Network Working Group
Internet Draft
expires in six months

W. Simpson, Editor
DayDreamer
November 1995

# Photuris Extensions
## draft-ietf-ipsec-photuris-ext-01.txt

Status of this Memo

This document is a submission to the IP Security Working Group of the Internet Engineering Task Force (IETF). Comments should be submitted to the ipsec@ans.net mailing list.

Distribution of this memo is unlimited.

This document is an Internet-Draft. Internet Drafts are working documents of the Internet Engineering Task Force (IETF), its Areas, and its Working Groups. Note that other groups may also distribute working documents as Internet Drafts.

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 not appropriate to use Internet Drafts as reference material, or to cite them other than as a ``working draft'' or ``work in progress.''

To learn the current status of any Internet-Draft, please check the ``1id-abstracts.txt'' listing contained in the internet-drafts Shadow Directories on:

ftp.is.co.za (Africa)
nic.nordu.net (Europe)
ds.internic.net (US East Coast)
ftp.isi.edu (US West Coast)
munnari.oz.au (Pacific Rim)

Abstract

Photuris is an experimental session-key management protocol intended for use with the IP Security Protocols (AH and ESP). Extensible Exchange Schemes and Attributes are provided to enable future implementation changes without affecting the basic protocol.

## 1. Additional Exchange Schemes

The packet format and basic facilities are already defined for Photuris [Firefly].

Up-to-date values for the Exchange Schemes are specified in the most recent "Assigned Numbers" [RFC-1700]. This document defines the following values:

(3) Implementation Optional. Modular Exponentiation using a 1024-bit strong prime (p), expressed in hex:

<tbd>

The recommended generator (g) for this prime is 3.

Provides 1024 bits of keying material. The cryptographic strength is currently estimated to be equivalent to 86 bits (pessimistic) through 98 bits (optimistic). Exponent lengths of 196 to 256 bits are recommended.

The Identification_Message and Change_Message Privacy-Method is DES-CBC-64.

The Change_Message Validity-Method is MD5.

(4) Implementation Optional. Modular Exponentiation using a 2048-bit strong prime (p), expressed in hex:

<tbd>

The recommended generator (g) for this prime is 2.

Provides 2048 bits of keying material. The cryptographic strength is currently estimated to be equivalent to ??? bits (pessimistic). Exponent lengths of ??? to 512 bits are recommended.

The Identification_Message and Change_Message Privacy-Method is 3DES-CBC-64.

The Change_Message Validity-Method is MD5.

(5) Implementation Optional. Modular Exponentiation using a 1024-bit strong prime (p), expressed in hex:

```
   a478 8e21 84b8 d68b  fe02 690e 4dbe 485b
   17a8 0bc5 f21d 680f  1a84 1313 9734 f7f2
   b0db 4e25 3750 018a  ad9e 86d4 9b60 04bb
   bcf0 51f5 2fcb 66d0  c5fc a63f bfe6 3417

   3485 bbbf 7642 e9df  9c74 b85b 6855 e942
   13b8 c2d8 9162 abef  f434 2435 0e96 be41
   edd4 2de9 9a69 6163  8c1d ac59 8bc9 0da0
   69b5 0c41 4d8e b865  2adc ff4a 270d 567f
```

The recommended generator (g) for this prime is 5.

Provides 1024 bits of keying material. The cryptographic strength is currently estimated to be equivalent to 86 bits (pessimistic) through 98 bits (optimistic). Exponent lengths of 196 to 256 bits are recommended.

The Identification_Message and Change_Message Privacy-Method is DES-CBC-64.

The Change_Message Validity-Method is MD5.

This prime modulus was randomly generated by a freely available program written by Phil Karn, verified using the mpz_probab_prime() function Miller-Rabin test in the Gnu Math Package (GMP) version 1.3.2; and also verified with GMP on another platform by Frank A Stevenson.

(6) Reserved.

(7) Implementation Optional. Elliptic curve:

<tbd>

The Identification_Message and Change_Message Privacy-Method is 3DES-CBC-64.

The Change_Message Validity-Method is SHA.

(8) Implementation Optional. Modular Exponentiation using a 4096-bit strong prime (p), expressed in hex:

<tbd>

The recommended generator (g) for this prime is 2.

Provides 4096 bits of keying material. The cryptographic

strength is currently estimated to be equivalent to ??? bits (pessimistic). Exponent lengths of ??? to 1024 bits are recommended.

The Identification_Message and Change_Message Privacy-Method is 3DES-CBC-64.

The Change_Message Validity-Method is SHA.

## 2. Additional Attributes

The basic Attribute formats are already defined for Photuris [Firefly].

Up-to-date values for the Attribute Type are specified in the most recent "Assigned Numbers" [RFC-1700]. This document concerns the following values:

```
   A  I    Type
   +  +       6  SHA
   +          15  RC5
   +          20  Triple DES-CBC, 0-bit IV
   +          21  Triple DES-CBC, 32-bit IV
   +          22  Triple DES-CBC, 64-bit IV
      +       26  PKCS
      +       27  DNS-SIG certificate
      +       28  PGP certificate
      +       29  X.509 certificate chain
   +          32  Sensitivity Label
   +          33  VJ Header Compression
   +          34  LZ77
   +          35  Stac LZS
   +          36  AH-Sequence

   A     Initiator/Responder Attribute-Choice
      I  Identity-Choice
      +  feature must be supported
         when algorithm optionally supported
```

### 2.1. SHA

```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |    Length     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type 6

Length 0

The selected Exchange Scheme SHOULD provide at least 80-bits of cryptographic strength.

Attribute-Choice

When selected as an Initiator or Responder Attribute-Choice, pursuant to [RFC-1852], SHA is also used as the key generation cryptographic hash for generating the SPI session-key. All 160-bits of the generated hash are used for the key.

Identity-Choice

When selected as an Identity-Choice, the resulting Verification field is 160-bits (22 octets including Size).

The SHA hash is calculated as described in "Identity Verification". The authentication secret-key (as specified) is selected based on the contents of the Identification field.

The Identification field contains a variable precision number. Valid Identifications and secret-keys are preconfigured by the parties.

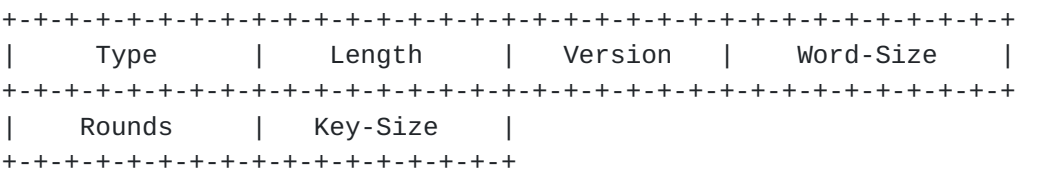
There is no required format or content for the Identification value. The value may be a number or string of any kind.

Validity-Method

When selected as a Validity-Method, the resulting Verification field is 160-bits (22 octets including Size).

The hash is calculated as described in "Change Verification". The leading shared-secret is not padded to any particular alignment.

## 2.2. RC5




Type 15

Length 4

Version Indicates the most recent version supported. All implementations must support version 16 (0x10).

Word-Size The number of bits used by internal calculations. All implementations must support at least 32-bits.

Rounds The number of rounds used. All implementations must support at least 12 rounds.

Key-Size The number of octets in the session-key. All implementations must support at least 5 octets.

When offered as an Attribute, the Version, Word-Size, Rounds, and Key-Size are set to the maximum supported.

When chosen as an Attribute, the Version, Word-Size, Rounds, and Key-Size are set to the actual values to be used.

Note that the Key-Size might be limited by available Exchange Schemes. The selected Exchange Scheme SHOULD provide at least Key-Size (in bits) of cryptographic strength.

Attribute-Choice

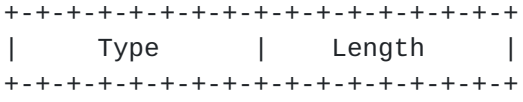
When selected as an Initiator or Responder Attribute-Choice, pursuant to [RFC-xxxx], MD5 is used as the key generation cryptographic hash for generating the SPI session-key. The most significant Key-Size octets of the generated hash are used for the key.

Privacy-Method

When selected as a Privacy-Method, MD5 is used as the key generation cryptographic hash for generating the privacy session-key. The most significant Key-Size octets of the generated hash are used for the key.

The least-significant bits of the ???-bit Initialization Vector (IV) are set to the least-significant bits of the Type, LifeTime, and SPI fields. Encryption begins with the next field, and continues to the end of the data indicated by the UDP Length.

## 2.3. Triple DES-CBC




Type 20, 21 or 22

Length 0

This attribute indicates EDE encryption (and DED decryption) with three 56-bit keys.

The selected Exchange Scheme SHOULD provide at least 112-bits of cryptographic strength.

Attribute-Choice

When selected as an Initiator or Responder Attribute-Choice, pursuant to [RFC-1851], MD5 is used as the key generation cryptographic hash for generating the three SPI session-keys.

The first MD5 hash is generated as described in [Firefly].

A second MD5 hash is calculated over the following concatenated values:

+ the computed shared-secret,
+ the first 128-bit hash,
+ the computed shared-secret again.

A third MD5 hash is calculated over the following concatenated values:

+ the computed shared-secret,
+ the second 128-bit hash,
+ the computed shared-secret again.

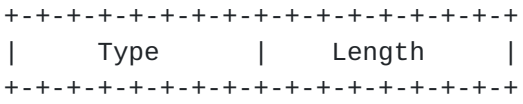
In all three keys, the most significant 64-bits of the generated hash are used for the key. The least significant bit of each octet is ignored (or set to parity).

Privacy-Method

When selected as a Privacy-Method, MD5 is used as the key generation cryptographic hash for generating the privacy session-keys. The three keys are generated as described above.

The 64-bit Initialization Vector (IV) is set to the Type, LifeTime, and SPI fields. Encryption begins with the next field, and continues to the end of the data indicated by the UDP Length.

## 2.4. PGP certificate




Type 28

Length 0

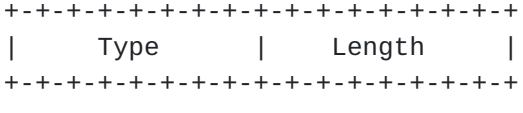
When selected as a Signature-Choice, the resulting Signature field size is variable. PGP certificates include an identification of the signature algorithm. As a minimum, it is required that all implementations support MD5 with RSA.

A Certificate field always follows the Signature field, and contains a PGP certificate. The PGP formats document is distributed with every copy of PGP. If the implementation cannot handle the given certificate, an Error_Message indicates Signature Failure.

PGP certificates include version numbers. All implementations must support version 3 (PGP 2.6) certificates. A certificate chain can include certificates with different version numbers.

The length of the RSA key is encoded in each certificate. All implementations must support a minimum of 2048-bit keys.

## 2.5. X.509 certificate chain




Type 29

Length 0

Future extensions to this attribute may add parameter values. This will be indicated by a non-zero value.

When selected as a Signature-Choice, the resulting Signature field size is variable. X.509 certificates include an identification of the signature algorithm. As a minimum, it is required that all implementations support MD5 with RSA.

A Certificate field always follows the Signature field, and contains a chain of X.509 certificates [??? reference]. If the implementation cannot handle the given certificate chain, an Error_Message indicates Signature Failure.

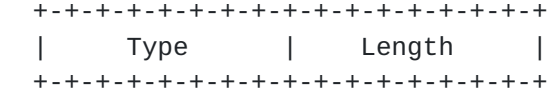
X.509 certificates include version numbers. All implementations must support X.509.v1 (1988) certificates. A certificate chain can include certificates with different version numbers.

The length of the RSA key is encoded in each certificate. All implementations must support a minimum of 512-bit keys.

Different certificates in the chain may have different signature algorithms and key lengths.

To improve performance, an implementation can cache the public keys for the issuers that frequently sign end-user certificates. These cached public keys can be used to verify the final certificate, and avoid the cost of verifying each certificate in the chain. However, the transmitter should always send the entire chain.

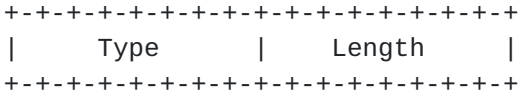
## 2.6. DNS-SIG




Type 27

Length 0

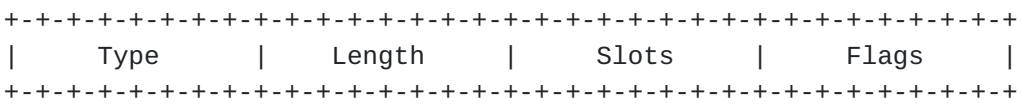
## 2.7. Sensitivity Label




Type 32

Length 0

## 2.8. VJ Header Compression




Type 33

Length 2

Slots indicates the maximum slot identifier. This is one less than the actual number of slots; the slot identifier has values from zero to Slots.

There may be implementations that have problems with small numbers. The example in [RFC-1144] will only work with 3 through 254 slots.

Flags (0) All compressed TCP packets must set the C bit in every change mask, and must include the slot identifier.

(1) The slot identifer may be compressed. This requires an ability for the implementation to indicate all errors in reception to the decompression module. Synchronization after errors depends on waiting for a packet with the slot identifier. See the discussion in [RFC-1144].

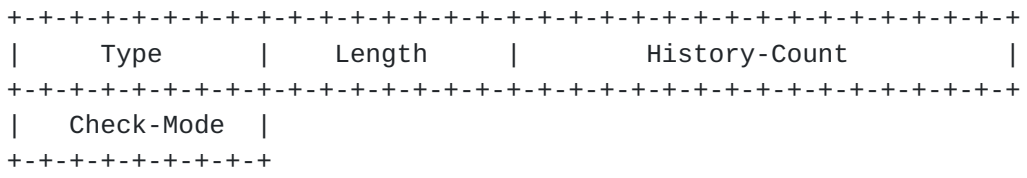
When selected as an Initiator or Responder Attribute-Choice, all data encapsulated in ESP [RFC-1827] is first compressed according to [RFC-1144].

Note that this attribute requires ordered delivery. Therefore, this

attribute is principly used for single network hops.

## 2.9. LZ77

## 2.10. Stac LZS




Type 35

Length 3

History-Count two octets, most significant octet first. Specifies the maximum number of Compression Histories.

(0) the implementation expects the peer to reset the Compression History at the beginning of every packet.

(1) only one history is maintained.

Other valid values range from 2 to 65535. The peer is not required to send as many histories as the implementation indicates that it can receive.

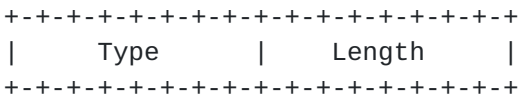
Check-Mode indicates support of LCB, CRC or Sequence checking.

| | |
|---|---|
| 0 | None (default) |
| 1 | LCB |
| 2 | CRC |
| 4 | Sequence Number |

When offered as an Attribute, the History-Count is set to the maximum histories that can be sent, and the Check-Mode is the XOR of the modes supported.

When selected as an Initiator or Responder Attribute-Choice, the History-Count is set to the maximum histories that can be received (less than or equal to the number offered), and the Check-Mode is set to only one of the modes supported.

## 2.11. AH-Sequence




Type 36

Length 0

When selected as an Initiator or Responder Attribute-Choice, the previously Reserved field of the Authentication Header (AH) [RFC-1826] contains a 16-bit sequence number. The SPI Owner (receiver) validates this number within an implementation dependent range of expected values. Any AH protected datagram that fails this test is silently discarded.

When the range has been exhausted, the SPI Owner (receiver) expires the SPI, despite any remaining SPI LifeTime. On arrival of an AH protected datagram with an expired SPI, an appropriate ICMP Security Failures message is generated (Type 40 Code 0), and the datagram is discarded.

## Security Considerations

Security issues are the primary topic of this memo.

## Acknowledgements

Robert W Baldwin of RSA provided text for RC5 and X.509 Certificates.

## References

[Firefly]
"Photuris" is the latin name for the firefly. "Firefly" is in turn the name for the USA National Security Administration's (classified) key exchange protocol for the STU-III secure telephone. Informed speculation has it that Firefly is based on very similar design principles.

[RFC-1700]
Reynolds, J., and Postel, J., "Assigned Numbers", STD 2, RFC-1700, USC/Information Sciences Institute, October 1994.

[RFC-1825]
Atkinson, R., "Security Architecture for the Internet Protocol", RFC-1825, Naval Research Laboratory, July 1995.

[RFC-1826]

[RFC-1827]

[RFC-1850]

[RFC-1851]

[Schneier94]
Schneier, B., "Applied Cryptography", John Wiley & Sons, New York, NY, 1994. ISBN 0-471-59756-2.

## Author's Address

Questions about this memo can also be directed to:

William Allen Simpson
Daydreamer
Computer Systems Consulting Services
1384 Fontaine

Madison Heights, Michigan 48071

Bill.Simpson@um.cc.umich.edu
bsimpson@MorningStar.com

Table of Contents