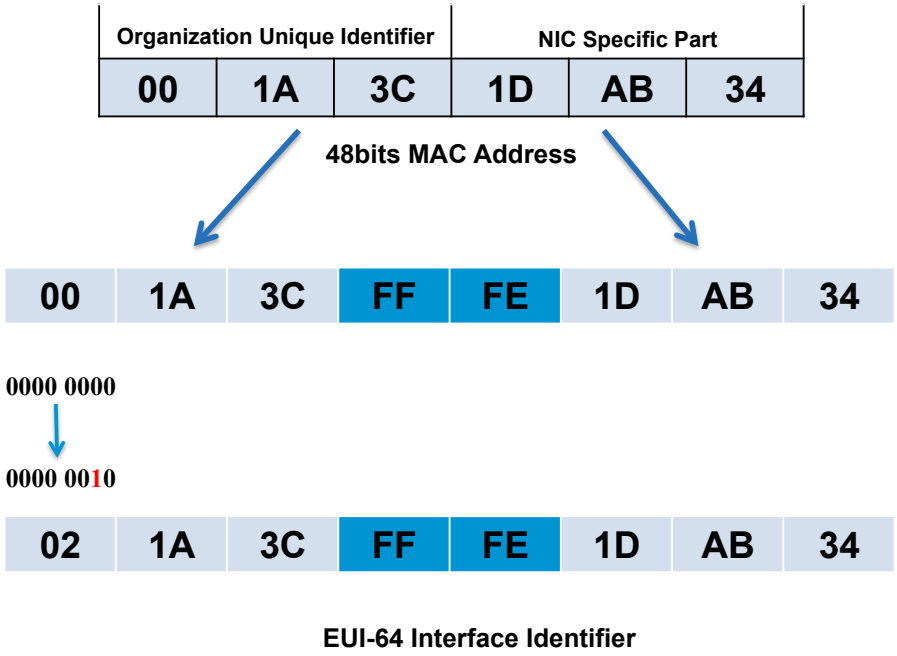
- The BIG address space make it harder for network reconnaissance using ping sweeps and hosts scans
  - No security scanners are yet capable to scan the default IPv6 /64 subnets.
    - 2^64 space needs around 5 Billions years to probe every service (RFC 5157, 2008)

```
nmap -6 2001:db8:130:20::/64

Starting Nmap 5.51 ( http://nmap.org ) at 2011-05-08 09:36 AST
Invalid host expression: 2001:db8:130:20::/64 -- slash not allowed.
IPv6 addresses can currently only be specified individually
QUITTING!
```

IPv6 Addressing Security

- 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 might be exposed
    - make it easier for attackers to scan your IPV6 network if they know/guess the vendor of the IEEE 802 network card
  - Compromise Layer2 based access controls ?
- Privacy enhanced EUI-64 (RFC 4941, 2007) addresses use temporarily random addresses 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.
  - Deploy statefull DHCPv6 when dynamic addressing is desired
  - Avoid using obvious and easy distinguished and memorable addresses

```
2001:db8:130:1234::cafe
```

  - Cryptographically Generated Addresses – CGA (RFC 3972, 2005)

IPv6 Addressing Security

- Cryptographically Generated Addresses – CGA
  - Interface identifiers are generated using one-way hashing function based on users public keys and auxiliary parameters
  - Prevent addresses spoofing and stealing
  - Limitations since addresses are not certified
  - Main application is secure neighbor discovery protocol (SEND)

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 with MTU less than 1280 Octets (RFC 2460, 1998)
  - Mitigations being tested
    - ACL with fragments keyword to permit or deny non initial fragments
    - Virtual Fragment Reassembly (VRF) for reassembling and examining fragments before passing to destination
- Spoofing Controls
  - Block spoofed packets according to (RFC 2827, 2000)
  - Block special use and non expected addresses (RFC 5156, 2008)

IPv6 Access Controls

- Broadcast Amplification Controls
  - IPv6 is designed to mitigate against such attacks
    - IPv6 nodes should not react to Broadcast or multicast addresses (RFC 4443, 2006)
    - But exceptions exist for “packet too big” and “parameter problem” icmpv6 messages destined to multicast groups
      - Mitigation is applied through rate-limiting these icmp messages.

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)	14	2011-03-29	f800:0000::/6	f800:2c00::/24	AS1273	AS6762	35579 8928 3257 6762 1273
Update (Bogon Prefix)	14	2011-03-29	f800:0000::/6	f800:2b00::/24	AS1273	AS6762	35579 8928 3257 6762 1273
Update (Bogon Prefix)	14	2011-03-29	a000:0000::/3	b800::/8	AS6774	AS1273	42708 21155 8455 3257 6762 1273 6774
Update (Bogon Prefix)	14	2011-03-29	8000:0000::/3	90a8::/24	AS47595	AS48287	8928 3257 6762 1273 15835 15835 48287 47595
Update (Bogon Prefix)	14	2011-03-29	6000:0000::/3	7c20:c00::/24	AS51408	AS15835	6850 3267 2603 3257 6762 1273 15835 15835 51408 51408
Update (Bogon Prefix)	14	2011-03-29	6000:0000::/3	7c01:5c00::/24	AS34387	AS6667	12637 3257 6762 1273 6667 34387
Update (Bogon Prefix)	14	2011-03-29	6000:0000::/3	7800::/8	AS5432	AS6774	42456 3257 6762 1273 6774 5432
Update (Bogon Prefix)	14	2011-03-29	4000:0000::/3	6000::/8	AS34171	AS13058	8607 3344 9153 3257 6762 1273 5539 13058 34171
Update (Bogon Prefix)	14	2011-03-29	4000:0000::/3	5000::/8	AS2609	AS5539	12637 3257 6762 1273 5539 2609
Update (Bogon Prefix)	14	2011-03-29	4000:0000::/3	4800::/8	AS1342	AS6667	6850 3267 2603 3257 6762 1273 6667 1342
Update (Bogon Prefix)	60	2011-04-19	2a00:0000::/12	2a03:d700::/32	AS35475	AS6939	32491 2914 6939 35475 35475 35475
Update (Bogon Prefix)	54	2011-04-12	2a00:0000::/12	2a03:9f00::/32	AS8676	AS6939	8928 2914 6939 8676
Update (Bogon Prefix)	6	2011-04-13	2a00:0000::/12	2a03:9f00::/32	AS8676	AS6939	39912 6939 8676
Update (Bogon Prefix)	56	2011-04-11	2a00:0000::/12	2a03:9700::/32	AS12859	AS6939	2497 6939 12859
Update (Bogon Prefix)	8	2011-04-12	2a00:0000::/12	2a03:9700::/32	AS12859	AS3257	378 20965 1299 3257 12859
Update (Bogon Prefix)	75	2011-03-25	2a00:0000::/12	2a03:900::/32	AS20574	AS15782	12859 16150 15782 20574
Update (Bogon Prefix)	54	2011-04-08	2a00:0000::/12	2a03:8500::/32	AS44291	AS21219	6453 6939 21219 44291

Snapshot of Bogonn prefixes seen on the Internet in May 6th , 2011
http://www.bgpmon.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
- Plan addressing strategy
  - You will still need both IPv4 and IPv6
  - Decide on transition approach
    - Dual stack IPv6/IPv4
    - Tunneling: Tunnel Broker, 6to4, TEREDO, 6RD, etc..
    - Translation: Address family translation - AFT
- Your link subnet is better to be /64 ?

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 your requirements
- Develop a transition plan
- Develop security policies and control mechanisms
- Develop awareness
- Decide on 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