IPPM WG K. Pentikousis, Ed.
Internet-Draft EICT
Intended status: Standards Track Y. Cui
Expires: August 18, 2014 E. Zhang
Huawei Technologies
February 14, 2014

Network Performance Measurement for IPsec
draft-ietf-ippm-ipsec-02

Abstract

The O/TWAMP security mechanism requires that endpoints (i.e. both the client and the server) 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 IKE SA as the shared key in O/TWAMP. If the shared key can be derived from the IKE SA, O/TWAMP can support cert-based key exchange, which would allow for more flexibility and efficiency. Such key derivation 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 may not be 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. This is the case when one wants to measure IP performance between an eNB and SeGW, for instance. 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, using keys derived from IKE 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 IKE 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.

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 reviewed separately in this section.

3.1. O/TWAMP-Control Security

O/TWAMP uses a simple cryptographic protocol which relies on

- AES in Cipher Block Chaining (AES-CBC) for confidentiality
- HMAC-SHA1 truncated to 128 bits for message authentication

Three modes of operation are supported in the OWAMP-Control protocol: unauthenticated, authenticated, and encrypted. Besides the above three modes supported, the TWAMP-Control protocol also supports an additional mode: 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 in 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 can be derived from the IKEv2 Security Association (SA). Note that we explicitly opt to derive the shared secret key from the IKE SA, rather than the child SA, since the use case whereby an IKE SA can be created without generating any child SA is possible [RFC6023].

If the shared secret key is derived from the IKE SA, SKEYSEED must be generated first. SKEYSEED and its derivatives are computed as per [RFC5996], where prf is a pseudorandom function:

```
SKEYSEED = prf( Ni | Nr, g^ir )
```

Ni and Nr are, respectively, the initiator and responder nonces, which are negotiated during the initial exchange (see Section 1.2 of [RFC5996]). g^ir is the shared secret from the ephemeral Diffie-Hellman exchange and is represented as a string of octets.

The shared secret key can be generated as follows:

```
Shared secret key = PRF{ SKEYSEED, "IPPM" }
```

The shared secret key is derived in the IPsec layer. Thus, the IPsec keying material is not be exposed to the O/TWAMP client. Note that the interaction between the O/TWAMP and IPsec implementations is outside the scope of this document, which focuses on the interaction between the O/TWAMP client and server. Of course, extracting the shared secret key from the IPsec layer can depend on the implementation. 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 IKE SA. At the server side, the IPSec layer can look up the corresponding IKE SA by using the SPIs sent by the client, and therefore extract the shared secret key.

If rekeying for the IKE SA or deletion of the IKE SA occurs, the corresponding shared secret key generated from the SA can continue to be used until the lifetime of the shared secret key expires.

4.2. Server Greeting Message Update

To achieve a binding association between the key generated from IKE 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, pending discussion in the IPPM WG, Modes value 8 extension MUST be supported by implementations compatible with this document, indicating support for deriving shared key from IKE SA. Modes value 16 indicates authenticated mode; Modes value 32 indicates encrypted mode; and Modes value 64 indicates mixed mode over IKEv2.

Authenticated mode over IKEv2 means that the client and server operate in authenticated mode with the shared secret key derived from IKE SA. Encrypted mode over IKEv2 means that the client and server operate in encrypted mode with the shared secret key derived from IKE SA. Mixed mode over IKEv2 means that the client and server operate in encrypted mode for the O/TWAMP-Control protocol while operating in unauthenticated mode for the O/TWAMP-Test protocol with shared secret key derived from IKE SA.

Server implementations compatible with this document MUST set the first 25 bits of the Modes field to zero. A client compatible with this specification MUST ignore the first 25 bits of the Modes field.

For backward compatibility, the server is obviously allowed to indicate support for the Modes defined in [RFC4656]

The choice of this set of Modes values poses the least backwards compatibility problems to existing O/TWAMP clients. Robust client implementations of [RFC4656] would disregard that the first 29 Modes bits in the Server Greeting is set. If the server supports other Modes, as one would assume, the client would then indicate any of the Modes defined in [RFC4656] and effectively indicate that it does not support key derivation from IKE. At this point, the Server would need to use the Modes defined in [RFC4656] only.

4.3. Set-Up-Response Update

The Set-Up-Response Message should be updated as in Figure 3.

```
   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 IKE SA, it will choose the corresponding mode value and carry SPIi and SPIr in the KeyID field. SPIi and SPIr are included in Key ID field of Set-Up-Response Message to indicate the IKE SA which O/TWAMP shared secret key derived from. The length of SPI is 4 octets. The first 4 octets of Key ID field carries SPIi and the second 4 octets carries SPIr.

The rest bits of the Key ID field is set to zero.

A server which supports deriving shared secret from an IKE SA can obtain the SPIi and SPIr from the first 8 octets and ignore the rest 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 server can not find the IKE SA corresponding to the SPIi and SPIr, the Accept field of Server-Start message is extended to indicate that. Accept value 6 can be used to indicate that server is not willing to conduct further transactions in this OWAMP-Control session since it can not find the corresponding IKE SA.

5. Security Considerations

As the shared secret key is derived from the IKE 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 will need to allocate additional values for the Modes options presented in this document.

7. Acknowledgments

Emily Bi contributed to an earlier version of this document.

We thank Eric Chen, Yakov Stein, and John Mattsson for their comments on this draft, and Al Morton for the discussion on related earlier

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.

[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.

[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
Torgauer Strasse 12-15
10829 Berlin
Germany

Email: k.pentikousis@eict.de

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

Email: cuiyang@huawei.com

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

Email: emma.zhanglijia@huawei.com