Network Working Group
Internet-Draft
Intended status: Informational
Expires: July 2, 2012

M. Bhatia
Alcatel-Lucent

December 30, 2011

Moving Authentication Header (AH) to Historic
draft-bhatia-moving-ah-to-historic-00

Abstract

This document recommends retiring Authentication Header (AH) and discusses the reasons for doing so. It recommends moving RFC 4302 to Historic status.

Requirements Language

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 RFC 2119 [RFC2119].

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 July 2, 2012.

Copyright Notice

1. Introduction

IPsec uses two protocols to provide traffic security services -- Authentication Header (AH) and Encapsulating Security Payload (ESP). Both protocols are described in detail in their respective RFCs [RFC4302] [RFC4303]

[RFC4301] recommends IPsec implementations to MUST support ESP and MAY support AH. Support for AH was downgraded to MAY because experience has shown that there are very few contexts in which ESP cannot provide the requisite security services. Note that ESP can be used to provide only integrity, without confidentiality, making it comparable to AH in most contexts.

AH offers integrity and data origin authentication, with optional (at the discretion of the receiver) anti-replay features. ESP, on the other hand, offers the same set of services, and also additionally offers confidentiality.

These protocols may be applied individually or in combination with each other to provide IPv4 and IPv6 security services. However, most security requirements can be met through the use of ESP by itself. Each protocol supports two modes of use: transport mode and tunnel mode. In transport mode, AH and ESP provide protection primarily for next layer protocols; in tunnel mode, AH and ESP are applied to tunneled IP packets. [RFC4301] describes detailed differences between these two modes.

There is no particular security problem with using AH. It lives up to its security claims. Its just that its completely redundant with ESP, since ESP will NULL encryption (ESP-NULL) [RFC2410] can provide the same functionality and the world can do with one less protocol.

Moving AH to historic doesn't mean that people have to stop using AH right now. It only means that in the opinion of the community there are now better alternatives. Moving AH to historic will discourage new protocols to mandate the use of AH. It however, does not preclude the possibility of new work to IETF that will require or enhance AH. It just means that the authors will have to explain why that solution is really needed and why ESP-NULL cant be used instead.

2. AH and ESP

It is alleged that AH provides more security than ESP in the transport mode as AH also authenticates the IP header fields. This argument is however moot as ESP in the tunnel mode can provide the same level of security since the payload now includes the original IP header. It is also believed by many that securing the IP header isnt really very important [Schneier].

It is commonly believed that AH is quite useful in securing the IPv6 extension headers. AH protects most of the basic IPv6 header, the non-mutable extension headers after the AH, and the IP payload. Protection for the IPv6 header excludes the mutable fields: DSCP, ECN, Flow Label, and Hop Limit. ESP, on the other hand, doesn't protect the immutable parts of the IPv6 header nor those of any extension header. This can however be fixed by putting the IPv6 extension headers that are required to be protected after the ESP header. Hop-by-Hop options are not an issue, as the intermediate hops do not have keys to verify the message authentication code so they cannot really be protected anyways.

AH breaks Network Address Translators (NATs). This is because AH relies on the sanctity of the IP header so that any tamperings, even by a NAT, get detected and packets get discarded. Solving this issue requires another device that fixes the NAT translation back to the original one (a specific case of Double NAT). ESP, on the other hand, fixes this problem by encapsulating ESP packets inside UDP packets for traversing NATs [RFC3948].

Firewalls in the enterprise environments often require visibility into packets, ranging from simple packet header inspection to deeper payload examination. Routers also often need to deep inspect control traffic to prioritize certain protocol packets over the others. This was initially difficult with ESP since was impossible to know whether an ESP packet was integrity protected or encrypted by merely inspecting the packet. This was easy with AH since the payload was transmitted in clear. This problem however has been solved by introducing WESP [RFC5840] which defines a mechanism to provide additional information in relevant IPsec packets so intermediate devices can efficiently differentiate between encrypted and integrity-only ESP packets.

ESP-NULL seems to do everything useful that can be done with AH. Given this, it makes sense to move AH to Historic status so that newer protocols dont mandate or propose extensions that rely on AH to be supported.

3. Security Considerations

Its argued that ESP in the tunnel mode is equivalent to the AH in the transport mode. It should however be noted that ESP tunnel mode SA applied to an IPv6 flow results in at least 50 bytes of additional overhead per packet. This additional overhead may be undesirable for many bandwidth-constrained wireless and/or satellite communications networks, as these types of infrastructure are not overprovisioned.

Packet overhead is particularly significant for traffic profiles characterized by small packet payloads (e.g., various voice codecs). If these small packets are afforded the security services of an IPsec tunnel mode SA, the amount of per-packet overhead is increased.

This issue will perhaps be alleviated by header compression schemes defined in [RFC5856] [RFC5857] and [RFC5858].

4. IANA Considerations

None

5. References

5.1. Normative References

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

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

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

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

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

5.2. Informative References

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

[RFC5840] Grewal, K., Montenegro, G., and M. Bhatia, "Wrapped Encapsulating Security Payload (ESP) for Traffic Visibility", RFC 5840, April 2010.

[RFC5856] Ertekin, E., Jasani, R., Christou, C., and C. Bormann, "Integration of Robust Header Compression over IPsec Security Associations", RFC 5856, May 2010.

[RFC5857] Ertekin, E., Christou, C., Jasani, R., Kivinen, T., and C. Bormann, "IKEv2 Extensions to Support Robust Header Compression over IPsec", RFC 5857, May 2010.

[RFC5858] Ertekin, E., Christou, C., and C. Bormann, "IPsec Extensions to Support Robust Header Compression over IPsec", RFC 5858, May 2010.

[Schneier] Ferguson, N. and B. Schneier, "A Cryptographic Evaluation of IPsec", December 2003, <http://www.schneier.com/paper-ipsec.pdf>.

Author's Address

Manav Bhatia
Alcatel-Lucent

Email: manav.bhatia@alcatel-lucent.com