Network Working Group
Internet-Draft
Intended status: Best Current Practice
Expires: April 21, 2007

L. Dondeti, Ed.
V. Narayanan, Ed.
QUALCOMM, Inc.

October 18, 2006

Guidelines for using IPsec and IKEv2
draft-dondeti-useipsec-430x-00

Status of this Memo

Copyright Notice

Abstract

IPsec encapsulation can be used to provide a secure channel between two entities, to enforce controlled access to a network, or to provide any combination of integrity protection, confidentiality, replay protection, and traffic flow confidentiality of data being transmitted between two or more endpoints over untrusted transmission media or networks. Whereas various assortments of the protections are possible to provide, it is not always safe to use some of the

combinations. Next, IPsec SAs are established either manually or using a key management protocol such as IKEv2 with entity authentication verified locally or with the assistance of a third party. This document specifies when and how to use IPsec and IKEv2 and what combinations of protections afforded by those protocols are safe and when.

Table of Contents

1. Introduction 3
2. Terminology 3
3. Why is this document needed? 3
3.1. On the types of use cases of IPsec 4
4. What IPsec provides 5
5. Why use IPsec and where to use IPsec? 6
6. How to use IPsec to establish secure channel(s) between network entities? 6
6.1. Identify the Requirements and Constraints 6
6.1.1. Requirements and Constraints on the use of IPsec encapsulation 6
6.1.2. Constraints and Requirements associated with Selection of Key Management Protocol 8
7. Key management for IPsec:IKEv2 9
7.1. IKEv2 usage guidelines 9
7.2. Guidelines for using Traffic Selectors 9
7.3. IKEv2 support for network access control: IKEv2-EAP . . . 9
8. Group Key management for IPsec 9
9. IPsec and mobility 9
9.1. IKEv2 support for mobility 9
9.2. MOBIKE applicability 9
10. Security Considerations 9
11. IANA Considerations 9
12. Acknowledgments 9
13. References 10
13.1. Normative References 10
13.2. Informative References 10
Authors' Addresses 10
Intellectual Property and Copyright Statements 12

1. Introduction

It is often a good idea to use an existing security encapsulation protocol rather than inventing a new one every time a protocol needs security guarantees such as integrity protection, message authentication, confidentiality, replay protection or traffic flow confidentiality of data in transit. IPsec is a natural candidate in many instances. However, it is not sufficient to simply say "use IPsec." For interoperability and effective use it is necessary to specify in detail what aspects of IPsec are used.

IPsec is the IP layer security encapsulation protocol used to create a secure channel between any combination of end hosts and security gateways, or to enforce network access control, or to provide any combination of integrity protection, confidentiality, replay protection, and traffic flow confidentiality of data being transmitted between two or more endpoints over untrusted transmission media or networks. While it is possible to enable any combination of the protections available, it is not always safe to use some of the combinations. For instance, encryption without integrity protection may not be safe in most usage scenarios, and especially when counter mode encryption is used.

This document has three overall goals: The first is to explain briefly what IPsec does and the second to make the case for IPsec as the protocol of choice to establish a secure channel or to enforce access control, and finally explain that just saying "use IPsec" is not sufficient and describe what needs to be specified to correctly use IPsec.

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 RFC 2119 [1].

This document reuses the terminology of the IPsec and IKEv2 specifications.

3. Why is this document needed?

Protocols defined in the IETF and in other standards bodies often need a security encapsulation protocol or an access control mechanism. In those cases, it is plausible to design a new protocol, which is a rather difficult thing to do. It is quite easy to get things wrong in designing a security protocol: simple oversights may

result in the entire process being useless. The other option is to reuse an existing security protocol, IPsec being one of them. However, simply stating that use IPsec is in most cases insufficient for interoperability and more importantly for effective use. Once again, it is plausible that careless employment of IPsec may result in unneeded processing or overhead or worse in the whole process being ineffective.

To that end, a BCP [6] was written to provide guidance on how to use IPsecv2. Since then, the IPsecv3 suite of specifications were written to make it easier to use IPsec. Let us consider the two primary types of employment of IPsec and motivate the need for this document.

3.1. On the types of use cases of IPsec

For instance, in many networks, including the Internet itself, the transmission path between two infrastructure entities cannot be trusted: the data may be sensitive and needs to be protected from eavesdroppers or from packet modification or replay attacks. In those instances, network architects or protocol designers simply state that there needs to be an IPsec secure channel between those entities. In most cases, that is insufficient. It is often the case that there are several types of sensitive data to be sent between the entities: some need confidentiality and integrity protection, others may need integrity protection alone etc. Despite assumptions to the contrary, with key management protocols such as IKEv2, it is plausible to establish and maintain multiple secure channels or tunnels quite easily. ESPv3, AHv3 and IKEv2 specifications were developed primarily to bring IPsec more inline with the security requirements of the various protocols and to make it easy to specify which traffic needs what kind of protection via the key management protocol.

Next, access control enforcement is another application of IPsec. There are at least two types of access control for which IPsec is best suited and commonly used. The first is "remote" access to enterprise networks. The second is controlled access to a service provider's network. In this model, there is a client attempting to access the network and a server authenticating the client and enforcing access control to the enterprise or the service provider's network. The extensible authentication protocol (EAP) [7] allows most flexibility for client authentication. The IKEv2 [2] protocol enables the use of IPsec for access control with EAP for client authentication. The catch here is that access control is only effective with a proper security policy database. The need for security policy enforcement is identified in other specifications employing controlled access to networks: the IEEE 802.1X

specification identifies "port control" as an essential part of enforcing access control. In brief, port control and security policy databases specify which traffic, e.g., EAP traffic in case of 802.1X, and key management traffic in case of IPsec, can bypass security encapsulation -- which provides a guarantee that the entity that established the SA is in fact sending the traffic -- requirements.

IPsec is also used for secure communication between end hosts. Transport mode is typically used for either secure unicast or multicast communication. IPsec encapsulation is also used for access control enforcement of data being broadcast or multicast.

In the rest of this document, we explain what IPsec does, make a case for using IPsec as a secure channel or an access control enforcement protocol and finally provide guidance on how to use IPsec.

4. What IPsec provides

IPsec SAs may be established manually or by way of a key management protocol: ESPv3 [3] or AHv3 [4] unicast SAs are established using IKEv2 [2] and Group SAs are established using GDOI [8] or GSAKMP. Manual keying has some limitations and must be employed with care. However, it may be better to use manual keyed IPsec SAs than inventing a new security encapsulation protocol.

Two different types of IPsec encapsulations have been specified in [5]: with the first, the Encapsulating Security Payload (ESP), a number of security properties can be provided, including integrity protection, confidentiality, replay protection, and traffic flow confidentiality. The second type of encapsulation, Authentication Header (AH), provides integrity and replay protection, and unlike ESP affords integrity protection of IP headers.

IPsec can be used in transport mode or a tunnel mode: transport mode is employed when two endpoints require ESP or AH protection for next layer protocol headers and the payload. Tunnel mode is employed between a host and a security gateway or between security gateways by encapsulating the entire IP packet and introducing an IP header for routing the packet to the appropriate IPsec entity on route to the final destination.

IPsec, especially when used to enforce access control, is associated with a security policy database (SPD) that dictates the types of traffic that needs what kind of IPsec protection and those that do not need any protection. When specifications require the use of IPsec, it is often useful to provide guidelines on SPD contents as well for proper use of the protections afforded by IPsec.

5. Why use IPsec and where to use IPsec?

6. How to use IPsec to establish secure channel(s) between network entities?

IPsec may be used as the security encapsulation protocol between two or more network infrastructure entities in many cases, including

- to protect routing protocol messages, for instance, OSPF, BGP
- to protect AAA messages between a AAA client and a server, typically in a hop-by-hop fashion
- to protect context transfer messages between two edge entities in a service provider's network
- to provide a blanket secure channel between two network entities.
- more ...

6.1. Identify the Requirements and Constraints

The first step of course is to take stock of the constraints and the requirements. The following questionnaire might help; note however that each situation is unique and may have requirements and constraints that may not be listed here.

6.1.1. Requirements and Constraints on the use of IPsec encapsulation

First we examine the requirements on the security encapsulation itself.

- Type of protection --
  - Specifically, is confidentiality a requirement for all traffic?
  - Would integrity protection alone be sufficient? Note that it is plausible to use ESP with NULL encryption, effectively providing integrity protection alone.
  - Does the outermost IP header need integrity protection? Note that AH mode of protection of headers implies that modification of headers en route is prohibited.
  - Is replay protection required? Note that IPsec specifications mandate the inclusion of a sequence number in the header. Turning off sequence number verification at the receiver only

saves the overhead of maintenance of a replay window and some associated packet processing. However, it is plausible that replay protection is provided through other means, breaks other aspects of higher layer protocols or simply not needed.

+ If replay protection is being employed, is an extended sequence number (ESN) required? ESN is typically needed for high data rate communication to avoid frequent rekeying. IPsecv3 assumes automatic use of ESN, unless it is explicitly turned off via a key management protocol.

* Is traffic flow confidentiality a requirement? When using ESP with non-NULL encryption, IPsec allows the sender to provide traffic flow confidentiality (TFC). TFC protects from entities observing the traffic over the air or a wire from making intelligent assessments about the contents of the traffic, based on the length of IP packets. TFC padding is in addition to the encryption related padding, and must be signaled.

o Granularity of protection or number of SAs between the same entities --

* Does all traffic between the network entities need protection? If so, is the protection required the same in all cases?

o Origin and destination of traffic being protection or selection of tunnel vs transport mode --

* Is the traffic originating and destined for the IPsec endpoints? This might imply the use of transport mode IPsec.

* Is the traffic originating or destined for entities beyond/ behind the IPsec endpoints? This generally implies the use of tunnel mode IPsec. However, if traffic were already in-IP tunneled it may be plausible to use transport mode IPsec. Care must be taken however in employing transport in this way as the SPD capabilities may be limited as described in Page 13 of [5]

o Unicast or Group SAs --

o Security Policy Database (SPD) and associated enforcement --

The next step is to identify any constraints in specifying the details of the security encapsulation needed.

o Is there a constraint that requires the design to turn off integrity protection? Note that if confidentiality is needed, integrity protection is automatically assumed to be needed in most

cases. The following process may help analyze whether an exception of turning off integrity protection is even necessary:

* Is overhead the reason to not use integrity protection?

* Would the use of Counter mode encryption help alleviate the per-packet overhead concerns? With CBC mode encryption, an IV of length 16 octets is required. With counter mode, a counter of length of 4 octets needs to be included in each packet. The counter serves as part of the per-packet IV as well as the sequence number for replay protection.

* Was MAC truncation considered? Use of an 8-octet MAC is well within the recommendation of AES-CMAC specification. An even shorter MAC, as short as 4 octets is better than no integrity protection at all.

o

6.1.2. Constraints and Requirements associated with Selection of Key Management Protocol

The second part of the exercise is to identify the requirements and constraints associated with key management.

o Key management protocol -- Is a key management protocol required? If so, which one?

  * The choice of key management protocol depends very much on whether unicast or group SAs are to be established. For unicast SA establishment, IKEv2 is the only key management protocol specified and for group IPsecv3 SA establishment, GKDP is the only key management protocol specified at the time of this writing.

o Entity authentication -- If a key management protocol is used, the first step is to figure out how the IPsec endpoints are authenticated to each other. In the use case under discussion, the two endpoints are infrastructure entities: in this case certificate based authentication or PSK-based authentication are two viable choices. Requirements analysis would need to determine if one of the options is better than the other.

o Security policy database reconciliation or Traffic selector negotiation --

o

The next step as in case of investigating the use of the security encapsulation is to investigate any constraints.

- Manual keying is definitely an option to establish IPsecv3 SAs. However manual keying has several inherent limitations. It is important to investigate whether the constraints forcing the use of manual keying are weighed against the following limitations of manual keying:
  - Rekeying is also manual and if manually keyed IPsec SAs are used to protect high data rate flows, key reuse might occur. Note that key reuse may result in compromising the protections afforded by IPsec.
  - Algorithm agility is not supported.
  - Replay protection is not supported.

7. Key management for IPsec:IKEv2

7.1. IKEv2 usage guidelines

7.2. Guidelines for using Traffic Selectors

7.3. IKEv2 support for network access control: IKEv2-EAP

8. Group Key management for IPsec

9. IPsec and mobility

9.1. IKEv2 support for mobility

9.2. MOBIKE applicability

10. Security Considerations

11. IANA Considerations

12. Acknowledgments

13. References

13.1. Normative References

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

[2] Kaufman, C., "Internet Key Exchange (IKEv2) Protocol", RFC 4306, December 2005.

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

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

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

13.2. Informative References

[6] Bellovin, S., "Guidelines for Mandating the Use of IPsec", draft-bellovin-useipsec-05 (work in progress), August 2006.

[7] Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J., and H. Levkowetz, "Extensible Authentication Protocol (EAP)", RFC 3748, June 2004.

[8] Baugher, M., Weis, B., Hardjono, T., and H. Harney, "The Group Domain of Interpretation", RFC 3547, July 2003.

[9] Housley, R. and B. Aboba, "Guidance for AAA Key Management", draft-housley-aaa-key-mgmt-04 (work in progress), October 2006.

[10] Aboba, B., "Extensible Authentication Protocol (EAP) Key Management Framework", draft-ietf-eap-keying-14 (work in progress), June 2006.

Authors' Addresses

Lakshminath Dondeti (editor)
QUALCOMM, Inc.
5775 Morehouse Dr
San Diego, CA
USA

Phone: +1 858-845-1267
Email: ldondeti@qualcomm.com

Vidya Narayanan (editor)
QUALCOMM, Inc.
5775 Morehouse Dr
San Diego, CA
USA

Phone: +1 858-845-2483
Email: vidyan@qualcomm.com

Full Copyright Statement

Intellectual Property

Acknowledgment

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).