NFSv4
Internet-Draft
Intended status: Standards Track
Expires: March 20, 2015

D. Quigley
J. Lu
Oracle
T. Haynes
Primary Data

September 16, 2014

# Registry Specification for Mandatory Access Control (MAC) Security Label Formats

draft-ietf-nfsv4-lfs-registry-01.txt

## Abstract

In the past Mandatory Access Control (MAC) systems have used very rigid policies which were implemented in particular protocols and platforms. As MAC systems became more widely deployed, additional flexibility in mechanism and policy will be required. While traditional trusted systems implemented Multi-Level Security (MLS) and integrity models, modern systems have expanded to include technologies such as type enforcement. Due to the wide range of policies and mechanisms which need to be accommodated, it is unlikely that use of a single security label format and model will be viable.

To allow multiple MAC mechanisms and label formats to co-exist in a network, this document proposes a registry of label format specifications. This registry would contain label format identifiers and would provide for the association of each such identifier with a corresponding extensive document document outlining the exact syntax and use of the particular label format.

## Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

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

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

This Internet-Draft will expire on March 20, 2015.

Table of Contents



## 1. Introduction

With the acceptance of security labels in several mainstream operating systems the need to communicate labels between these systems becomes more important. In a typical client and server scenario, the client request to the server acts as a subject trying to access an object on the server [RFC7204]. Unfortunately these systems are diverse enough that attempts at establishing one common label format have been unsucessful. The reason for this is that systems implement different Mandatory Access Control (MAC) models, which typically do not share any common ground.

One solution might be to define a single label format which consists of the union of the requirements of all MAC models/implementations, known at a given time. This approach is not desirable because it introduces an environment where many MAC models would either have blank fields for many of the label's components or where many implementations would ignore many of values that are present altogether. The resulting complexity would be likely to result in a confusing situation in which the interaction of fields that that derive from different MAC models is never clearly specified and the addition of new models or extension of existing models is unduly difficult.

An additional consideration is that if a policy authority or identifier field is specified in the label format it would require a robust description that encompassed multiple MAC models where implementation would lock policy administration into the described model.

Ideally a mechanism to address this problem should allow the most flexibility possible in terms of policy administration while providing a specification that is suffient to allow for implementation of the label format and understanding of the semantics of the label. This means that the label format specification would ideally contain a syntactic description of the label format and a description of the semantics for each component in the label. This allows protocols to specify the type of label and label semantics that it requires while leaving policy and policy administration to the individual organizations using the protocol in their environment.

Policy administration within an organization is a difficult problem. This should not be made even more difficult by having to request permission from external entities when crafting new policy or just making department specific modifications to existing policies. The policy authority field would allow an label format specification to specify a scheme for policy administration without forcing it on all users of security labels. However by agreeing to implement a particular label format specification, the protocol agrees to that policy administration mechanism when processing labels of that type.

## 2. Definitions

Label Format Specifier: an identifier used by the client to establish the syntactic format of the security label and the semantic meaning of its components.

Label Format Specification: is a reference to a stable, public document that specifies the label format.

Multi-Level Security (MLS): a traditional model where subjects are given a security level (Unclassified, Secret, Top Secret, etc.) and objects are given security labels that mandate the access of the subject to the object (see [BL73] and [RFC2401]).

object: a passive resource within the system that we wish to protect. Objects can be entities such as files, directories, pipes, sockets, and many other system resources relevant to the protection of the system state.

subject: an active entity, usually a process, user, or client, that is requesting access to an object.

## 3. Requirements Language

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].

## 4. Exisiting Label Format Specifications

### 4.1. IP Security Option (IPSO), Basic Security Option (BSO)

The "IP Security Option (IPSO)" label format is defined in [RFC1108]. IANA has assigned IPv4 Option 130 to the IPSO Basic Security Option (BSO). IPSO is the only IPv4 sensitivity label option implemented in commercial IP routers. IPSO BSO continues to have widespread implementation in hosts, and widespread deployment. For the purposes of this document, only the BSO labels in Table 1 on Page 3 of [RFC1108] are used.

In some locales, the BSO value "(Reserved 2)" is used for marking information that is considered "Restricted" by local policy, where "Restricted" is less sensitive than "Confidential" but more sensitive than "Unclassified".

### 4.2. Commercial IP Security Option (CIPSO)

The "Commercial IP Security Option (CIPSO)" label format is documented in [CIPSO] and in [FIPS-188]. While the cited Internet-Draft is long expired, it is widely supported in deployed MLS systems that support IPv4. IANA has assigned IPv4 option number 134 to CIPSO. CIPSO is defined ONLY as an IPv4 option. IANA has never assigned any IPv6 option value to CIPSO.

### 4.3. Common Architecture Label IPv6 Security Option (CALIPSO)

The "Common Architecture Label IPv6 Security Option (CALIPSO)" label format is specified in [RFC5570] and is defined for IPv6. As noted in Section 10 of [RFC5570] CALIPSO is a direct derivative of the IPv4 "Simple IP Security Option (SIPSO)", therefore CALIPSO is NOT derived from CIPSO in any way.

### 4.4. Flux Advanced Security Kernel (FLASK)

The Flux Advanced Security Kernel (FLASK) [FLASK99] is an impelementation of an architecture to provide flexible support for security policies. Section 2.1 of [FLASK99b], summarizes the architecture of FLASK to:

1. describe the interactions between a subsystem which enforces security policy decisions and a subsystem which makes those decisions

2. the requirements on the components within each subsystem.

## 5. Security Considerations

This document defines a mechanism to associate LFS identifier with a document outlining the syntax and format of a label. There is no security consideration in such an association. The label specification documents referenced by each registration entry should state security considerations for the label mechanism it specifies.

## 6. IANA Considerations

This section provides guidance to the Internet Assigned Numbers Authority (IANA) regarding creation of a new registry in accordance with [RFC5226].

This submission requests the creation of a new registry called "Security Label Format Selection Registry". The new registry has the following fields:

Label Format Specifier: An integer number that maps to a particular label format, e.g., the CALIPSO label format defined by [RFC5570]. The name space of this identifier has the range of 0..65,535.

Label Description: A human readable ASCII text string that describes the label format, e.g., "Common Architecture Label IPv6 Security Option (CALIPSO)". The length of this field is limited to 128 bytes.

Status: A short ASCII text string indicating the status of an entry in the registry. The status field for most entries should have the value "active". In the case that a label format selection entry is obsolete, the status field of the obsoleted entry should be "obsoleted by entry NNN".

Label Format Specification: A reference to a stable, public document that specifies the label format, e.g., an URL to [RFC5570].

### 6.1. Initial Registry

The initial assignments of the registry are as follows:

| Label Format Specifier | Description | Status | Reference |
|---|---|---|---|
| 0 | Reserved | - | - |
| 1 - 127 | Private Use | - | - |
| 128 - 255 | Experimental Use | - | - |
| 256 | CIPSO (tag type #1) | active | [[CIPSO] URL] |
| 257 | CALIPSO ([RFC5570]) | active | [[RFC5570] URL] |
| 258 | FLASK Security Context | active | [[FLASK99] URL] |
| 259 | IPSO | active | [[RFC1108] URL] |
| 260 - 65535 | Unassigned | - | - |

Label Format Specifier Ranges

Table 1

### 6.2. Adding a New Entry to the Registry

A label format specification document is required to add a new entry to this registry. If the label format document is inside the RFC path, then The IANA Consideration section of the label format document should clearly reference the Label Format Selection registry and request allocation of a new entry. The well-known IANA policy, Specification Required, as defined in section 4.1 of [RFC5226], will be used to handle such requests. Note that "Specification Required" policy implies this process requires a Designated Expert reviewer, i.e., adding a new entry to this registry requires both a published label format specification and a Designated Expert review.

### 6.3. Obsoleting a Label Format Specifier

In the case that a label format selector number is assigned to a label format and the label format specification is changed later, a new selector assignment should be requested. The same Specification Required IANA policy applies to such requests. The IANA Consideration section of the updated label format specification should be explicit in which old label selector assignment it obsoletes. Below is an example of obsoleted entry in the registry:

| Label Format Specifier | Description | Status | Reference |
|---|---|---|---|
| 0 | Reserved | - | - |
| 1 - 127 | Private Use | - | - |
| 128 - 255 | Experimental Use | - | - |
| 256 | CIPSO (tag type #1) | active | [[CIPSO] URL] |
| 257 | CALIPSO ([RFC5570]) | active | [[RFC5570] URL] |
| 258 | FLASK Security Context | obsoleted by 263 | [[FLASK99] URL] |
| ... | | | |
| 263 | FLASK Security Context (v2) | active | [new spec URL] |
| 264 - 65535 | Unassigned | - | - |

Example Label Format Specifier Updated Ranges

Table 2

## 7. References

### 7.1. Normative References

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

[RFC5226] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 5226, May 2008.

## 7.2. Informative References

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

[CIPSO] IETF CIPSO Working Group, "Commercial IP Security Option (CIPSO 2.2)", draft-ietf-cipso-ipsecurity-01 (expired), July 1992.

[FIPS-188] US National Institute of Standards and Technology, "Standard Security Labels for Information Transfer", Federal Information Processing Standard (FIPS) 188, September 1994.

[FLASK99] Spencer, R., Smalley, S., Loscocco, P., Hibler, M., Andersen, D., and J. Lepreau, "The Flask Security Architecture: System Support for Diverse Security Policies", In Proceedings of the Eighth USENIX Security Symposium, pages 123-139, August 1999.

[FLASK99b] Secure Computing Corporation, "Assurance in the Fluke Microkernel Formal Security Policy Model", Document 00-0930896A001 Rev B, 17 Feb 1999, Secure Computing Corporation, Roseville, MN, USA, February 1999.

[RFC1108] Kent, S., "Security Options for the Internet Protocol", RFC 1108, November 1991.

[RFC2401] Kent, S. and R. Atkinson, "Security Architecture for the Internet Protocol", RFC 2401, November 1998.

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

[RFC7204] Haynes, T., "Requirements for Labeled NFS", RFC 7204, April 2014.

## Appendix A. Acknowledgments

Ran Atkinson contributed the text for IPSO.

Dave Noveck helped detangle the terminology.

## Appendix B. RFC Editor Notes

[RFC Editor: please remove this section prior to publishing this document as an RFC]

Authors' Addresses

David P. Quigley

Email: dpquigl@davequigley.com

Jarrett Lu
Oracle

Email: jarrett.lu@oracle.com

Thomas Haynes
Primary Data, Inc.
4300 El Camino Real Ste 100
Los Altos, CA 94022
USA

Phone: +1 408 215 1519
Email: thomas.haynes@primarydata.com