Network Working Group
Internet-Draft
Intended Status: Standards Track
Expires: July 27, 2011

J. Latten
IBM
D. Quigley
J. Lu
Oracle

January 28, 2011

Security Label Extension to IKE
draft-jml-ipsec-ikev2-security-label-01

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), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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".

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt.

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

This Internet-Draft will expire on July 27, 2011.

Copyright Notice

Abstract

This document describes extensions to the Internet Key Exchange Protocol Version 2 [RFC5996] to support Mandatory Access Control (MAC) security labels used on deployed systems.

1. Introduction

In computer security, Mandatory Access Control usually refers to systems in which all subjects and objects are assigned a security label. A security label is comprised of a set of security attributes. The security labels along with a system authorization policy 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.

Traditionally, security labels used by Multilevel Systems (MLS) are comprised of a sensitivity level (or classification) field and a compartment (or category) field, as defined in [FIPS188] and [RFC5570]. As MAC systems evolved, other MAC models gained in 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.

This document will describe extensions to IKEv2 to support its handling of security labels for implicit labeling schemes on network communications.

2. Terminology

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].

3. Implicit Labeled Networking

Within a MAC environment, a security label is applied to data (e.g. IP packets) transmitted over the network. The MAC policy can then use the label information to make informed access decisions.

In a traditional Multilevel System envionment, IP packets are labeled with clear text labels. This is acceptable because the underlying physical network is assumed to be secure in an MLS environment and clear text labeling has performance advantage in secure physical network envionments. An obvious disadvantage of labeling data in

clear text is its reliance on a secure physical network. This limitaion prevents traditional MLS MAC systems from being useful on public networks. With the proposed label extension to IKEv2, security labels can be established as part of the IKE negotiation. The security label is stored in the Security Association making it unnecessary for data packets to carry security label information, i.e. making packet labeling implicit. The implicit label scheme retains security label requirements demanded by MAC systems, but removes the reliance of underlying secure physical networks.

4. Security Label Transform

This document introduces a new transform type to communicate the security label when creating Child SAs during the IKE_AUTH exchange and CREATE_CHILD_SA exchange. Security label transforms are only included in IPsec SAs and not IKE SAs.

The transform type value is:

Description	Transform Type	Used In
Security Label	IANA	ESP and AH

Only one security label transform containing only one security label is required per protocol. The security label data MUST be the same for each protocol within each proposal for a particular SA payload. In other words, only one instance of a security label is communicated for the proposed SA.

For Security Label Transform Type, the defined Transform IDs are:

Name	Number	Defined In
None	0	
Label_Format_Selector_1	1	TBD
Label_Format_Selector_2	2	TBD
...		

The acceptable Label_Format_Selectors (LFSs) are described in draft-quigley-label-format-regisry-00 (work-in-progress). The LFS indicates the format of the security label and how the security label is to be interpreted by the MAC layer.

This transform requires a transform attribute to communicate the actual security label data.

The Transform Attribute Type:

Attribute Type	Value	Attribute Format
Security Label	IANA	TLV

4.1 Attribute Negotiation

The LFS indicates to a remote peer whether the security label can be understood and interpreted by the peer's MAC layer.

An initiating IKE communicates the LFS and the security label data in the security label transform of a proposal. If the responder receives an LFS it does not understand, then it MUST consider the proposal unacceptable. IKE does not interpret the security label data itself.

5. Security Considerations

[RFC5996] describes the NO_ADDITIONAL_SAS notification.
It is possible that a traffic stream may require an SA for each instance of a security label on it. Thus a responder SHOULD be willing to accept more than one SA pair on an IKE_SA in this case.

The addition of the security label transform should not change the underlying security characteristics of IKE.

6. IANA Considerations

This document introduces the following IANA assignments:

- IKEv2 Transform Type for the security label.

Description	Transform type
Security Label	To be assigned by IANA

- IKEv2 Transform Attribute Type

Attribute Type	Value	Attribute Format
Security Label	To be assigned by IANA	TLV

7. Acknowledgements

The authors would like to acknowledge Trent Jaeger, Serge Hallyn, and George Wilson, architects of the original design and implementation of labeled IPsec in Linux. The authors would also

like to thank Stephen Smalley, James Morris and members of the SELinux community for their contributions during the initial design

The original design of labeled IPsec was implemented in Linux with SELinux as it's MAC. Sun Microsystems also has a version of labeled IPsec in OpenSolaris Trusted Extensions.

8. References

8.1 Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Level", BCP 14, RFC 2119, March 1997.

[RFC5996] Kaufman, C., Hoffman, P., Nir, Y., Eronen, P., "Internet Key Exchange (IKEv2) Protocol", RFC 5996, September 2010.

8.2 Informative References

[FIPS188] National Institute of Standards and Technology, "Standard Security Label for Information Transfer", Federal Information Processing Standard (FIPS) Publication 188, September 1994, http://www.itl.nist.gov/fipspubs/fip188.htm

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

Authors' Addresses

Joy Latten
email: latten@austin.ibm.com

David Quigley
email: dpquigl@tycho.nsa.gov

Jarrett Lu
email: Jarrett.Lu@oracle.com