Network Working Group
Internet Draft
draft-belgaied-ipv6-lsopt-00.txt

K. Belgaied
Sun Microsystems Inc.
G. Winiger
Sun Microsystems Inc.
February 2001

Generalized Labeled Security Option for IPv6

Status of this Memo

This Internet Draft expires August 22, 2001.

Abstract

This memo describes a new IPv6 Hop-by-Hop Option type used as an explicit security label. The hosts supporting Labeled Security add this option to the packets they originate in order to convey the sensitivity of the data. The routers that recognize this option will use it to make routing decision, in conformance with a pre-established policy. The IPSec protection requirements and a transition scheme from the existing IPv4 security options to the LS option are also proposed.

Table of Contents

1. Introduction

Information in a multilevel security environment is labeled. The label of a process may represent the credentials of that process. The label on an object (file, device, ...) may represent the sensitivity, as in the Bell and Lapadula model [BL73], the integrity, as in the Biba model [Bib77], or other security attributes of the data.

Multilevel secure operating systems enforce a set of mandatory access control rules, in order to guarantee that information is protected to a certain level of assurance, that can be evaluated according to predefined criteria [LSPP], [DoD85].

In order to enforce those access controls across a network, routing needs to be controlled so as to select specific network links in accordance with the security policy [DoD87], and host need to be able to retrieve the security attributes of data coming from the network, and to communicate those of their own processes when they access data at remote hosts.

Making the security attributes of the information available to the entities that need it can be achieved by either explicitly or implicitly labeling the IP packets, as discussed in [RFC-1457], Security Labeling Framework for the Internet.
Dedicating an IPSec security association for each sensitivity level is one way of implicit labeling [RFC-2401]. I has the advantage of tying the security attribute of the information to an SA, thus guaranteeing that the former is always protected by the latter.
The implicit labeling has the following limitations though:

. Scalability. Implicit binding of security attributes to SAs may be sufficient when there is a small set of values for those attributes. Communicating LS systems may exchange data at a wide range of sensitivities, produced by processes with varying credentials, and would need a separate SA for each combination.
. Practical consideration. Although an IPSec SA can scale down to selectively protect a single socket (one connection / liaison), it is more efficient in practice to aggregate the flows by broader selectors, like host or subnet addresses or transport level port numbers, due to the cost of the SA establishment including the key management.
. Routers cannot figure out the security attributes of the packets, unless they are members of the security association.

IPv4 had previous experience with explicit labeling:
[RFC-1108] defined the IPSO, a security option in the IPv4 header that can be used for a small number of possible labels mainly in use by the US Government.

An IETF working group, cipso, was later formed to propose an IP labeling scheme more suitable to commercial use, and did produce an Internet draft, the Common IP Security Option specification.

Although the IETF draft expired, the proposal was adopted in 1994 by the US Government as a Federal Information Processing Standard (FIPS) [CIPSO].

IPv6 [RFC2460] offers a convenient mechanism to carry ancillary data with packets, using options in the hop-by-hop and the destination extension headers. Such an option seems to be the natural choice for use as security label for IPv6 packets.

The remainder of this memo proposes a generalized approach to the explicit labeling for IPv6 packet and to the migration of the currently most used labeling IPv4 options (CIPSO and IPSO) to the LS IPv6 option. It applies mainly to the [BL] model, although it may be adopted for an integrity model with some limitations. We'll also discuss the IPSec [RFC-2401] protection requirements when operating in the real world, outside the assumptions of a Trusted Computing Base [DoD85].

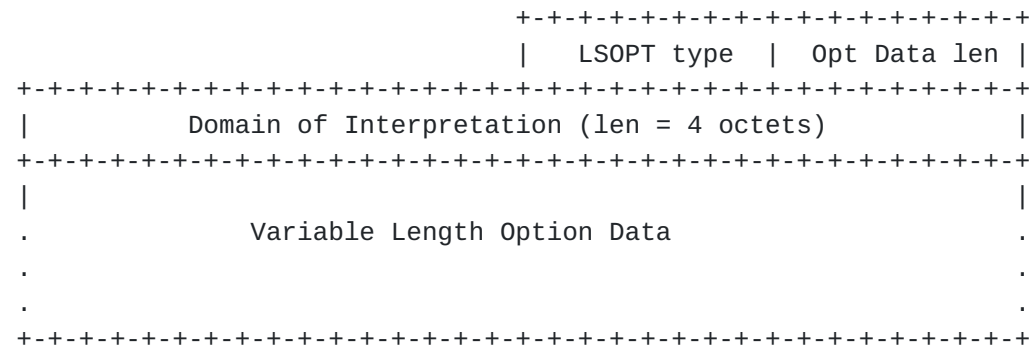
The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC-2119].

Unless otherwise stated, references to the link-local, site-local or global addressing scopes mean both unicast and multicast address types, as defined in [RFC-2373].

2. LS option specification

2.1. Syntax

The general format of an LS option is:



All the fields are stored in the network-byte order.

LSOPT type's value is an octet value to be requested from IANA, with the following constraints:
. First 2 MSB are 00, instructing the non supporting nodes to skip

over this option and continue processing the header

. The next MSB is 0, indicating that the Option Data does not change en-route

The Opt Data length is expressed in octets.

The Domain of Interpretation field is a 4 octet integer that identifies the semantics of the option data to follow. Communicating nodes have to agree on a common interpretation of the LS option before acting upon it.

The value DOI=0 is dedication for the transition from IPv4 security options.

This specification proposes also to reserve the values 1-255.

The option Data option is a list of self-describing tags.
Each tag has the following format:

The Tag Type (TT) identifies the type of the information in the Tag Info (TI) field. Tag length (TL) to total length of the tag, expressed in octets.

The following types are predefined in this document. The implementations are required to use them in the way indicated herein. All these tag types can be used in both hop-by-hop and destination headers, unless otherwise specified.
We also provide how entities of each type are compared.

TT 1: The tag is a hierarchical 2-octet entity.
TL is 4.
This can be thought of as a level or classification.
The comparison of fields of this type is the conventional mathematical relation (<=, <, >, >=, ==, !=)

TT 2: Non-hierarchical bit-vector.
TL is a variable number of octets. TL MUST be an even number.
This type is intended for categories/compartments bit sets.
The comparison of fields of this type is the inclusion relation.

TT 3: Enumeration.
TL is a variable number of octets.
This is a list of items. Each item is a short. It is a compact way of coding categories and compartments.
The comparison of fields of this type is the inclusion relation.

TT 4: List of ranges.

TL is a variable number of octets. TL must be a 4n+2 integer.
Each range has 2 shorts: lower and upper boundaries of the

interval. The intervals MUST NOT overlap.
The ranges are intended as an efficient grouping of categories and compartments.
The comparison of fields of this type is the inclusion relation.

TT 5: IPv4-Compatible option.
TL is a variable number of octets. TL must be an even number.
This tag contains an IPv4 security option.
The intent of this tag is to provide an easy transition to IPv6 for the LS systems that already use legacy IPv4 options.

TT 6: Destination-only data
TL is a variable number of octets in this TI. TL must be an even number.
Only the destinations that understand the DOI are able to interpret it.
This option is not understood by routers when present in a hop-by-hop header and MUST be skipped.

TT 7-255: Available for future use, to be requested from IANA.

2.2 Alignment

The DOI MUST be aligned on an 8n+4 octet boundary.

If the packet contains other options in the hop-by-hop extension header, Pad1 or PadN options MUST be used in order to ensure the DOI in the LS option fall in that boundary, in accordance with the formatting guidelines in [RFC2460]

Tags MUST be aligned so that their fields fall in their natural boundaries.

2.3 Order and coexistence of Tags

For implementation efficiency, fields with fixed size (TT1) MUST appear first, when present.

The LS option MAY carry more than one tag of the same type, however, only the first tag of that type will be used for consistency checks at the interfaces.

In order to avoid ambiguity, IPv4 compatibility tags MUST NOT be used with other tags.

3. Functional specification

3.1 Domain of Interpretation

Communicating hosts sharing the same set of security policies and a common interpretation of security attributes will use a unique value of the DOI in the labels of the packets they exchange.
The DOI identifies the security domain made of that collection of hosts.

For example, a label with a classification field TT1=5, may mean "public information" for a company A. Another company, B, may choose to assign the "competition-sensitive information" meaning to the same value, TT1=5. Obviously A and B cannot use TT1=5 to label packets between them. However, if A and B agree on a common set of labels and how to interpret them, they have to choose a unique DOI value, C, that identifies that common understanding.
A and B will have to choose different DOI values for communication within their respective domains.

A host can be a member of several domains, and use a different DOI value for communicating with peers in each.

When A and B in the example above use the services of an application server provided by an outsourcing company, the server can be a member of the 3 domains, A, B and the C. It will use labels with DOI A to communicate with A, for instance, and apply the policy enforcement checks suitable for DOI A, in choosing routes or offering the appropriate IPSec protection,
The server will use the DOI C for packets addressed to a multicast group containing both A and B.

3.2 Interface protection table

An implementation that supports the LS option may associate with each network interface a table that specifies what domains of interpretations are supported and what are the constraints on the packets coming through or going out of that interface, for a given DOI.

An example of such a table would look like:

DOI	Constraints
doi1	TT1: [min-max]
	TT2: <some bit vector V]
	TT3: {item1, ..., itemN}
	TT4: [r11,r12], ... [r1N-r1M]

```
                  doi2   |   TT1: ....
                         .
                         .
                         .
```

A label is admitted through an interface if it passes the constraints defined on that interface, for the label's DOI.
If the node does not recognize the DOI of the packet then it MUST be discarded.

For the predefined tag types, passing the constraint means:

TT1: the tag value is within the range.
TT2: All the bits set in the packet label bit vector MUST be set in the interface's bit vector.
TT3: All the items enumerated in the label belong to either a TT3 or a TT4 on the interface.
TT4: All the items in the ranges enumerated in the label belong to either a TT3 or a TT4 on the interface.

The way of checking the destination-only tags is part of the agreement between the endpoints.

3.3 Host behavior

The implementation SHOULD use the LS option in a destination extension header when:
. The security information is relevant to the endpoint only.
. Non trusted entities can access the packet en route, mandating the use of ESP's [RFC-2406] protection in order to preserve confidentiality.
. The destination address is a link-local one.

The following is the typical sequence of operations a sending and receiving host will perform, including the ICMPv6 packets to be generated [RFC-2463]:

3.3.1 Originating host:

. Choose a route to destination and an outgoing interface that conforms the security attributes of the packet to be sent.

. If no route was found, locally generate an ICMPv6 error message with type 1: Destination unreachable, code 1: communication with destination administratively prohibited.

. Create the LS option from the packet's security attributes, and add it to the packet in the appropriate extension header.

. Calculate and add the ESP and or the AH [RFC-2402] header as necessary.

. Send the packet out.

3.3.2 Destination host:

. Authenticate the packet and log an audit record on failure.

. Check if the packet was allowed through the incoming interface and log an audit record on failure.
If the failure was due to an unrecognized DOI for this interface then send back an ICMPv6 error message with type 1 and code 1. If the incoming packet was encrypted, then the returned ICMPv6 MUST NOT contain any clear portion of the original packet.

Rationale: The packet was authentic, so the failure is either due to a subject on the originating host attempting to defy the security policy, or there is a misconfiguration in the network. In both cases, the ICMPv6 is useful to the originating host'administrator to help identify the violating subject, or to figure out which nodes have the wrong settings on their interface protection tables.

. Retreive the security attributes from the label and deliver the packet to the right client.

3.4 Router behavior

One of the design considerations was to suggest a way for routers to implement the support for the LS option, without requiring that they understand the meaning of the labels, yet enforce the label checks necessary for the security policy in a multilevel security environment.

Routers that do not understand the LS option will simply skip over it, as mandated by the choice of the LS option type.

A router needs to trust the authenticity and integrity of a packet before making routing decision based on the content of its label. This is a strong assumption, however there are situations when it may apply. Examples include operating in a restricted environment where there is control on what devices are physically sharing the network, and on what privileges processes are granted. Another example is when the router is acting as the secure gateway that will provide the IPSec protection and possibly add the security label on behalf of non LS hosts. A multi-site organization usually has very good control on who accesses what inside each site, but needs secure gateways to communicate between sites.

A router ([RFC2401] and [DoD87]) may associate with each interface a set of sensitivity information allowed to or forbidden from flowing through that interface.

The router MUST perform the accreditation checks described in the previous section on both the incoming and outgoing interface for all the site-local packets. When discarding violating packets, the routers MUST send an ICMPv6 Type 1, code 1 back to the originator of the packet.

When routing OUT non-site local packets, if the router is acting as the secure gateway that will add the ESP or AH header, then it MUST use the explicit label on the packet to:

. Select the right security association to use for the flow to be protected, in accordance with the security policy.
. perform the incoming interface accreditation checks.

When routing IN non-site local packets, if the router is acting as the secure gateway at the receiving end of the SA, then it MUST

. Retrieve the explicit label from the packet (after decryption and authentication)
. forward the packet in using a route and an interface permitted for the packet.

IPSec authentication failure MUST NOT generate an ICMPv6 back, however, the implementations SHOULD increment a counter of the number of such failures, and, optionally, log an audit record. The router MUST send an ICMPv6 Type 1, code 1 back to the originator of an authentic packets failing the forwarding accreditation checks, however, it MUST NOT send any decrypted portion of the original one.

In all the other cases, routers MUST skip the LS option.
There are three reasons for this recommendation:

. Although it is possible to have enough control inside a site, and therefore trust the clear header on a packet, it is impossible to to guarantee that condition across the Internet, without the router being involved in at least an AH SA.
. Doing anything other than silently skipping the option for alien packets opens an easy denial of service exposure.
. There is no global registration for the registration for the DOI values and the way to interpret them, so a router is unlikely to choose the same interpretation meant by the originator of the packet.

4. Deployment considerations

4.1 Policy information setting

The mechanism of distributing the security policy constraints on all the nodes of a site implementing the LS option is beyond the scope of this memo. However, one way to approach this problem is to use a

mechanism similar to the RSVP [RFC-2205]. Both situation face the problem of segregating the treatment one flow of information gets. In one case, it is based on the resources reserved for that flow,

in the other case it is based on its security attributes.
Similarly to what is proposed for RSVP in [RFC-2749], the LS case may use the framework provided by the Common Open Policy Service protocol (COPS) [RFC-2748].
A central PDP (Policy Decision Point) node would have knowledge of the topology of a site and sensitivity associated with each link in that site (identified by its prefixes, for example), and the hosts and routers would, acting as PEPs (Policy Enforcement Points), use the attributes of a link in order to set the protection table on their interfaces connected to that link.

4.2 IPv4 Security Options Transition

The following are optional guidelines for the existing implementations that use IPv4 security options and wish to migrate to IPv6, in the order of preference:

. Use implicit labeling if the amount of security information is small enough.

. Translate the IPv4 option in order to map to the proposed format. A separate document specifying the translation of legacy IPv4 option should be proposed.

. Use the DOI=0 dedicated for the IPv4 options compatible mode only, and use a Tag type 5 to carry the full IPv4 option inside an LS option. The tag will have the same syntax and semantics of the IPv4 option, and MUST be interpreted by the supporting nodes as if it came in an IPv4 packet.

4.3 Key management

During the deployment, the key management traffic MUST NOT introduce an additional vulnerability to the flows to be protected by SAs established using that key management. Ideally, the key management traffic follows the trusted path reserved for information at the highest sensitivity it will help protect. However, since the SAs are yet to be established, the labels on the key management packets are not protected, and not guaranteed any authenticity. Solving this issue is beyond the scope of this document, but the users should be aware of its existence.

5. Security Considerations

When deploying this explicit labeling scheme, the authenticity and the integrity of the labels and the data being labeled MUST be guaranteed. Unless operating inside a perimeter of trust that isolates the network, AH must be used, as required by [RFC2401].

The implementations SHOULD make the requirement for
AH when LS option is present as a configurable parameter, leaving

that policy choice to the discretion of the administrator.

The immutability requirement is a potential limitation to the use of the LS option as an integrity label. When data is handled by an entity with an integrity label lower than the integrity label of the data, the data has to be relabeled with the integrity label of the entity. This limitation can be overcome by the use of ESP when the inegrity label is in a destination extention header (the case of link local scope) and the use of both AH and ESP when the label is in the hop-by-hop header (site or global scope). The confidence that is placed in encrypted and authentic data is therefore preserved, eliminating the need for relabeling.

6. IANA Considerations

The value of the LS option type is to be registered and maintained by IANA.
New reserved DOI values, and new tag types are to be assigned via IETF Consensus as defined in RFC 2434 [RFC-2434].

7. References

[BL73] Bell, D.E. & LaPadula, L.J., "Secure Computer Systems: Mathematical Foundations and Model", Technical Report M74-244, The MITRE Corporation, Bedford, MA, May 1973.

[Bib77] Biba, K. J. "Integrity Considerations for Secure Computer Systems", MTR-3153, The Mitre Corporation, April 1977.

[CIPSO] National Institute of Standards and Technology, "Standard Security Label for Information Transfer", Federal Information Processing Standard Publication 188, 1994 September 6.

[DoD85] US National Computer Security Center, "Department of Defense Trusted Computer System Evaluation Criteria", DoD 5200.28-STD, US Department of Defense, Ft. Meade, MD., December 1985. (aka the Orange Book)

[DoD87] US National Computer Security Center, "Trusted Network Interpretation of the Trusted Computer System Evaluation Criteria", NCSC-TG-005, Version 1, US Department of Defense, Ft. Meade, MD., 31 July 1987. (aka the Red Book)

[LSPP] Information Systems Security Organization. "Labeled Security Protection Profile". National Security Agency, Ft. Meade, MD., 8 October 1999.

[RFC-1108] Kent, Stephen. "U.S. Department of Defense Security Options for the Internet Protocol", RFC 1108, November 1991

[RFC-1457] Housley, Russell. "Security Label Framework for the Internet", RFC 1457, May 1993.

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

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

[RFC-2373] Hinden, R. and S. Deering, "IP Version 6 Addressing Architecture", RFC 2373, July 1998.

[RFC-2401] Kent, S., and R. Atkinson, "Security Architecture for the Internet Protocol", RFC 2401, November 1998.

[RFC-2402] Kent, S., and R. Atkinson, "IP Authentication Header", RFC 2402, November 1998.

[RFC-2406] Kent, S., and R. Atkinson, "IP Encapsulating Security Payload", RFC 2402, November 1998.

[RFC-2434] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 2434, October 1998.

[RFC-2460] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, December 1998.

[RFC-2463] Conta, A. and S. Deering, "Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification", RFC 2463, December 1998.

[RFC-2748] Boyle, J., Cohen, R., Durham, D., Herzog, S., Raja, R. and A. Sastry, "The COPS (Common Open Policy Service) Protocol", RFC 2748, January 2000.

[RFC-2749] Boyle, J., Cohen, R., Durham, D., Herzog, S., Raja, R. and A. Sastry, "COPS Usage for RSVP", RFC 2749, January 2000.

8. Acknowledgments and Authors' Addresses

Many thanks to Erik Nordmark and Dan McDonald for their feedback, suggestions, and comments that helped writing this draft.

Kais Belgaied
Sun Microsystems, Inc.
901 San Antonio Road
M/S USJC01-201.
Palo Alto, CA 94303, USA
email: kais.belgaied@sun.com

Gary Winiger
Sun Microsystems, Inc.
901 San Antonio Road
M/S USJC01-201.
Palo Alto, CA 94303, USA
email: gary.winiger@sun.com