Internet Engineering Task Force
INTERNET-DRAFT
draft-mostafa-qesp-00.txt
Date: December 2, 2009
Expires: June, 2010

M. MOSTAFA
A. ABOU EL KALAM
C. FRABOUL
INPT-ENSEEIHT, IRIT-CNRS

QoS-friendly Encapsulating Security Payload (Q-ESP)

Status of this Memo

Copyright Notice

Abstract

This document describes a new IPSec protocol called QoS-friendly

Encapsulating Security Payload (Q-ESP). Q-ESP provides confidentiality, data origin authentication, anti-reply, connection less integrity, and facilitates QoS active admission control. The currently implemented IPSec Encapsulating Security Payload (ESP) protocol is not QoS friendly as it encrypts the upper layer transmission protocol and prevents network control devices such as routers and switches from utilizing this information in performing classification appropriately. In this document we provide the specification of Q-ESP which gives the same security services provided by ESP, in addition to strong source and destination addresses authentication and its ability to facilitate QoS classification.

Table of Contents

1. Introduction

The Internet has become essential for information exchange. Various activities are carried out via the Internet: between companies (B2B), among businesses and consumers (B2C), or between individuals who create their own virtual communities (e.g., P2P). This clearly causes a huge demand for the network bandwidth. Moreover, many real-time applications such as video conferencing and Voice over Internet Protocol (VoIP) have been developed. These types of traffic-demanding applications suffer greatly from congestion and delay. Thus, there is a great need to find methods and mechanisms to manipulate traffic more efficiently according to their needs. Quality of service (QoS) has emerged to deal with this kind of problem. Basically, it refers to the nature of packet delivery service provided, as described by parameters such as bandwidth, delay, jitter, and packet loss [Shenker and Wroclawski, 1997]. The way of classifying traffic and providing QoS levels defines different QoS architectures [Nguyen, 2003]. Mainly, we distinguish two standard QoS architectures: Integrated service [Braden, Clark and Shenker, 1994] and Differentiated service [Blake, Black, Carlson, Davies, Wang and Weiss, 1998].

Actually, in the QoS field, the "Class of Service"concept divides the network traffic into different classes and provides a class-dependent service to each packet (depending on which class it belongs to).
To classify packets, each packet is assigned a priority value. The latter is stored in the "Type of Service" (ToS)[Postel, 1981] field in the IPv4 header (also called "Traffic Class" in IPv6) [Deering and Hinden, 1998]. In the differentiated service architecture, this priority value is called Differentiated service code point (DSCP) [Nichols, Blake,

Baker and Black, 1998].However, it is obvious that allowing the sending device to classify traffic or to set traffic priorities may be subject to threats, as the sender may classify his traffic in a way that gives him upper priorities. This is clearly the disadvantage of what is called passive admission control. Conversely, service providers perform active admission control by allowing edge routers (neither users nor the sending devices) to inspect the incoming traffic and classify it.
Note that in both architectures (the differentiated service and integrated service), the packet classifier component inspects incoming packets and classifies them. As the classifier inspects multiple fields in the packet, it is called Multi-Field (MF) classifier [Borg, Savanberg and Schelen, 1999].

Actually, the fields needed to be inspected belong to different network layer headers [Gupta, 2000]:

_Transport Layer Protocol Header: the MF packet classifier inspects two fields of the transport layer protocol (TCP/UDP) header, the source and destination port numbers; these fields naturally help to identify the applications running over TCP/UDP.

_Network Layer Protocol Header: three fields are inspected at this layer, the source host IP address that helps to identify the sending host, the destination host IP address, which helps to identify the end-system receiving the data, and the protocol identifier that is used to identify the transport-layer protocol in use.

The previously mentioned five fields are used to define the traffic flow [Huston, 2000]. However, even if these fields are required for QoS processing, some of them are unfortunately hidden (encrypted) when using security protocols such as IPSec [Kent and Atkinson, 1998] ESP [Kent, 2005].

To solve this problem, we propose a new security protocol the "QoS-friendly Encapsulated Security Payload (Q-ESP)". Not only Q-ESP provides stronger security protection but also supports QoS active admission control.

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 [Bradner, 1997].

3 Q-ESP: QoS-friendly Encapsulating Security Payload

3.1. QoS friendly Encapsulating Security Payload(Q-ESP) packet format

The major aim of the Q-ESP protocol is to construct packets that are QoS controllable according to active admission control.

In addition to security services provided by the IPSec ESP (i.e. Data origin authentication, Anti-reply integrity, connectionless integrity and confidentiality), Q-ESP supports QoS by providing the necessary and sufficient information for the controlling devices to enable them performing active admission control.

Besides that, Q-ESP prevents replay attacks. In fact, while the anti-reply function is optional in ESP and AH [Kent and Atkinson, 1998], it is mandatory in Q-ESP. In addition, while authentication is optional in ESP, it is mandatory in Q-ESP as it prevents against attacks that form malicious packet from valid IP and ESP headers but with invalid payload (which will be discarded later after doing the most resource intensive process of decryption). Moreover, Q-ESP authentication provides data origin authentication (as it covers the source and destination addresses fields of the outer IP-header).

Figure 1 depicts the structures of Q-ESP in IP versions 4 and 6. An Q-ESP packet contains eight additional octets. Like ESP, the structure of Q-ESP is composed of the header, the payload, the trailer, and the authentication data area. All the fields of the Q-ESP packet are described below.

```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                              IP Header                           |
~                                                                  ~
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-----
|               IP header       Source IP Address                  |  ^
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-|  |
|               IP header  Destination IP Address                  |  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-|  |
|                                                                  |  |
0               1               2               3                  |  |
0 1 2 3 4 5 6 7 0 1 2 3 4 5 6 7 0 1 2 3 4 5 6 7 0 1 2 3 4 5 6 7 |  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-| Authent-
|               Source Port      |      Destination Port           |  ication
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-| Coverage
|       TLP      |                         Reserved                |  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-|  |
|              Security Parameters Index (SPI)                     |  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-|  |
|                      Sequence Number                             |  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-|  | -------
|                    Payload Data* (variable)                      |  |    ^
~                                                                  ~  |    |
|                                                                  |  | Confid-
+                 -+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+ |  | entiality
|                 |     Padding (0-255 bytes)                      |  | Coverage
+-+-+-+-+-+-+-+-+-+               +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-|  |    |
|                                 |  Pad Length   | Next Header|  v    v
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-|-----------
|                      Authentication Data (variable)              |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 1: Q-ESP packet format

3.1.1 The Q-ESP header

The Q-ESP header contains a Security Parameters Index and a Sequence Number.

In addition, to cope with QoS requirements, we copy the first two fields (source and destination ports) of the upper layer transfer protocols and place them in clear (without encryption) in the Q-ESP header. Also, the value of the transport layer protocol is recorded in the TLP field; This clearly allows MF packet classifier to perform efficient packet classification. In this respect, the Q-ESP header includes the following six fields:

3.1.1.1 Source Port

This is a 16-bit fixed-length field; it contains the first field of the upper layer transport protocol (TCP/UDP) source port number; this field is needed to be in clear to enable network edge routers to check traffic and set priorities.

3.1.1.2 Destination Port

This is also a 16-bit fixed-length field; it contains the second field of the upper layer transport protocol (TCP/UDP) destination Port number; as the source port, this field is also needed to be in clear to enable network edge routers to check traffics and set priorities.

3.1.1.3 Transmission Layer Protocol (TLP)

This is an 8-bit fixed-length field that indicates the protocol of the transport layer.

The previously mentioned three fields (Source Port, Destination Port and TLP) are used with IP source and destination addresses to identify traffic flow.

3.1.1.4 Reserved

This is a 24-bit fixed-length field that is not used (reserved for future uses) and must be set to zero.

3.1.1.5 Security Parameters Index

This is an arbitrary 32-bit fixed length identifier that in combination with the destination address and security protocol (Q-ESP) uniquely identifies the security association (SA) in use.

3.1.1.6 Sequence Number

This is an unsigned 32 bit field. It is a monotonically increasing ID that is used to detect replay attacks. This value is authenticated, so that malicious or accidental modifications could be detected.

3.1.2 The Q-ESP payload

The payload encrypts the upper layer transport protocol and its payload data in transport mode, while in tunnel mode it encrypts the entire original IP packet including its header.

3.1.3 The Q-ESP trailer

The Q-ESP trailer includes the Padding, the pad length field and the Next Header field.

3.1.3.1 Padding

This is provided to allow block-oriented encryption algorithms area for multiples of their block size.

3.1.3.2 Pad length

This is an 8-bit fixed-length field that indicates the length of the included pad.

3.1.3.3 Next Header

This is a mandatory, 8-bit fixed-length field that points backward to refer to the type of the protocol (IP, TCP, UDP, etc.) in the encrypted payload.

3.1.4. Authentication data area

It is a variable length area that is used to store the Integrity check value (ICV). The Integrity Check Value (ICV) is calculated over the Q-ESP headers and the Payload. In Q-ESP, to inherit the capability of AH, we also apply the authentication algorithm over the source IP address and destination IP address fields of the IP header.
However, unlike AH, we think that authenticating the rest of the IP header fields is meaningless as they will be used before the packet reaches the IPSec layer (i.e. before verifying their integrity); therefore, any change in their values will not affect the IPSec processing.
Besides, in Q-ESP, both authentication and encryption are mandatory.
Actually,authentication helps to prevent DoS attacks [Nikov, 2006].
Moreover,implementing authentication with encryption provides in depth-defense if the encryption secret key is corrupted; in fact even if the attacker succeeds in reading the content of the payload, he will not be able to alter its content.

3.2. Q-ESP Mode of operations

Q-ESP must be supported in both transport and tunnel mode. We now Show the Q-ESP transport mode for a typical IPv4 packet.

IP PACKET BEFORE APPLYING Q-ESP

```
                            ----------------------------
                            |  IP  |  TCP  |    Data   |
                            ----------------------------
```

AFTER APPLYING Q-ESP IN TRANSPORT MODE

```
                 <-----Q-ESP header------>
  -------------------------------------------------------------------
  |  IP  ~ Src|Dst |Src |Dst |TLP| |SPI|Seq|TCP|Data| Q-ESP | Q-ESP |
  |header| IP@|IP@ |Port|Port|   | |   | # |   |    |trailer| Auth  |
  -------------------------------------------------------------------
                               <->       <---Encrypted---->
                            Reserved
         <---------------------Authenticated---------------->
```

Figure 2: Q-ESP in transport mode

We now show the Q-ESP tunnel mode for a typical Ipv4 packet.

AFTER APPLYING Q-ESP IN TUNNEL MODE

```
                    <-----Q-ESP header------>
  ----------------------------------------------------------------------------
  |Outer IP ~ Src|Dst |Src |Dst |TLP| |SPI|Seq|inner|TCP|Data| Q-ESP | Q-ESP |
  | header  | IP@|IP@ |Port|Port|   | |   | # |  IP |   |    |trailer|  Auth |
  ----------------------------------------------------------------------------
                                  <->       <-------Encrypted------>
                               Reserved
             <---------------------Authenticated--------------------->
```

Figure 3: Q-ESP in tunnel mode

In both the transport and the tunnel mode, the Protocol field of the outer IP header should have a new value indicating that the next protocol is Q-ESP.
Thus, we should assign a new protocol identifier to Q-ESP protocol.

3.3 Q-ESP Processing

The same processing steps performed for ESP are performed for Q-ESP, however there are some differences. In this draft, we only mention these differences.

3.3.1. Outbound processing

In the outbound processing, the differences between Q-ESP and ESP processing are concerned with Q-ESP header construction and Integrity Check Value (ICV) Calculation.

3.3.1.1: Constructing the Q-ESP header

To construct Q-ESP header, we will copy the first two fields (source and destination ports) of the upper layer header protocol (TCP/UDP) at the beginning of Q-ESP header. Then, we will put the protocol number of the upper layer transmission protocol in the TLP field. Next we set the value of the reserved field to zero. After that, we place the security parameter index (SPI) obtained from the SA in its field (to tell the receiver how to react with this packet); and finally, we increment the sequence number and place it at the last field of the header. In this respect, the Q-ESP header will contain the following fields: source port number, destination port number, TLP, reserved, security parameter index (SPI) and sequence number.

3.3.1.2: Computing the authentication value

Recall that Q-ESP must authenticate the source and the destination IP addresses, to achieve this goal:
We use the standard authentication algorithm (specified by the SA) such as SHA-1 and its associated key to compute the integrity check value according to equation 1. Then, we store the computed ICV value in the Q-ESP authentication data area.

$$ICV = H(MH \,||\, P \,||\, Src\ IP \,||\, Dst\ IP,\ KA) \quad (1)$$

Where, ICV is the integrity check value, H is the keyed-authentication algorithm, MH is the Q-ESP header, P is the Q-ESP encrypted payload, and the "Src IP" and "Dst IP" are the the source IP address and the destination IP address fields of the external IP header respectively, KA is the authentication key, and || is the concatenation symbol.

3.3.2. Inbound processing

In the inbound processing, the differences between Q-ESP and ESP processing exist in sequence number checking and Integrity Check Value (ICV) calculation.

3.3.2.1: Checking sequence number

In Q-ESP, this step is mandatory to prevent replay attacks. If the sequence number of the packet is valid (i.e., it is not a duplicate and is not to the right of the sequence number window contained in the SA), proceed to the next step, otherwise the packet is dropped.

It is important to note that the window must not be advanced until the packet that would cause its advancement has been authenticated. Otherwise, an attacker can generate bogus packets with large sequence numbers that would move the window outside the range of valid sequence numbers and causes valid packets dropping [Dowaswamy and Harkins, 2003].

3.3.2.2: Verifying the authentication value

Again, the difference here is in the authentication coverage; use the standard authentication algorithm specified by the SA such as SHA-1 and its associated key to re-compute the integrity check value (ICV)(using equation 1) for the Q-EPS header and its payload, the protocol identifier, the source IP address, and the destination IP address fields of the external IP header. Then, the result is compared with the value stored in the Authentication data area; if they are equal, proceed to the next step, if not, drop the packet.

Actually, we have modified the IPSec kernel implementation of NetBSD version 5 to implement Q-ESP protocol [Mostafa, Abou El Kalam and Fraboul, 2008; 2009; 2010]. We tested our implementation and compared its performance with ESP protocol. We built two different testbeds and used different scenarios. The test results show that, in best effort environment both ESP and Q-ESP have almost the same throughput for the same packet size; While in QoS managed environment, Q-ESP has the advantage of allowing network control devices to perform QoS classification adequately.

4. QoS classification batch

In order to deploy Q-ESP protocol, a slight software batch is needed to be implemented and installed in the currently used network control devices (such as routes) that perform QoS classification. The goal of this batch is to tell classification algorithm where to find the needed fields to perform classification. Actually, the position of these fields differs from normal IP packet to Q-ESP protected packet. While the positions of IP source and destination addresses are not changed, the position of source and destination port numbers are moved to the beginning of the Q-ESP header. In addition, the transport layer transfer protocol identifier is placed in the TLP field in the Q-ESP header.

5. Possible applications of Q-ESP

Generally speaking, Q-ESP can be used, instead of ESP, in all applications that need both security and QoS such as VoIP, VoD, satellite data, etc. Moreover, Q-ESP can be used on top of MPLS to guarantee the confidentiality of client data (as regards ISPs) while ensuring the other security and QoS services.

Basically, Q-ESP has the added benefits of facilitating QoS classification, allowing active admission control and separating security administrative tasks from QoS administrative tasks.
Now, we could control the security of our data and let internet service providers (ISPs) mange only QoS aspects. A Q-ESP packet can be handled within different types of QoS domains. It can enter an integrated service domain and exit it to enter another differentiated service or MPLS domain. The needed information to perform classification is available and the security of the packet is guaranteed. Clearly, the priority value of the packet could be changed from domain to another depending on the QoS policy defined in each domain.

Current solutions must classify packets and set each packet' priority before encrypting it with ESP. Using Q-ESP, we encrypt our packets first before sending it to ISPs QoS managed domains; in this way, the packets could be easily classified and handled in all domains without any fear regarding its security.

```
Clinet1       Integrated       Differentiated                  Clinet2
Security --->  service  ----->  service   ----->  MPLS  -----> Security
Gateway         domain           domain          domain        Gateway
```

In addition, if a packet filtering firewall is installed before the VPN module (which is common architecture), the packet filtering firewall could easily manipulate the packet as the needed fields to perform filtering policy is available. In this way we could minimize the possibility of DoS attack to the VPN module, as unconcerned packets will be filtered by the firewall.

References

Blake, S., Black, D. Carlson, M. Davies, E. Wang, Z. and Weiss, W. (1998) 'An Architecture for Differentiated Services', RFC 2475.

Borg, N., Savanberg, E. and Schelen, O. (1999) 'Efficient Multi-Field Packet Classification for QoS Purposes', International Workshop on Quality of Service, p. 109-118.

Braden, R., Clark, D. and Shenker, S. (1994) 'Integrated Services in the Internet Architecture: an Overview', RFC 1633.

Bradner, S. (1997) Key words for use in RFCs to Indicate Requirement Levels. RFC 2119.

Deering, S., Hinden, R. (1998) Internet Protocol, Version 6 (IPv6) Specification , RFC 2460.

Dowaswamy, N. and Harkins, D. (2003) IPSec, 'The New Security Standard for the Internet, Intranets, and Virtual Private Networks', Prentice Hall PTR.

Ferguson, N., Schneier, B. (2003) A Cryptographic Evaluation of IPsec, Technical report.

Gupta, P. (2000) 'Algorithms for routing lookups and packet classification,'. PhD. Thesis, Stanford University, Stanford, CA.

Huston, G. (2000) 'Next Steps for the IP QoS Architecture', RFC 2990.

Kent, S. and Atkinson, R. (1998) 'IP authentication header', RFC 2402.

Kent, S. (2005) 'IP Encapsulating security Payload (ESP)', RFC 4303.

Kent, S. and Atkinson, R. (1998) 'Security architecture for the Internet protocol', RFC 2401.

Mostafa, M., Abou El Kalam, A., Fraboul, C. (2009) 'Q-ESP: a QoS-compliant Security Protocol to enrich IPSec Framework'. IFIP / IEEE, The Third International Conference on New Technologies, Mobility and Security, Cairo, Egypt, 20-23 December 2009.

Mostafa, M., Abou El Kalam, A., Fraboul, C. (2010) 'A New Protocol for Security and QoS in IP Networks',to appear in Int. J. Information and Computer Security, Inderscience Publishers, 15 PP.

Mostafa, M., Abou El Kalam, A., Fraboul, C. (2008) 'EESP: A Security Protocol that Supports QoS Management',IEEE International Conference on Risks and Security of Internet and Systems, Tunisie, 28-30 october 2008.

Nichols, K., Blake, S. Baker, F. and Black, D. (1998) 'Definition of the Differentiated Services Field in the IPv4 and IPv6 Headers', RFC 2474.

Nikov, V. (2006) 'A DoS Attack Against the Integrity-Less ESP (IPSEC)', International Conference on Security and Cryptograph, p. 192-199

Postel, J. (1981) 'Internet Protocol Darpa Internet Program Protocol Specification', RFC 791.

Shenker, S., Wroclawski, J. (1997) 'Network Element Service Specification Template', RFC 2216.

Thi Mai Trang Nguyen T.M. (2003), 'Service Level Negotiation for Heterogeneous IP-Based Networks,'. PhD. Thesis, ENST, Paris, France.

Authors' Addresses

Mahmoud MOSTAFA, Anas ABOU EL KALAM, Christian FRABOUL
ENSEEIHT - IRIT
2 rue Charles Camichel
B.P. 7122
F-31071 TOULOUSE Cedex 7
France
Voice : +33 5 61 58 80 12
fax : +33 5 61 58 83 06
E-mail: {firstname.lastname}@enseeiht.fr