MACSec Sample Packets

Guy Hutchison

July 14, 2006

1 Overview

While golden vectors are available for AES and GCM, there is presently no equivalent for a complete, MACSec-processed packet. This document presents a number of packet pairs, consisting of an unencrypted Ethernet packet and a transformed packet after MACSec processing.

This paper describes 8 different packet pairs, representing a mix of interesting cases. Four different packet sizes were chosen, two representing common sizes of internet packets, and two representing corner cases for GCM padding length. As MACSec lives above the MAC in the 802 stack, all packet sizes in this paper are packet sizes prior to the addition of the 32-bit CRC.

The two internet packet sizes are 54 bytes and 60 bytes, which are two most common representations of a TCP/IP SYN packet. A TCP SYN is 40 bytes in size, plus 14 bytes of MAC DA+SA+Ethertype. The packet may or may not be padded to 60 bytes to meet minimum Ethernet frame length prior to MACSec processing.

The remaining two packet sizes represent the two ”corners” of the GCM padding algorithm on encrypted packets. A 61 byte packet, when encrypted, has a 49 byte payload, which results in the maximum 15 bytes of padding for ICV calculation. A 75 byte packet has a 63 byte payload, resulting in 1 byte of padding. The zero-byte padding case is covered by the 60-byte packet, above.

For each of these four length cases, the resulting authenticated-only and authenticated-and-encrypted (confidentiality) packets are presented, along with the plaintext packets which they were created from and their associated encryption parameters.

2 54-Byte Packet

This packet size represents the size of a TCP/IP SYN packet, without Ethernet padding. The first pair of packets is authenticate- only and the second pair auth and encrypt.

2.1 Before MACSec Processing

MAC DA	d609b1f05663
MAC SA	7a0d46df998d

Packet Data (Length=54)

```
d6 09 b1 f0 56 63 7a 0d 46 df 99 8d 08 00 0f 10
11 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f 20
21 22 23 24 25 26 27 28 29 2a 2b 2c 2d 2e 2f 30
31 32 33 34 00 01
```

2.2 After MACSec Processing

Key	ad7a2bd03eac835a6f620fdcb506b345
SCI	12153524c0895e81
TCI	22
PN	b2c28465
MAC DA	d609b1f05663
MAC SA	7a0d46df998d

Packet Data (Length=86)

```
d6 09 b1 f0 56 63 7a 0d 46 df 99 8d 88 e5 22 2a
b2 c2 84 65 12 15 35 24 c0 89 5e 81 08 00 0f 10
11 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f 20
21 22 23 24 25 26 27 28 29 2a 2b 2c 2d 2e 2f 30
31 32 33 34 00 01 f0 94 78 a9 b0 90 07 d0 6f 46
e9 b6 a1 da 25 dd
```

2.3 Before MACSec Processing

MAC DA	d609b1f05663
MAC SA	7a0d46df998d

Packet Data (Length=60)

```
d6 09 b1 f0 56 63 7a 0d 46 df 99 8d 08 00 0f 10
11 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f 20
21 22 23 24 25 26 27 28 29 2a 2b 2c 2d 2e 2f 30
31 32 33 34 35 36 37 38 39 3a 00 02
```

2.4 After MACSec Processing

Key	ad7a2bd03eac835a6f620fdcb506b345
SCI	12153524c0895e81
TCI	2e
PN	b2c28465
MAC DA	d609b1f05663
MAC SA	7a0d46df998d

Packet Data (Length=92)

```
d6 09 b1 f0 56 63 7a 0d 46 df 99 8d 88 e5 2e 00
b2 c2 84 65 12 15 35 24 c0 89 5e 81 70 1a fa 1c
c0 39 c0 d7 65 12 8a 66 5d ab 69 24 38 99 bf 73
18 cc dc 81 c9 93 1d a1 7f be 8e dd 7d 17 cb 8b
4c 26 fc 81 e3 28 4f 2b 7f ba 71 3d 4f 8d 55 e7
d3 f0 6f d5 a1 3c 0c 29 b9 d5 b8 80
```

3 60-Byte Packet

This packet size represents a generic minimum-size Ethernet frame, such as a padded SYN packet.

3.1 Before MACSec Processing

MAC DA	e20106d7cd0d
MAC SA	f0761e8dcd3d

Packet Data (Length=60)

```
e2 01 06 d7 cd 0d f0 76 1e 8d cd 3d 08 00 0f 10
11 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f 20
21 22 23 24 25 26 27 28 29 2a 2b 2c 2d 2e 2f 30
31 32 33 34 35 36 37 38 39 3a 00 03
```

3.2 After MACSec Processing

Key	071b113b0ca743fecccf3d051f737382
SCI	f0761e8dcd3d0001
TCI	40
PN	76d457ed
MAC DA	e20106d7cd0d
MAC SA	f0761e8dcd3d

Packet Data (Length=84)

```
e2 01 06 d7 cd 0d f0 76 1e 8d cd 3d 88 e5 40 00
76 d4 57 ed 08 00 0f 10 11 12 13 14 15 16 17 18
19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25 26 27 28
29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35 36 37 38
39 3a 00 03 0c 01 7b c7 3b 22 7d fc c9 ba fa 1c
41 ac c3 53
```

3.3 Before MACSec Processing

MAC DA	e20106d7cd0d
MAC SA	f0761e8dcd3d

Packet Data (Length=54)

```
e2 01 06 d7 cd 0d f0 76 1e 8d cd 3d 08 00 0f 10
11 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f 20
21 22 23 24 25 26 27 28 29 2a 2b 2c 2d 2e 2f 30
31 32 33 34 00 04
```

3.4 After MACSec Processing

Key	071b113b0ca743fecccf3d051f737382
SCI	f0761e8dcd3d0001
TCI	4c
PN	76d457ed
MAC DA	e20106d7cd0d
MAC SA	f0761e8dcd3d

Packet Data (Length=78)

```
e2 01 06 d7 cd 0d f0 76 1e 8d cd 3d 88 e5 4c 2a
76 d4 57 ed 13 b4 c7 2b 38 9d c5 01 8e 72 a1 71
dd 85 a5 d3 75 22 74 d3 a0 19 fb ca ed 09 a4 25
cd 9b 2e 1c 9b 72 ee e7 c9 de 7d 52 b3 f3 d6 a5
28 4f 4a 6d 3f e2 2a 5d 6c 2b 96 04 94 c3
```

4 One Byte Remainder

This packet size results in a packet with a single byte remainder for the ICV calcuation, and hence the maximum amount of ICV padding (15 bytes). For the authenticate-only case, a 65 byte packet creates this result, and for auth and encrypt, a 61 byte packet is used.

4.1 Before MACSec Processing

MAC DA	84c5d513d2aa
MAC SA	f6e5bbd27277

Packet Data (Length=65)

```
84 c5 d5 13 d2 aa f6 e5 bb d2 72 77 08 00 0f 10
11 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f 20
21 22 23 24 25 26 27 28 29 2a 2b 2c 2d 2e 2f 30
31 32 33 34 35 36 37 38 39 3a 3b 3c 3d 3e 3f 00
05
```

4.2 After MACSec Processing

Key	013fe00b5f11be7f866d0cbbc55a7a90
SCI	7cfde9f9e33724c6
TCI	23
PN	8932d612
MAC DA	84c5d513d2aa
MAC SA	f6e5bbd27277

Packet Data (Length=97)

```
84 c5 d5 13 d2 aa f6 e5 bb d2 72 77 88 e5 23 00
89 32 d6 12 7c fd e9 f9 e3 37 24 c6 08 00 0f 10
11 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f 20
21 22 23 24 25 26 27 28 29 2a 2b 2c 2d 2e 2f 30
31 32 33 34 35 36 37 38 39 3a 3b 3c 3d 3e 3f 00
05 21 78 67 e5 0c 2d ad 74 c2 8c 3b 50 ab df 69
5a
```

4.3 Before MACSec Processing

MAC DA	84c5d513d2aa
MAC SA	f6e5bbd27277

Packet Data (Length=61)

```
84 c5 d5 13 d2 aa f6 e5 bb d2 72 77 08 00 0f 10
11 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f 20
21 22 23 24 25 26 27 28 29 2a 2b 2c 2d 2e 2f 30
31 32 33 34 35 36 37 38 39 3a 3b 00 06
```

4.4 After MACSec Processing

Key	013fe00b5f11be7f866d0cbbc55a7a90
SCI	7cfde9f9e33724c6
TCI	2f
PN	8932d612
MAC DA	84c5d513d2aa
MAC SA	f6e5bbd27277

Packet Data (Length=93)

```
84 c5 d5 13 d2 aa f6 e5 bb d2 72 77 88 e5 2f 00
89 32 d6 12 7c fd e9 f9 e3 37 24 c6 3a 4d e6 fa
32 19 10 14 db b3 03 d9 2e e3 a9 e8 a1 b5 99 c1
4d 22 fb 08 00 96 e1 38 11 81 6a 3c 9c 9b cf 7c
1b 9b 96 da 80 92 04 e2 9d 0e 2a 76 42 bf d3 10
a4 83 7c 81 6c cf a5 ac 23 ab 00 39 88
```

5 Fifteen Byte Remainder

This packet size results in a packet with the maximum remainder (15 bytes), and therefore minimum non-zero amount of ICV padding (1 byte). The auth-only packet is 79 bytes long and the auth-and-encrypt packet is 75 bytes.

5.1 Before MACSec Processing

MAC DA	68f2e77696ce
MAC SA	7ae8e2ca4ec5

Packet Data (Length=79)

```
68 f2 e7 76 96 ce 7a e8 e2 ca 4e c5 08 00 0f 10
11 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f 20
21 22 23 24 25 26 27 28 29 2a 2b 2c 2d 2e 2f 30
31 32 33 34 35 36 37 38 39 3a 3b 3c 3d 3e 3f 40
41 42 43 44 45 46 47 48 49 4a 4b 4c 4d 00 07
```

5.2 After MACSec Processing

Key	88ee087fd95da9fbf6725aa9d757b0cd
SCI	7ae8e2ca4ec50001
TCI	41
PN	2e58495c
MAC DA	68f2e77696ce
MAC SA	7ae8e2ca4ec5

Packet Data (Length=103)

```
68 f2 e7 76 96 ce 7a e8 e2 ca 4e c5 88 e5 41 00
2e 58 49 5c 08 00 0f 10 11 12 13 14 15 16 17 18
19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25 26 27 28
29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35 36 37 38
39 3a 3b 3c 3d 3e 3f 40 41 42 43 44 45 46 47 48
49 4a 4b 4c 4d 00 07 07 92 2b 8e bc f1 0b b2 29
75 88 ca 4c 61 45 23
```

5.3 Before MACSec Processing

MAC DA	68f2e77696ce
MAC SA	7ae8e2ca4ec5

Packet Data (Length=75)

```
68 f2 e7 76 96 ce 7a e8 e2 ca 4e c5 08 00 0f 10
11 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f 20
21 22 23 24 25 26 27 28 29 2a 2b 2c 2d 2e 2f 30
31 32 33 34 35 36 37 38 39 3a 3b 3c 3d 3e 3f 40
41 42 43 44 45 46 47 48 49 00 08
```

5.4 After MACSec Processing

Key	88ee087fd95da9fbf6725aa9d757b0cd
SCI	7ae8e2ca4ec50001
TCI	4d
PN	2e58495c
MAC DA	68f2e77696ce
MAC SA	7ae8e2ca4ec5

Packet Data (Length=99)

```
68 f2 e7 76 96 ce 7a e8 e2 ca 4e c5 88 e5 4d 00
2e 58 49 5c c3 1f 53 d9 9e 56 87 f7 36 51 19 b8
32 d2 aa e7 07 41 d5 93 f1 f9 e2 ab 34 55 77 9b
07 8e b8 fe ac df ec 1f 8e 3e 52 77 f8 18 0b 43
36 1f 65 12 ad b1 6d 2e 38 54 8a 2c 71 9d ba 72
28 d8 40 88 f8 75 7a db 8a a7 88 d8 f6 5a d6 68
be 70 e7
```

6 Machine-Readable Distribution

For convenience in testing compliance of these vectors with existing implementations, the above data is also available in a form that may be easily read into a simulation environment. The data is distributed as an XML file, with tags defined for the parameters used above.

The format uses the following tags: ref_pkts, packet, sci, mac_da, mac_sa, pn, key, tci, pre, post, and data. The file is organized as a series of packet pairs, representing a packet before and after MACSec processing. All data for a given pair is contained in the ”packet” tag.

```
<ref_pkts>
  <packet>
    <sci>...</sci>
    <mac_da>000102...</mac_da>
    <mac_sa>050607...</mac_sa>
    <pn>...</pn>
    <tci>...</tci>
    <key>...</key>
    <pre>
      <data>00</data>
      <data>01</data>
      <data>02</data>
      ...
    </pre>
    <post>
      <data>00</data>
      <data>01</data>
      <data>02</data>
      ...
    </post>
  </packet>
  <packet>
  ...
  </packet>
</ref_pkts>
```

All numerical values within the file are in hexadecimal.