DICE
Internet-Draft
Intended status: Standards Track
Expires: January 24, 2015

D. Migault (Ed)
Orange
C. Bormann
Universitaet Bremen TZI

July 23, 2014

IPsec/ESP for Application Payload
draft-mglt-dice-ipsec-for-application-payload-00.txt

Abstract

This document is a strawman specification describing how IPsec/ESP could be used to secure application payloads, in particular to enable multicast applications where DTLS would be used for unicast.

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 January 24, 2015.

Table of Contents

1. Introduction

[I-D.keoh-dice-multicast-security] defines a way to protect multicast traffic against group outsiders using a modified DTLS record protocol. Reservations have been voiced about modifying DTLS this way without strengthening security by adding data origin authentication.

However, many applications do not require this additional security. One protocol that already supports group-level security for multicast is IPsec.

This document discusses how IPsec can be used to secure data at the application layer. The resulting packet structure is expected to resemble a DTLS flavor as represented in Figure 1.

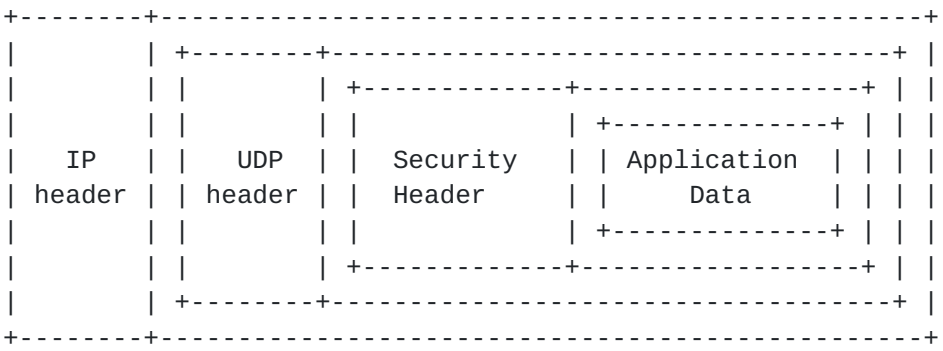

Figure 1: Securing Application Data

1.1. 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. State of the Art

IPsec/ESP [RFC4303] has been designed to secure IP payload according to two different modes: the transport mode and the tunnel mode. Figure 2 represents an non protected UDP packet that is protected with IPsec/ESP. UDP is chosen as an example and could be any other transport mode like TCP or SCTP, or ANY for unknown transport. Figure 3 illustrates how IPsec/ESP secures the non protected packet using the transport mode and Figure 4 illustrates how IPsec/ESP secures the packet with the tunnel mode.

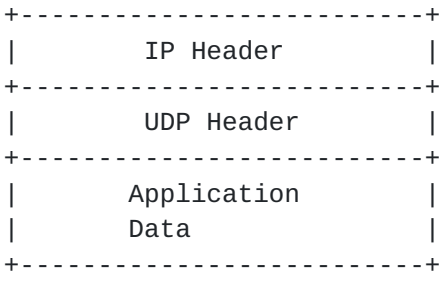

Figure 2: Example: non protected IP Packet

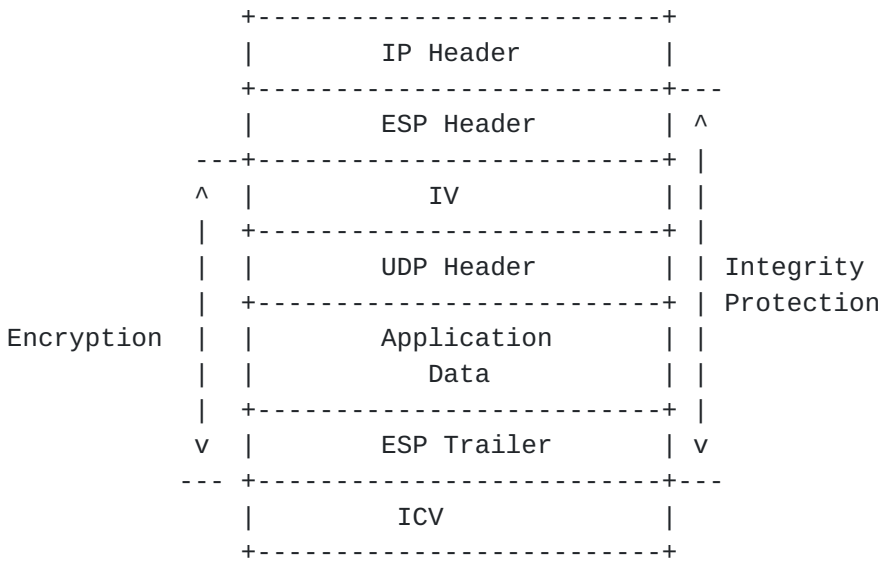

Figure 3: Example: IPsec/ESP with transport mode

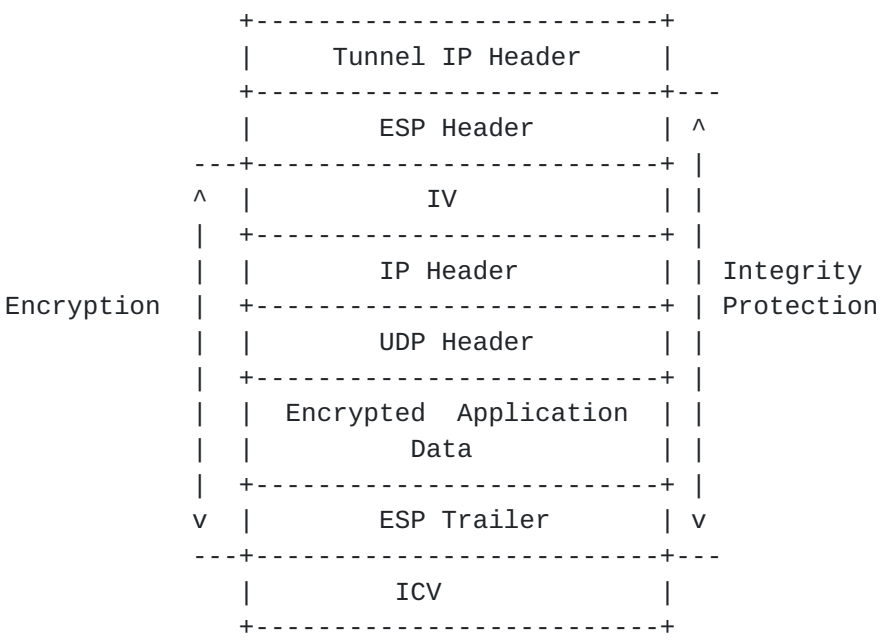

Figure 4: Ex: IPsec/ESP with tunnel mode

This document does not consider the tunnel mode and only the transport mode. DTLS is usually used to secure application data. Among other differences, IPsec/ESP with transport mode differs from DTLS on the following aspects: 1) The Security Header is placed before the transport header, as a result 2) the transport header is encrypted. Then 3) IPsec/ESP is an extension of IP which makes the whole packet described in Figure 3 and Figure 4 an IP packet with an empty IP payload. One consequence is that the packet has to respect the bit alignment required for IP headers, that is 32 bit alignment for IPv4 and 64 bit alignment for IPv6. This is why the ESP Trailer presents some Padding.

Figure 3 and Figure 4 mentions the IV which is necessary for encryption and decryption. The IV is usually not part of the IPsec/ESP protocol, but is defined by the encryption protocol used by IPsec/ESP. Each encryption protocol defines the size of its IV. It is mentioned in the figures in order to clarify the way we compute the overhead.

For NAT traversal, IPsec has defined a UDP encapsulation in [RFC3948]. UDP encapsulation of the IPsec/ESP packet with transport mode is illustrated in Figure 5.

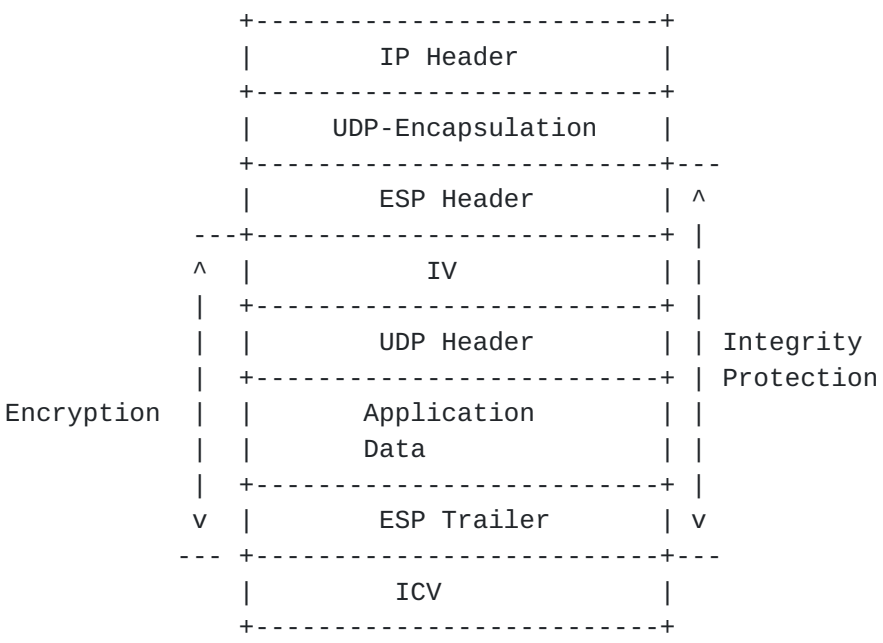

Figure 5: Ex: UDP Encapsulation of IPsec/ESP Transport mode

As illustrated in Figure 5, using IPsec/ESP with UDP encapsulation achieves our goal: A UDP packet carries a encrypted payload. In Figure 5, the encrypted payload is the concatenation of the IV, the UDP header, the application data and the ESP Trailer.

The overhead of such a packet is the ESP Header (8 bytes), the IV (8 bytes for AES-CCM mode [RFC4309]), an extra UDP header (8 bytes), the ESP Trailer (2 bytes and padding bytes. Padding bytes are between 0 and 8 for 64 bit alignment in IPv6 and between 0 and 4 bytes for IPv4. As a result, the average is 6 bytes for IPv6 and 4 bytes for IPv4). This leads to a 30 bytes overhead for IPv6 and 28 byte overhead for IPv4.

If this approach is to be pursued, it is probably worthwhile to reduce this overhead

The remaining sections describe ways to do that.

3. UDP-Encapsulation Header

[RFC3948] specifies that ports of the UDP-Encapsulation Header MUST be the one used during the IKEv2 negotiation. In addition IKEv2 is listening for UDP encapsulation on port 4500. As a result, the port of the responder is always set to 4500 for any ESP packet.

The use of a fix port in 4500 for IKEv2 is a standard port that specifies, IKEv2 packets are expected to be UDP encapsulated. The

reason to keep these ports in the ESP UDP encapsulated communication, is that 1) IKEv2 has set a channel between the peers through a NAT -- note that each peer may have a different set of (port source, port destination). 2) IKEv2 is used to set up the IPsec/ESP communication on each peer by setting the various IPsec database. Since IKEv2 is aware of a through-NAT-reachable channel, IKEv2 can proceed to UDP encapsulation setting on each hosts.

Port fixing is not required in applications other than the UDP encapsulation or if IKEv2 is not used to setup the IPsec/ESP communication.

4. Removing Transport Header

The Transport Header is used to identify the application with ports, once IPsec has decrypted an incoming packet. For sending packets, the ports in the transport header can be used as Traffic Selectors to identify the right Securicy Policy.

Removing the Transport Header implies that none of the ports or transport protocol can be used as selectors. IPsec [RFC4301] does not prevent that, and only the IP addresses will be considered, and thus all applications that do not use ports as selectors between the two peers will be protected with the same SA. Note that IPsec SPD is an ordered database. This means that if an application between the two peers with ports specified as Traffic Selectors needs a specific Security Association, this is still possible. The policy has simply to be placed before the policy using only IP addresses.

5. Additional Compression

With the current standard [RFC3948], [RFC4301], no additional compression can be completed, which leaves an overhead of 22 bytes for IPv4 and 20 bytes for IPv4.

Protocols like 6LowPAN [I-D.raza-6lowpan-ipsec], ROHC [RFC3095], [RFC5225] can compress the ESP Header up to zero bytes. The ESP Header contains a Security Policy Index (SPI) of 4 bytes and a Sequence Number (SN) of 4 bytes. The SPI may be completely compressed if the UDP decapsulation decompressor is able to derive the SPI from UDP ports. Both SPI and SN are necessary to perform authentication and integrity check.

Compression of the ESP Trailer cannot be currently performed. However, ongoing work [I-D.mglt-ipsecme-diet-esp] makes possible the compression of all fields of the ESP Trailer.

Compression of IV is not currently permitted with IPsec, and this field MUST be included in each IP packet. However, some ongoing work [I-D.mglt-ipsecme-diet-esp-iv-generation].

Finally, compression of the transport header may also be performed using [I-D.mglt-ipsecme-diet-esp-payload-compression]. The advanatge of compressing it over removing it is that compression enables the use of ports as Traffic Selectors without carrying the transport header. Note that this is done under conditions.

6. IANA Considerations

There are no IANA consideration for this document.

7. Security Considerations

The security considerations of IPsec and Diet-ESP (if used) apply.

8. References

8.1. Normative References

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

[RFC3095] Bormann, C., Burmeister, C., Degermark, M., Fukushima, H., Hannu, H., Jonsson, L-E., Hakenberg, R., Koren, T., Le, K., Liu, Z., Martensson, A., Miyazaki, A., Svanbro, K., Wiebke, T., Yoshimura, T., and H. Zheng, "RObust Header Compression (ROHC): Framework and four profiles: RTP, UDP, ESP, and uncompressed", RFC 3095, July 2001.

[RFC3948] Huttunen, A., Swander, B., Volpe, V., DiBurro, L., and M. Stenberg, "UDP Encapsulation of IPsec ESP Packets", RFC 3948, January 2005.

[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.

[RFC4309] Housley, R., "Using Advanced Encryption Standard (AES) CCM Mode with IPsec Encapsulating Security Payload (ESP)", RFC 4309, December 2005.

[RFC5225] Pelletier, G. and K. Sandlund, "RObust Header Compression Version 2 (ROHCv2): Profiles for RTP, UDP, IP, ESP and UDP-Lite", RFC 5225, April 2008.

8.2. Informational References

[I-D.keoh-dice-multicast-security]
Keoh, S., Kumar, S., Garcia-Morchon, O., Dijk, E., and A. Rahman, "DTLS-based Multicast Security in Constrained Environments", draft-keoh-dice-multicast-security-08 (work in progress), July 2014.

[I-D.mglt-ipsecme-diet-esp]
Migault, D. and T. Guggemos, "Diet-ESP: a flexible and compressed format for IPsec/ESP", draft-mglt-ipsecme-diet-esp-01 (work in progress), July 2014.

[I-D.mglt-ipsecme-diet-esp-iv-generation]
Migault, D. and T. Guggemos, "Diet-ESP: Generating compressed IV and SN", draft-mglt-ipsecme-diet-esp-iv-generation-00 (work in progress), July 2014.

[I-D.mglt-ipsecme-diet-esp-payload-compression]
Migault, D. and T. Guggemos, "Diet-IPsec: ESP Payload Compression of IPv6 / UDP / TCP / UDP-Lite", draft-mglt-ipsecme-diet-esp-payload-compression-00 (work in progress), July 2014.

[I-D.raza-6lowpan-ipsec]
Raza, S., Duquennoy, S., and G. Selander, "Compression of IPsec AH and ESP Headers for Constrained Environments", draft-raza-6lowpan-ipsec-01 (work in progress), September 2013.

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

Carsten Bormann
Universitaet Bremen TZI
Postfach 330440
D-28359 Bremen
Germany

Phone: +49-421-218-63921
Email: cabo@tzi.org