



# IPv6 Dual Stack Security Implications

---

Darrin Miller [dmiller@cisco.com](mailto:dmiller@cisco.com)

Sean Convery [sean@cisco.com](mailto:sean@cisco.com)



# Agenda

---

- Dual Stack Threat Comparison
- Dual Stack Implementation Considerations
- Dual Stack Security Architecture Implications



# Motivations and Research

---

- Discussions around IPv6 security have centered on IPsec
- 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
  - Though IPsec is mandatory in IPv6, the same issues with IPsec deployment remain from IPv4:
    - Configuration complexity
    - Key management
- Examine many common threats against IPv4 and determine how these threats might affect an IPv6 network
  - 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

[http://www.cisco.com/security\\_services/ciag/documents/v6-v4-threats.pdf](http://www.cisco.com/security_services/ciag/documents/v6-v4-threats.pdf)



# Attacks with New Considerations

---

- Reconnaissance
- Unauthorized Access
- Header Manipulation and Fragmentation
- Layer 3-Layer 4 Spoofing
- Broadcast Amplification Attacks (smurf)
- Routing Attacks
- Viruses and Worms
- Translation, Transition, and Tunneling Mechanisms
- ARP and DHCP attacks



# ARP and DHCP Attacks

---

- ARP and DHCP Attacks
  - IPv4 ARP attacks are replaced 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 to mitigate the ND attacks



# IPv6 Attacks with Similarities

---

- Sniffing
- Application Layer Attacks
- Rogue Devices
- Man-in-the-Middle Attacks (MITM)
- Flooding



# Maturity of IPv6 Code Base

---

- IPv6 Stacks themselves
  - Base IPv6 stack stable and functioning
  - Several cases of DoS in OS and infrastructure devices dealing with IPv6
- Many security products do not support IPv6, but may still allow an IPv6 attack vector
- Some security products offer partial IPv6 support

The misunderstanding of IPv6 as an attack vector can result in a false sense of security



# Looking to the Future

---

- IPv6 security goals are on a collision course with IPv4 security methods
  - End-to-end crypto breaks granular visibility in the network (FWs, SSL offload, IDS)
    - Confidentiality is a subset of security
    - Possible solutions include host-to-network notification messages and \*gasp\* key escrow of some kind
  - Notion of perimeters is changing in IPv4 (PFWs, HIPS) but comfort with current best practices will not (and should not) change overnight
    - Customers will not implement host to host security in IPv6 just because the protocol supports it
    - Assumptions about the trustworthiness of the host are what started the network security market in the first place
- Security cooperation between the network and the host is already under way and should continue with IPv6



# Summary Findings

---

- In current deployments IPv6 makes some things better/worse/different, but no more or less secure
- Software Security Issues still exist, but there is an opportunity to make sure the code base is more stable before large scale deployments
- Further research is necessary to reconcile traditional security techniques with IPv6 capabilities