Network Working Group
Internet Draft
Intended Status: Proposed Standard
Expires: May 2009

Manav Bhatia
Alcatel-Lucent

Identifying ESP-NULL Packets

draft-bhatia-ipsecme-esp-null-00.txt

Status of this Memo

Abstract

Encapsulating Security Payload (ESP) [RFC4303] provides data integrity protection, confidentiality and data origin authentication for data transported in an IP packet.

There are various applications and protocols that do not require confidentiality but only need data integrity assurance or data origin authentication. Since ESP support is mandatory for IPSec, such applications end up using ESP with NULL encryption.

However, because of the way ESP is defined, it is impossible for firewalls and intermediate routers to differentiate between encrypted ESP and ESP NULL packets by simply examining them. This poses

problems for the firewalls since such packets cannot be filtered and identified. It poses a different set of problems for routers since such packets cannot be properly filtered, classified and prioritized.

This document proposes an extension to ESP so that firewalls and routers can disambiguate between ESP encrypted and ESP NULL encrypted packets.

Conventions used in this document

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].

1. Introduction

ESP-NULL is used when confidentiality is not required and only source authentication and data integrity assurance is desired.

IPSec mandates the use of ESP while keeps support for Authentication Header (AH) [RFC4302] as optional. Thus, new protocols using IPSec for data integrity also mandate the use of ESP-NULL. It is also mandatory [RFC4835] for all ESP implementations to provide support for ESP NULL encryption. Because of these factors a lot of vendors do not implement AH and only support ESP-NULL for data integrity and source authentication. The traffic using ESP-NULL is thus only going to increase with time.

Firewalls and intermediate routers in the network find it impossible to parse ESP packets since they have no idea whether the packet is encrypted or not. They cannot for this reason implement filters and access control lists (ACLs).

ACLs are highly desirable and used extensively by service providers to block undesired traffic coming from other domains.

This draft therefore proposes an extension to ESP with which identifying an ESP-NULL packet from an ESP encrypted packet becomes trivial. It is backward compatible, therefore devices that do not understand this extension would treat packets using this extension as normal ESP packets.

The extension described in this draft is applicable for both the tunnel and the transport modes of ESP.

2. Explicitly Marking ESP NULL Packets

ESP-NULL packets, for both implementations based on [RFC2410] and [RFC4543] MUST be sent with a well known, reserved SPI of 1. The

original SPI should be included as part of the payload. This is encoded in the first 4 octets of the payload section of the ESP header. An implementation MUST put the next-header and the ESP header length as the 4th and the 5th octets of the payload.

Since the packet is not encrypted these fields would be sent in clear text and would be visible to all.

An extended ESP packet using NULL encryption would thus look like this:

```
0                   1                   2                   3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|        Reserved Security Parameters Index (RSPI) = 1          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                      Sequence Number                          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|          Original Security Parameters Index (SPI)             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  next-header  |  eESP HDRLen  |                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+                               +
|                    Payload Data* (variable)                   |
~                                                               ~
|                                                               |
+               +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|               |     Padding (0-255 bytes)                     |
+-+-+-+-+-+-+-+-+               +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                               |  Pad Length   | Next Header   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                  Authentication Data  (variable)              |
~                                                               ~
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 1

Reserved Security Parameters Index (RSPI): Well known value that should be given by IANA to indicate that it is an ESP-NULL packet.

next-header: This is a one octet field that indicates the next protocol header. Explicitly mentioning this provides an easy access to a HW parser to extract the upper layer protocol.

eESP HDRLen: This is a one octet field that gives the length of the extended ESP header + IV (if mandated by the authentication algorithm). It is an offset to the beginning of the payload data.

Intermediate nodes (routers, firewalls, etc) interested in inspecting the packets en route can look at the SPI value at the start of the ESP header. If there are unaware of this extension then this packet would appear like a normal ESP packet. However, compliant implementations will understand that this is an extended ESP packet and would have enough information to be able to deep inspect the ESP-NULL packet.

The compliant end nodes (routers) can similarly parse the packet easily. If the SPI value is 1, then it can extract the original SPI from the payload and process the packet accordingly.

3. Authenticating the Packets

All fields of the extended ESP header starting with the RSPI and ending with the Next Header in the ESP trailer are included in the ESP data integrity check.

The authentication data field is used to hold the result of the data integrity check done on the ESP packet. The length of this field depends on the authentication algorithm employed by the Security Association (SA) used to process this packet.

4. Acknowledgements

The author would like to thank Jack Kohn for his useful comments.

5. IANA Considerations

IANA must assign a value that for Reserved SPI which will be used as described above. The draft uses a value 1 to foster pre-standard implementations.

6. Security Considerations

This proposal neither increases nor decreases the security for ESP. All considerations valid for ESP also apply here.

7. References

7.1 Normative References

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

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", RFC 2119, BCP 14, February 2001.

[RFC2410] Glenn, R., and Kent, S., "The NULL Encryption Algorithm and its Use With IPsec", RFC 2410, November 1998.

[RFC4543] McGrew, D. and Viega, J., "The Use of Galois Message Authentication Code (GMAC) in IPsec ESP and AH", RFC 4543, May 2006.

7.2 Informative References

[RFC4302] Kent, S., "IP Authentication Header", RFC 4302, December 2005.

[RFC4835] Manral, V., "Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)", RFC 4835, APRIL 2007.

8. Author's Addresses

Manav Bhatia
Alcatel-Lucent,
Bangalore, India
Email: manav@alcatel-lucent.com

Full Copyright Statement

Intellectual Property