Network
Internet-Draft
Intended status: Standards Track
Expires: January 8, 2008

L. Dondeti, Ed.
QUALCOMM, Inc.
R. Canetti
IBM Research

July 7, 2007

The Use of Timed Efficient Stream Loss-Tolerant Authentication (TESLA) in IPsec

draft-dondeti-msec-ipsec-tesla-02

Status of this Memo

Copyright Notice

Abstract

This document specifies the use of Timed Efficient Stream Loss-tolerant Authentication (TESLA) -- a source authentication mechanism for multicast or broadcast data streams -- with IPsec ESP. In addition to the source authentication using TESLA, group authentication of the ESP packet can be provided using a shared symmetric group key. Thus, the proposed extension to ESP combines

group secrecy, group authentication, and source authentication transforms in an ESP packet.

Contributors

Adrian Perrig, Ran Canetti, and Bram Whillock were the original contributors of the TESLA work. Mark Baugher, Ran Canetti, Pau-Chen Cheng and Pankaj Rohatgi were the original contributors to the multicast ESP transform design.

Table of Contents

1. Introduction

The IPsec Encapsulation Security Payload (ESP) [RFC4303] transform provides a set of security services that include data origin authentication, which enables an IPsec receiver to validate that a received packet originated from a peer-sender in a pairwise security association (SA). A Message Authentication Code (MAC) based on a symmetric key is the common means to provide data origin authentication for pairwise IPsec SAs. However, for secure groups such as IP multicast groups, a MAC supports only "group authentication" and not data origin authentication. This document specifies a ESP data origin authentication transform based on TESLA for source authentication of data sent to groups of receivers.

The description of the TESLA protocol itself is available in RFC 4082 [RFC4082]. The TESLA authentication itself is protected from DoS attacks by an external authentication transform using a symmetric-key based MAC. Thus senders first source authenticate a packet and then protect it with group authentication. The receivers verify the external MAC to rule out any attacks from parties outside of the secure group and then proceed to verify that the message originated from the claimed source following the TESLA procedures.

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 RFC 2119 [RFC2119]. In addition, the following terms are defined and used in this document:

Group Secrecy (GS): Group Secrecy ensures that transmitted data is accessible only to group members. This is often used as the means to enforce access control. A typical realization of GS is to encrypt data using a key known only to group members. Essentially, the solution for group secrecy is the same as the solution for two party confidential communication.

Group Authentication (GA): The GA functionality enables a group member to verify that the received data originated from someone in the group and was not modified en-route by a non-group member. Note that group authentication by itself does not identify the source of the data. For example, the data might have been forged by any malicious group member. GA can be efficiently realized using standard shared key authentication mechanisms such as Message Authentication Codes (MACs), e.g., CBC-MAC or HMAC.

Source and Data Authentication (SrA): The SrA functionality enables a group member to verify that the received data originated from the claimed source and was not modified en-route by anyone (including other group members). Unlike Group Authentication, SrA provides the IPsec data origin authentication function. SrA provides a much stronger security guarantee than GA in that a particular group member can be identified as a source of a packet.

3. Notes on IPsec ESP and TESLA

IPsec ESP provides confidentiality, integrity protection, replay protection and traffic flow confidentiality. Integrity protection may be provided using symmetric keys or digital signatures [RFC4359]. For unicast communication, integrity protection using either mechanism provides data origin authentication. In case of multicast or group communication, symmetric-key based integrity protection supports group authentication only. For source authentication of multicast streams, the sender may sign every packet [RFC4359], use TESLA or another source authentication mechanism.

TESLA uses symmetric key chain commitment, delayed disclosure of a key from the key chain, and loose time synchronization between the sender's and the receivers' clocks to support source and data origin authentication. The delayed disclosure of keys from the key chain implies that the receivers must buffer packets until the authentication can be verified. To avoid denial of service attacks taking advantage of this buffering requirement, TESLA protected packets may be further protected using group authentication of packets. That limits any such denial of service attacks to from members of the secure group.

TESLA receivers may be bootstrapped using a digitally signed broadcast message containing the commitment to a key chain, local time, disclosure delay and other TESLA parameters from the sender or via individual registration processes with the sender. Bootstrapping of TESLA is out of scope for this document. The key management protocol that establishes the IPsec SA can be used for bootstrapping TESLA at the receivers.

4. IPsec ESP Packet Format with TESLA

In the following we first describe the TESLA authentication fields, followed by a depiction of where the those fields fit in an IPsec ESP packet. Figure 2 also shows the coverage of encryption (when the encryption algorithm is non-NULL), IPsec integrity protection (IPsec ICV), and the TESLA MAC.

The TESLA Authentication Fields are as follows:

o Id i of K_i (OPTIONAL) -- The 32-bit Id of the key used to compute the TESLA-MAC of the current packet: Within the TESLA tag, the Id i of K_i MAY be sent with the MAC of the message M computed using K_i. If i is not included in the message, the receiver determines i by the time the packet was received and the maximum time displacement from the server. With this time it then can determine the sender's current interval i.

o Disclosed Key K_(i-d) -- Variable length disclosed key is MANDATORY and is used to authenticate previous packets from earlier time intervals.

o TESLA MAC (K'_i, M): Variable length, MANDATORY. TESLA MAC is computed using the key K'_i (derived from K_i) [RFC4082], which is disclosed in a subsequent packet (in the Disclosed Key field). The MAC coverage is shown 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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                     Id i of K_i(optional)                     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
~                      Disclosed Key K_(i-d)                    ~
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
~                          MAC(K'_i, M)                         ~
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 1: TESLA Authentication Fields.

TESLA authentication fields are added to IPsec ESP packets as shown 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
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+---
    |               Security Parameters Index (SPI)                 |  ^
  --+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+  |
  ^ |                      Sequence Number                          |  |
  | +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+- I
  T |                    IV (optional)                              |^ P
  E +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+| s
  S |                    Rest of Payload Data  (variable)           |E e
  L ~                                                               ~N c
  A |                                                               |C
    +               +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+R I
  M |               |         TFC Padding * (optional, variable)    |Y C
  A +-+-+-+-+-+-+-+-+         +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+P V
  C |                         |        Padding (0-255 bytes)        |T |
  | +-+-+-+-+-+-+-+-+-+-+-+-+-+     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+| |
  v |                               |  Pad Length   | Next Header   |v |
  --+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+- |
    ~            TESLA Authentication Fields   (variable)           ~  v
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+---
    ~             Integrity Check Value-ICV   (variable)            ~
    +---------------------------------------------------------------+
```

Figure 2: IPsec ESP Packet Format with TESLA MAC and IPsec ICV

In the figure,

- o The label "Encyrpt" indicates the coverage of IPsec encryption. It is the same as that described in the IPsec ESP specification [RFC4303].
- o The label "IPsec ICV" indicates IPsec ESP's ICV coverage. Whether the ICV is present and its coverage of the fields of the IPsec packet is as specified in the ESP specification.
- o The label "TESLA MAC" indicates the TESLA MAC coverage. The TESLA MAC protects the IPsec ESP packet starting with the Sequence number and ending with the Next Header field.

4.1. On the IPsec ICV in TESLA Protected ESP packets

IPsec ESP mandates the presence of an Integrity Check Value (ICV), except when combined mode algorithms are used to protect the packet and the ICV is part of the combined mode algorithm. In case of CCM, the ICV is encrypted and only parseable at the receiver after

decryption. With TESLA protection of a packet, technically an ICV is not required for integrity protection of the packet. However, as noted above, a symmetric-key based ICV has the advantage of protecting against some DoS attacks on TESLA, so ICV is REQUIRED to be present in ESP-TESLA.

5. Cryptographic Algorithms for IPsec ESP with TESLA

TESLA needs a PRF algorithm to derive keys in the key chain. TESLA PRF algorithm is specified through the key management protocol that distributes the ESP SA.

The TESLA MAC algorithm is also specified through the key management protocol. There is no reason for this algorithm to be different from the IPsec ICV algorithm. When the TESLA MAC algorithm is not explicitly specified, the receivers are REQUIRED to use the IPsec ICV algorithm to compute the TESLA MAC algorithm.

In the single sender group communication, all encryption algorithms that are appropriate for unicast communication are also suitable for secure group communication. In the multi-sender communication case, the counter mode algorithms must be used as specified in . [I-D.weis-esp-group-counter-cipher]

6. Sender Processing of TESLA Protected Packets

In addition to the steps in [RFC4303], the sender follows the steps below for TESLA protected packets:

- The sender determines the current TESLA time interval i. The sender may include the time interval i in the message.

- It then includes the TESLA Key, K_(i-d), where d is the TESLA disclosure delay.

- Next, it computes the TESLA MAC over the IPsec ESP packet, starting at the Sequence Number field and ending with the Next Header field, using the TESLA Key K_i. That key itself SHALL NOT be disclosed until the TESLA interval i+d.

- The sender includes all the TESLA Authentication Fields after the Next Header field of the ESP packet and proceeds to compute the IPsec ICV over the entire ESP packet excluding the ICV field itself.

7. Receiver Processing of TESLA Protected Packets

Receiver processing of TESLA packets contains the following steps. Note that the symmetric key MAC or the group MAC verification is similar to the MAC verification process specified in Section 3.4.4 of [RFC4303]. We limit the specification below for TESLA MAC verification.

- When a receiver receives an ESP packet with TESLA fields, it must first check to see that the time interval of the message does not violate the security conditions for the keys used. The message is buffered, and the receiver attempts to authenticate any messages which are authenticated using K_(i-d), i.e., messages received with the index i-d.

- If i is not included in the message, the receiver determines i by the time the packet was received and the maximum time displacement from the server. With this time it then can determine the sender's current interval i.

- When the receiver receives a TESLA protected ESP packet, it first needs to verify whether the packet is safe, which is to verify that the key used to compute the MAC of the packet was still secret upon packet arrival. For the verification, the receiver computes an upper bound on the sender's clock, and checks that the MAC key is still secret (based on the key disclosure schedule). If the packet is safe, the receiver buffers the packet. The "safe packet test" is explained in detail in Section 3.5 of [RFC4082].

- Once the receiver has determined i, it checks K_(i-d) against the most recently stored key, K_c. If i-d=c then the receiver does nothing. Otherwise it applies the PRF (i-d)-c times to K_(i-d) which should yield K_c. If K_(i-d) is authentic, the receiver uses it to authenticate all buffered messages which used keys in the range K_(c+1) .. K_(i-d) as the MAC key. Finally the receiver replaces K_c with K_(i-d). If K_(i-d) is not authentic, the receiver discards the received message. If the MAC verification on any individual buffered packet fails, the receiver discards that buffered packet.

- Note, that if i-d < c the packet would have been unsafe and discarded before this step.

- After the TESLA MAC has been verified, the receiver updates the replay window.

8. Security Considerations

This document specifies the use of a source authentication scheme TESLA with IPsec ESP. TESLA provides source authentication using a symmetric key MAC but relies on loose time synchronization and delayed MAC key disclosure. The scheme is safe as long as receivers can estimate an upper bound on the sender's time and accept packets only if there is a local assurance that the sender has not revealed the MAC key used to authenticate the received packet. To that end, the security considerations in [RFC4082] apply.

A group member cannot authenticate the source of the packet for a multicast group where multiple members share the MAC key. Thus, a rogue member of the group has all the keying material needed to impersonate a sender of the group if that attacker is able to inject packets into the network using that sender's IP address. TESLA-ESP addresses this problem by augmenting the IPsec ICV with the TESLA MAC protection. Source authentication schemes leave multicast receivers vulnerable to DoS attacks if the receiver is duped into performing computationally-expensive validation of bogus packets or buffering of bogus packets. An IPsec ICV is RECOMMENDED to accompany the TESLA MAC so as to limit the effectiveness of bogus packets sent by non-group members.

Unfortunately, group members are still capable of sending packets with a valid external-authenticating MAC and invalid TESLA MAC, i.e., any group member can launch a DoS attack. In this case, the IPsec ICV verification will succeed only to have the TESLA MAC verification to fail.

The new transform includes the ESP sequence number in the TESLA MAC to protect against a replay attack by a group member. When the TESLA MAC is used, however, the ESP receiver MUST validate both the authentication tags before updating the ESP replay window.

9. IANA Considerations

IANA considerations associated with this work will appear in future version of this document.

10. References

10.1. 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.

10.2. Informative References

[RFC4082] Perrig, A., Song, D., Canetti, R., Tygar, J., and B. Briscoe, "Timed Efficient Stream Loss-Tolerant Authentication (TESLA): Multicast Source Authentication Transform Introduction", RFC 4082, June 2005.

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

[RFC4359] Weis, B., "The Use of RSA/SHA-1 Signatures within Encapsulating Security Payload (ESP) and Authentication Header (AH)", RFC 4359, January 2006.

[I-D.weis-esp-group-counter-cipher] McGrew, D. and B. Weis, "Using Counter Modes with Encapsulating Security Payload (ESP) and Authentication Header (AH) to Protect Group Traffic", draft-weis-esp-group-counter-cipher-00 (work in progress), October 2006.

Authors' Addresses

Lakshminath Dondeti (editor)
QUALCOMM, Inc.
5775 Morehouse Dr
San Diego, CA
USA

Phone: +1 858-845-1267
Email: ldondeti@qualcomm.com

Ran Canetti
IBM Research
30 Saw Mill River Rd
Hawthorne, NY
USA

Phone:
Email: canetti@watson.ibm.com

Full Copyright Statement

Intellectual Property

Acknowledgment

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).