Internet Engineering Task Force
INTERNET-DRAFT
Expires: Apr 21, 2004

Craig Metz
Extreme Networks
Jun-ichiro itojun Hagino
Research Lab, IIJ
Oct 21, 2003

IPv4-Mapped Addresses on the Wire Considered Harmful
draft-itojun-v6ops-v4mapped-harmful-02.txt

Status of this Memo

Abstract

The IPv6 Addressing Architecture [Hinden, 2003] defines the "IPv4-mapped IPv6 address." These addresses are used in the IPv6 basic API [Gilligan, 2003] to denote IPv4 addresses using AF_INET6 sockets. These addresses are used in protocol proposals such as SIIT [Nordmark, 2000] to denote IPv6 communication using AF_INET6 sockets. Therefore, IPv4-mapped addresses have two different meanings, and they are not distinguishable from the user-land applications.

This draft discusses security threats due to this ambiguity of IPv4-mapped address. It also discusses threats due to the additional complexities introduced by IPv4-mapped addresses. Finally, it proposes to resolve these problems by forbidding protocols from using IPv4-mapped addresses for IPv6 communications.

1. Dual meaning of IPv4-mapped address

Basic Socket Interface Extensions for IPv6 [Gilligan, 2003] defines the use of IPv4-mapped address with AF_INET6 sockets. IPv4-mapped addresses are used to represent IPv4 addresses using the IPv6 API (e.g., on AF_INET6 sockets). The API is designed with IPv4/v6 dual stack nodes in mind. When an IPv4 packet reaches an IPv4/v6 dual stack node, the node's IPv4 layer will process it, then pass it to the transport layer. When the transport layer finds an AF_INET6 listening socket, it will pass the packet to the listening socket as if it was from the corresponding IPv4-mapped address. In this document, we will refer to this as the "basic API behavior."

Some IPv6 translation protocols, such as SIIT [Nordmark, 2000] , uses IPv4-mapped addresses actual IPv6 packets on the wire. These protocols are designed for use with IPv6-only nodes. When an IPv6 packet containing these addresses reaches a node, the node's IPv6 layer will process it, then pass it to the transport layer. When the transport layer finds an AF_INET6 listening socket, it will pass the packet to the listening socket with the IPv4-mapped address intact. In this document, we will refer to this as the "SIIT behavior."

2. Threats due to the use of IPv4-mapped address on wire

When an application using the AF_INET6 API receives an IPv4-mapped addresses (for example, returned by getpeername(2) or recvfrom(2)), it cannot detect if the packet received by the node actually used IPv4 (basic API behavior) or IPv6 (SIIT behavior).

This ambiguity creates an opportunity that a malicious party can exploit in order to deceive victim nodes. For example:

o If an attacker transmits an IPv6 packet with ::ffff:127.0.0.1 in the IPv6 source address field, he might be able to bypass a node's access controls by deceiving applications into believing that the packet is from the node itself (e.g., the IPv4 loopback address, 127.0.0.1). The same attack might be performed using the node's IPv4 interface address instead.

o If an attacker transmits an IPv6 packet with IPv4-mapped addresses in the IPv6 destination address field corresponding to IPv4 addresses inside a site's security perimeter (e.g., ::ffff:10.1.1.1), he might be able to bypass IPv4 packet filtering rules and traverse a site's firewall.

o If an attacker transmits an IPv6 packet with IPv4-mapped addresses in the IPv6 source and destination fields to a protocol that swaps IPv6

source and destination addresses, he might be able to use a node as a proxy for certain types of attacks. For example, this might be used to construct broadcast multiplication and proxy TCP port scan attacks.

3. Recommended solution

Forbid the use of IPv4-mapped address on wire.

The IPv6 node requirements:

- IPv6 nodes MUST NOT generate packets that contain IPv4-mapped addresses in any network layer field. Specifically, the IPv6 header, routing header, options headers, and any other chained headers MUST NOT contain IPv4-mapped addresses.

- IPv6 nodes SHOULD NOT generate packets that contain IPv4-mapped addresses in any field. (As a particular exception, it MAY be acceptable for fields referring to third-party nodes to contain IPv4-mapped addresses. Implementors must ensure that, where this is allowed, it is done with great care.)

- IPv6 nodes MUST silently discard packets that contain IPv4-mapped address in IPv6 header fields, or IPv6 extension header fields.

The IPv6 router requirements:

- IPv6 routers MUST NOT forward packets that contain IPv4-mapped addresses in any field the router processes. Specifically, the IPv6 header, routing header, and the hop-by-hop options headers parsed by the router MUST NOT contain IPv4-mapped addresses.

- IPv6 routers MUST NOT advertise any prefixes into a routing protocol that are within the IPv4-mapped address space. Further, IPv6 routers MUST appropriately discard and/or ignore any received prefixes within the IPv4-mapped address space.

Standards requirements:

- The IPv6 address architecture document [Hinden, 2003] MUST explicitly state that IPv4-mapped addresses are exclusively for uses local to a node as specified in the basic API [Gilligan, 2003] and MUST never appear in the wire.

- Any document that suggests the use of IPv4-mapped addresses in packets on the wire SHOULD be modified to remove such usage. This will remove the threat due to the use of IPv4-mapped address on wire.

An alternate solution is to deprecate IPv4-mapped addresses from the basic API. Due to the wide deployment of applications that use IPv6 basic API, further study of this option's feasibility is required. This solution is not mutually exclusive with the recommended solution.

4. Suggested implementation tips

4.1. System (e.g., kernel and library) developers

o Drop any IPv6 packet with IPv4-mapped addresses in any of IPv6 header fields as well as IPv6 extension header fields. (N.B., this will make the system incompatible with the current version of SIIT [Nordmark, 2000])

o Drop any AAAA DNS response that contains IPv4-mapped addresses.

5. Security considerations

This document discusses security issues with the use of IPv4-mapped address. A recommended and alternate solution is provided.

6. Change History

00 -> 01
Craig Metz joins the team. Updates based on feedback given at v6ops interim meeting fall 2002. Move API issues to a separate draft.

01 -> 02
2553bis draft is now RFC3493. Refer RFC3513 instead of RFC2373.

References

Hinden, 2003.
R. Hinden and S. Deering, "IP Version 6 Addressing Architecture" in RFC3513 (April 2003). ftp://ftp.isi.edu/in-notes/rfc3513.txt.

Gilligan, 2003.
R. Gilligan, S. Thomson, J. Bound, J. McCann, and W. R. Stevens, "Basic Socket Interface Extensions for IPv6" in RFC3493 (February 2003). ftp://ftp.isi.edu/in-notes/rfc3493.txt.

Nordmark, 2000.
E. Nordmark, "Stateless IP/ICMP Translator (SIIT)" in RFC2765 (February, 2000). ftp://ftp.isi.edu/in-notes/rfc2765.txt.

Author's addresses

^L

Craig Metz
Extreme Networks
220 Spring Street, Suite 100
Herndon, VA 20170-5209, USA
Tel: +1 703 885 6721
email: cmetz@inner.net

Jun-ichiro itojun Hagino
Research Laboratory, Internet Initiative Japan Inc.
Takebashi Yasuda Bldg.,
3-13 Kanda Nishiki-cho,
Chiyoda-ku,Tokyo 101-0054, JAPAN
Tel: +81-3-5259-6350
Fax: +81-3-5259-6351
email: itojun@iijlab.net

^L