

opsec  
Internet-Draft  
Updates: [2827](#), [3704](#) (if approved)  
Intended status: Best Current Practice  
Expires: March 1, 2015

F. Gont  
UTN-FRH / SI6 Networks  
R. Hunter  
Globis Consulting BV  
J. Massar  
Massar Networking  
W. Liu  
Huawei Technologies  
August 28, 2014

Network Ingress Filtering: Defeating Attacks which employ Forged ICMP/  
ICMPv6 Error Messages  
draft-gont-opsec-icmp-ingress-filtering-00.txt

Abstract

Over the years, a number of attack vectors that employ forged ICMP/ICMPv6 error messages have been disclosed and exploited in the wild. The aforementioned attack vectors do not require that the source address of the packets be forged, but do require that the addresses of the IP/IPv6 packet embedded in the ICMP/ICMPv6 payload be forged. This document discusses a simple, effective, and straightforward method for using ingress traffic filtering to mitigate attacks that use forged addresses in the IP/IPv6 packet embedded in an ICMP/ICMPv6 payload. This advice is in line with the recommendations in [BCP38](#).

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of [BCP 78](#) and [BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <http://datatracker.ietf.org/drafts/current/>.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on March 1, 2015.

Internet-Draft

ICMP Ingress Filtering

August 2014

## Copyright Notice

Copyright (c) 2014 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

## Table of Contents

<a href="#">1.</a>	Introduction . . . . .	<a href="#">2</a>
<a href="#">2.</a>	Terminology . . . . .	<a href="#">3</a>
<a href="#">3.</a>	Overview . . . . .	<a href="#">3</a>
3.1.	Generation of ICMP Error Messages in Legitimate Scenarios	3
<a href="#">3.2.</a>	Attack Scenario . . . . .	<a href="#">5</a>
<a href="#">4.</a>	ICMP/ICMPv6 Network Ingress Filtering . . . . .	<a href="#">6</a>
<a href="#">5.</a>	IANA Considerations . . . . .	<a href="#">7</a>
<a href="#">6.</a>	Security Considerations . . . . .	<a href="#">7</a>
<a href="#">7.</a>	Acknowledgements . . . . .	<a href="#">7</a>
<a href="#">8.</a>	References . . . . .	<a href="#">7</a>
<a href="#">8.1.</a>	Normative References . . . . .	<a href="#">7</a>
<a href="#">8.2.</a>	Informative References . . . . .	<a href="#">8</a>
	Authors' Addresses . . . . .	<a href="#">8</a>

[1.](#) Introduction

Over the years, a number of attack vectors that employ forged ICMP/ICMPv6 error messages have been disclosed and exploited in the wild. The effects of these attack vectors have ranged from Denial of Service (DoS) to performance degradation [[US-CERT](#)] [[RFC5927](#)] [[I-D.gont-v6ops-ipv6-ehs-in-real-world](#)].

The aforementioned attack vectors do not require that the Source Address of the ICMP [[RFC0792](#)] or ICMPv6 [[RFC4443](#)] attack packets to be forged, but do require that the Destination Address of the IP [[RFC0791](#)] (in the case of ICMP) or IPv6 (in the case of ICMPv6)

packet embedded in the ICMP/ICMPv6 payload be forged. Thus, performing ingress filter (ala [BCP38](#) [[RFC2827](#)]) on the Destination Address of the embedded IP/IPv6 packet results in a simple, effective, and straightforward mitigation for any attack vectors based on ICMP/ICMPv6 error messages.

This document describes the network ingress filtering on ICMP/ICMPv6 payloads, and formally updates [BCP38](#) ([[RFC2827](#)]) such that the aforementioned filtering method is enforced as part of a general network ingress filtering strategy.

[Section 3](#) provides an overview of how ICMP/ICMPv6 error messages are generated, and how packets are crafted to perform attacks based on ICMP/ICMPv6 error messages. [Section 4](#) specifies network ingress filtering based on the ICMP/ICMPv6 payload.

## [2.](#) Terminology

Throughout this document the term "IP" is employed to refer to both the IPv4 [[RFC0791](#)] and IPv6 [[RFC2460](#)] protocols. That is, the term "IP" is employed when we do not mean to make a distinction between both versions of the protocol. In a similar vein, the term "ICMP" is employed to refer to both the ICMPv4 [[RFC0792](#)] and ICMPv6 [[RFC4443](#)] protocols. That is, the term "ICMP" is employed when we do not mean to make a distinction between both versions of the protocol.

For obvious reasons, ICMPv4 will only be employed in conjunction with IPv4, and ICMPv6 will always be employed in conjunction with IPv6. That is, the phrase "the IP packet embedded in the ICMP payload" means "the IPv4 packet embedded in the ICMPv4 payload" payload or "the IPv6 packet embedded in the ICMPv6 payload" (but NOT e.g. "the IPv4 packet embedded in the ICMPv6 payload").

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [[RFC2119](#)].

## [3.](#) Overview

Attack vectors based on ICMP error messages have been known for a long time, and have been described in detail in [[RFC5927](#)]. The following subsections provide an overview of how ICMP error messages

are generated in legitimate scenarios, and how an attacker would forge an ICMP error message in order to perform an attack based n ICMP error messages.

3.1. Generation of ICMP Error Messages in Legitimate Scenarios

The following figure illustrates a very simple network scenario in which two hosts (H1 and H2) are connected to each other by means of the router R1:

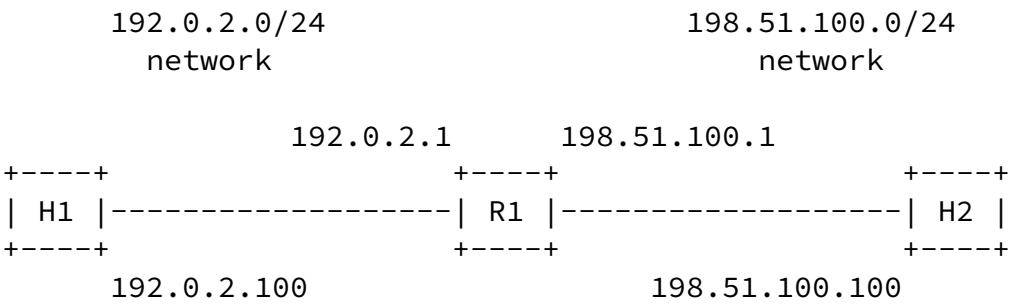
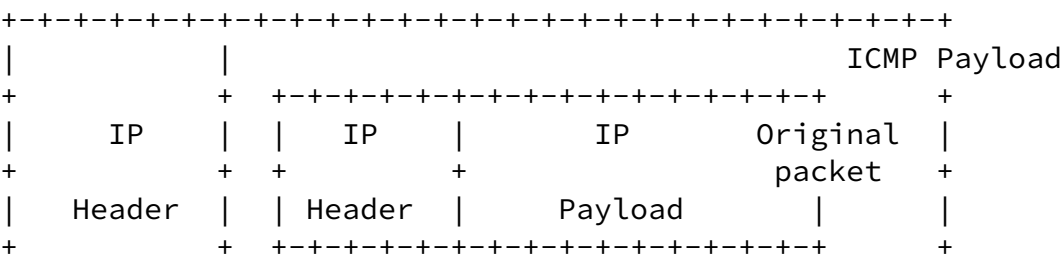


Figure 1: Sample Scenario for ICMP/ICMPv6 Error Generation

The aforementioned figure illustrates the IP addresses assigned to each of the involved network interfaces. For simplicity sake, this figure employs only IPv4 addresses, but the same logic applies to the IPv6 case.

Let us assume that H1 sends a packet towards H2, and that R1 encounters an error condition while processing such a packet. Typically, the error condition will be reported to H1 by means of an ICMP error message. The error message will have the following structure:



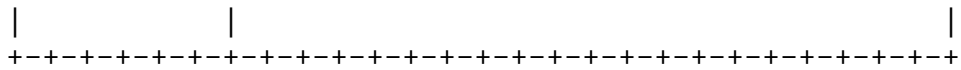


Figure 2: Structure of ICMP/ICMPv6 Error Messages

where the ICMP error message embeds the whole (or part of) the original packet that elicited the error message.

In our scenario, the relevant header fields would have the following values:

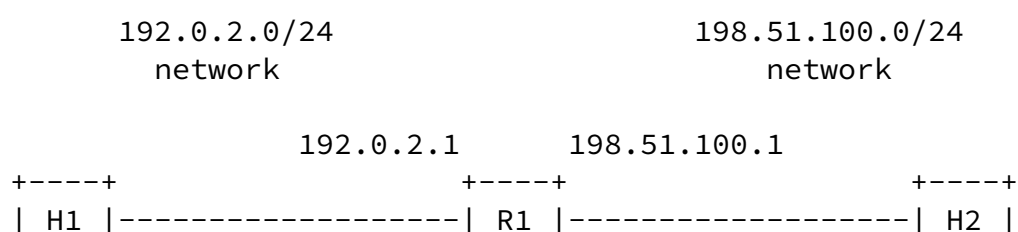
- o Source Address: 192.0.2.1
- o Destination Address: 192.0.2.100
- o Source Address (embedded packet): 192.0.2.100
- o Destination Address (embedded packet): 198.51.100.100

It should be clear that the Source Address of the packet could be virtually any address (since it corresponds to the IP address of a router reporting the error), while the Destination Address of the packet will be that of the target/destination of the ICMP error message. On the other hand, the IP addresses of the embedded packet will be those of the packet that elicited the ICMP error message.

The embedded IP packet is typically employed by the receiving system to demultiplex the ICMP error message.

### [3.2.](#) Attack Scenario

The following figure illustrates a very simple attack scenario in which an attacker (H3) tries to perform an attack against H1, while H1 is communicating with H2:



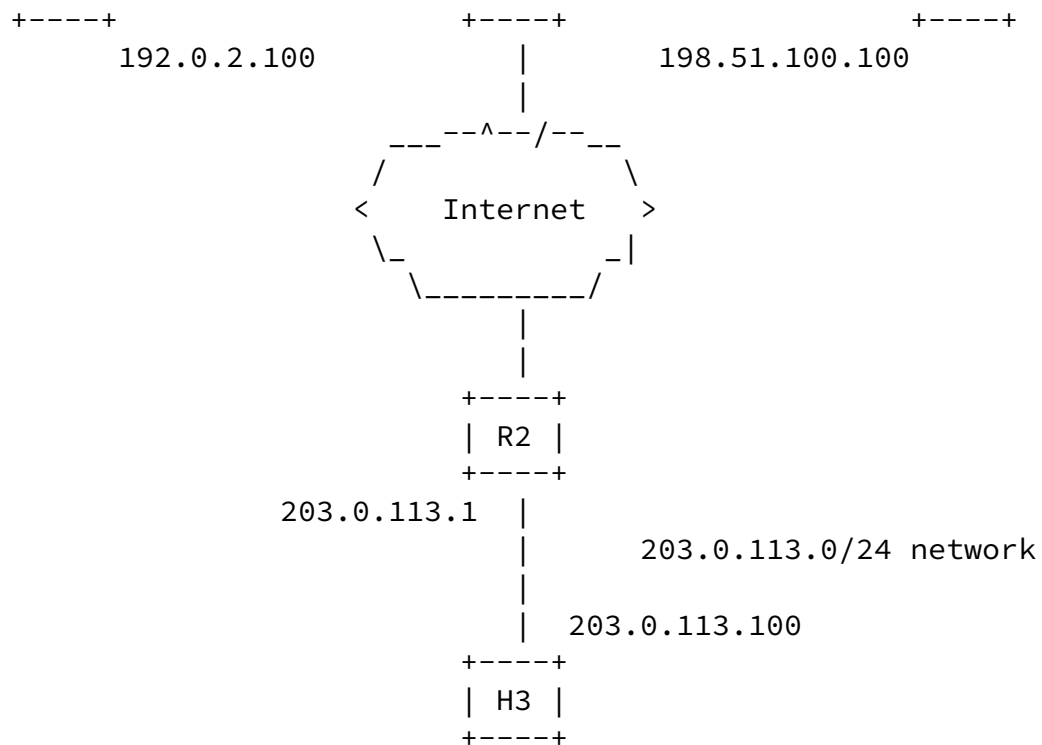


Figure 3: Hypothetical Attack Scenario

In our scenario, the attack packet sent by the attacker would have the same structure as that of Figure 2, with the following values:

- o Source Address: 203.0.113.100 (or forged address)
- o Destination Address: 192.0.2.100
- o Source Address (embedded packet): 192.0.2.100
- o Destination Address (embedded packet): 198.51.100.100

The Source Address of the packet is rather irrelevant and need not be forged. The Destination Address of the packet will be that of the attack target (H1 in our case). The Source Address of the embedded packet will be that of the attack target (H1 in our case). Finally, the Destination Address of the embedded packet will be that of the peer with which the attack target is communicating (H2 in our case).

If router R2 were to inspect the payload of the ICMP attack packet, it would conclude that the attack packet cannot be possibly valid, since packets destined to 198.51.100.100 would never be forwarded to the network from which the error message is originating. In a similar vein, if R1 were to examine the payload of the aforementioned ICMP error message, it would also conclude that the ICMP error message cannot be possibly valid, for the same reason stated before. Thus, filtering ICMP messages based on the ICMP payload could be employed as a countermeasure for attacks based on ICMP error messages.

#### [4.](#) ICMP/ICMPv6 Network Ingress Filtering

IPv4 and IPv6 nodes SHOULD perform ingress filtering on the Destination Address of the IP packet embedded in the ICMP payload.

In the most simple case, where network ingress filtering is implemented at an edge network with ingress access lists (as suggested in [[RFC2827](#)]), a router should check:

IF     embedded packet's Destination Address is from within my network  
THEN   forward as appropriate

IF     embedded packet's Destination Address is anything else  
THEN   deny packet

Alternatively, in the same "edge network" scenario, the aforementioned network ingress filtering could possibly be implemented by performing unicast Reverse Path Forwarding (uRPF) on the Destination Address of the embedded IP packet.

We note, however, that the techniques described in [[RFC3704](#)] should be evaluated when the aforementioned network ingress filtering is to

be implemented in more complex network scenarios, such as that of a multihomed networks.

Finally, we note that packet drops SHOULD be logged, since this then provides a basis for monitoring any suspicious activity.

#### [5.](#) IANA Considerations

This document has no actions for IANA.

## 6. Security Considerations

This document provides advice on performing network ingress filtering on ICMPv4 and ICMPv6 error messages, such that attacks based on such messages are mitigated.

We note that a given platform may or may not be able to filter ICMP error messages base on the ICMP payload. Thus, the aforementioned filter SHOULD only be performed where applicable. Additionally, enforcing the aforementioned filtering method might impact the performance of the filtering device (see e.g., [[Cisco-EH-Cons](#)] and [[Zack-FW-Benchmark](#)] for a discussion of the IPv6 case). This should be considered before enabling the aforementioned filtering method.

## 7. Acknowledgements

The authors of this document would like to thank (in alphabetical order) [TBD] for providing valuable comments on earlier versions of this document.

## 8. References

### 8.1. Normative References

- [RFC0791] Postel, J., "Internet Protocol", STD 5, [RFC 791](#), September 1981.
- [RFC0792] Postel, J., "Internet Control Message Protocol", STD 5, [RFC 792](#), September 1981.
- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), March 1997.
- [RFC2460] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", [RFC 2460](#), December 1998.



## [8.2.](#) Informative References

### [Cisco-EH-Cons]

Cisco, , "IPv6 Extension Headers Review and Considerations", October 2006,  
<[http://www.cisco.com/en/US/technologies/tk648/tk872/technologies\\_white\\_paper0900aecd8054d37d.pdf](http://www.cisco.com/en/US/technologies/tk648/tk872/technologies_white_paper0900aecd8054d37d.pdf)>.

### [I-D.gont-v6ops-ipv6-ehs-in-real-world]

Gont, F., Linkova, J., Chown, T., and W. Will, "IPv6 Extension Headers in the Real World", [draft-gont-v6ops-ipv6-ehs-in-real-world-00](#) (work in progress), August 2014.

[RFC2827] Ferguson, P. and D. Senie, "Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing", [BCP 38](#), [RFC 2827](#), May 2000.

[RFC3704] Baker, F. and P. Savola, "Ingress Filtering for Multihomed Networks", [BCP 84](#), [RFC 3704](#), March 2004.

[RFC5927] Gont, F., "ICMP Attacks against TCP", [RFC 5927](#), July 2010.

[US-CERT] US-CERT, , "US-CERT Vulnerability Note VU#222750: TCP/IP Implementations do not adequately validate ICMP error messages", <http://www.kb.cert.org/vuls/id/222750>, 2005, .

### [Zack-FW-Benchmark]

Zack, E., "Firewall Security Assessment and Benchmarking IPv6 Firewall Load Tests", IPv6 Hackers Meeting #1, Berlin, Germany. June 30, 2013,  
<<http://www.ipv6hackers.org/meetings/ipv6-hackers-1/zack-ipv6hackers1-firewall-security-assessment-and-benchmarking.pdf>>.

## Authors' Addresses

Fernando Gont  
UTN-FRH / SI6 Networks  
Evaristo Carriego 2644  
Haedo, Provincia de Buenos Aires 1706  
Argentina

Phone: +54 11 4650 8472  
Email: fgont@si6networks.com  
URI: <http://www.si6networks.com>

Ray Hunter  
Globis Consulting BV  
Weegschaalstraat 3  
Eindhoven 5632CW  
NL

Email: v6ops@globis.net

Jeroen Massar  
Massar Networking  
Swiss Post Box 101811  
Zuercherstrasse 161  
Zuerich CH-8010  
CH

Email: jeroen@massar.ch  
URI: <http://jeroen.massar.ch>

Will(Shucheng) Liu  
Huawei Technologies  
Bantian, Longgang District  
Shenzhen 518129  
P.R. China

Email: liushucheng@huawei.com

