GDOI Key Establishment for SRTP

<http://tools.ietf.org/wg/msec/draft-baugher-msec-gdoi-srtp-00.txt>

Mark Baugher

Adrian-Ken Rüegsegger

Overview

- What is SRTP?
  - It is Secure RTP (RFC 3711).
  - What is RTP (RFC 3550, 3551) and how does SRTP secure it?
- What is GDOI?
  - It's RFC 3547, the ISAKMP Group "domain of interpretation"
  - What is ISAKMP (RFC 2408) and GDOI group key management?
- Why do GDOI-SRTP?
  - It is useful for multicast SRTP sessions, SRTP translators, etc.
  - What are the payloads and operational framework of GDOI-SRTP?

This work extends GDOI to establish an SRTP cryptographic context (GDOI "data security association") that is suitable for Secure RTP multicast sessions, translators, and other group-key applications.

What is SRTP?

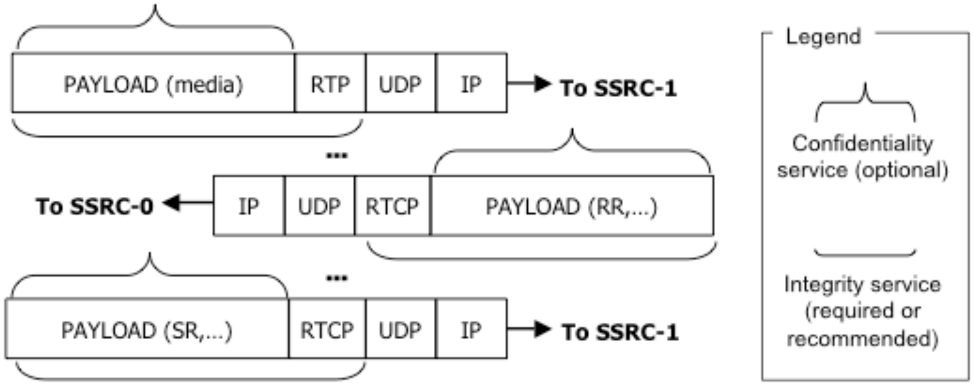
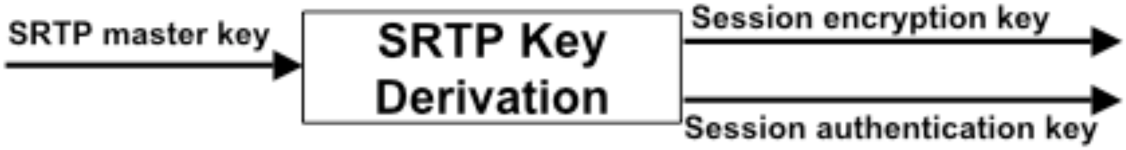


Figure: Packet flows between SSRCs of an RTP session

- SRTP provides confidentiality & integrity to RTP sessions
  - An RTP session carries RTP packets of media payloads from an SSRC
  - There should be a management back-channel of RTCP packets
  - RFC 3711 appends HMAC tag to packet for integrity service (not shown in Figure)
- Defaults to AES Counter Mode for confidentiality
  - REQUIRES: Unique SRTP master key per SSRC or a non-colliding SSRC

SRTP Key Management



- SRTP keys are derived from SRTP master key
  - Default lifetime is 2^48 packets for SRTP (2^31 for SRTCP)
  - Most secure configuration is one master key per sender (SSRC)
  - SSRCs to a session can share a key but SSRC collision is a risk
- At least a dozen SRTP parameters in session “crypto context”
  - Master key bound to CC by GDOI or EKT (see below)
  - SSRC can be bound by GDOI or first SRTP/SRTCP packet
  - RTP/SRTP SSRC & ROC also used in key management
- GDOI-SRTP establishes an SRTP crypto context using GDOI

What is GDOI?

```
+--------+                   +--------+
|  GDOI  |   GDOI with     +--------+ |
| GCKS & |<--------------->|  GDOI  | |
| Member |   SRTP payloads | Member |-+
+--------+                 +--------+
    ^                          ^
    |                          |
   API                        API
    |                          |
    V                          V
+--------+    SRTP/SRTCP   +--------+
|  SRTP  |---------------->|  SRTP  |
| Source |<----------------|Receiver|
+--------+      SRTCP      +--------+
```

- Establishes “group” keys
  - Uses IKE SA between member and GCKS
  - Has authenticated exchange for application keying
    - IPsec ESP done today
    - SRTP proposed here
- GDOI is a framework
  - Based on ISAKMP (RFC 2408)
  - Supports multiple “data security” protocols, e.g. IPsec, SRTP
- GDOI-SRTP extends GDOI for the SRTP data security protocol
  - Adds new payloads
  - Supports SRTP “Encrypted Key Transport” (EKT) protocol

GDOI-SRTP Payloads

```
 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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-!
!  SRC ID Type  !         SRC ID Port           !SRC ID Date Len!
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-!
!                    SRC Identification Data                    ~
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-!
! DST ID Type   !         DST ID Port           !DST ID Data Len!
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-!
!                    DST Identification Data                    ~
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-!
! Replay Window !     KD Rate   ! SRTP Lifetime ! SRTCP Lifetime!
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-!
!   Options     ! Crypto Suite  ! SPI Length    ! SPI (variable)~
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-!
~                          Attributes                           ~
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-!
```

Attribute Class	Value	Type
RESERVED	0	
SSRC	1	B
ROC	2	B
SEQ	3	B
MKI	4	V

- SA-TEK shown at left
  - RFC 3711 parameters
  - SRTP options & attributes
- Options field of SA-TEK
  - Unencrypted RTP
  - Unencrypted SRTCP
  - Unauthenticated SRTP
  - Encrypted key transport (EKT) is used
- If EKT is used
  - EKT SA-TEK follows
    - Not shown
  - EKT key is downloaded
- Else, an SRTP master key download payload follows

GDOI Signaling of EKT

- draft-mcgrew-srtp-ekt-01.txt
- Passes ROC and SRTP master key
  - Useful when GCKS is remote to SRTP sender
  - EKT is useful if firewalls block GDOI push operations
  - EKT fixes some problems in SIP forking and early media, but GDOI does not use and is not used by SIP at present
- ROC & SRTP master key encrypted with an EKT key
- GDOI-SRTP signals the EKT key
  - When EKT signaled, GDOI doesn’t download SRTP master key as the TEK
  - EKT is signaled by an EKT SA-TEK and a key-download payload carrying EKT key

Summary

- By design, GDOI (RFC 3547) supports new “data security protocols” such as SRTP
- We propose to do 3 things
  - Complete the GDOI-SRTP specification
  - Add it to Brian Weis’s GDOI reference code
  - Add it to David McGrew’s libSRTP
- Should this work be an msec WG item?

Acknowledgements

The authors wish to thank Brian Weis and David McGrew for their many suggestions for improvements and for helping us decide how to signal EKT. Brian also helped us better structure the SA-TEK payload.

Thank You