# IPv6 Security
# Why you should care

Stefan Avgoustakis - CSE

CISCO

# Why you should care about IPv6 Security now

- Most networks have already (partially) deployed IPv6
- You will likely perform a deployment in the near term
- You may communicate with IPv6 systems (via transition/co-existence technologies)


© 2013 Cisco Systems, Inc. All rights reserved.

# State of IPv6 Security

- Less experience/knowledge with IPv6
- IPv6 implementations are much less mature
- Security products less support for IPv6
- Transition increases complexity :
  - Dual Stack (IPv4 and IPv6)
  - Increased use of NATs
  - Increased use of tunnels


© 2013 Cisco Systems, Inc. All rights reserved.

# Key observations

IPv6 robustness

- Implementations have not really been the target of attackers, yet
- Only a handful of publicly available attack tools
- Lots of vulnerabilities and bugs still to be discovered.

IPv6 control policy points

- IPv6 inspection is not broadly supported in security devices

Education/Training/Awareness

- Pushing people to “Enable IPv6” as turn-key solution doesn’t work
- Creating awareness and expertise

CISCO

# Extension Header – Route Header type 0 Threat

- RH=0 provides similar functionality to that of IPv4 source routing
  - Can be leveraged to make packets bounce between network addresses
  - Higher impact due to some hosts "forwarded" them
- Attacker creates payload (A->B->A-B..) resulting in packet loop

# Extension Header – Route Header type 0 Mitigation

- Apply same policy for IPv6 as for Ipv4:
  - Block Routing Header type 0
- Prevent processing at the intermediate nodes
  - no ipv6 source-route
  - Windows, Linux, Mac OS: default setting
- RFC 5095 (Dec 2007) RH0 is deprecated
- Caution required – default enable prior to 2007

CISCO

# ARP Spoofing is now NDP Spoofing - Threat

- ARP is replaced by Neighbor Discovery Protocol
  - Nothing authenticated
  - Static entries overwritten by dynamic ones
- Stateless Address Autoconfiguration
  - Rogue RA (malicious or not)
  - All nodes badly configured
    - DoS
    - Traffic interception (Man In the Middle Attack)

CISCO

# ARP Spoofing is now NDP Spoofing – Mitigation RFC6104

- Manual configuration of host – discards RA's
- RA Snooping aka RA Guard
- Port ACL options – filter on RA packets (ICMP 134)
- Secure Neighbor Discovery SEND = NDP + crypto
- Host isolation :
  - Private VLAN works with IPv6
  - Port security works with IPv6
  - 802.1x works with IPv6

# IPv6 – Security Myths : Absence of Reconnaissance

- Default subnets in IPv6 have $2^{64}$ addresses - 10 Mpps = more than 50 000 years

Reconnaissance techniques get smarter :

- IPv6 addresses embedding IEEE IDs (Mac derived info)
- Increased deployment/reliance on dynamic DNS
- Human factor : Easy to remember addresses (wordy, IPv4 last octet)
- Multicast :
  - 3 site-local multicast addresses (not enabled by default)
    FF05::2 all-routers, FF05::FB mDNSv6, FF05::1:3 all DHCP servers
  - Several link-local multicast addresses (enabled by default)
    FF02::1 all nodes, FF02::2 all routers, FF02::F all UPnP, …

CISCO

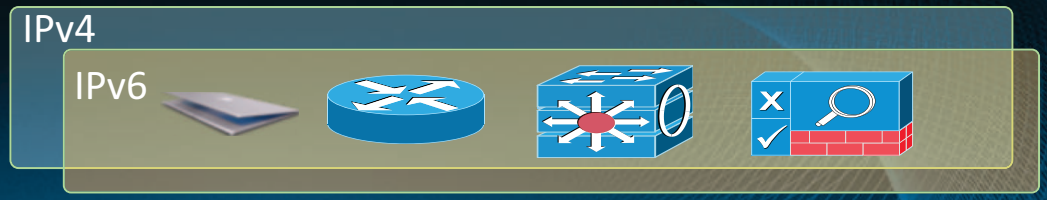
# IPv6 – Security Myths : IPSec will save the world

- IPv6 originally mandated the implementation of Ipsec - but not its use
- RFC 6434 "IPsec SHOULD be supported by all IPv6 nodes"
- IPSec comes with challenges:
  - Interesting scalability issue (n2 issue with IPsec)
  - Need to trust endpoints and end-users because the network cannot secure the traffic: no IPS, no ACL, no firewall
  - Network telemetry is blinded: NetFlow of little use
  - Network services hindered: QoS ?

CISCO

# IPv6 – Transition Mechanisms

## Dual Stack




Recommended Enterprise Co-existence strategy

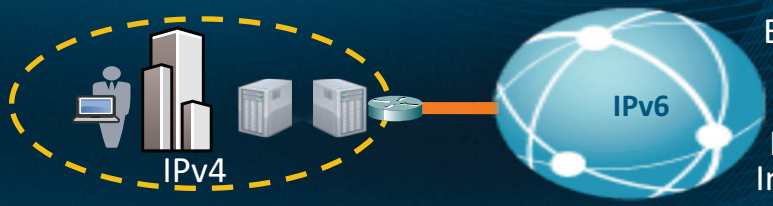
## Tunneling Services

IPv4 over IPv6

IPv6 over IPv4

Connect Islands of IPv6 or IPv4

## Translation Services




Business Partners
Government Agencies
International Sites
Remote Workers
Internet consumers

Connect to the IPv6 community

CISCO

# Dual Stack - intro

- Each node's IP stack supports both IPv4 and IPv6
- Domain names include both A and AAAA records
- IPv4 or IPv6 are used as needed or preferred – eg Happy Eyeballs
- Main operating systems include native IPv6 support enabled by default and prefer IPv6 over IPv4
- Dual-stack is the recommended strategy for hosts

CISCO

# Dual Stack – Threats and mitigation

- Lack of awareness that IPv6 is enabled – even on IPv4 only networks
- Rogue IPv6 Router uses RA's to configure IPv6 stack
- Host security mechanisms not IPv6 aware
- IPv6 used to evade network security controls

- Disable IPv6 stack on host if not used
- Create IPv6 control policy – host and network

CISCO

# Tunnels - Intro

Transport IPv6 packets over IPv4

- Configured: Manual configuration
  - 6in4
  - Tunnel broker
- Automatic: Tunnel end-points derived from the IPv6 addresses
  - ISATAP
  - Teredo
  - 6to4
  - 6rd

# Tunnels – Threats

ISATAP : Intra-Site Automatic Tunnel and Addressing Protocol

- Unauthorized tunnels—firewall bypass (protocol 41)
- IPv4 infrastructure looks like a Layer 2 network to ALL ISATAP hosts in the enterprise
- No authentication in ISATAP—rogue routers are possible
- Windows default to isatap.example.com
- IPv6 addresses can be guessed based on IPv4 prefix (scanning is back!)

CISCO

# Tunnels – Threats

Toredo :

- IPv6 over UDP (port 3544) - FW just sees IPv4 UDP traffic
- Hosts behind a NAT may become reachable from the public Internet
- Windows systems resole “teredo.ipv6.microsoft.com” – impersonate a Teredo server if he can attack the DNS

# Tunnels – Mitigations

Toredo :

- Filter IPv4.dst == known_teredo_servers && UDP.DstPort == 3544

ISATAP :

- Filter IPv4.Protocol == 41
- Check DNS logs for ISATAP resolving

# How imminent are IPv6 attacks ?

- The tools :
  - THC-IPv6 by Van Hauser
  - SI6 IPv6 Toolkit by Fernando Gont
- The exploits :
  - Zeus botnet is IPv6 compliant

CISCO

# Resources

- RFC's are your friend
- NIST Special Publication 800-119. Guidelines for the Secure Deployment of IPv6
- Cisco.com/go/ipv6
- 6lab.cisco.com
- IPv6 Security – Erick Vyncke and Scott Hogg @ Cisco Press

# Questions ?

savgoust@cisco.com - @savgoust

CISCO