

Internet Engineering Task Force
MSEC Working Group
INTERNET-DRAFT
EXPIRES: August 2005

Baugher (Cisco)
Carrara (Ericsson)

February 2005

The Use of TESLA in SRTP
<[draft-ietf-msec-srtp-tesla-03.txt](#)>

Status of this memo

By submitting this Internet-Draft, the authors certify that any applicable patent or other IPR claims of which I am (we are) aware have been disclosed, and any of which I (we) become aware will be disclosed, in accordance with [RFC 3668](#) ([BCP 79](#)).

By submitting this Internet-Draft, the authors accept the provisions of [Section 3 of RFC 3667](#) ([BCP 78](#)).

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 inappropriate to use Internet-Drafts as reference material or cite them other than as "work in progress".

The list of current Internet-Drafts can be accessed at <http://www.ietf.org/ietf/lid-abstracts.txt>

The list of Internet-Draft Shadow Directories can be accessed at <http://www.ietf.org/shadow.html>

Abstract

This memo describes the use of the Timed Efficient Stream loss-tolerant Authentication (TESLA) transform within the Secure Real-time Transport Protocol (SRTP), to provide data origin authentication for multicast and broadcast data streams.

TABLE OF CONTENTS

1.	Introduction.....	2
1.1.	Notational Conventions.....	3
2.	SRTP.....	3
3.	TESLA.....	4
4.	Usage of TESLA within SRTP.....	4
4.1.	The TESLA extension.....	4
4.2.	SRTP Packet Format.....	5
4.3.	Extension of the SRTP Cryptographic Context.....	7
4.4.	SRTP Processing.....	8
4.4.1	Sender Processing.....	8
4.4.2	Receiver Processing.....	9
4.5.	SRTCP Packet Format.....	10
4.6.	TESLA MAC.....	12
4.7.	PRFs.....	12
5.	TESLA Bootstrapping and Cleanup.....	13
6.	SRTP TESLA Default parameters.....	13
6.2	Transform-dependent Parameters for TESLA MAC.....	14
7.	Security Considerations.....	15
8.	IANA Considerations.....	15
9.	Acknowledgements.....	15
10.	Author's Addresses.....	15
11.	References.....	16

[1.](#) Introduction

Multicast and broadcast communications introduce some new security challenges compared to unicast communication. Many multicast and broadcast applications need "data origin authentication" (DOA), or "source authentication", in order to guarantee that a received message had originated from a given source, and was not manipulated during the transmission. In unicast communication, a pairwise security association between one sender and one receiver can provide data origin authentication using symmetric-key cryptography (such as a message authentication code, MAC). When the communication is strictly pairwise, the sender and receiver agree upon a key that is known only to them.

In groups, however, a key is shared among more than two members, and this symmetric-key approach does not guarantee data origin authentication. When there is a group security association [[gkmarch](#)] instead of a pairwise security association, any of the

members can alter the packet and impersonate any other member. The MAC in this case only guarantees that the packet was not manipulated by an attacker outside the group (and hence not in possession of the

group key), and that the packet was sent by a source within the group.

Some applications cannot tolerate source ambiguity and must discern the true sender from any other group member. A common way to solve the problem is by use of asymmetric cryptography, such as digital signatures. This method, unfortunately, suffers from high overhead, in terms of time (to sign and verify) and bandwidth (to convey the signature in the packet).

Several schemes have been proposed to provide efficient data origin authentication in multicast and broadcast scenarios. The Timed Efficient Stream loss-tolerant Authentication (TESLA) is one such scheme.

This memo specifies TESLA authentication for SRTP. SRTP TESLA can provide data origin authentication to RTP applications that use group security associations (such as multicast RTP applications) so long as receivers abide by the TESLA security invariants [[TESLA](#)].

[1.1](#). Notational Conventions

The keywords "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](#)].

This specification assumes the reader familiar with both SRTP and TESLA. Few of their details are explained in this document, and the reader can find them in their respective specifications, [[RFC3711](#)] and [[TESLA](#)]. This specification uses the same definitions as TESLA for common terms and assumes that the reader is familiar with the TESLA algorithms and protocols [[TESLA](#)].

[2](#). SRTP

The Secure Real-time Transport Protocol (SRTP) [[RFC3711](#)] is a

profile of RTP, which can provide confidentiality, message authentication, and replay protection to the RTP traffic and to the RTP control protocol, the Real-time Transport Control Protocol (RTCP). Note, the term "SRTP" may often be used to indicate SRTCP as well.

SRTP is a framework that allows new security functions and new transforms to be added. SRTP currently does not define any mechanism to provide data origin authentication for group security associations. Fortunately, it is straightforward to add TESLA to the SRTP cryptographic framework.

The TESLA extension to SRTP is defined in this specification, which assumes that the reader is familiar with the SRTP specification [[RFC3711](#)], its packet structure, and processing rules.

[3.](#) TESLA

TESLA provides delayed per-packet data authentication and is specified in [[TESLA](#)].

In addition to its SRTP data-packet definition given here, TESLA needs an initial synchronization protocol and initial bootstrapping procedure. The synchronization protocol allows the sender and the receiver to compare their clocks and determine an upper bound of the difference. The synchronization protocol is outside the scope of this document.

TESLA also requires an initial bootstrapping procedure to exchange needed parameters and the initial commitment to the key chain [[TESLA](#)]. For SRTP, it is assumed that the bootstrapping is performed out-of-band, possibly using the key management protocol that is exchanging the security parameters for SRTP, e.g. [GDOI, [RFC3830](#)]. Initial bootstrapping of TESLA is outside the scope of this document.

[4.](#) Usage of TESLA within SRTP

The present specification is an extension to the SRTP specification

[RFC3711] and describes the use of TESLA with only a single key chain and delayed-authentication [TESLA].

4.1. The TESLA extension

TESLA is an OPTIONAL authentication transform for SRTP. When used, TESLA adds the fields shown in Figure 1 per-packet. The fields added by TESLA are called "TESLA authentication extensions" altogether, whereas "authentication tag" or "integrity protection tag" indicate the normal SRTP integrity protection tag, when the SRTP master key is shared by more than two endpoints [RFC3711].

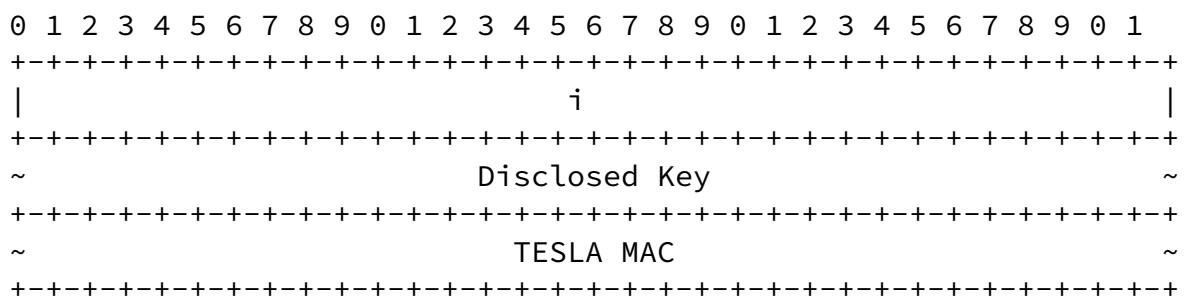


Figure 1: The "TESLA authentication extension".

i: 32 bit, MANDATORY

Identifier of the time interval i , corresponding to the key K_i that is used to calculate the TESLA MAC of the current packet (and other packets sent in the current time interval i).

Disclosed Key: variable length, MANDATORY

The disclosed key ($K_{(i-d)}$), that can be used to authenticate previous packets from earlier time intervals [TESLA].

a flag indicating the use of TESLA in SRTP. When this bit is set, the following TESLA transform-dependent parameters define the particular TESLA configuration (see [TESLA] for the TESLA-parameter definition).

Transform-dependent Parameters

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, see [Section 6.2](#) for the default value.
2. a non-negative integer n_p , 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), see [Section 6.2](#) for the default value.
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, see [Section 6.2](#) for the default value.
4. a non-negative integer n_f , determining the length of the output of F' , i.e. of the key for the TESLA MAC, see [Section 6.2](#) for the default value.
5. an identifier for the TESLA MAC, that accepts the output of $F'(x)$ as its key, e.g. to indicate HMAC-SHA1, see [Section 6.2](#) for the default value.
6. a non-negative integer n_m , determining the length of the output of the TESLA MAC, see [Section 6.2](#) for the default value.
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. the upper bound D_t (in sec) on the lag of the receiver clock relative to the sender clock (this quantity has to be

calculated by the peers out-of-band)

11. non-negative integer n_c , determining the length of the key chain, which is determined based upon the expected duration of the stream.
12. the initial key of the chain to which the sender has committed himself.

$F(x)$ is used to compute a keychain of keys in SRTP TESLA, as defined in [Section 6](#). Also according to TESLA, $F'(x)$ computes a TESLA MAC key with inputs as defined in [Section 6](#).

[Section 6](#) of this document defines the default values for the transform-independent and transform-specific TESLA parameters.

[4.4](#). SRTP Processing

The SRTP packet processing is described in [Section 3.3](#) of the SRTP specification [[RFC3711](#)]. The use of TESLA slightly changes the processing, as the SRTP MAC is checked upon packet arrival for DoS prevention, but the current packet is not TESLA-authenticated. Each packet is buffered until a subsequent packet discloses its TESLA key. The TESLA verification itself consists of some steps, such as tests of TESLA security invariants, that are described in [Section 3.5–3.7](#) of [[TESLA](#)]. The words "TESLA computation" and "TESLA verification" hereby imply all those steps, which are not all spelled out in the following. In particular, notice that the TESLA verification implies checking the safety condition (Section 3.5 of [[TESLA](#)]).

As pointed out in [[TESLA](#)], if the packet is deemed "unsafe", then the receiver considers the packet unauthenticated. It should discard unsafe packets but, at its own risk, it may choose to use them unverified. Hence, if the safe condition does not hold, it is RECOMMENDED to discard the packet and log the event.

[4.4.1](#) Sender Processing

The sender processing is as described in [Section 3.3 of \[RFC3711\]](#), up to step 5 included. After that the following process is followed:

6. When TESLA is applied, identify the key in the TESLA chain to be used in the current time interval, and the TESLA MAC key derived

from it. Execute the TESLA computation to obtain the TESLA authentication extension for the current packet, by appending the current interval identifier (as *i* field), the disclosed key of the chain for an earlier interval, and the TESLA MAC under the current key from the chain. This step uses the related TESLA parameters from the crypto context as for Step 4.

7. If the MKI indicator in the SRTP crypto context is set to one, append the MKI to the packet.

8. When TESLA is applied, and if the SRTP authentication (external tag) is required (for DoS), compute the authentication tag as described in step 7 of [Section 3.3](#) of the SRTP specification, but with coverage as defined in this specification (see [Section 4.6](#)).

9. If necessary, update the ROC (step 8 in [Section 3.3 of \[RFC3711\]](#)).

[4.4.2](#) Receiver Processing

The receiver processing is as described in [Section 3.3 of \[RFC3711\]](#), up to step 4 included.

To authenticate and replay-protect the current packet, the processing is the following:

First check if the packet has been replayed (as for [Section 3.3 of \[RFC3711\]](#)). Note however, the SRTP replay list contains SRTP indices of recently received packets that have been authenticated by TESLA (i.e. replay list updates MUST NOT be based on SRTP MAC). If the packet is judged to be replayed, then the packet MUST be discarded, and the event SHOULD be logged.

Next, perform verification of the SRTP integrity protection tag (note, not the TESLA MAC), if present, using the rollover counter from the current packet, the authentication algorithm indicated in the cryptographic context, and the session authentication key. If the verification is unsuccessful, the packet MUST be discarded from further processing and the event SHOULD be logged.

If the verification is successful, remove and store the MKI (if present) and authentication tag fields from the packet. The packet is buffered, awaiting disclosure of the TESLA key in a subsequent packet.

TESLA authentication is performed on a packet when the key is disclosed in a subsequent packet. When such key is disclosed,

perform the TESLA verification of the packet using the rollover

counter from the packet, the TESLA security parameters from the cryptographic context, and the disclosed key. If the verification is unsuccessful, the packet **MUST** be discarded from further processing and the event **SHOULD** be logged. If the TESLA verification is successful, remove the TESLA authentication extension from the packet.

To decrypt the current packet, the processing is the following:

Decrypt the Encrypted Portion of the packet, using the decryption algorithm indicated in the cryptographic context, the session encryption key and salt (if used) found in Step 4 with the index from Step 2.

(Note that the order of decryption and TESLA verification is not mandated. It is **RECOMMENDED** to perform the TESLA verification before decryption. TESLA application designers might choose to implement optimistic processing techniques such as notification of TESLA verification results after decryption or even after plaintext processing. Optimistic verification is beyond the scope of this document.)

Update the rollover counter and highest sequence number, `s_l`, in the cryptographic context, using the packet index estimated in Step 2. If replay protection is provided, also update the Replay List (i.e., the Replay List is updated after the TESLA authentication is successfully verified).

[4.5](#). SRTCP Packet Format

Figure 3 illustrates the format of the SRTCP packet when TESLA is applied. The TESLA authentication extension **SHALL** be inserted before the MKI and authentication tag. Recall from [\[RFC3711\]](#) that in SRTCP the MKI is **OPTIONAL**, while the E-bit, the SRTCP index, and the authentication tag are **MANDATORY**. This means that the SRTP (external) MAC is **MANDATORY** also when TESLA is used.

As in SRTP, the "Encrypted Portion" of an SRTCP packet consists of the encryption of the RTCP payload of the equivalent compound RTCP packet, from the first RTCP packet, i.e., from the ninth (9) octet

to the end of the compound packet.

The "Authenticated Portion" of an SRTCP packet consists of the entire equivalent (eventually compound) RTCP packet, the E flag, the SRTCP index (after any encryption has been applied to the payload), and the TESLA extension. Note that the definition is extended from [RFC3711] by the inclusion of the TESLA authentication extension.

Baugher, Carrara

[Page 10]

INTERNET-DRAFT

TESLA-SRTP

February 2005

We define the "TESLA Authenticated Portion" of an SRTCP packet as consisting of the RTCP header (first 8 bytes) and the Encrypted Portion of the SRTCP packet.

Processing of an SRTP packets is similar to the SRTP processing ([Section 4.3](#)), but there are SRTP-specific changes described in [Section 3.4](#) of the SRTP specification [[RFC3711](#)] and in [Section 4.6](#) of this memo.

[illegible]

- for SRTCP: Authenticated Portion (with the extended definition of SRTCP Authentication Portion as for [Section 4.2](#)).

The pre-defined authentication transform in SRTP, HMAC-SHA1 [[RFC2104](#)], is also used to generate the TESLA MAC. For SRTP (respectively SRTCP), the HMAC SHALL be applied to the key in the TESLA chain corresponding to a particular time interval, and M' as specified above. The HMAC output SHALL then be truncated to the n_m left-most bits. Default values are in [Section 6.2](#).

[4.7](#). PRFs

TESLA requires two pseudo-random functions (PRFs), f and f', to implement

- * one one-way function F(x) to derive the key chain, and
- * one one-way function F'(x) to derive (from each key of the chain) the key that is actually used to calculate the TESLA MAC.

When TESLA is used within SRTP, the default choice of the two PRFs SHALL be HMAC-SHA1. Default values are in [Section 6.2](#).

Other PRFs can be chosen, and their use SHALL follow the common guidelines in [[RFC3711](#)] when adding new security parameters.

[5](#). TESLA Bootstrapping and Cleanup

The extensions to the SRTP cryptographic context include a set of TESLA parameters that are listed in [section 4.3](#) of this document. Furthermore, TESLA MUST be bootstrapped at session set-up (for the parameter exchange and the initial key commitment) through a regular data authentication system (a digital signature algorithm is RECOMMENDED). Key management procedures can take care of this bootstrapping prior to the commencement of an SRTP session where TESLA authentication is used. The bootstrapping mechanism is out of scope for this document (it could for example be part of the key management protocol).

A critical factor for the security of TESLA is that the sender and receiver need to be loosely synchronized. TESLA requires a bound on

clock drift to be known (D_t). Use of TESLA in SRTP assumes that the time synchronization is guaranteed by out-of-band schemes (e.g. key management), i.e. it is not in the scope of SRTP.

It also should be noted that TESLA has some reliability requirements in that a key is disclosed for a packet in a subsequent packet, which can get lost. Since a key in a lost packet can be derived from a future packet, TESLA is robust to packet loss. This repetition might abruptly stop, however, if the key-bearing packets stop abruptly at the end of the stream. To avoid this nasty boundary condition, send null packets with TESLA keys for one entire interval following the interval in which the stream ceases.

[6.](#) SRTP TESLA Default parameters

Key management procedures establish SRTP TESLA operating parameters, which are listed in [section 4.3](#) of this document. The operating parameters appear in the SRTP cryptographic context and have the default values that are described in this section. In the future, an Internet RFC MAY define alternative settings for SRTP TESLA that are different than those specified here. In particular, it should be noted that the settings defined in this memo can have a large impact on bandwidth, as it adds 38 bytes to each packet (when the field length values are the default ones). For certain applications, this overhead may represent more than a 50% increase in packet size. Alternative settings might seek to reduce the number and length of various TESLA fields and outputs. No such optimizations are considered in this memo.

It is RECOMMENDED that the SRTP MAC be truncated to 32 bits since the SRTP MAC provides only group authentication and serves only as protection against external DoS.

[6.1](#) Transform-independent Parameters

The value of the flag indicating the use of TESLA in SRTP is by default zero (TESLA not used).

[6.2](#) Transform-dependent Parameters for TESLA MAC

The default values for the security parameters are listed in the following. "OWF" denotes a one-way function.

Parameter -----	Mandatory-to-support -----	Default -----
TESLA KEYCHAIN OWF ($F(x)$) OUTPUT LENGTH	HMAC-SHA1 160	HMAC-SHA1 160
TESLA MAC KEY OWF ($F'(F(x))$) OUTPUT LENGTH n_f	HMAC-SHA1 160	HMAC-SHA1 160
TESLA MAC (TRUNCATED) OUTPUT LENGTH n_m	HMAC-SHA1 80	HMAC-SHA1 80

As shown above, TESLA implementations MUST support HMAC-SHA1 for the TESLA MAC, the MAC key generator, and the TESLA keychain generator one-way function. The TESLA keychain generator is recursively defined as follows [[TESLA](#)].

$$K_i = \text{HMAC_SHA1}(K_{i+1}, 0), i=0..N-1$$

where $N-1=n_c$ from the cryptographic context.

The TESLA MAC key generator is defined as follows [[TESLA](#)].

$$K'_i = \text{HMAC_SHA1}(K_i, 1)$$

The TESLA MAC uses a truncated output of ten bytes [[RFC2104](#)] and is defined as follows.

$$\text{HMAC_SHA1}(K'_i, M')$$

where M' is as specified in [Section 4.6](#).

[7](#). Security Considerations

Denial of Service (DoS) attacks on delayed authentication are discussed in [[PCST](#)]. TESLA requires receiver buffering before

authentication, therefore the receiver can suffer a denial of service attack due to a flood of bogus packets. To address this problem, the external SRTP MAC, based on the group key, MAY be used in addition to the TESLA MAC. The short size of the SRTP MAC (default 32 bits) is here motivated by the fact that that MAC served purely for DoS prevention from attackers external to the group. [TESLA] describes other mechanisms that can be used to prevent DoS, in alternative to the external group-key MAC. Where these are used, they need to be add as processing steps (following the guidelines of [TESLA]).

The use of TESLA in SRTP defined in this specification is subject to the security considerations discussed in the SRTP specification [RFC3711] and in the TESLA specification [TESLA]. In particular, the TESLA security is dependent on the computation of the "safety condition" as defined in Section 3.5 of [TESLA].

SRTP TESLA depends on the effective security of the systems that perform bootstrapping (time synchronization) and key management. These systems are external to SRTP and are not considered in this specification.

[8](#). IANA Considerations

No IANA registration is required.

[9](#). Acknowledgements

The authors would like to thanks Ran Canetti, Karl Norrman, Mats N  slund, Fredrik Lindholm, David McGrew, and Bob Briscoe for their valuable help.

[10](#). Author's Addresses

Questions and comments should be directed to the authors and msec@ietf.org:

Mark Baugher
Cisco Systems, Inc.
5510 SW Orchid Street Phone: +1 408-853-4418

Portland, OR 97219 USA Email: mbaugher@cisco.com

Elisabetta Carrara

Ericsson Research

SE-16480 Stockholm

Sweden

Phone: +46 8 50877040

E-Mail: elisabetta.carrara@ericsson.com

11. References

Normative

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

[RFC1305] Mills D., Network Time Protocol (Version 3) Specification, Implementation and Analysis, [RFC 1305](#), March, 1992.

[RFC3711] Baugher, McGrew, Naslund, Carrara, Norrman, "The Secure Real-time Transport Protocol", [RFC 3711](#), March 2004.

[TESLA] Perrig, Canetti, Song, Tygar, Briscoe, "TESLA: Multicast Source Authentication Transform Introduction", December 2004, [draft-ietf-msec-tesla-intro-04.txt](#).

Informative

[gkmarch] Baugher, Canetti, Dondeti, Lindholm, "MSEC Group Key Management Architecture", June 2004, <[draft-ietf-msec-gkmarch-08.txt](#)>.

[GDOI] Baugher, Weis, Hardjono, Harney, "The Group Domain of Interpretation", [RFC 3547](#), July 2003.

[RFC3830] Arkko et al., "MIKEY: Multimedia Internet KEYing", December 2003, [RFC 3830](#), August 2004.

Copyright Notice

Copyright (C) The Internet Society (2004). This document is subject to the rights, licenses and restrictions contained in [BCP 78](#), and except as set forth therein, the authors retain all their rights.

Disclaimer of Validity

INTERNET-DRAFT

TESLA-SRTP

February 2005

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

This draft expires in August 2005.

