Host Scanning in IPv6 Networks
(draft-gont-opsec-ipv6-host-scanning)

Fernando Gont

IETF 84
Vancouver, Canada. July 29-August 3, 2012

Overview

- IPv6 address-scanning attacks have long been considered unfeasible

- This myth has been based on the assumption that:

    - IPv6 subnets are /64s, **and**,

    - Host addresses are "randomly" selected from that /64

- However, IPv6 address-scanning attacks have already been seen in the wild

SI6
NETWORKS

draft-gont-opsec-ipv6-host-scanning

- Raises awareness about IPv6 address-scanning attacks

- Sheds some light on what the real search space is

- Explores a number of techniques for IPv6-address scanning

- Discusses possible mitigations to these attacks

- It is expected to explore other host-scanning techniques in detail (in future revisions) – in the TODO list!

SI6
NETWORKS

IPv6 address scanning of remote networks

SI6 NETWORKS

IPv6 addresses in the real world

- Malone measured (*) the address generation policy of hosts and routers in real networks

Address type	Percentage
SLAAC	50%
IPv4-based	20%
Teredo	10%
Low-byte	8%
Privacy	6%
Wordy	<1%
Others	<1%

Hosts

Address type	Percentage
Low-byte	70%
IPv4-based	5%
SLAAC	1%
Wordy	<1%
Privacy	<1%
Teredo	<1%
Others	<1%

Routers

Malone, D., "Observations of IPv6 Addresses", Passive and Active Measurement Conference (PAM 2008, LNCS 4979), April 2008, <http://www.maths.tcd.ie/~dwmalone/p/addr-pam08.pdf>.

IETF 84, OPSEC WG meeting
Vancouver, Canada. July 29-August 3, 2012

SI6
NETWORKS

IPv6 addresses embedding IEEE IDs

24 bits	16 bits	24 bits
IEEE OUI	**FF FE**	Lower 24 bits of MAC
Known or guessable	Known	Unknown
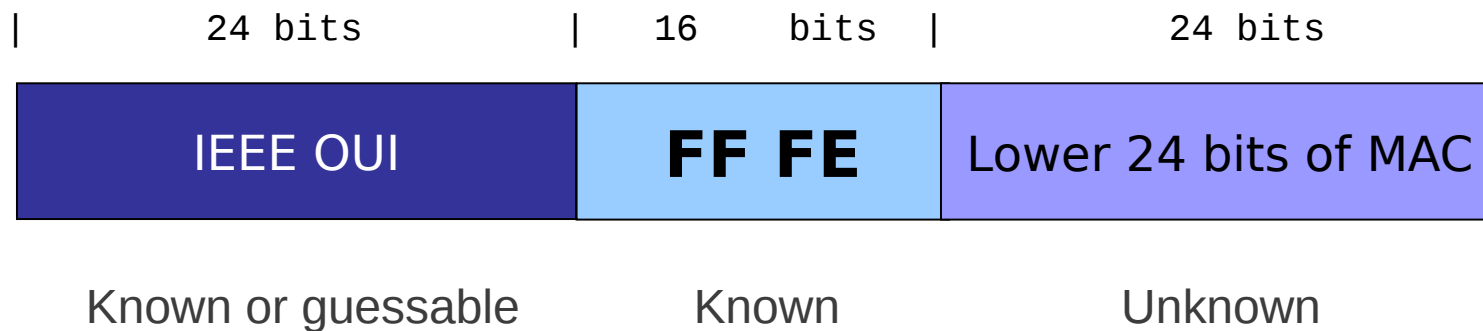
- In practice, the search space is at most ~2^{23} bits – **feasible!**

- The low-order 24-bits are not necessarily random:

  - An organization buys a large number of boxes

  - In that case, MAC addresses are usually consecutive

  - Consecutive MAC addresses are generally in use in geographically-close locations

SI6
NETWORKS

IPv6 addresses embedding IEEE IDs (II)

- Virtualization technologies present an interesting case

- Virtual Box employs OUI 08:00:27 (search space: ~2^{23})

- VMWare ESX employs:

  - Automatic MACs: OUI 00:05:59, and next 16 bits copied from the low order 16 bits of the host's IPv4 address (search space: ~2^8)

  - Manually-configured MACs:OUI 00:50:56 and the rest in the range 0x000000-0x3fffff (search space: ~2^{22})

SI6
NETWORKS

IPv6 addresses embedding IPv4 addr.

- They simply embed an IPv4 address in the IID

  - e.g.: 2000:db8::192.168.0.1

- Search space: same as the IPv4 search space – feasible!

IETF 84, OPSEC WG meeting
Vancouver, Canada. July 29-August 3, 2012

SI6
NETWORKS

IPv6 "low-byte" addresses

- The IID is set to all-zeros, except for the last byte

  - e.g.: 2000:db8::1

  - There are other variants..

- Search space: usually 2^8 or 2^{16} – feasible!

IETF 84, OPSEC WG meeting
Vancouver, Canada. July 29-August 3, 2012

SI6
NETWORKS

Possible mitigations

- Do not employ predictable Interface IDs

  - Replace traditional SLAAC addresses with draft-ietf-6man-stable-privacy-addresses

  - Manually-configured addresses should not result in "low-byte" addresses

  - etc.

- You may employ IPS'es – large number of non-existent IPv6 addresses will be probed!

SI6
NETWORKS

IPv6 address scanning of local networks

SI6
NETWORKS

Overview

- Leverage IPv6 all-nodes link-local multicast address

- Employ multiple probe types:

    - Normal multicasted ICMPv6 echo requests (don't work for Windows)

    - Unrecognized options of type 10xxxxxx

- Combine learned IIDs with known prefixes to learn all addresses

- Technique implemented in the scan6 tool of SI6's IPv6 toolkit

    - Available at: http://www.si6networks.com/tools

SI6
NETWORKS

Possible mitigations

- Do not respond to multicasted ICMPv6 echo requests

  - Currently implemented in Windows

- Multicasted IPv6 packets containing unsupported options of type 10xxxxxx should not elicit ICMPv6 errors

  - See draft-gont-6man-ipv6-smurf-amplifier

- **However**, it's virtually impossible to mitigate IPv6 address scanning of local networks

  - Think about mDNS, etc.

Moving forward

- Adopt as wg item?

IETF 84, OPSEC WG meeting
Vancouver, Canada. July 29-August 3, 2012

SI6
NETWORKS

Thanks!

Fernando Gont

fgont@si6networks.com

www.si6networks.com