IP Security Maintenance and Extensions (ipsecme)
Internet-Draft
Intended status: Standards Track
Expires: August 4, 2014

D. Migault (Ed)
Orange
T. Guggemos
Orange / LMU Munich
D. Palomares
Orange / LIP6

January 31, 2014

Minimal ESP
draft-mglt-lwig-minimal-esp-00.txt

Abstract

This document describes a minimal version of the IP Encapsulation Security Payload (ESP) described in RFC 4303 which is part of the IPsec suite.

ESP is used to provide confidentiality, data origin authentication, connectionless integrity, an anti-replay service (a form of partial sequence integrity), and limited traffic flow confidentiality.

This document does not update or modify RFC 4303, but provides a compact description of the minimal version of the protocol. If this document and RFC 4303 conflicts then RFC 4303 is the authoritative description.

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 August 4, 2014.

Table of Contents

1. Requirements notation

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].

2. Introduction

ESP [RFC4303] is part of the IPsec suite protocol [RFC4301] . It is used to provide confidentiality, data origin authentication, connectionless integrity, an anti-replay service (a form of partial sequence integrity), and limited traffic flow confidentiality.

The ESP Packet description is described in Figure 1. Currently ESP is part of the kernel of devices that are IPsec aware. In this document we are interested in providing a minimal ESP implementation

so that smaller devices like sensor without kernel and with hardware restriction can implement ESP on their own and benefit from IPsec.

Minimal ESP describes the best suited configuration for the regular ESP protocol.

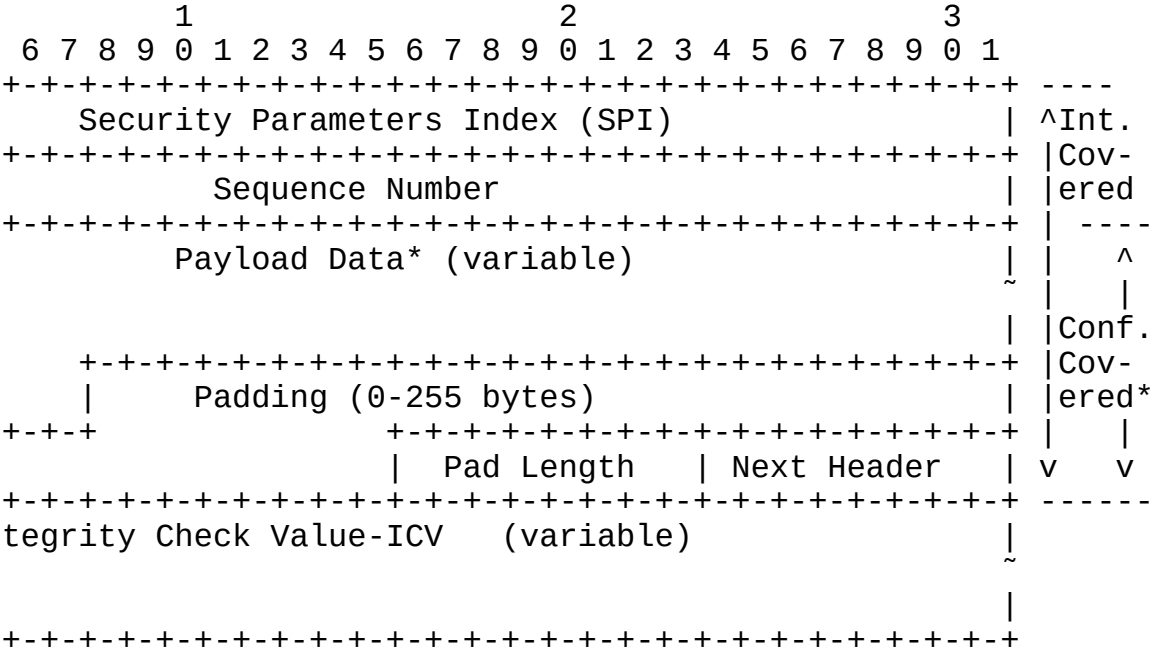

Figure 1: ESP Packet Description

The following sections describe each field of the ESP packet format in figure 1 and explain how minimal implementations are dealing with each one of them.

3. Security Parameter Index (SPI) (32 bit)

According to the [RFC4303], the SPI is a mandatory 32 bits field and is not allowed to be removed.

A device can use a fixed value that is believed to be unique by the device. A 32 bit identifier or an IPv4 address for example. Using fix value for the SPI is only to be considered if the device expects to have a single IPsec communication per device. Note that communication cannot proceed if the SPI is not available for the other peer. Values 0-255 SHOULD NOT be used. Values 1-255 are reserved and 0 is only allowed to be used internally and it must not be sent on the wire.

"The SPI is an arbitrary 32-bit value that is used by a receiver to identify the SA to which an incoming packet is bound. The SPI field is mandatory. [...]"

"For a unicast SA, the SPI can be used by itself to specify an SA, or it may be used in conjunction with the IPsec protocol type (in this case ESP). Because the SPI value is generated by the receiver for a unicast SA, whether the value is sufficient to identify an SA by itself or whether it must be used in conjunction with the IPsec protocol value is a local matter. This mechanism for mapping inbound traffic to unicast SAs MUST be supported by all ESP implementations."

4. Sequence Number(SN) (32 bit)

According to [RFC4303], the sequence number is a mandatory 32 bits field in the packet. The field wants to be present in the packet, either the receiver decides whether it wants to use it for anti-replay or not. In addition, it is possible to extend the SN to 64 bits in the SAD. The SN is incremented by the sender, and the usage of fixed values is not allowed. However, this rule has been set so any initiator can set an ESP secure communication with any ESP peer. In the IoT world, some devices may be configured to establish a connection with a specific and dedicated device. In that case, if the device knows the other peer does not read the SN, it MAY then use a fix value.

"This unsigned 32-bit field contains a counter value that increases by one for each packet sent, i.e., a per-SA packet sequence number. For a unicast SA or a single-sender multicast SA, the sender MUST increment this field for every transmitted packet. Sharing an SA among multiple senders is permitted, though generally not recommended. [...] The field is mandatory and MUST always be present even if the receiver does not elect to enable the anti-replay service for a specific SA."

5. Next Header (8 bit)

According to [RFC4303], "The Next Header is a mandatory, 8-bit field that identifies the type of data contained in the Payload Data field, e.g., an IPv4 or IPv6 packet, or a next layer header and data. [...] the protocol value 59 (which means "no next header") MUST be used to designate a "dummy" packet. A transmitter MUST be capable of generating dummy packets marked with this value in the next protocol field, and a receiver MUST be prepared to discard such packets, without indicating an error."

6. ICV

The ICV is an optional value with variable length. Although optional, we recommend strongly to use the ICV. Furthermore, the [RFC4303] allows combined encryption and authentication ciphers, which enables the use of modes like GCM, CCM and AES-CTR which make ICV mandatory.

IoT devices may allow weak security by removing the ICV, and gateways wanting to connect to IoT devices SHOULD be able to deal with NULL authentication.

"The Integrity Check Value is a variable-length field computed over the ESP header, Payload, and ESP trailer fields. Implicit ESP trailer fields (integrity padding and high-order ESN bits, if applicable) are included in the ICV computation. The ICV field is optional. It is present only if the integrity service is selected and is provided by either a separate integrity algorithm or a combined mode algorithm that uses an ICV. The length of the field is specified by the integrity algorithm selected and associated with the SA. The integrity algorithm specification MUST specify the length of the ICV and the comparison rules and processing steps for validation."

7. Encryption

[RFC4303] specifies AES in CBC mode as mandatory for implementing ESP. For maximum interoperability with any gateway, it is recommended to implement AES in CBC mode. As for the Sequence Number, the minimal ESP implementation may be used for specific devices that will establish an ESP communication with a specific target. If so AES-CTR can be chosen as the unique encryption algorithm. The key advantage of AES-CTR is that it does not have a specific block size, which may reduce the Pad Length value.

8. IANA Considerations

There are no IANA consideration for this document.

9. Security Considerations

Security considerations are those of [RFC4303].

Using a fix value for SPI may isolate the device, as it will not be able to set a communication with the peer if that SPI value is not available.

10. Acknowledgment

11. Normative References

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

[RFC4301] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, December 2005.

[RFC4303] Kent, S., "IP Encapsulating Security Payload (ESP)", RFC 4303, December 2005.

Appendix A. Document Change Log

[RFC Editor: This section is to be removed before publication]

-00: First version published.

Authors' Addresses

Daniel Migault
Orange
38 rue du General Leclerc
92794 Issy-les-Moulineaux Cedex 9
France

Phone: +33 1 45 29 60 52
Email: daniel.migault@orange.com

Tobias Guggemos
Orange / LMU Munich
Am Osteroesch 9
87637 Seeg, Bavaria
Germany

Email: tobias.guggemos@gmail.com

Daniel Palomares
Orange / LIP6
10, Rue du Moulin
92170 Vanves, Ille-de-France
France

Email: daniel.palomares@orange.com