Internet Engineering Task Force (IETF)
Request for Comments: 9478
Category: Standards Track
ISSN: 2070-1721

P. Wouters
Aiven
S. Prasad
Red Hat

October 2023

Labeled IPsec Traffic Selector Support for the Internet Key Exchange Protocol Version 2 (IKEv2)

Abstract

This document defines a new Traffic Selector Type (TS Type) for the Internet Key Exchange Protocol version 2 (IKEv2) to add support for negotiating Mandatory Access Control (MAC) security labels as a Traffic Selector of the Security Policy Database (SPD). Security Labels for IPsec are also known as "Labeled IPsec". The new TS Type, TS_SECLABEL, consists of a variable length opaque field that specifies the security label.

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 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at https://www.rfc-editor.org/info/rfc9478.

Copyright Notice

Copyright (c) 2023 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents (https://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Revised BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Revised BSD License.

Table of Contents

1. Introduction

In computer security, Mandatory Access Control (MAC) usually refers to systems in which all subjects and objects are assigned a security label. A security label is composed of a set of security attributes. Along with a system authorization policy, the security labels determine access. Rules within the system authorization policy determine whether the access will be granted based on the security attributes of the subject and object.

Historically, security labels used by Multi-Level Secure (MLS) systems are comprised of a sensitivity level (or classification) field and a compartment (or category) field, as defined in [RFC5570]. As MAC systems evolved, other MAC models gained popularity. For example, SELinux, a Flux Advanced Security Kernel (FLASK) implementation, has security labels represented as colon-separated ASCII strings composed of values for identity, role, and type. The security labels are often referred to as security contexts.

Traffic Selector (TS) payloads specify the selection criteria for packets that will be forwarded over the newly set up IPsec Security Association (SA) as enforced by the Security Policy Database (SPD) [RFC4301].

This document specifies a new TS Type, TS_SECLABEL, for IKEv2 that can be used to negotiate security labels as additional selectors for the SPD to further restrict the type of traffic that is allowed to be sent and received over the IPsec SA.

1.1. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

1.2. Traffic Selector Clarification

The negotiation of Traffic Selectors is specified in Section 2.9 of [RFC7296], where it defines two TS Types (TS_IPV4_ADDR_RANGE and TS_IPV6_ADDR_RANGE). The TS payload format is specified in Section 3.13 of [RFC7296]. However, the term "Traffic Selector" is used to denote the TS payloads and individual Traffic Selectors of that payload. Sometimes, the exact meaning can only be learned from context or if the item is written in plural ("Traffic Selectors" or "TSes"). This section clarifies these terms as follows:

A Traffic Selector (capitalized, no acronym) is one selector for traffic of a specific Traffic Selector Type (TS Type). For example, a Traffic Selector of TS Type TS_IPV4_ADDR_RANGE for UDP (protocol 17) traffic in the IP network 198.51.100.0/24 covering all ports is denoted as (17, 0, 198.51.100.0-198.51.100.255).

A TS payload is a set of one or more Traffic Selectors of the same or different TS Types. It typically contains one or more of the TS Type of TS_IPV4_ADDR_RANGE and/or TS_IPV6_ADDR_RANGE. For example, the above Traffic Selector by itself in a TS payload is denoted as TS((17, 0, 198.51.100.0-198.51.100.255))

1.3. Security Label Traffic Selector Negotiation

The negotiation of Traffic Selectors is specified in Section 2.9 of [RFC7296] and states that the TSi/TSr payloads MUST contain at least one TS Type. This document adds a new TS Type of TS_SECLABEL that is valid only with at least one other TS Type. That is, it cannot be the only TS Type present in a TSi or TSr payload. It MUST be used along with an IP address selector type, such as TS_IPV4_ADDR_RANGE and/or TS_IPV6_ADDR_RANGE.

2. TS_SECLABEL Traffic Selector Type

This document defines a new TS Type, TS_SECLABEL, that contains a single new opaque Security Label.

2.1. TS_SECLABEL Payload Format

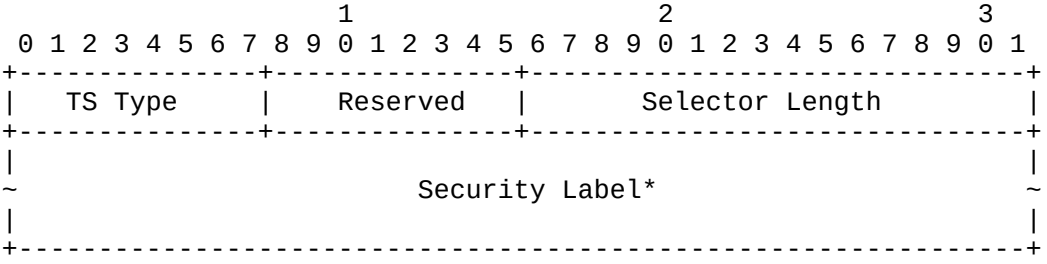

Figure 1: Labeled IPsec Traffic Selector

Note: All fields other than TS Type and Selector Length depend on the TS Type. The fields shown are for TS Type TS_SECLABEL, which is the selector that this document defines.

TS Type (one octet):
Set to 10 for TS_SECLABEL.

Selector Length (two octets, unsigned integer):
Specifies the length of this Traffic Selector substructure including the header.

Security Label:
An opaque byte stream of at least one octet.

2.2. TS_SECLABEL Properties

The TS_SECLABEL TS Type does not support narrowing or wildcards. It MUST be used as an exact match value.

The TS_SECLABEL TS Type MUST NOT be the only TS Type present in the TS payload, as TS_SECLABEL is complimentary to another type of Traffic Selector. There MUST be an IP address Traffic Selector Type in addition to the TS_SECLABEL TS Type in the TS payload. If a TS payload is received with only TS_SECLABEL TS Types, the exchange MUST be aborted with an Error Notify message containing TS_UNACCEPTABLE.

The Security Label contents are opaque to the IKE implementation. That is, the IKE implementation might not have any knowledge regarding the meaning of this selector other than recognizing it as a type and opaque value to pass to the SPD.

A zero-length Security Label MUST NOT be used. If a received TS payload contains a TS Type of TS_SECLABEL with a zero-length Security Label, that specific TS payload MUST be ignored. If no other TS payload contains an acceptable TS_SECLABEL TS Type, the exchange MUST be aborted with a TS_UNACCEPTABLE Error Notify message. A zero-

length Security Label MUST NOT be interpreted as a wildcard security label.

If multiple Security Labels are allowed for a Traffic Selector's IP address range, protocol, and port range, the initiator includes all of these acceptable Security Labels. The responder MUST select exactly one of the Security Labels.

A responder that selected a TS with TS_SECLABEL MUST use the Security Label for all selector operations on the resulting TS. It MUST NOT select a TS_SECLABEL without using the specified Security Label, even if it deems the Security Label optional, as the initiator has indicated (and expects) that the Security Label will be set for all traffic matching the negotiated TS.

3. Traffic Selector Negotiation

If the TSi payload contains a Traffic Selector with TS Type TS_SECLABEL (along with another TS Type), the responder MUST create each TS response for the other TS Types using its normal rules specified for each of those TS Types, such as narrowing them following the rules specified for that TS Type and then adding exactly one for the TS Type of TS_SECLABEL to the TS payload(s). If this is not possible, it MUST return a TS_UNACCEPTABLE Error Notify payload.

If the Security Label TS Type is optional from a configuration point of view, an initiator will add the TS_SECLABEL to the TSi/TSr payloads. If the responder replies with TSi/TSr payloads that include the TS_SECLABEL, then the Child SA MUST be created and include the negotiated Security Label. If the responder did not include a TS_SECLABEL in its response, then the initiator (which deemed the Security Label optional) will install the Child SA without including any Security Label. If the initiator required the TS_SECLABEL, it MUST NOT install the Child SA and it MUST send a Delete notification for the Child SA so the responder can uninstall its Child SA.

3.1. Example TS Negotiation

An initiator could send the following:

```
TSi = ((17,24233,198.51.100.12-198.51.100.12),
       (0,0,198.51.100.0-198.51.100.255),
       (0,0,192.0.2.0-192.0.2.255),
       TS_SECLABEL1, TS_SECLABEL2)

TSr = ((17,53,203.0.113.1-203.0.113.1),
       (0,0,203.0.113.0-203.0.113.255),
       TS_SECLABEL1, TS_SECLABEL2)
```

Figure 2: Initiator TS Payloads Example

The responder could answer with the following:

```
TSi = ((0,0,198.51.100.0-198.51.100.255),
       TS_SECLABEL1)

TSr = ((0,0,203.0.113.0-203.0.113.255),
       TS_SECLABEL1)
```

Figure 3: Responder TS Payloads Example

3.2. Considerations for Using Multiple TS Types in a TS

It would be unlikely that the traffic for TSi and TSr would have a

different Security Label, but this specification allows this to be specified. If the initiator does not support this and wants to prevent the responder from picking different labels for the TSi/TSr payloads, it should attempt a Child SA negotiation and start with the first Security Label only. Upon failure, the initiator should retry a new Child SA negotiation with only the second Security Label.

If different IP ranges can only use different specific Security Labels, then these should be negotiated in two different Child SA negotiations. In the example above, if the initiator only allows 192.0.2.0/24 with TS_SECLABEL1 and 198.51.100.0/24 with TS_SECLABEL2, then it MUST NOT combine these two ranges and security labels into one Child SA negotiation.

4. Security Considerations

It is assumed that the Security Label can be matched by the IKE implementation to its own configured value, even if the IKE implementation itself cannot interpret the Security Label value.

A packet that matches an SPD entry for all components, except the Security Label, would be treated as "not matching". If no other SPD entries match, the (mislabeled) traffic might end up being transmitted in the clear. It is presumed that other MAC methods are in place to prevent mislabeled traffic from reaching the IPsec subsystem or that the IPsec subsystem itself would install a REJECT/DISCARD rule in the SPD to prevent unlabeled traffic otherwise matching a labeled security SPD rule from being transmitted without IPsec protection.

5. IANA Considerations

IANA has added a new entry in the "IKEv2 Traffic Selector Types" registry [RFC7296] as follows.

Value	TS Type	Reference
10	TS_SECLABEL	RFC 9478

Table 1: IKEv2 Traffic Selector Types Registry

6. References

6.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC7296] Kaufman, C., Hoffman, P., Nir, Y., Eronen, P., and T. Kivinen, "Internet Key Exchange Protocol Version 2 (IKEv2)", STD 79, RFC 7296, DOI 10.17487/RFC7296, October 2014, <https://www.rfc-editor.org/info/rfc7296>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

6.2. Informative References

[LABELED-IPSEC] Latten, J., Quigley, D., and J. Lu, "Security Label

Extension to IKE", Work in Progress, Internet-Draft, draft-jml-ipsec-ikev2-security-label-01, 28 January 2011, <https://datatracker.ietf.org/doc/html/draft-jml-ipsec-ikev2-security-label-01>.

[RFC4301] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, DOI 10.17487/RFC4301, December 2005, <https://www.rfc-editor.org/info/rfc4301>.

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

Acknowledgements

A large part of the introduction text was taken verbatim from [LABELED-IPSEC], whose authors are Joy Latten, David Quigley, and Jarrett Lu. Valery Smyslov provided valuable input regarding IKEv2 Traffic Selector semantics.

Authors' Addresses

Paul Wouters
Aiven
Email: paul.wouters@aiven.io

Sahana Prasad
Red Hat
Email: sahana@redhat.com