MSEC
Internet-Draft
Expires: April 16, 2005

S. Fries
H. Tschofenig
Siemens

October 16, 2004

Bootstrapping TESLA
draft-fries-msec-bootstrapping-tesla-00.txt

Status of this Memo

Copyright Notice

Abstract

With the Timed Efficient Stream Loss-tolerant Authentication protocol (TESLA) a protocol for providing source authentication in multicast scenarios was introduced. A mapping for TESLA to the Secure Real-time Transport Protocol (SRTP) has been published which assumes that some TESLA parameters are made available by out-of-band mechanisms. This document describes payloads for bootstrapping these parameters with the help of the Multimedia Internet KEYing (MIKEY)

protocol.

Table of Contents

1. Introduction

[I-D.ietf-msec-srtp-tesla] describes extensions for SRTP [RFC3711] in order to support TESLA [I-D.ietf-msec-tesla-intro] for source authentication in multicast scenarios. Therefore the cryptographic context needs to be enhanced with a set of TESLA parameters. It is necessary to provide these parameters before the actual multicast session starts. [I-D.ietf-msec-srtp-tesla] does not address the bootstrapping for these parameters.

This document details bootstrapping of TESLA using the Multimedia Internet Keying (MIKEY) [RFC3830] protocol. MIKEY defines an authentication and key management framework that can be used for real-time applications (both for peer-to-peer communication and group communication). In particular, [RFC3830] is defined in a way to support SRTP in the first place but is open to enhancements to be used for other purposes too.

The three authentication and key exchange protocols defined in [RFC3830] as well as the fourth protocol provided by [I-D.ietf-msec-mikey-dhhmac] may be used to provide also the TESLA parameters. The required TESLA parameters to be exchanged are already described in [I-D.ietf-msec-srtp-tesla], while this document describes their transport within MIKEY.

The following security requirements have to be placed on the exchange of TESLA parameters:

- Integrity MUST be provided when sending the TESLA parameters, especially for the initial key.
- Confidentiallity MAY be provided for the TESLA parameter

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. TESLA Parameter Overview

According to [I-D.ietf-msec-srtp-tesla] the following transform dependent parameters need to be provided for proper TESLA operation:

1. An identifier for the PRF, f, implementing the one-way function F(x) in TESLA (to derive the keys in the chain), e.g. to indicate HMAC-SHA1.

2. A non-negative integer n_c, determining the length of the F output, i.e. the length of the keys in the chain (that is also

the key disclosed in an SRTP packet).

3. An identifier for the PRF, f', implementing the one-way function F'(x) in TESLA (to derive the keys for the TESLA MAC, from the keys in the chain), e.g. to indicate HMAC-SHA1.

4. A non-negative integer n_f, determining the length of the output of F', i.e. of the key for the TESLA MAC.

5. An identifier for the TESLA MAC, that accepts the output of F'(x) as its key, e.g. to indicate HMAC-SHA1.

6. A non-negative integer n_m, determining the length of the output of the TESLA MAC.

7. The beginning of the session T_0,

8. The interval duration T_int (in msec),

9. The key disclosure delay d (in number of intervals)

10. Non-negative integer n_c, determining the length of the key chain, which is determined based up the expected duration of the stream.

11. The initial key of the chain to which the sender has committed himself.

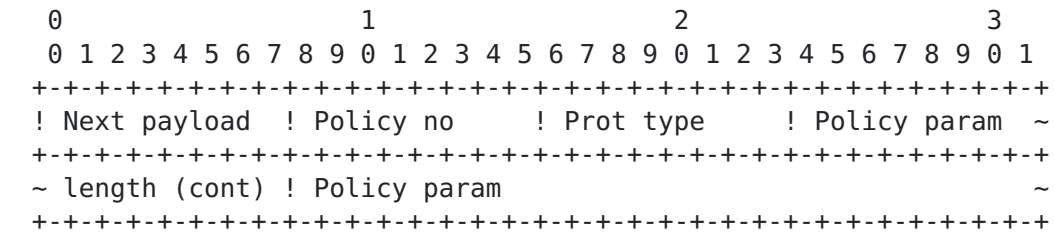
Section 6.2 in [I-D.ietf-msec-srtp-tesla] provides information about the default value for the above-listed parameters.

4. Parameter encoding within MIKEY

As mentioned in Section 3, TESLA parameters need to be transported before actually starting a session. MIKEY currently only defines a payload for transporting the SRTP policy (see Section 6.10 of [RFC3830]). This section describes the enhancement of MIKEY to allow the transport of a TESLA policy and additionally the initial TESLA key.

4.1 Security Policy payload (SP)

The Security Policy payload defines a set of policies that apply to a specific security protocol. The definition here relies on the security policy payload definition in [RFC3830].



* Next payload (8 bits):
  Identifies the payload that is added after
  this payload. See Section 6.1 of [RFC3830] for
  more details.

* Policy no (8 bits):
  Each security policy payload must be given a
  distinct number for the current MIKEY session by the
  local peer. This number is used to map a cryptographic session
  to a specific policy (see also Section 6.1.1 of [RFC3830]).

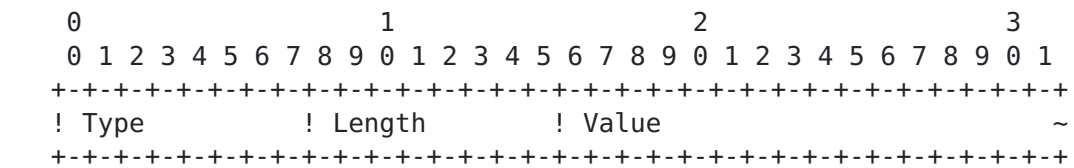
* Prot type (8 bits):
  This value defines the security protocol.
  A second value needs to be defined as shown below:

Prot type	Value
SRTP	0
TESLA	1

* Policy param length (16 bits):
  This field defines the total length of the
  policy parameters for the selected security protocol.

* Policy param (variable length):
  This field defines the policy for the specific
  security protocol.

The Policy param part is built up by a set of Type/Length/Value (TLV) payloads. For each security protocol, a set of possible type/value pairs can be negotiated as defined.



* Type (8 bits):
  Specifies the type of the parameter.

* Length (8 bits):
  Specifies the length of the Value field (in bytes).

* Value (variable length):
  Specifies the value of the parameter.

4.2 TESLA policy

This policy specifies the parameters for TESLA. The types/values that can be negotiated are defined by the following table. The concrete default values are taken from [I-D.ietf-msec-srtp-tesla], but other values may also be used:

Type	Meaning	Possible values
1	PRF identifier for f, realising F(x)	see below
2	Length of PRF f output	160
3	PRF identifier for f', realising F'(x)	see below
4	Length of PRF f' output	160
5	Identifier for the TESLA MAC	see below
6	Length of TESLA MAC output	80 (trunkened)
7	Start of session	in bytes
8	Interval duration T_int (in msec)	in bytes
9	Key disclosure delay d	in bytes
10	Key chain length (numer of intervals)	in bytes

For the PRF realising F(x), a one byte length is sufficient. The currently defined possible values are:

TESLA PRF F(x)	Value
NULL	0
HMAC-SHA1	1

For the PRF realising F'(x), a one byte length is enough.
The currently defined possible values are:

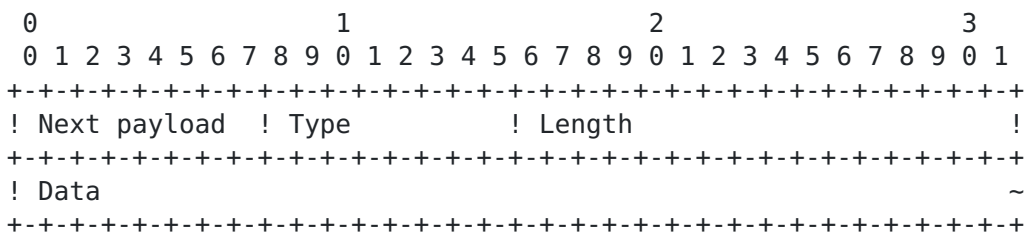
TESLA PRF F'(x)	Value
NULL	0
HMAC-SHA1	1

For the TESLA MAC, a one byte length is enough.
The currently defined possible values are:

TESLA MAC	Value
NULL	0
HMAC-SHA1	1

4.3 Key data transport within MIKEY's General Extension Payload

The General Extensions Payload was defined to allow possible extensions to MIKEY without the need for defining a completely new payload each time. This payload can be used in any MIKEY message and is part of the authenticated/signed data part.



* Next payload (8 bits):
  Identifies the payload following this payload.

* Type (8 bits):
  Identifies the type of general payload. MIKEY already defines the Values 0 and 1.
  This document introduces a new value (2).

Type	Value	Comments
Vendor ID	0	Vendor specific byte string
SDP IDs	1	List of SDP key mgmt IDs

TESLA I-Key | 2 | TESLA initial key

* Length (16 bits):
  The length in bytes of the Data field.

* Data (variable length):
  The general payload data.

5. Security Considerations

The security properties of multi-media data in a multicast environment depends on a number of building blocks.

SRTP-TESLA [I-D.ietf-msec-srtp-tesla] describes extensions for SRTP [RFC3711] in order to support TESLA [I-D.ietf-msec-tesla-intro] for source authentication in multicast scenarios. As such, security considerations described with TESLA (see [PCST] and [I-D.ietf-msec-tesla-intro]), the TESLA SRTP mapping [I-D.ietf-msec-srtp-tesla] and SRTP [RFC3711] itself are relevant in this context.

Furthermore, since this document details bootstrapping of TESLA using the Multimedia Internet Keying (MIKEY) [RFC3830] protocol the security considerations of MIKEY are immediately applicable to this document.

As mentioned in Section 1 the TESLA parameters described in Section 3 MUST be integrity protected and MAY be confidentiality protected. Integrity protection is necessary to avoid a man-in-the-middle adversary to modify parameters to mount a number of attacks. Confidentity protection, if desired, can be provided by a subset of the available MIKEY authentication and key exchange protocols, namely those providing public key encryption and symmetric key encryption. Without confidentiality protection an adversary might be able to learn the parameters later used to secure the end-to-end multi-media communication (if the adversary is located along the signaling path). This might be undesirable in high-security environments. Please note that the initial hash key, which is also one of the TESLA bootstrapping parameters, does not require confidentiality protection due to the properties of a hash chain. This aspect is described in great detail in the respective TESLA documents since hash chains represent a core concept of TESLA.

6. References

6.1 Normative References

[I-D.ietf-msec-srtp-tesla]
Baugher, M., "The Use of TESLA in SRTP", draft-ietf-msec-srtp-tesla-01 (work in progress), July 2004.

[I-D.ietf-msec-tesla-intro]
Perrig, A., Canetti, R., Song, D., Tygar, D. and B. Briscoe, "TESLA: Multicast Source Authentication Transform Introduction", draft-ietf-msec-tesla-intro-03 (work in progress), August 2004.

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

[RFC3830] Arkko, J., Carrara, E., Lindholm, F., Naslund, M. and K. Norrman, "MIKEY: Multimedia Internet KEYing", RFC 3830, August 2004.

6.2 Informative References

[I-D.ietf-msec-mikey-dhhmac]
Euchner, M., "HMAC-authenticated Diffie-Hellman for MIKEY", draft-ietf-msec-mikey-dhhmac-06 (work in progress), May 2004.

[PCST] Perrig, A., Canetti, R., Song, D. and D. Tygar, ""Efficient and Secure Source Authentication for Multicast", in Proc. of Network and Distributed System Security Symposium NDSS 2001, pp. 35-46", 2001.

[RFC3711] Baugher, M., McGrew, D., Naslund, M., Carrara, E. and K. Norrman, "The Secure Real-time Transport Protocol (SRTP)", RFC 3711, March 2004.

Authors' Addresses

Steffen Fries
Siemens
Otto-Hahn-Ring 6
Munich, Bayern 81739
Germany

EMail: steffen.fries@siemens.com

Hannes Tschofenig
Siemens
Otto-Hahn-Ring 6
Munich, Bayern 81739
Germany

EMail: Hannes.Tschofenig@siemens.com

Intellectual Property Statement

Disclaimer of Validity

Copyright Statement

Acknowledgment

Funding for the RFC Editor function is currently provided by the Internet Society.