Operational Security Capabilities for
IP Network Infrastructure (opsec)
Internet-Draft
Intended status: BCP
Expires: June 19, 2012

F. Gont
UTN/FRH
R. Atkinson
Consultant
December 17, 2011

Recommendations on filtering of IP packets containing IP options
draft-gont-opsec-ip-options-filtering-02.txt

Abstract

This document document provides advice on the filtering of packets based on the IP options they contain. Additionally, it discusses the operational and interoperability implications of such filtering.

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 June 19, 2012.

Copyright Notice

Table of Contents

1. Introduction

Various protocols may use IP Options to some extent, therefore the filtering of such options may have implications on proper functioning of the protocol. As such, this document attempts to discuss the operational and interoperability implications of such filtering. Additionally, this document will outline what a network operator might do in a typical enterprise or Service Provider environment.

We note that data seems to indicate that there is a current widespread practice of blocking IPv4 optioned packets. There are various plausible approaches to minimize the potential negative effects of IPv4 optioned packets while allowing some options semantics. One approach is to allow for specific options that are expected or needed, and a default deny. A different approach is to deny unneeded options and a default allow. Yet a third option is to allow for end-to-end semantics by ignoring options and treating packets as un-optioned while in transit. The current state tends to support the first or third approaches as more realistic. Some results of regarding the current state of affairs with respect to filtering of packets containing IP options can be found in [MEDINA].

We also note that while this document provides advice on a "per IP option type", not all devices may provide functionality to filter IP packets on a "per IP option type". Additionally, even in cases in which such functionality is provided, the operator might want to specify a filtering policy with a coarser granularity (rather than on a "per IP option type" granularity), as indicated above.

Finally, in scenarios in which processing of IP options by intermediate systems is not required, a widespread approach is to simply ignore IP options, and process the corresponding packets as if they do not contain any IP options.

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].

2. IP Options

IP options allow for the extension of the Internet Protocol

There are two cases for the format of an option:

- Case 1: A single byte of option-type.

- Case 2: An option-type byte, an option-length byte, and the actual option-data bytes.

In the Case 2, the option-length byte counts the option-type byte and the option-length byte, as well as the actual option-data bytes.

All current and future options except "End of Option List" (Type = 0) and "No Operation" (Type = 1), are of Class 2.

The option-type has three fields:

- 1 bit: copied flag.
- 2 bits: option class.
- 5 bits: option number.

The copied flag indicates whether this option should be copied to all fragments in the event the packet carrying it needs to be fragmented:

- 0 = not copied.
- 1 = copied.

The values for the option class are:

- 0 = control.
- 1 = reserved for future use.
- 2 = debugging and measurement.
- 3 = reserved for future use.

This format allows for the creation of new options for the extension of the Internet Protocol (IP).

Finally, the option number identifies the syntax of the rest of the option.

[IANA2006b] contains the list of the currently assigned IP option numbers.

3. General security implications of IP options

3.1. Processing requirements

Router manufacturers tend to do IP option processing in a slower path. Unless special care is taken, this represents Denial of Service (DoS) risk, as there is potential for overwhelming the router with option processing.

The following sections contain a description of each of the IP options that have so far been specified, a discussion of possible interoperability implications if packets containing such options are filtered, and specific advice on whether to filter packets containing these options in a typical enterprise or Service Provider environment.

4. Advice on handling of specific IP Options

4.1. End of Option List (Type = 0)

4.1.1. Uses

This option is used to indicate the "end of options" in those cases in which the end of options would not coincide with the end of the Internet Protocol Header.

4.1.2. Option specification

Specified in RFC 791 [RFC0791].

4.1.3. Threats

No security issues are known for this option, other than the general security implications of IP options discussed in Section 3.

4.1.4. Operational/interoperability impact if blocked

Packets containing any IP options are likely to include an End of Option List. Therefore, if packets containing this option are filtered, it is very likely that legitimate traffic is filtered.

4.1.5. Advice

Do not filter packets containing this option.

4.2. No Operation (Type = 1)

4.2.1. Uses

The no-operation option is basically meant to allow the sending system to align subsequent options in, for example, 32-bit boundaries.

4.2.2. Option specification

Specified in RFC 791 [RFC0791].

4.2.3. Threats

No security issues are known for this option, other than the general security implications of IP options discussed in Section 3.

4.2.4. Operational/interoperability impact if blocked

4.2.5. Advice

Do not filter packets containing this option.

4.3. Loose Source and Record Route (LSRR) (Type = 131)

RFC 791 states that this option should appear, at most, once in a given packet. Thus, if a packet contains more than one LSRR option, it should be dropped, and this event should be logged (e.g., a counter could be incremented to reflect the packet drop). Additionally, packets containing a combination of LSRR and SSRR options should be dropped, and this event should be logged (e.g., a counter could be incremented to reflect the packet drop).

4.3.1. Uses

This option lets the originating system specify a number of intermediate systems a packet must pass through to get to the destination host. Additionally, the route followed by the packet is recorded in the option. The receiving host (end-system) must use the reverse of the path contained in the received LSRR option.

The LSSR option can be of help in debugging some network problems. Some ISP (Internet Service Provider) peering agreements require support for this option in the routers within the peer of the ISP.

4.3.2. Option specification

Specified in RFC 791 [RFC0791].

4.3.3. Threats

The LSRR option has well-known security implications. Among other things, the option can be used to:

- Bypass firewall rules
- Reach otherwise unreachable internet systems
- Establish TCP connections in a stealthy way
- Learn about the topology of a network
- Perform bandwidth-exhaustion attacks

Of these attack vectors, the one that has probably received least attention is the use of the LSRR option to perform bandwidth exhaustion attacks. The LSRR option can be used as an amplification method for performing bandwidth-exhaustion attacks, as an attacker could make a packet bounce multiple times between a number of systems by carefully crafting an LSRR option.

> This is the IPv4-version of the IPv6 amplification attack that was widely publicized in 2007 [Biondi2007]. The only difference is that the maximum length of the IPv4 header (and hence the LSRR option) limits the amplification factor when compared to the IPv6 counter-part.

4.3.4. Operational/interoperability impact if blocked

Network troubleshooting techniques that may employ the LSRR option (such as ping or traceroute) would break. Nevertheless, it should be noted that it is virtually impossible to use such techniques due to widespread filtering of the LSRR option.

4.3.5. Advice

All systems should, by default, drop IP packets that contain an LSRR option.

4.4. Strict Source and Record Route (SSRR) (Type = 137)

4.4.1. Uses

This option allows the originating system to specify a number of intermediate systems a packet must pass through to get to the destination host. Additionally, the route followed by the packet is recorded in the option, and the destination host (end-system) must

use the reverse of the path contained in the received SSRR option.

This option is similar to the Loose Source and Record Route (LSRR) option, with the only difference that in the case of SSRR, the route specified in the option is the exact route the packet must take (i.e., no other intervening routers are allowed to be in the route).

The SSSR option can be of help in debugging some network problems. Some ISP (Internet Service Provider) peering agreements require support for this option in the routers within the peer of the ISP.

4.4.2. Option specification

Specified in RFC 791 [RFC0791].

4.4.3. Threats

The SSRR option has the same security implications as the LSRR option. Please refer to Section 4.3 for a discussion of such security implications.

4.4.4. Operational/interoperability impact if blocked

Network troubleshooting techniques that may employ the SSRR option (such as ping or traceroute) would break. Nevertheless, it should be noted that it is virtually impossible to use such techniques due to widespread filtering of the SSRR option.

4.4.5. Advice

All systems should, by default, drop IP packets that contain an SSRR option.

4.5. Record Route (Type = 7)

4.5.1. Uses

This option provides a means to record the route that a given packet follows.

4.5.2. Option specification

Specified in RFC 791 [RFC0791].

4.5.3. Threats

This option can be exploited to map the topology of a network. However, the limited space in the IP header limits the usefulness of

this option for that purpose.

4.5.4. Operational/interoperability impact if blocked

Network troubleshooting techniques that may employ the RR option (such as ping with the RR option) would break. Nevertheless, it should be noted that it is virtually impossible to use such techniques due to widespread filtering of the RR option.

4.5.5. Advice

Drop IP packets that contain a Record Route option.

4.6. Stream Identifier (Type = 136)

The Stream Identifier option originally provided a means for the 16-bit SATNET stream Identifier to be carried through networks that did not support the stream concept.

However, as stated by Section 4.2.2.1 of RFC 1812 [RFC1812], this option is obsolete. Therefore, it must be ignored by the processing systems.

In the case of legacy systems still using this option, the length field of the option should be checked to be 4. If the option does not pass this check, it should be dropped, and this event should be logged (e.g., a counter could be incremented to reflect the packet drop).

RFC 791 states that this option appears at most once in a given datagram. Therefore, if a packet contains more than one instance of this option, it should be dropped, and this event should be logged (e.g., a counter could be incremented to reflect the packet drop).

4.6.1. Uses

4.6.2. Option specification

Specified in RFC 791 [RFC0791].

4.6.3. Threats

TBD

4.6.4. Operational/interoperability impact if blocked

None.

4.6.5. Advice

Filter IP packets that contain a Stream Identifier option.

4.7. Internet Timestamp (Type = 68)

4.7.1. Uses

This option provides a means for recording the time at which each system processed this datagram.

4.7.2. Option specification

Specified by RFC 791 [RFC0791].

4.7.3. Threats

The timestamp option has a number of security implications. Among them are:

- It allows an attacker to obtain the current time of the systems that process the packet, which the attacker may find useful in a number of scenarios.
- It may be used to map the network topology, in a similar way to the IP Record Route option.
- It may be used to fingerprint the operating system in use by a system processing the datagram.
- It may be used to fingerprint physical devices, by analyzing the clock skew.

[Kohno2005] describes a technique for fingerprinting devices by measuring the clock skew. It exploits, among other things, the timestamps that can be obtained by means of the ICMP timestamp request messages [RFC0791]. However, the same fingerprinting method could be implemented with the aid of the Internet Timestamp option.

4.7.4. Operational/interoperability impact if blocked

No security issues are known for this option, other than the general security implications of IP options discussed in Section 3.

4.7.5. Advice

Filter IP packets that contain an Internet Timestamp option.

4.8. Router Alert (Type = 148)

4.8.1. Uses

The Router Alert option has the semantic "routers should examine this packet more closely, if they participate in the functionality denoted by the Value of the option".

4.8.2. Option specification

The Router Alert option is defined in RFC 2113 [RFC2113] and later updates to it have been clarified by RFC 5350 [RFC5350]. It contains a 16-bit Value governed by an IANA registry (see [RFC5350]).

4.8.3. Threats

The security implications of the Router Alert option have been discussed in detail in [I-D.ietf-intarea-router-alert-considerations]. Basically, the Router Alert option might be exploited to perform a Denial of Service (DoS) attack by exhausting CPU resources at the processing routers.

4.8.4. Operational/interoperability impact if blocked

Applications that employ the Router Alert option (such as RSVP [RFC2205]) would break.

4.8.5. Advice

This option should be allowed only on controlled environments, where the option can be used safely ([I-D.ietf-intarea-router-alert-considerations] identifies such environments). In other environments, packets containing this option should be dropped.

4.9. Probe MTU (Type = 11) (obsolete)

4.9.1. Uses

This option originally provided a mechanism to discover the Path-MTU. It has been declared obsolete.

4.9.2. Option specification

This option was defined in RFC 1063 [RFC1063]. This option is obsolete.

4.9.3. Threats

None

4.9.4. Operational/interoperability impact if blocked

None

4.9.5. Advice

Filter IP packets that contain a Probe MTU option.

4.10. Reply MTU (Type = 12) (obsolete)

4.10.1. Uses

This option and originally provided a mechanism to discover the Path-MTU. It is now obsolete.

4.10.2. Option specification

This option was originally specified by RFC 1063 [RFC1063], and is now obsolete.

4.10.3. Threats

None.

4.10.4. Operational/interoperability impact if blocked

None

4.10.5. Advice

Filter IP packets that contain a Reply MTU option.

4.11. Traceroute (Type = 82)

4.11.1. Uses

This option originally provided a mechanism to trace the path to a host.

4.11.2. Option specification

This option was originally specified by RFC 1393 [RFC1393]. It has been declared obsolete.

4.11.3. Threats

None

4.11.4. Operational/interoperability impact if blocked

None

4.11.5. Advice

Filter IP packets that contain a Traceroute option.

4.12. DoD Basic Security Option (Type = 130)

4.12.1. Uses

This option is used by Multi-Level-Secure (MLS) end-systems and intermediate systems in specific environments to [RFC1108]:

- Transmit from source to destination in a network standard representation the common security labels required by computer security models [Landwehr81],
- Validate the datagram as appropriate for transmission from the source and delivery to the destination, and,
- Ensure that the route taken by the datagram is protected to the level required by all protection authorities indicated on the datagram.

The DoD Basic Security Option (BSO) is currently implemented in a number of operating systems (e.g., [IRIX2008], [SELinux2008], [Solaris2008], and [Cisco2008]), and deployed in a number of high-security networks. These networks are typically either in physically secure locations, protected by military/governmental communications security equipment, or both. Such networks are typically built using commercial off-the-shelf (COTS) IP routers and Ethernet switches, but are not normally interconnected with the global public Internet. This option probably has more deployment now than when the IESG removed this option from the IETF standards-track. [RFC5570] describes a similar option recently defined for IPv6 and has much more detailed explanations of how sensitivity label options are used in real-world deployments.

4.12.2. Option specification

It is specified by RFC 1108 [RFC1108] (which obsoletes RFC 1038 [RFC1038]).

RFC 791 [RFC0791] defined the "Security Option" (Type = 130), which used the same option type as the DoD Basic Security option discussed in this section. The "Security Option" specified in RFC 791 is considered obsolete by Section 3.2.1.8 of RFC 1122, and therefore the discussion in this section is focused on the DoD Basic Security option specified by RFC 1108 [RFC1108].

Section 4.2.2.1 of RFC 1812 states that routers "SHOULD implement this option".

[IOS-12.2][RFC4949][RFC3585][RFC4807]

4.12.3. Threats

Presence of this option in a packet does not by itself create any specific new threat (other than the usual generic issues that might be created if packets with options are forwarded via the "slow path"). Packets with this option ought not normally be seen on the global public Internet.

4.12.4. Operational/interoperability impact if blocked

If packets with this option are blocked or if the option is stripped from the packet during transmission from source to destination, then the packet itself is likely to be dropped by the receiver because it isn’t properly labelled. In some cases, the receiver might receive the packet but associate an incorrect sensitivity label with the received data from the packet whose BSO was stripped by an intermediate router or firewall. Associating an incorrect sensitivity label can cause the received information either to be handled as more sensitive than it really is ("upgrading") or as less sensitive than it really is ("downgrading"), either of which is problematic.

4.12.5. Advice

Routers and firewalls ought not by default drop packets containing IPSO and also ought not by default strip the IPSO from the packet. For auditing reasons, routers and firewalls SHOULD be capable of logging the numbers of packets containing the BSO on a per-interface basis. Also, routers and firewalls SHOULD be capable of filtering packets based on the BSO presence as well as the BSO values.

4.13. DoD Extended Security Option (Type = 133)

4.13.1. Uses

This option permits additional security labeling information, beyond that present in the Basic Security Option (Section 4.12), to be supplied in an IP datagram to meet the needs of registered authorities.

4.13.2. Option specification

The DoD Extended Security Option (ESO) is specified by RFC 1108 [RFC1108].

[IOS-12.2][RFC4949][RFC3585][RFC4807]

4.13.3. Threats

Presence of this option in a packet does not by itself create any specific new threat (other than the usual generic issues that might be created if packets with options are forwarded via the "slow path"). Packets with this option ought not normally be seen on the global public Internet

4.13.4. Operational/interoperability impact if blocked

If packets with this option are blocked or if the option is stripped from the packet during transmission from source to destination, then the packet itself is likely to be dropped by the receiver because it isn’t properly labelled. In some cases, the receiver might receive the packet but associate an incorrect sensitivity label with the received data from the packet whose ESO was stripped by an intermediate router or firewall. Associating an incorrect sensitivity label can cause the received information either to be handled as more sensitive than it really is ("upgrading") or as less sensitive than it really is ("downgrading"), either of which is problematic.

4.13.5. Advice

Routers and firewalls ought not by default drop packets containing an ESO and also ought not by default strip the ESO from the packet. For auditing reasons, routers and firewalls SHOULD be capable of logging the numbers of packets containing the ESO on a per-interface basis. Also, routers and firewalls SHOULD be capable of filtering packets based on the ESO presence as well as the ESO values.

4.14. Commercial IP Security Option (CIPSO) (Type = 134)

4.14.1. Uses

This option was proposed by the Trusted Systems Interoperability Group (TSIG), with the intent of meeting trusted networking requirements for the commercial trusted systems market place.

It is currently implemented in a number of operating systems (e.g., IRIX [IRIX2008], Security-Enhanced Linux [SELinux2008], and Solaris [Solaris2008]), and deployed in a number of high-security networks.

4.14.2. Option specification

This option is specified in [CIPSO1992] and [FIPS1994]. There are zero known IP router implementations of CIPSO. Several MLS operating systems support CIPSO, generally the same MLS operating systems that support IPSO.

4.14.3. Threats

Presence of this option in a packet does not by itself create any specific new threat (other than the usual generic issues that might be created if packets with options are forwarded via the "slow path"). Packets with this option ought not normally be seen on the global public Internet.

4.14.4. Operational/interoperability impact if blocked

If packets with this option are blocked or if the option is stripped from the packet during transmission from source to destination, then the packet itself is likely to be dropped by the receiver because it isn’t properly labelled. In some cases, the receiver might receive the packet but associate an incorrect sensitivity label with the received data from the packet whose CIPSO was stripped by an intermediate router or firewall. Associating an incorrect sensitivity label can cause the received information either to be handled as more sensitive than it really is ("upgrading") or as less sensitive than it really is ("downgrading"), either of which is problematic.

4.14.5. Advice

Because of the design of this option, with variable syntax and variable length, it is not practical to support specialized filtering using the CIPSO information. No routers or firewalls are known to support this option. However, by default a router or firewall should not modify or remove this option from IP packets and a router or

firewall should not by default drop packets containing this option.

4.15. Sender Directed Multi-Destination Delivery (Type = 149)

4.15.1. Uses

This option originally provided unreliable UDP delivery to a set of addresses included in the option. It is currently obsolete.

4.15.2. Option specification

This option is defined in RFC 1770 [RFC1770].

4.15.3. Threats

This option could have been exploited for bandwidth-amplification in Denial of Service (DoS) attacks.

4.15.4. Operational/interoperability impact if blocked

None.

4.15.5. Advice

Filter IP packets that contain a Sender Directed Multi-Destination Delivery option.

5. Security Considerations

This document provides advice on the filtering of IP packets that contain IP options. Filtering of such packets can help to mitigate the security issues that arise from use of different IP options.

6. Acknowledgements

The authors would like to thank Carlos Pignataro and Donald Smith for providing valuable comments on earlier versions of this document.

Part of this document is based on the document &Security Assesment of the Internet Protocol& [CPNI2008] that is the result of a project carried out by Fernando Gont on behalf of UK CPNI (formerly NISCC).

Fernando Gont would like to thank UK CPNI (formerly NISCC) for their continued support.

7. Contributors

Carlos Pignataro provided material that was incorporated into this document.

8. References

8.1. Normative References

[RFC0791] Postel, J., "Internet Protocol", STD 5, RFC 791, September 1981.

[RFC0826] Plummer, D., "Ethernet Address Resolution Protocol: Or converting network protocol addresses to 48.bit Ethernet address for transmission on Ethernet hardware", STD 37, RFC 826, November 1982.

[RFC1038] St. Johns, M., "Draft revised IP security option", RFC 1038, January 1988.

[RFC1063] Mogul, J., Kent, C., Partridge, C., and K. McCloghrie, "IP MTU discovery options", RFC 1063, July 1988.

[RFC1108] Kent, S., "U.S", RFC 1108, November 1991.

[RFC1112] Deering, S., "Host extensions for IP multicasting", STD 5, RFC 1112, August 1989.

[RFC1122] Braden, R., "Requirements for Internet Hosts - Communication Layers", STD 3, RFC 1122, October 1989.

[RFC1191] Mogul, J. and S. Deering, "Path MTU discovery", RFC 1191, November 1990.

[RFC1349] Almquist, P., "Type of Service in the Internet Protocol Suite", RFC 1349, July 1992.

[RFC1393] Malkin, G., "Traceroute Using an IP Option", RFC 1393, January 1993.

[RFC1770] Graff, C., "IPv4 Option for Sender Directed Multi-Destination Delivery", RFC 1770, March 1995.

[RFC1812] Baker, F., "Requirements for IP Version 4 Routers", RFC 1812, June 1995.

[RFC2113] Katz, D., "IP Router Alert Option", RFC 2113,

February 1997.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2474] Nichols, K., Blake, S., Baker, F., and D. Black, "Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers", RFC 2474, December 1998.

[RFC2475] Blake, S., Black, D., Carlson, M., Davies, E., Wang, Z., and W. Weiss, "An Architecture for Differentiated Services", RFC 2475, December 1998.

[RFC2644] Senie, D., "Changing the Default for Directed Broadcasts in Routers", BCP 34, RFC 2644, August 1999.

[RFC3927] Cheshire, S., Aboba, B., and E. Guttman, "Dynamic Configuration of IPv4 Link-Local Addresses", RFC 3927, May 2005.

[RFC4821] Mathis, M. and J. Heffner, "Packetization Layer Path MTU Discovery", RFC 4821, March 2007.

[RFC5735] Cotton, M. and L. Vegoda, "Special Use IPv4 Addresses", BCP 153, RFC 5735, January 2010.

8.2. Informative References

[Barisani2006]
Barisani, A., "FTester - Firewall and IDS testing tool", Available at: http://dev.inversepath.com/trac/ftester , 2001.

[Biondi2007]
Biondi, P. and A. Ebalard, "IPv6 Routing Header Security", CanSecWest 2007 Security Conference http://www.secdev.org/conf/IPv6_RH_security-csw07.pdf, 2007.

[CERT1996a]
CERT, "CERT Advisory CA-1996-01: UDP Port Denial-of-Service Attack", http://www.cert.org/advisories/CA-1996-01.html, 1996.

[CERT1996c]
CERT, "CERT Advisory CA-1996-26: Denial-of-Service Attack via ping", http://www.cert.org/advisories/CA-1996-26.html, 1996.

[CERT1997]
CERT, "CERT Advisory CA-1997-28: IP Denial-of-Service Attacks", http://www.cert.org/advisories/CA-1997-28.html, 1997.

[CERT1999]
CERT, "CERT Advisory CA-1999-17: Denial-of-Service Tools", http://www.cert.org/advisories/CA-1999-17.html, 1999.

[CIPSO1992]
CIPSO, "COMMERCIAL IP SECURITY OPTION (CIPSO 2.2)", IETF Internet-Draft (draft-ietf-cipso-ipsecurity-01.txt), work in progress , 1992.

[CIPSOWG1994]
CIPSOWG, "Commercial Internet Protocol Security Option (CIPSO) Working Group", http://www.ietf.org/proceedings/94jul/charters/cipso-charter.html, 1994.

[CPNI2008]
Gont, F., "Security Assessment of the Internet Protocol", http://www.cpni.gov.uk/Docs/InternetProtocol.pdf, 2008.

[Cisco2008]
Cisco, "Cisco IOS Security Configuration Guide, Release 12.2", http://www.cisco.com/en/US/docs/ios/12_2/security/configuration/guide/scfipso.html, 2003.

[FIPS1994]
FIPS, "Standard Security Label for Information Transfer", Federal Information Processing Standards Publication. FIP PUBS 188 http://csrc.nist.gov/publications/fips/fips188/fips188.pdf, 1994.

[Haddad2004]
Haddad, I. and M. Zakrzewski, "Security Distribution for Linux Clusters", Linux Journal http://www.linuxjournal.com/article/6943, 2004.

[I-D.ietf-intarea-router-alert-considerations]
Faucheur, F., "IP Router Alert Considerations and Usage", draft-ietf-intarea-router-alert-considerations-10 (work in progress), August 2011.

[I-D.templin-mtuassurance]
Templin, F., "Requirements for IP-in-IP Tunnel MTU Assurance", draft-templin-mtuassurance-02 (work in progress), October 2006.

[I-D.wilson-class-e]
Wilson, P., Michaelson, G., and G. Huston, "Redesignation of 240/4 from "Future Use" to "Private Use"", draft-wilson-class-e-02 (work in progress), September 2008.

[IANA2006a]
Ether Types, "http://www.iana.org/assignments/ethernet-numbers".

[IANA2006b]
IP Parameters, "http://www.iana.org/assignments/ip-parameters".

[IANA2006c]
Protocol Numbers, "http://www.iana.org/assignments/protocol-numbers".

[IOS-12.2]
Cisco, "IP Security Options Commands", http://www.cisco.com/en/US/docs/ios/12_2/security/command/reference/srfipso.html, 2011.

[IRIX2008]
IRIX, "IRIX 6.5 trusted_networking(7) manual page", http://techpubs.sgi.com/library/tpl/cgi-bin/getdoc.cgi?coll=0650&db=man&fname=/usr/share/catman/a_man/cat7/trusted_networking.z, 2008.

[Kohno2005]
Kohno, T., Broido, A., and kc. Claffy, "Remote Physical Device Fingerprinting", IEEE Transactions on Dependable and Secure Computing Vol. 2, No. 2, 2005.

[Landwehr81]
Landwehr, C., "Formal Models for Computer Security", ACM Computing Surveys Vol 13, No 3, September 1981, Assoc for Computing Machinery, New York, NY, USA, 1981.

[Linux2006]
The Linux Project, "http://www.kernel.org".

[MEDINA]
Medina, A., Allman, M., and S. Floyd, "Measuring Interactions Between Transport Protocols and Middleboxes", Proc. 4th ACM SIGCOMM/USENIX Conference on Internet Measurement, October 2004.

[Microsoft1999]

Microsoft, "Microsoft Security Program: Microsoft Security Bulletin (MS99-038). Patch Available for "Spoofed Route Pointer" Vulnerability", http://www.microsoft.com/technet/security/bulletin/ms99-038.mspx, 1999.

[Northcutt2000] Northcut, S. and Novak, "Network Intrusion Detection - An Analyst's Handbook", Second Edition New Riders Publishing, 2000.

[OpenBSD-PF] Sanfilippo, S., "PF: Scrub (Packet Normalization)", http://www.openbsd.org/faq/pf/scrub.html, 2010.

[OpenBSD1998] OpenBSD, "OpenBSD Security Advisory: IP Source Routing Problem", http://www.openbsd.org/advisories/sourceroute.txt, 1998.

[Paxson2001] Paxson, V., Handley, M., and C. Kreibich, "Network Intrusion Detection: Evasion, Traffic Normalization, and End-to-End Protocol Semantics", USENIX Conference, 2001, 2001.

[RFC0815] Clark, D., "IP datagram reassembly algorithms", RFC 815, July 1982.

[RFC1858] Ziemba, G., Reed, D., and P. Traina, "Security Considerations for IP Fragment Filtering", RFC 1858, October 1995.

[RFC1918] Rekhter, Y., Moskowitz, R., Karrenberg, D., Groot, G., and E. Lear, "Address Allocation for Private Internets", BCP 5, RFC 1918, February 1996.

[RFC2205] Braden, B., Zhang, L., Berson, S., Herzog, S., and S. Jamin, "Resource ReSerVation Protocol (RSVP) -- Version 1 Functional Specification", RFC 2205, September 1997.

[RFC2544] Bradner, S. and J. McQuaid, "Benchmarking Methodology for Network Interconnect Devices", RFC 2544, March 1999.

[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.

[RFC3056] Carpenter, B. and K. Moore, "Connection of IPv6 Domains

via IPv4 Clouds", RFC 3056, February 2001.

[RFC3128] Miller, I., "Protection Against a Variant of the Tiny Fragment Attack (RFC 1858)", RFC 3128, June 2001.

[RFC3168] Ramakrishnan, K., Floyd, S., and D. Black, "The Addition of Explicit Congestion Notification (ECN) to IP", RFC 3168, September 2001.

[RFC3530] Shepler, S., Callaghan, B., Robinson, D., Thurlow, R., Beame, C., Eisler, M., and D. Noveck, "Network File System (NFS) version 4 Protocol", RFC 3530, April 2003.

[RFC3585] Jason, J., Rafalow, L., and E. Vyncke, "IPsec Configuration Policy Information Model", RFC 3585, August 2003.

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

[RFC4459] Savola, P., "MTU and Fragmentation Issues with In-the-Network Tunneling", RFC 4459, April 2006.

[RFC4632] Fuller, V. and T. Li, "Classless Inter-domain Routing (CIDR): The Internet Address Assignment and Aggregation Plan", BCP 122, RFC 4632, August 2006.

[RFC4807] Baer, M., Charlet, R., Hardaker, W., Story, R., and C. Wang, "IPsec Security Policy Database Configuration MIB", RFC 4807, March 2007.

[RFC4949] Shirey, R., "Internet Security Glossary, Version 2", RFC 4949, August 2007.

[RFC4963] Heffner, J., Mathis, M., and B. Chandler, "IPv4 Reassembly Errors at High Data Rates", RFC 4963, July 2007.

[RFC4987] Eddy, W., "TCP SYN Flooding Attacks and Common Mitigations", RFC 4987, August 2007.

[RFC5082] Gill, V., Heasley, J., Meyer, D., Savola, P., and C. Pignataro, "The Generalized TTL Security Mechanism (GTSM)", RFC 5082, October 2007.

[RFC5350] Manner, J. and A. McDonald, "IANA Considerations for the IPv4 and IPv6 Router Alert Options", RFC 5350, September 2008.

[RFC5570] StJohns, M., Atkinson, R., and G. Thomas, "Common Architecture Label IPv6 Security Option (CALIPSO)", RFC 5570, July 2009.

[SELinux2008] Security Enhanced Linux, "http://www.nsa.gov/selinux/".

[Silbersack2005] Silbersack, M., "Improving TCP/IP security through randomization without sacrificing interoperability", EuroBSDCon 2005 Conference http://www.silby.com/eurobsdcon05/eurobsdcon_slides.pdf, 2005.

[Solaris2008] Solaris Trusted Extensions - Labeled Security for Absolute Protection, "http://www.sun.com/software/solaris/ds/trusted_extensions.jsp#3", 2008.

[US-CERT2001] US-CERT, "US-CERT Vulnerability Note VU#446689: Check Point FireWall-1 allows fragmented packets through firewall if Fast Mode is enabled", http://www.kb.cert.org/vuls/id/446689, 2001.

[US-CERT2002] US-CERT, "US-CERT Vulnerability Note VU#310387: Cisco IOS discloses fragments of previous packets when Express Forwarding is enabled", http://www.kb.cert.org/vuls/id/310387, 2002.

[Zakrzewski2002] Zakrzewski, M. and I. Haddad, "Linux Distributed Security Module", http://www.linuxjournal.com/article/6215, 2002.

Appendix A. Changes from previous versions of the draft (to be removed by the RFC Editor before publishing this document as an RFC)

A.1. Changes introduced in draft-gont-opsec-ip-options-filtering-01

- Populated many sections that had a "TBD" placeholder.
- Many unused references were prunned from the "References" section.
- Addresses part of the comments provided by Carlos Pignataro and Donald Smith.

Authors' Addresses

Fernando Gont
Universidad Tecnologica Nacional / Facultad Regional Haedo
Evaristo Carriego 2644
Haedo, Provincia de Buenos Aires 1706
Argentina

Phone: +54 11 4650 8472
Email: fernando@gont.com.ar
URI: http://www.gont.com.ar

RJ Atkinson
Consultant
McLean, VA 22103
USA

Email: rja.lists@gmail.com