IPv6- IPv4 Threat Comparison v1.0

Darrin Miller dmiller@cisco.com
Sean Convery sean@cisco.com

Motivations

- Discussions around IPv6 security have centered on IPsec
  - Though IPsec is mandatory in IPv6, the same issues with IPsec deployment remain from IPv4:
    - Configuration complexity
    - Key management
  - Therefore, IPv6 will be deployed largely without cryptographic protections of any kind
- Security in IPv6 is a much broader topic than just IPsec
  - Even with IPsec, there are many threats which still remain issues in IP networking

Research

- Examine many common threats against IPv4 and determine how these threats might affect an IPv6 network
  - Some new threats specific to IPv6 are also considered
- Present candidate IPv6 network best practices to the Internet community for discussion and revision
  - Best practices are edge specific though many apply to SPs
- Version 1.0 of the research results can be found here: http://www.cisco.com/security_services/ciag/documents/v6-v4-threats.pdf

IPv6 Attacks with Strong IPv4 Similarities (1/2)

- Sniffing
  - Without IPsec, IPv6 is no more or less likely to fall victim to a sniffing attack than IPv4
- Application Layer Attacks
  - Even with IPsec, the majority of vulnerabilities on the Internet today are at the application layer, something that IPsec will do nothing to prevent
- Rogue Devices
  - Rogue devices will be as easy to insert into an IPv6 network as in IPv4

IPv6 Attacks with Strong IPv4 Similarities (2/2)

- Man-in-the-Middle Attacks (MITM)
  - Without IPsec, any attacks utilizing MITM will have the same liklihood in IPv6 as in IPv4
- Flooding
  - Flooding attacks are identical between IPv4 and IPv6

Attacks with New Considerations

- Reconnaissance
  - Common subnet size of 2^{64} vs. 2^{8} will complicate brute force network enumeration attempts (years vs. seconds)
  - Well known multicast addresses make it easier to find key systems within a network (FF05::2 is a site-local all routers address)
- Unauthorized Access
  - Many new filtering considerations with ICMP, Multicast, IPsec, and extension headers

Attacks with New Considerations (cont.)

- Header Manipulation and Fragmentation
  - Fragmentation is no longer done by intermediatry devices and MTU discovery is required
    - Various extension header options may complicate traditional fragmentation reassembly as done by network devices today
- Layer 3-Layer 4 Spoofing
  - Global aggregation of IPv6 addresses should enhance anti-spoof filtering
  - Transition methods (such as 6to4 relay routers) enable spoofing in the interim

Attacks with New Considerations (cont.)

- ARP and DHCP Attacks
  - IPv4 ARP attacks are replace with IPv6 ND attacks with roughly the same issues
  - IPv4 DHCP attacks are augmented by stateless-autoconfiguration attacks in addition to traditional DHCP issues for IPv6
  - Secure Neighbor Discovery (SEND) is now a proposed standard
- Broadcast Amplification Attacks (smurf)
  - There is no IPv6 equivalent of an IPv4 directed broadcast packet making traditional smurf attacks impossible
  - fraggle type attacks may still be feasible

Attacks with New Considerations (cont.)

- Routing Attacks
  - IPv6 routing protocols are moving towards IPsec to secure transport as opposed to application specific protections (i.e. MD5)
- Viruses and Worms
  - Traditional viruses do not change
  - Worm / Viruses which use Internet scanning for propogation will need to adapt to the vastly increased size of IPv6 subnets

Attacks with New Considerations (cont.)

- Translation, Transition, and Tunneling Mechanisms
  - Various techniques in this space create new attack vectors around spoofing, redirecting, flooding, and encapsulating traffic
  - Lots of emphasis on not needing NAT, but organizations have already stated they will use NAT in their security designs.

Summary Findings

- IPv6 makes some things better/worse/different, but no more or less secure
- Better
  - Automated scanning and worm propagation is harder due to huge subnets
  - Link-local addressing can limit infrastructure attacks
  - IPsec is a mandatory feature
- Worse
  - Increased complexity in addressing and configuration
  - Lack of familiarity with IPv6 among operators
  - Immaturity of software
  - Vulnerabilities in transition techniques

Summary Findings (cont.)

- Most of the legacy issues with IPv4 security remain in IPv6
  - For example, ARP security issues in IPv4 are replaced with ND security issues in IPv6
  - SEND is now a proposed standard, but public key/private key crypto on every endpoint and certificate chains on every router. (needs more review)

Candidate Best Practices - sample

- Implement privacy extensions carefully - using them everywhere will complicate attack traceback and troubleshooting within your own organization
- Selectively filter ICMPv6 - Our intent is to make people aware you will need to allow more ICMPv6 through your firewalls to implement IPv6 effectively.
- Ensure adequate IPv6 fragmentation reassembly capabilities - Make sure you filter IPv6 fragments on infrastructure devices sufficiently to handle obsfucation and DOS attack vectors

Candidate Best Practices (cont.)

- Implement ingress filtering of packet with IPv6 multicast source addresses - SMURF is resolved in IPv6. Multicast filtering should mitigate potential fraggle-type attacks.
- Use IPv6 hop limits to protect network devices - Raise awareness of the GTSM in the enterprise.

Comments from IPv6/IPv4 Threat Comparison Review

- Font to small/lines to long
- ICMP filtering you should also allow more unreachables, such as port unreachables, or be prepared to sit through lengthy timeouts
- Too many implementations exist can't test for fragments less than 1280. Consider around ~600 bytes for non-last fragments as there is no legitimate need to fragment packets that are already 1280 bytes or smaller

Moving Forward

- Moving forward with IPv6 security stack testing to attempt to find IPv6 implementation flaws prior to widespread deployment
- New Section on MIPv6 or possibly a small paper on MIPv6 security
- Other research areas are identified in the document
  - IPv6 Worm Propagation Research
  - Amplification Attack Research
  - Possible opportunities for NANOG input and collaborative work moving forward

Questions?