Internet Engineering Task Force (IETF)
Request for Comments: 7569
Category: Standards Track
ISSN: 2070-1721

D. Quigley

J. Lu
Oracle

T. Haynes
Primary Data

July 2015

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

Abstract

In the past, Mandatory Access Control (MAC) systems have used very rigid policies that were implemented in particular protocols and platforms. As MAC systems become 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 such technologies as type enforcement. Due to the wide range of policies and mechanisms that need to be accommodated, it is unlikely that the 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 creates a registry of label format specifications. This registry contains label format identifiers and provides for the association of each such identifier with a corresponding extensive document outlining the exact syntax and use of the particular label format.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc7569.

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 unsuccessful. This is because 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 that 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 either (1) many MAC models would have blank fields for many of the label's components or (2) many implementations would ignore altogether many of the values that are present. The resulting complexity would be likely to result in a confusing situation in which the interaction of fields that are derived from different MAC models is never clearly specified and the addition of new models or extensions 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 would encompass multiple MAC models where an 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 sufficient 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 a 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.

This document creates a registry of label format specifications to allow multiple MAC mechanisms and label formats to co-exist in a network. While the initial use of this registry is for the Network File System (NFS) protocol, it might also be referenced and used by other IETF protocols in the future.

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: 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]).

(Although RFC 2401 has been obsoleted by RFC 4301, RFC 2401 is still the definitive reference for MLS as discussed in this document.)

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. Existing Label Format Specifications

3.1. 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".

3.2. Commercial IP Security Option (CIPSO)

The "Commercial IP Security Option (CIPSO)" label format is documented in [CIPSO] and in [FIPS-188]. While [CIPSO] 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.

3.3. 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 "Son of IPSO" (SIPSO); therefore, CALIPSO is NOT derived from CIPSO in any way.

3.4. Flux Advanced Security Kernel (FLASK)

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

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

2. the requirements on the components within each subsystem.

4. Security Considerations

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

5. IANA Considerations

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

Per this document, IANA has created a new registry called "Security Label Format Selection Registry". The new registry has the following fields:

Label Format Specifier: An integer that maps to a particular label format, e.g., the CALIPSO label format defined by [RFC5570]. The namespace of this identifier has the range of 0..65535.

Label Description: A human-readable ASCII [RFC20] 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 where 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., a URL to [RFC5570].

5.1. 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	[FIPS-188]
257	CALIPSO [RFC5570]	active	[RFC5570]
258	FLASK Security Context	active	[FLASK99]
259	IPSO	active	[RFC1108]
260 - 65535	Available for IANA Assignment	-	-

Label Format Specifier Ranges

Table 1

5.2. Adding a New Entry to the Registry

A label format specification document is required to add a new entry to the "Security Label Format Selection Registry". If the label format document is inside the RFC path, then the IANA Considerations section of the label format document should clearly reference the "Security 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 the "Specification Required" policy implies that this process requires a Designated Expert, i.e., adding a new entry to this registry requires both a published label format specification and a Designated Expert review.

In reviewing the published label format specification, the Designated Expert should consider whether or not the specification provides sufficient semantics for the object and subject labels to enforce the MAC model and policy administration when deployed within an organization. Another consideration is if the label format allows a correct and complete implementation of the protocol to process and enforce labels as a policy administration mechanism. Finally, to reduce interoperability issues, the reviewer must determine if the new label format specification has clearly defined syntax and semantics for the proposed new labels.

5.3. Obsoleting a Label Format Specifier

In the case where 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 Considerations section of the updated label format specification should be explicit regarding which old label selector assignment it obsoletes. Below is an example of an 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	[FIPS-188]
257	CALIPSO [RFC5570]	active	[RFC5570]
258	FLASK Security Context	obsoleted by 263	[FLASK99]
...			
263	FLASK Security Context (v2)	active	[new spec URL]
264 - 65535	Available for IANA Assignment	-	-

Example Label Format Specifier Updated Ranges

Table 2

5.4. Modifying an Existing Entry in the Registry

A request to modify either the Description or the published label format specification will also require the Specification Required IANA policy to be applied. The Designated Expert reviewer will need to determine if the published label format specification either obsoletes the Label Format Specifier or updates the label syntax and/or model. If the Label Format Specifier is obsoleted, then the reviewer will follow the process defined in Section 5.3. Otherwise, for the update of the label syntax and/or the model, the reviewer will approve the change.

6. References

6.1. Normative References

[RFC20] Cerf, V., "ASCII format for network interchange", STD 80, RFC 20, DOI 10.17487/RFC0020, October 1969, <http://www.rfc-editor.org/info/rfc20>.

[RFC5226] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 5226, DOI 10.17487/RFC5226, May 2008, <http://www.rfc-editor.org/info/rfc5226>.

6.2. 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)", Work in Progress, draft-ietf-cipso-ipsecurity-01, July 1992.

[FIPS-188] US National Institute of Standards and Technology, "Standard Security Labels for Information Transfer", Federal Information Processing Standards (FIPS) 188, September 1994, <http://csrc.nist.gov/publications/fips/fips188/fips188.pdf>.

[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, <https://www.cs.cmu.edu/~dga/papers/flask-usenixsec99.pdf>.

[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, <http://www.cs.utah.edu/flux/fluke/html/fspm.ps.gz>.

[RFC1108] Kent, S., "U.S. Department of Defense Security Options for the Internet Protocol", RFC 1108, DOI 10.17487/RFC1108, November 1991, <http://www.rfc-editor.org/info/rfc1108>.

[RFC2401] Kent, S. and R. Atkinson, "Security Architecture for the Internet Protocol", RFC 2401, DOI 10.17487/RFC2401, November 1998, <http://www.rfc-editor.org/info/rfc2401>.

[RFC5570] StJohns, M., Atkinson, R., and G. Thomas, "Common Architecture Label IPv6 Security Option (CALIPSO)", RFC 5570, DOI 10.17487/RFC5570, July 2009, <http://www.rfc-editor.org/info/rfc5570>.

[RFC7204] Haynes, T., "Requirements for Labeled NFS", RFC 7204, DOI 10.17487/RFC7204, April 2014, <http://www.rfc-editor.org/info/rfc7204>.

Acknowledgments

Ran Atkinson contributed the text for IPSO.

Dave Noveck helped detangle the terminology.

Alexey Melnikov caught that a process was needed for modifying entries in the registry.

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
United States

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