Best Effort SRTP

draft-kaplan-mmusic-best-effort-srtp-01

Hadriel Kaplan
hkaplan@acmepacket.com

François Audet
audet@nortel.com

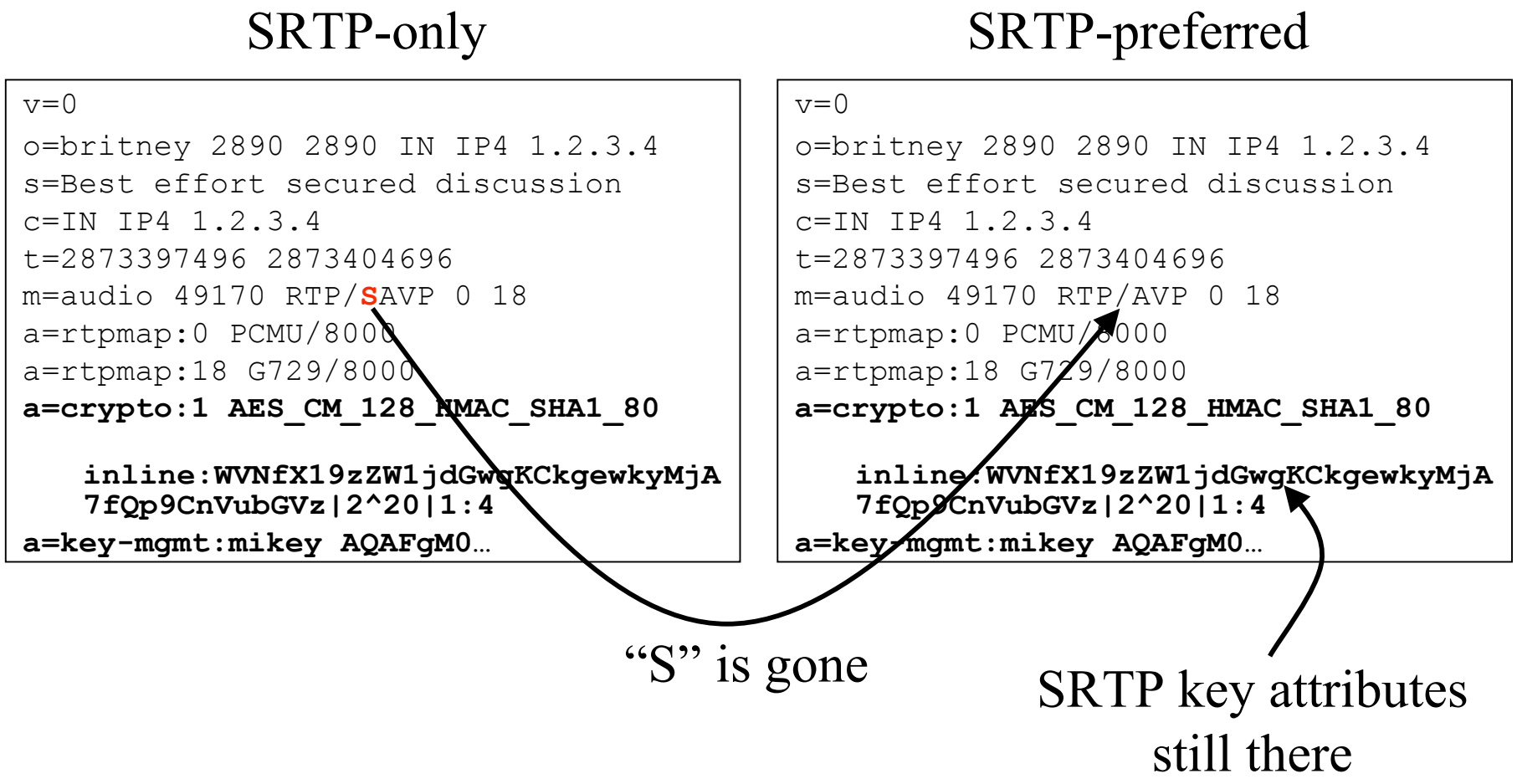
The Problem

- Current mechanism for SRTP key exchange in SDP offer is an all-or-nothing approach:
  - This call/media must be secure
  - This call/media must not be secure
- This is NOT how most people want to communicate – they want security if they can get it, but still want to talk otherwise
  - No one would even try an SAVP offer today unless they absolutely refused to talk otherwise

The Solution

- Don’t offer SAVP if you don’t demand it
  - SAVP means “only SRTP”
    - If you want that, do that
    - NOT encoding SAVP does not mean “Not SRTP”
- Make SRTP a preferred, optional attribute
  - Backwards compatible: legacy RTP UA’s ignore it
  - Tested 10 UA’s at SIPit: all ignored it

The Offer:
a HUGE change for SDP



The Answer:
Still no “S”

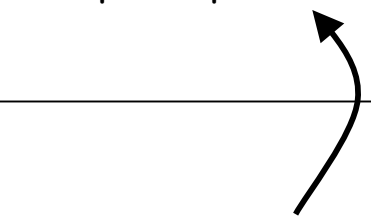
RTP

```
v=0
o=kevin 8675 8675 IN IP4 192.0.2.2
s=Open discussion
c=IN IP4 192.0.2.2
t=8675309 8675309
m=audio 54320 RTP/AVP 0
a=rtpmap:0 PCMU/8000
```

SRTP

```
v=0
o=kevin 8675 8675 IN IP4 192.0.2.2
s=Secret discussion
c=IN IP4 192.0.2.2
t=8675309 8675309
m=audio 54320 RTP/AVP 0
a=rtpmap:0 PCMU/8000
a=crypto:1 AES_CM_128_HMAC_SHA1_80

    inline:WVNfX19zZW1jdGwgKCkgewkyMjA
    7fQp9CnVubGVz|2^20|1:4
```



SRTP key attributes still there

More Problems

- Pre-answer SRTP media packets cannot be differentiated from RTP
  - Need to know so SRTP is not rendered as RTP
- Session-level MIKEY doesn't necessarily apply to all media streams
  - Some can be RTP, some SRTP, so need to know which is which

The Solution

- New “srtp” attribute
  - Says “I’m offering/answering SRTP”
- New “map” attribute value for srtp attribute
  - Maps payload-types from rtp to srtp
  - Says “For the following RTP PT’s, I will receive SRTP using these PT’s”
- Example:

```
m=audio 49170 RTP/AVP 0 18 101
a=srtp: map:0=96,18=97,101=102
```

Benefits

- SRTP can be offered to non-SRTP UA's without call failure
  - Works with legacy devices (even those nasty SBCs!)
- "Early" RTP media can be rendered, SRTP safely avoided
- RTP can be upgraded to SRTP cleanly, and SRTP keys can be refreshed
- No extra UDP ports
- Most importantly: it's easy to do, not a big change

Options/Questions

- Current proposal: too simple?
  - Do we add AVPF?
  - Do we mandate use of srtp attribute, even if it‘s not ambiguous?
  - Do we separate the payload mapping?
    - Does it have value beyond SRTP differentiation?
  - What do we do about pre-answer SRTCP?
    - Ignore it
    - Payload-map it
    - Register/standardize SRTCP payload types for SR/RR