IKEv2-based Shared Secret Key for O/TWAMP
draft-ietf-ippm-ipsec-05

Abstract

   The O/TWAMP security mechanism requires that both the client and
   server endpoints possess a shared secret. Since the currently-
   standardized O/TWAMP security mechanism only supports a pre-shared
   key mode, large scale deployment of O/TWAMP is hindered
   significantly. At the same time, recent trends point to wider IKEv2
   deployment which, in turn, calls for mechanisms and methods that
   enable tunnel end-users, as well as operators, to measure one-way and
   two-way network performance in a standardized manner. This document
   discusses the use of keys derived from an IKEv2 SA as the shared key
   in O/TWAMP. If the shared key can be derived from the IKEv2 SA, O/
   TWAMP can support certificate-based key exchange, which would allow
   for more operational flexibility and efficiency. The key derivation
   presented in this document can also facilitate automatic key
   management.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

   The One-way Active Measurement Protocol (OWAMP) [RFC4656] and the
   Two-Way Active Measurement Protocol (TWAMP) [RFC5357] can be used to
   measure network performance parameters, such as latency, bandwidth,
   and packet loss by sending probe packets and monitoring their
   experience in the network. In order to guarantee the accuracy of
   network measurement results, security aspects must be considered.
   Otherwise, attacks may occur and the authenticity of the measurement
   results may be violated. For example, if no protection is provided,
   an adversary in the middle may modify packet timestamps, thus
   altering the measurement results.

   The currently-standardized O/TWAMP security mechanism [RFC4656]
   [RFC5357] requires that endpoints (i.e. both the client and the
   server) possess a shared secret. In today's network deployments,
   however, the use of pre-shared keys is far from optimal. For
   example, in wireless infrastructure networks, certain network
   elements, which can be seen as the two endpoints from an O/TWAMP
   perspective, support certificate-based security. For instance,
   consider the case in which one wants to measure IP performance
   between an eNB and SeGW. Both eNB and SeGW are 3GPP LTE nodes and
   support certificate mode and IKEv2. Since the currently standardized
   O/TWAMP security mechanism only supports pre-shared key mode, large
   scale deployment of O/TWAMP is hindered significantly. Furthermore,
   deployment and management of "shared secrets" for massive equipment
   installation consumes a tremendous amount of effort and is prone to
   human error.

   With IKEv2 widely used, employing keys derived from IKEv2 SA as
   shared key can be considered as a viable alternative. In mobile
   telecommunication networks, the deployment rate of IPsec exceeds 95%
   with respect to the LTE serving network. In older-technology
   cellular networks, such as UMTS and GSM, IPsec use penetration is
   lower, but still quite significant. If the shared key can be derived
   from the IKEv2 SA, O/TWAMP can support cert-based key exchange and
   make it more flexible in practice and more efficient. The use of
   IKEv2 also makes it easier to extend automatic key management. In
   general, O/TWAMP measurement packets can be transmitted inside the
   IPsec tunnel, as it occurs with typical user traffic, or transmitted
   outside the IPsec tunnel. This may depend on the operator's policy
   and is orthogonal to the mechanism described in this document.

   When IPsec is deployed, protecting O/TWAMP traffic in unauthenticated
   mode using IPsec is one option. Another option is to protect O/TWAMP
   traffic using O/TWAMP layer security established using the PSK
   derived from IKEv2 but bypassing the IPsec tunnel. Protecting
   unauthenticated O/TWAMP control and/or test traffic via AH or ESP
   cannot provide various security options, e.g. it cannot authenticate
   part of a O/TWAMP packet as mentioned in [RFC4656]. For measuring
   latency, timestamp is carried in O/TWAMP traffic. The sender has to
   fetch the timestamp, encrypt it, and send it. In this case, the
   middle step can be skipped, potentially improving accuracy as the
   sequence number can be encrypted and authenticated before the
   timestamp is fetched. It is the same case for the receiver since it
   can obtain the timstamp by skipping the decryption step. In such
   cases, protecting O/TWAMP traffic using O/TWAMP layer security but
   bypassing IPsec tunnel has its advantages. This document describes
   how to derive the shared secret key from the IKEv2 SA and employ the
   security service at the O/TWAMP layer. This method SHOULD be used

   when O/TWAMP traffic is bypassing IPsec protection and is running
   over an external network exactly between two IKEv2 systems.

   The remainder of this document is organized as follows. Section 3
   summarizes O/TWAMP protocol operation with respect to security.
   Section 4 presents a method of binding O/TWAMP and IKEv2 for network
   measurements between the client and the server which both support
   IKEv2. Finally, Section 5 discusses the security considerations
   arising from the proposed mechanisms.

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 [RFC2119].

3. O/TWAMP Security

   Security for O/TWAMP-Control and O/TWAMP-Test are briefly reviewed in
   the following subsections.

3.1. O/TWAMP-Control Security

   O/TWAMP uses a simple cryptographic protocol which relies on

   o AES in Cipher Block Chaining (AES-CBC) for confidentiality

   o HMAC-SHA1 truncated to 128 bits for message authentication

   Three modes of operation are supported in the OWAMP-Control protocol:
   unauthenticated, authenticated, and encrypted. In addition to these
   modes, the TWAMP-Control protocol also supports a mixed mode, i.e.
   the TWAMP-Control protocol operates in encrypted mode while TWAMP-
   Test protocol operates in unauthenticated mode. The authenticated,
   encrypted and mixed modes require that endpoints possess a shared
   secret, typically a passphrase. The secret key is derived from the
   passphrase using a password-based key derivation function PBKDF2
   (PKCS#5) [RFC2898].

   In the unauthenticated mode, the security parameters are left unused.
   In the authenticated, encrypted and mixed modes, the security
   parameters are negotiated during the control connection
   establishment.

   Figure 1 illustrates the initiation stage of the O/TWAMP-Control
   protocol between a client and the server. In short, the client opens
   a TCP connection to the server in order to be able to send O/TWAMP-
   Control commands. The server responds with a Server Greeting, which

contains the Modes, Challenge, Salt, Count, and MBZ fields (see
Section 3.1 of [RFC4656]). If the client-preferred mode is
available, the client responds with a Set-Up- Response message,
wherein the selected Mode, as well as the KeyID, Token and Client IV
are included. The Token is the concatenation of a 16-octet
Challenge, a 16-octet AES Session-key used for encryption, and a
32-octet HMAC-SHA1 Session-key used for authentication. The Token is
encrypted using AES-CBC.

```
    +--------+                      +--------+
    | Client |                      | Server |
    +--------+                      +--------+
        |                             |
        |<---- TCP Connection ----->|
        |                             |
        |<---- Greeting message ----|
        |                             |
        |----- Set-Up-Response ---->|
        |                             |
        |<---- Server-Start --------|
        |                             |
```
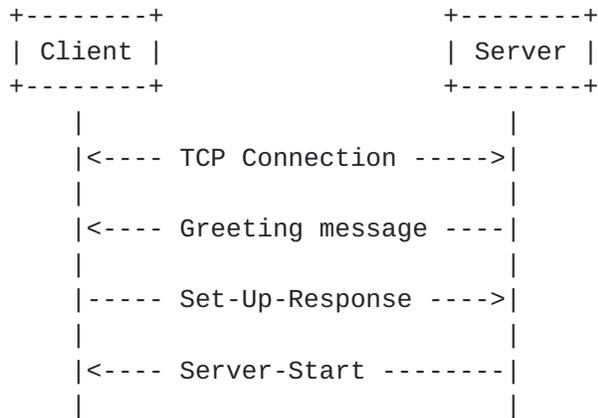
                 Figure 1: Initiation of O/TWAMP-Control

Encryption uses a key derived from the shared secret associated with
KeyID. In the authenticated, encrypted and mixed modes, all further
communication is encrypted using the AES Session-key and
authenticated with the HMAC Session-key. After receiving Set-Up-
Response the server responds with a Server-Start message containing
Server-IV. The client encrypts everything it transmits through the
just-established O/TWAMP-Control connection using stream encryption
with Client- IV as the IV. Correspondingly, the server encrypts its
side of the connection using Server-IV as the IV. The IVs themselves
are transmitted in cleartext. Encryption starts with the block
immediately following that containing the IV.

The AES Session-key and HMAC Session-key are generated randomly by
the client. The HMAC Session-key is communicated along with the AES
Session-key during O/TWAMP-Control connection setup. The HMAC
Session-key is derived independently of the AES Session-key.

3.2. O/TWAMP-Test Security

The O/TWAMP-Test protocol runs over UDP, using the client and server
IP and port numbers that were negotiated during the Request-Session
exchange. O/TWAMP- Test has the same mode with O/TWAMP-Control and
all O/TWAMP-Test sessions inherit the corresponding O/TWAMP-Control
session mode except when operating in mixed mode.

The O/TWAMP-Test packet format is the same in authenticated and
encrypted modes. The encryption and authentication operations are,
however, different. Similarly with the respective O/TWAMP-Control
session, each O/TWAMP-Test session has two keys: an AES Session-key
and an HMAC Session-key. However, there is a difference in how the
keys are obtained:

O/TWAMP-Control: the keys are generated by the client and
         communicated to the server during the control connection
         establishment with the Set-Up-Response message (as part of
         the Token).

O/TWAMP-Test: the keys are derived from the O/TWAMP-Control keys and
         the session identifier (SID), which serve as inputs of the
         key derivation function (KDF). The O/TWAMP-Test AES Session-
         key is generated using the O/TWAMP- Control AES Session-key,
         with the 16-octet session identifier (SID), for encrypting
         and decrypting the packets of the particular O/TWAMP-Test
         session. The O/TWAMP-Test HMAC Session-key is generated
         using the O/TWAMP-Control HMAC Session-key, with the 16-octet
         session identifier (SID), for authenticating the packets of
         the particular O/TWAMP-Test session.

3.3. O/TWAMP Security Root

As discussed above, the AES Session-key and HMAC Session-key used by
the O/TWAMP-Test protocol are derived from the AES Session-key and
HMAC Session-key which are used in O/TWAMP-Control protocol. The AES
Session-key and HMAC Session-key used in the O/TWAMP-Control protocol
are generated randomly by the client, and encrypted with the shared
secret associated with KeyID. Therefore, the security root is the
shared secret key. Thus, for large deployments, key provision and
management may become overly complicated. Comparatively, a
certificate-based approach using IKEv2 can automatically manage the
security root and solve this problem, as we explain in Section 4.

4. O/TWAMP for IPsec Networks

This section presents a method of binding O/TWAMP and IKEv2 for
network measurements between a client and a server which both support
IPsec. In short, the shared key used for securing O/TWAMP traffic is
derived using IKEv2 [RFC5996].

4.1. Shared Key Derivation

In the authenticated, encrypted and mixed modes, the shared secret
key MUST be derived from the IKEv2 Security Association (SA). Note
that we explicitly opt to derive the shared secret key from the IKEv2

SA, rather than the child SA, since the use case whereby an IKEv2 SA can be created without generating any child SA is possible [RFC6023].

When the shared secret key is derived from the IKEv2 SA, SK_d must be generated first. SK_d MUST be computed as per [RFC5996].

The shared secret key MUST be generated as follows:

Shared secret key = PRF(SK_d, "IPPM")

Wherein the string "IPPM" comprises four ASCII characters and prf is a pseudorandom function. It is recommended that the shared secret key is derived in the IPsec layer. This way, the IPsec keying material is not exposed to the O/TWAMP client. Note, however, that the interaction between the O/TWAMP and IPsec layers is host-internal and implementation-specific. Therefore, this is clearly outside the scope of this document, which focuses on the interaction between the O/TWAMP client and server. That said, one possible way could be the following: at the client side, the IPSec layer can perform a lookup in the Security Association Database (SAD) using the IP address of the server and thus match the corresponding IKEv2 SA. At the server side, the IPSec layer can look up the corresponding IKEv2 SA by using the SPIs sent by the client, and therefore extract the shared secret key. In case that both client and server do support IKEv2 but there is no current IKEv2 SA, two alternative ways could be considered. First, the O/TWAMP client initiates the establishment of the IKEv2 SA, logs this operation, and selects the mode which supports IKEv2. Alternatively, the O/TWAMP client does not initiate the establishment of the IKEv2 SA, logs an error for operational management purposes, and proceeds with the modes defined in [RFC4656][RFC5357][RFC5618]. Again, although both alternatives are feasible, they are in fact implementation-specific.

If rekeying for the IKEv2 SA or deletion of the IKEv2 SA occurs, the corresponding shared secret key generated from the SA can continue to be used until the O/TWAMP session terminates.

4.2. Server Greeting Message Update

To achieve a binding association between the key generated from IKEv2 and the O/TWAMP shared secret key, Server Greeting Message should be updated as in Figure 2.

```
    0                   1                   2                   3
    0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                                                               |
   |                     Unused (12 octets)                        |
   |                                                               |
   |+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-++-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                        Modes                                  |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                                                               |
   |                   Challenge (16 octets)                       |
   |                                                               |
   |                                                               |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                                                               |
   |                     Salt (16 octets)                          |
   |                                                               |
   |                                                               |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                     Count (4 octets)                          |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                                                               |
   |                     MBZ (12 octets)                           |
   |                                                               |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```
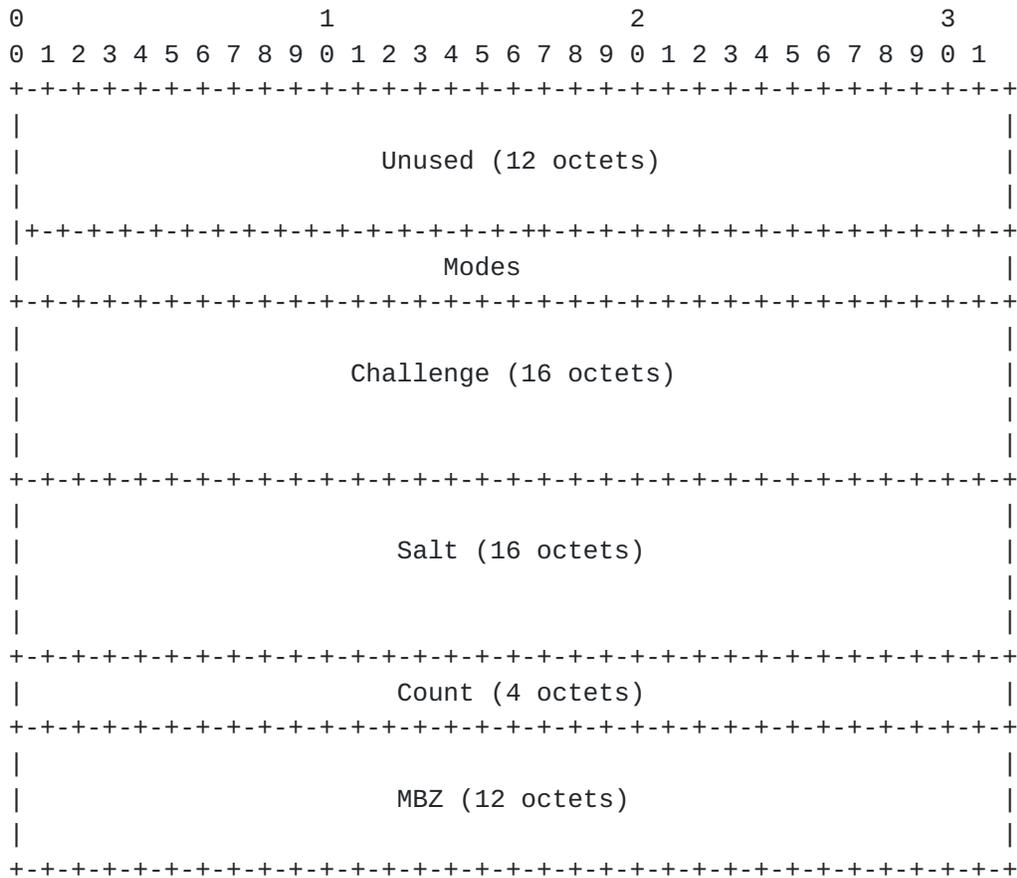
                  Figure 2: Server Greeting format

The Modes field in Figure 2 will need to allow for support of key
derivation as discussed in Section 4.1. As such, the Modes value
extension MUST be supported by implementations compatible with this
document, indicating support for deriving the shared key from the
IKEv2 SA. The new Modes value indicating support for this
specification is IANA.TBA.TWAMP.IKEv2Derived (note to IANA: 128 is
preferred, i.e. bit in position 7). Clearly, an implementation
compatible with this specification MUST support the authenticated,
encrypted and mixed modes as per [RFC4656][RFC5357][RFC5618].

The choice of this set of Modes values poses no backwards
compatibility problems to existing O/TWAMP clients. Robust legacy
client implementations would disregard the fact that the
IANA.TBA.TWAMP.IKEv2Derived Modes bit in the Server Greeting is set.
On the other hand, a client compatible with this specification can
easily identify that the O/TWAMP server contacted does not support
this specification. If the server supports other Modes, as one could
assume, the client would then decide which Mode to use and indicate
such accordingly as per [RFC4656][RFC5357]. A client compatible with

this specification which decides not to employ IKEv2 derivation, can
simply behave as a purely [RFC4656]/[RFC5357] compatible client.

4.3. Set-Up-Response Update

The Set-Up-Response Message should be updated as in Figure 3. When a
O/TWAMP client compatible with this specification receives a Server
Greeting indicating support for Mode IANA.TBA.TWAMP.IKEv2Derived it
SHOULD reply to the O/TWAMP server with a Set-Up response that
indicates so. For example, a compatible O/TWAMP client choosing the
authenticated mode with IKEv2 shared secret key derivation should set
Mode to 130, i.e. set the bits in positions 1 and 7 (TBD IANA) to
one.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                             Mode                              |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
|                      Key ID (80 octets)                       |
|                                                               |
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
|                      Token (16 octets)                        |
|                                                               |
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
|                     Client-IV (12 octets)                     |
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```
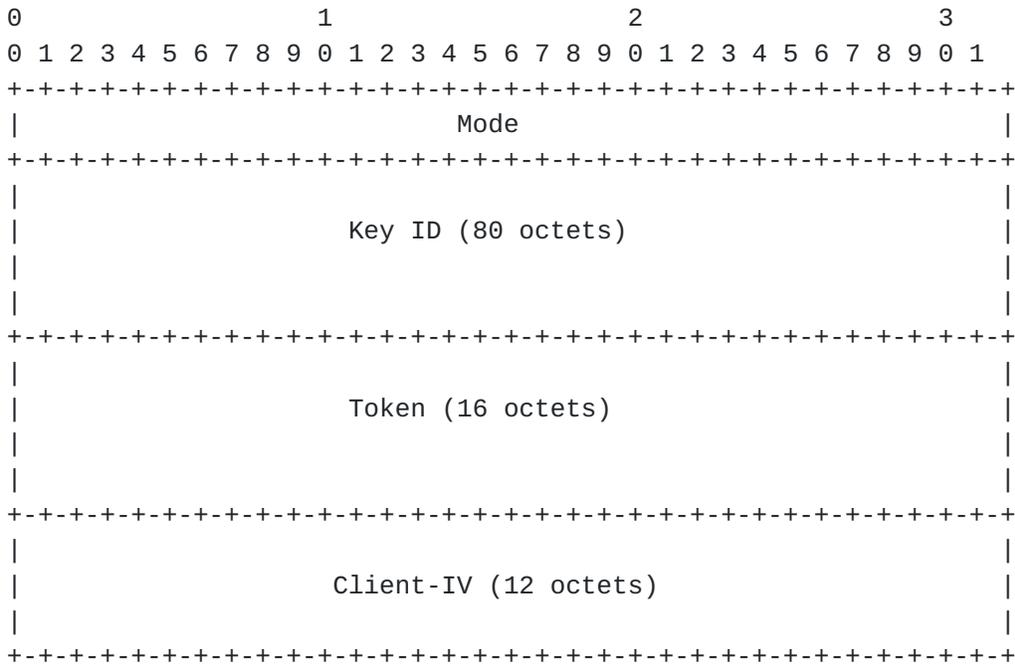
Figure 3: Set-Up-Response Message

The Security Parameter Index (SPI)(see [RFC4301] [RFC5996]) can
uniquely identify the Security Association (SA). If the client
supports the derivation of shared secret key from IKEv2 SA, it will
choose the corresponding mode value and carry SPIi and SPIr in the
Key ID field. SPIi and SPIr MUST be included in the Key ID field of
Set-Up-Response Message to indicate the IKEv2 SA from which the O/
TWAMP shared secret key derived from. The length of SPI is 4 octets.
Therefore, the first 4 octets of Key ID field MUST carry SPIi and the
second 4 octets MUST carry SPIr. The remaining bits of the Key ID
field MUST set to zero.

A O/TWAMP server which supports the specification of this document, MUST obtain the SPIi and SPIr from the first 8 octets and ignore the remaining octets of the Key ID field. Then, the client and the server can derive the shared secret key based on the mode value and SPI. If the O/TWAMP server cannot find the IKEv2 SA corresponding to the SPIi and SPIr received, it MUST log the event for operational management purposes. In addition, the O/TWAMP server SHOULD set the Accept field of the Server-Start message to the value 6 to indicate that server is not willing to conduct further transactions in this O/TWAMP-Control session since it can not find the corresponding IKEv2 SA.

4.4. O/TWAMP over an IPsec tunnel

IPsec AH [RFC4302] and ESP [RFC4303] provide confidentiality and data integrity to IP datagrams. Thus an IPsec tunnel can be used to provide the protection needed for O/TWAMP Control and Test packets, even if the peers choose the unauthenticated mode of operation. If the two endpoints are already connected through an IPSec tunnel it is RECOMMENDED that the O/TWAMP measurement packets are forwarded over the IPSec tunnel if the peers choose the unauthenticated mode in order to ensure authenticity and security.

5. Security Considerations

As the shared secret key is derived from the IKEv2 SA, the key derivation algorithm strength and limitations are as per [RFC5996]. The strength of a key derived from a Diffie-Hellman exchange using any of the groups defined here depends on the inherent strength of the group, the size of the exponent used, and the entropy provided by the random number generator employed. The strength of all keys and implementation vulnerabilities, particularly Denial of Service (DoS) attacks are as defined in [RFC5996].

As a more general note, the IPPM community may want to revisit the arguments listed in [RFC4656], Sec. 6.6. Other widely-used Internet security mechanisms, such as TLS and DTLS, may also be considered for future use over and above of what is already specified in [RFC4656] [RFC5357].

6. IANA Considerations

IANA is requested to allocate the IANA.TBA.TWAMP.IKEv2Derived Modes value in the TWAMP-Modes registry.

7. Acknowledgments

We thank Eric Chen, Yaakov Stein, Brian Trammell, Emily Bi, John Mattsson, and Steve Baillargeon for their comments and text suggestions. Al Morton deserves a special mention for his text contributions and the good discussion and pointers to earlier related work in IPPM WG.

8. References

8.1. Normative References

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

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

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

[RFC4656]   Shalunov, S., Teitelbaum, B., Karp, A., Boote, J., and M. Zekauskas, "A One-way Active Measurement Protocol (OWAMP)", RFC 4656, September 2006.

[RFC5357]   Hedayat, K., Krzanowski, R., Morton, A., Yum, K., and J. Babiarz, "A Two-Way Active Measurement Protocol (TWAMP)", RFC 5357, October 2008.

[RFC5618]   Morton, A. and K. Hedayat, "Mixed Security Mode for the Two-Way Active Measurement Protocol (TWAMP)", RFC 5618, August 2009.

[RFC5996]   Kaufman, C., Hoffman, P., Nir, Y., and P. Eronen, "Internet Key Exchange Protocol Version 2 (IKEv2)", RFC 5996, September 2010.

8.2. Informative References

[RFC2898]   Kaliski, B., "PKCS #5: Password-Based Cryptography Specification Version 2.0", RFC 2898, September 2000.

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

   [RFC6023]   Nir, Y., Tschofenig, H., Deng, H., and R. Singh, "A
               Childless Initiation of the Internet Key Exchange Version
               2 (IKEv2) Security Association (SA)", RFC 6023, October
               2010.

Authors' Addresses

   Kostas Pentikousis (editor)
   EICT GmbH
   EUREF-Campus Haus 13
   Torgauer Strasse 12-15
   10829 Berlin
   Germany

   Email: k.pentikousis@eict.de

   Emma Zhang
   Huawei Technologies
   Huawei Building, Q20, No.156, Rd. BeiQing
   Haidian District , Beijing   100095
   P. R. China

   Email: emma.zhanglijia@huawei.com

   Yang Cui
   Huawei Technologies
   Otemachi First Square 1-5-1 Otemachi
   Chiyoda-ku, Tokyo   100-0004
   Japan

   Email: cuiyang@huawei.com