Operational Security Capabilities for                          F. Gont
IP Network Infrastructure (opsec)                 UTN-FRH / SI6 Networks
Internet-Draft                                               R. Atkinson
Intended status: BCP                                          Consultant
Expires: September 12, 2012                                 C. Pignataro
                                                                   Cisco
                                                          March 11, 2012

# Recommendations on filtering of IPv4 packets containing IPv4 options
# draft-gont-opsec-ip-options-filtering-04.txt

## Abstract

This document document provides advice on the filtering of IPv4 packets based on the IPv4 options they contain. Additionally, it discusses the operational and interoperability implications of dropping packets based on the IP options they contain.

## Status of this Memo

## Copyright Notice

Table of Contents

## 1. Introduction

This document document discusses the filtering of IPv4 packets based on the IPv4 options they contain. Since various protocols may use IPv4 options to some extent, dropping packets based on the options they contain may have implications on the proper functioning of the protocol. Therefore, this document attempts to discuss the operational and interoperability implications of such dropping. Additionally, it outlines what a network operator might do in a typical enterprise or Service Provider environments.

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 possible approach is to allow for end-to-end semantics by ignoring options and treating packets as un-optioned while in transit. Experiments and currently-available data tends to support the first or third approaches as more realistic. Some results of regarding the current state of affairs with respect to dropping packets containing IP options can be found in [MEDINA].

We also note that while this document provides advice on dropping packets on a "per IP option type", not all devices may provide this capability with such granularity. Additionally, even in cases in which such functionality is provided, the operator might want to specify a dropping 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.

### 1.1. Terminology and Conventions Used in This Document

The terms "fast path", "slow path", and associated relative terms ("faster path" and "slower path") are loosely defined as in Section 2 of [RFC6398].

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.

IP options of Case 1 have the following syntax:

```
+-+-+-+-+-+-+-+-+- - - - - - - - -
|  option-type  |  option-data
+-+-+-+-+-+-+-+-+- - - - - - - - -
```

The length of IP options of Case 1 is implicitly specified by the option-type byte.

IP options of Case 2 have the following syntax:

```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+- - - - - - - - -
|  option-type  | option-length |  option-data
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+- - - - - - - - -
```

In this case, 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:

- o 0 = control.

- o 1 = reserved for future use.

- o 2 = debugging and measurement.

- o 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.

The "IP OPTION NUMBERS" registry [IANA-IP] contains the list of the currently assigned IP option numbers.

## 3. General Security Implications of IP options

### 3.1. Processing Requirements

Router architectures can perform IP option processing in a slower path. Unless protective measures are taken, this represents a potential Denial of Service (DoS) risk, as there is possibility for the option processing to overwhelm the router's CPU or the protocols processed in the router's slow path. Additional considerations for protecting the router control plane from IP optioned packets can be found in [RFC6192].

## 4. Advice on the Handling of Packets with Specific IP Options

The following subsections 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 dropped, and specific advice on whether to drop packets containing these options in a typical enterprise or Service Provider environment.

### 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 and 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 dropped, it is very likely that legitimate traffic is blocked.

### 4.1.5. Advice

Routers, security gateways, and firewalls SHOULD NOT drop 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 and Interoperability Impact if Blocked

Packets containing any IP options are likely to include a No Operation option.  Therefore, if packets containing this option are dropped, it is very likely that legitimate traffic is blocked.

### 4.2.5. Advice

Routers, security gateways, and firewalls SHOULD NOT drop 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.

Additionally, some implementations have been found to fail to include proper sanity checks on the LSRR option, thus leading to security issues.

> [Microsoft1999] is a security advisory about a vulnerability arising from improper validation of the Pointer field of the LSRR option.

Finally, we note that some systems were known for providing a system-wide toggle to enable support for this option for those scenarios in which this option is required. However, improper implementation of such system-wide toggle caused those systems to support the LSRR option even when explicitly configured not to do so.

> [OpenBSD1998] is a security advisory about an improper implementation of such a system-wide toggle in 4.4BSD kernels.

#### 4.3.4. Operational and 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 the LSRR option for troubleshooting, due to widespread dropping of packets that contain such option.

#### 4.3.5. Advice

Routers, security gateways, and firewalls 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 and 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 the SSR option for trouble-shooting, due to widespread dropping of packets that contain such option.

### 4.4.5. Advice

Routers, security gateways, and firewalls 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 and 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 dropping of packets that contain RR options.

### 4.5.5. Advice

Routers, security gateways, and firewalls SHOULD drop IP packets containing a Record Route option.

## 4.6. Stream Identifier (Type = 136) (obsolete)

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 3.2.1.8 of RFC 1122 [RFC1122] and Section 4.2.2.1 of RFC 1812 [RFC1812], this option is obsolete. Therefore, it must be ignored by the processing systems. See also Section 5.

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

This option is obsolete. There is no current use for this option.

### 4.6.2. Option Specification

Specified in RFC 791 [RFC0791], and obsoleted in RFC 1122 [RFC1122] and RFC 1812 [RFC1812].

### 4.6.3. Threats

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

### 4.6.4. Operational and Interoperability Impact if Blocked

None.

#### 4.6.5. Advice

Routers, security gateways, and firewalls SHOULD drop IP packets containing 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 and 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

Routers, security gateways, and firewalls SHOULD drop IP packets containing 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 [RFC6398]. 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 and 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 in controlled environments, where the option can be used safely. [RFC6398] identifies some such environments. In unsafe environments, packets containing this option SHOULD be dropped.

A given router, security gateway, or firewall system has no way of knowing a priori whether this option is valid in its operational environment. Therefore, routers, security gateways, and firewalls SHOULD, by default, ignore the Router Alert option. Additionally, Routers, security gateways, and firewalls SHOULD have a configuration setting that indicates whether they should react act on the Router Alert option as indicated in the corresponding specification or ignore the option, or whether packets containing this option should be dropped (with the default configuration being to ignore the Router Alert option).

### 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 originally defined in RFC 1063 [RFC1063], and was obsoleted with RFC 1191 [RFC1191]. This option is now obsolete, as RFC 1191 obsoletes RFC 1063 without using IP options.

#### 4.9.3. Threats

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

#### 4.9.4. Operational and Interoperability Impact if Blocked

None

#### 4.9.5. Advice

Routers, security gateways, and firewalls SHOULD drop 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 defined in RFC 1063 [RFC1063], and was obsoleted with RFC 1191 [RFC1191]. This option is now obsolete, as RFC 1191 obsoletes RFC 1063 without using IP options.

#### 4.10.3. Threats

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

#### 4.10.4. Operational and Interoperability Impact if Blocked

None

#### 4.10.5. Advice

Routers, security gateways, and firewalls SHOULD drop 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]. The Traceroute option is defined as "experimental" and it was never widely deployed on the public Internet.

#### 4.11.3. Threats

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

#### 4.11.4. Operational and Interoperability Impact if Blocked

None

#### 4.11.5. Advice

Routers, security gateways, and firewalls SHOULD drop 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 [Cisco-IPSO]), 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 obsoleted RFC 1038 [RFC1038] (which in turn obsoleted the Security Option defined in RFC 791 [RFC0791]).

> 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. Later, RFC 1038 [RFC1038] revised the IP security options, and in turn was obsoleted by RFC 1108 [RFC1108]. The "Security Option" specified in RFC 791 is considered obsolete by Section 3.2.1.8 of RFC 1122 [RFC1122] and Section 4.2.2.1 of RFC 1812 [RFC1812], 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".

> Many Cisco routers that run Cisco IOS include support dropping packets that contain this option with per-interface granularity. This capability has been present in many Cisco routers since the early 1990s [Cisco-IPSO-Cmds]. Some governmental products reportedly support BSO, notably CANEWARE [RFC4949]. Support for BSO is included in the "IPsec Configuration Policy Information Model" [RFC3585] and in the "IPsec Security Policy Database Configuration MIB" [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 and 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, security gateways, and firewalls SHOULD NOT by default modify or remove this option from IP packets and SHOULD NOT by default drop packets containing this option. For auditing reasons, Routers, security gateways, and firewalls SHOULD be capable of logging the numbers of packets containing the BSO on a per-interface basis. Also, Routers, security gateways, and firewalls SHOULD be capable of dropping 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].

Many Cisco routers that run Cisco IOS include support for dropping packets that contain this option with a per-interface granularity. This capability has been present in many Cisco routers since the early 1990s [Cisco-IPSO-Cmds]. Some governmental products reportedly support ESO, notably CANEWARE [RFC4949]. Support for ESO is included in the "IPsec Configuration Policy Information Model" [RFC3585] and in the "IPsec Security Policy Database Configuration MIB" [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 and 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, security gateways, and firewalls SHOULD NOT by default modify or remove this option from IP packets and SHOULD NOT by default drop packets containing this option. For auditing reasons, Routers, security gateways, and firewalls SHOULD be capable of logging the numbers of packets containing the ESO on a per-interface basis. Also, Routers, security gateways, and firewalls SHOULD be capable of dropping 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.

> The TSIG proposal was taken to the Commercial Internet Security Option (CIPSO) Working Group of the IETF [CIPSOWG1994], and an Internet-Draft was produced [CIPSO1992]. The Internet-Draft was never published as an RFC, but the proposal was later standardized by the U.S. National Institute of Standards and Technology (NIST) as "Federal Information Processing Standard Publication 188" [FIPS1994].

### 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 and 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, Routers, security gateways, and firewalls SHOULD NOT by default modify or remove this option from IP packets and SHOULD NOT by default drop packets containing this option.

## 4.15.  VISA (Type = 142)

### 4.15.1.  Uses

This options was part of an experiment at USC and was never widely deployed.

### 4.15.2.  Option Specification

Not publicly available.

### 4.15.3.  Threats

Not possible to determine (other the general security implications of IP options discussed in Section 3), since the corresponding specification is not publicly available.

### 4.15.4.  Operational and Interoperability Impact if Blocked

None.

### 4.15.5.  Advice

Routers, security gateways, and firewalls SHOULD drop IP packets that contain this option.

## 4.16.  Extended Internet Protocol (Type = 145)

### 4.16.1.  Uses

The EIP option was introduced by one of the proposals submitted during the IPng efforts to address the problem of IPv4 address exhaustion.

### 4.16.2.  Option Specification

Specified in [RFC1385].  This option is in the process of being formally obsoleted by [I-D.gp-intarea-obsolete-ipv4-options-iana].

### 4.16.3.  Threats

There are no know threats arising from this option, other than the general security implications of IP options discussed in Section 3.

#### 4.16.4. Operational and Interoperability Impact if Blocked

None.

#### 4.16.5. Advice

Routers, security gateways, and firewalls SHOULD drop packets that contain this option.

### 4.17. Address Extension (Type = 147)

#### 4.17.1. Uses

The Address Extension option was introduced by one of the proposals submitted during the IPng efforts to address the problem of IPv4 address exhaustion.

#### 4.17.2. Option Specification

Specified in [RFC1475]. This option is in the process of being formally obsoleted by [I-D.gp-intarea-obsolete-ipv4-options-iana].

#### 4.17.3. Threats

There are no know threats arising from this option, other than the general security implications of IP options discussed in Section 3.

#### 4.17.4. Operational and Interoperability Impact if Blocked

None.

#### 4.17.5. Advice

Routers, security gateways, and firewalls SHOULD drop packets that contain this option.

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

#### 4.18.1. Uses

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

#### 4.18.2. Option Specification

This option is defined in RFC 1770 [RFC1770].

### 4.18.3. Threats

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

### 4.18.4. Operational and Interoperability Impact if Blocked

None.

### 4.18.5. Advice

Routers, security gateways, and firewalls SHOULD drop IP packets that contain a Sender Directed Multi-Destination Delivery option.

## 4.19. Dynamic Packet State (Type = 151)

### 4.19.1. Uses

The Dynamic Packet State option was used to specify specified Dynamic Packet State (DPS) in the context of the differentiated service architecture.

### 4.19.2. Option Specification

The Dynamic Packet State option was specified in [I-D.stoica-diffserv-dps]. The aforementioned document was meant to be published as "Experimental", but never made it into an RFC. This option is in the process of being formally obsoleted by [I-D.gp-intarea-obsolete-ipv4-options-iana].

### 4.19.3. Threats

Possible threats include theft of service and Denial of Service. However, we note that is option has never been widely implemented or deployed.

### 4.19.4. Operational and Interoperability Impact if Blocked

None.

### 4.19.5. Advice

Routers, security gateways, and firewalls SHOULD drop packets that contain this option.

### 4.20. Upstream Multicast Pkt. (Type = 152)

#### 4.20.1. Uses

This option was meant to solve the problem of doing upstream forwarding of multicast packets on a multi-access LAN.

#### 4.20.2. Option Specification

This option was originally specified in [draft-farinacci-bidir-pim]. Its use was obsoleted by [RFC5015], which employs a control plane mechanism to solve the problem of doing upstream forwarding of multicast packets on a multi-access LAN. This option is in the process of being formally obsoleted by [I-D.gp-intarea-obsolete-ipv4-options-iana].

#### 4.20.3. Threats

TBD.

#### 4.20.4. Operational and Interoperability Impact if Blocked

None.

#### 4.20.5. Advice

Routers, security gateways, and firewalls SHOULD drop packets that contain this option.

### 4.21. Quick-Start (Type = 25)

#### 4.21.1. Uses

This IP Option is used in the specification of Quick-Start for TCP and IP, which is an experimental mechanism that allows transport protocols, in cooperation with routers, to determine an allowed sending rate at the start and, at times, in the middle of a data transfer (e.g., after an idle period) [RFC4782].

#### 4.21.2. Option Specification

Specified in RFC 4782 [RFC4782], on the "Experimental" track.

#### 4.21.3. Threats

Section 9.6 of [RFC4782] notes that Quick-Start is vulnerable to two kinds of attacks:

- attacks to increase the routers' processing and state load, and,

- attacks with bogus Quick-Start Requests to temporarily tie up available Quick-Start bandwidth, preventing routers from approving Quick-Start Requests from other connections

### 4.21.4. Operational and Interoperability Impact if Blocked

The Quick-Start functionality would be disabled, and additional delays in e.g. TCP's connection establishment could be introduced (please see Section 4.7.2 of [RFC4782]. We note, however, that Quick-Start has been proposed as mechanism that could be of use in controlled environments, and not as a mechanism that would be intended or appropriate for ubiquitous deployment in the global Internet [RFC4782].

### 4.21.5. Advice

A given router, security gateway, or firewall system has no way of knowing a priori whether this option is valid in its operational environment. Therefore, routers, security gateways, and firewalls SHOULD, by default, ignore the Quick Start option. Additionally, routers, security gateways, and firewalls SHOULD have a configuration setting that indicates whether they should react act on the Quick Start option as indicated in the corresponding specification or ignore the option, or whether packets containing this option should be dropped (with the default configuration being to ignore the Quick Start option).

We note that if routers in a given environment do not implement and enable the Quick-Start mechanism, only the general security implications of IP options (discussed in Section 3) would apply.

## 4.22. RFC3692-style Experiment (Types = 30, 94, 158, and 222)

Section 2.5 of RFC 4727 [RFC4727] allocates an option number with all defined values of the "copy" and "class" fields for RFC3692-style experiments. This results in four distinct option type codes: 30, 94, 158, and 222.

### 4.22.1. Uses

It is only appropriate to use these values in explicitly-configured experiments; they MUST NOT be shipped as defaults in implementations.

### 4.22.2. Option Specification

Specified in RFC 4727 [RFC4727] in the context of RFC3692-style experiments.

### 4.22.3. Threats

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

### 4.22.4. Operational and Interoperability Impact if Blocked

None.

### 4.22.5. Advice

Routers, security gateways, and firewalls SHOULD drop IP packets that contain RFC3692-style Experiment options.

## 4.23. Other IP Options

Unrecognized IP Options are to be ignored.  Section 3.2.1.8 of RFC 1122 [RFC1122] and Section 4.2.2.6 of RFC 1812 [RFC1812] specify this behavior as follows:

RFC 1122:  "The IP and transport layer MUST each interpret those IP options that they understand and silently ignore the others."

RFC 1812:  "A router MUST ignore IP options which it does not recognize."

This document adds that unrecognized IP Options MAY also be logged.

A number of additional options are specified in the "IP OPTIONS NUMBERS" IANA registry [IANA-IP].  Specifically:

| Copy | Class | Number | Value | Name | Reference |
|---|---|---|---|---|---|
| 0 | 0 | 10 | 10 | ZSU - Experimental Measurement | [ZSu] |
| 1 | 2 | 13 | 205 | FINN - Experimental Flow Control | [Finn] |
| 0 | 0 | 15 | 15 | ENCODE - ??? | [VerSteeg] |
| 1 | 0 | 16 | 144 | IMITD - IMI Traffic Descriptor | [Lee] |
| 1 | 0 | 22 | 150 | - Unassigned (Released 18 Oct. 2005) | |

## 5. IANA Considerations

The "IP OPTION NUMBERS" registry [IANA-IP] contains the list of the currently assigned IP option numbers. This registry also denotes an obsoleted IP Option Number by marking it with a single asterisk ("*"). The Stream Identifier Option (Type = 136) is obsolete (see Section 4.6 and should therefore be marked as such.

[[ IANA is requested to mark it as such, please remove this note upon publication. ]] [[ IANA is also requested to fix the "Expermental" typo. ]]

## 6. Security Considerations

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

## 7. Acknowledgements

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

Part of this document is based on the document "Security Assessment 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.

## 8. References

### 8.1. Normative References

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

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

[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.

[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.

[RFC4727] Fenner, B., "Experimental Values In IPv4, IPv6, ICMPv4, ICMPv6, UDP, and TCP Headers", RFC 4727, November 2006.

[RFC4782] Floyd, S., Allman, M., Jain, A., and P. Sarolahti, "Quick-Start for TCP and IP", RFC 4782, January 2007.

[RFC5015] Handley, M., Kouvelas, I., Speakman, T., and L. Vicisano, "Bidirectional Protocol Independent Multicast (BIDIR-PIM)", RFC 5015, October 2007.

## 8.2. Informative References

[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.

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

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

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

[Cisco-IPSO]
Cisco Systems, Inc., "Cisco IOS Security Configuration Guide, Release 12.2 - Configuring IP Security Options", < http://www.cisco.com/en/US/docs/ios/12_2/security/configuration/guide/scfipso.html>, 2006.

[Cisco-IPSO-Cmds]
Cisco Systems, Inc., "Cisco IOS Security Command Reference, Release 12.2 - IP Security Options Commands", <http://www.cisco.com/en/US/docs/ios/12_2/security/command/reference/srfipso.html>.

[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.

[I-D.gp-intarea-obsolete-ipv4-options-iana]
Pignataro, C. and F. Gont, "Formally Obsoleting some Historic IPv4 Options", draft-gp-intarea-obsolete-ipv4-options-iana-00 (work in progress), February 2012.

[I-D.stoica-diffserv-dps]
Stoica, I., Zhang, H., Baker, F., and Y. Bernet, "Per Hop Behaviors Based on Dynamic Packet State", draft-stoica-diffserv-dps-02 (work in progress), October 2002.

[IANA-IP]  Internet Assigned Numbers Authority, "IP OPTION NUMBERS", April 2011, <http://www.iana.org/assignments/ip-parameters>.

[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.

[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", 1999, <http://www.microsoft.com/technet/security/bulletin/ms99-038.mspx>.

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

[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.

[RFC1385] Wang, Z., "EIP: The Extended Internet Protocol", RFC 1385, November 1992.

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

[RFC1475] Ullmann, R., "TP/IX: The Next Internet", RFC 1475, June 1993.

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

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

[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.

[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.

[RFC6192]  Dugal, D., Pignataro, C., and R. Dunn, "Protecting the Router Control Plane", RFC 6192, March 2011.

[RFC6398]  Le Faucheur, F., "IP Router Alert Considerations and Usage", BCP 168, RFC 6398, October 2011.

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

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

[draft-farinacci-bidir-pim]
Estrin, D. and D. Farinacci, "Bi-Directional Shared Trees in PIM-SM",  IETF Internet Draft, draft-farinacci-bidir-pim, work in progress, May 1999.

## 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

RJ Atkinson
Consultant
McLean, VA  22103
USA

Email: rja.lists@gmail.com

Carlos Pignataro
Cisco Systems, Inc.
7200-12 Kit Creek Road
Research Triangle Park, NC  27709
US

Email: cpignata@cisco.com