An Opportunistic Approach for Secure Real-Time Transport Protocol (OSRTP)

draft-johnston-dispatch-osrtp-02

Alan Johnston <alan.b.johnston@gmail.com>
Bernard Aboba <bernard.aboba@gmail.com>
Andy Hutton <andrew.hutton@unify.com>
Laura Liess <laura.liess.dt@googlemail.com>
Thomas Stach <thomass.stach@gmail.com>

Opportunistic Security (OS)

- “Some Protection Most of the Time”
- Opportunistic Security (OS) is an approach to security that:
  - Defines a third mode for security between "cleartext" and "comprehensive protection”
  - Allows encryption and authentication to be used if supported but will not result in failures if it is not supported.
  - Is not a substitute for authenticated, encrypted communication policies
- Defined in RFC 7435

Approach

- Caller indicates support for OSRTP by offering SRTP attributes (can offer multiple keying methods) for an m= line but use AVP profile, not SAVP profile
- Called indicates usage of OSRTP by answering with SRTP attributes (only one) for an m= line, and again using AVP instead of SAVP
- Not specific to any SRTP keying method
  - DTLS-SRTP, SDP Security Descriptions, and ZRTP discussed
- Relaxes authentication requirements, but not confidentiality
- Example: SDP Security Descriptions still requires confidential signaling (TLS transport), but DTLS-SRTP does not require authenticated signaling

Example: Success

Offer

```
v=0
o=alice 2890844526 2890844526 IN IP4
    host.atlanta.example.com
s=
c=IN IP4 host.atlanta.example.com
t=0 0
m=audio 49170 RTP/AVP 0 8 97
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:97 iLBC/8000
a=fingerprint:sha-256
    77:6A:1F:E9:D4:F8:2A:97:3C:49:B5:F9
    :8D:52:10:62:89:C0:19:55:2C:48:3F:84
    :ED:A1:A1:7D:F4:EC:65:E7
```

Answer

```
v=0
o=bob 2808844564 2808844564 IN IP4
    host.biloxi.example.com
s=
c=IN IP4 host.biloxi.example.com
t=0 0
m=audio 49174 RTP/AVP 0
a=rtpmap:0 PCMU/8000
a=fingerprint:sha-256
    6A:1F:E9:D4:F8:2A:97:3C:49:B5:F9:8
    D:1A:52:10:62:
    89:C0:19:55:2C48:3F84:ED:A1:A1:7D:
    F4:EC:65:7E
```

OSRTP is used!

Example: Failure

Offer

```
v=0
o=alice 2890844526 2890844526 IN IP4
    host.atlanta.example.com
s=
c=IN IP4 host.atlanta.example.com
t=0 0
m=audio 49170 RTP/AVP 0 8 97
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:97 iLBC/8000
a=fingerprint:sha-256
    77:6A:1F:E9:D4:F8:2A:97:3C:49:B5:F9
    :8D:52:10:62:89:C0:19:55:2C:48:3F:84
    :ED:A1:A1:7D:F4:EC:65:E7
```

Answer

```
v=0
o=bob 2808844564 2808844564 IN IP4
    host.biloxi.example.com
s=
c=IN IP4 host.biloxi.example.com
t=0 0
m=audio 49174 RTP/AVP 0
a=rtpmap:0 PCMU/8000
```

OSRTP is not used!

Changes since -01

- Removed MIKEY key agreement
- Added Applicability Statement:
  - OSRTP is a transitional approach that provides a migration path from unencrypted communication (RTP) to fully encrypted communication (SRTP). It is only to be used in existing deployments which are attempting to transition to fully secure communications. New applications and new deployments will not use OSRTP.
- Mentioned capneg RFC 5939 (but said not used)

Open Issues

- Intended Status: Info or Stds Track?

Next Steps

- Adopt as SIPBRANDY WG item for Opportunistic SRTP milestone?
- Reviews?

Backup

From RFC 7435 on OS

“ With unauthenticated, encrypted communication, OS protocols may employ more liberal settings than would be best practice when security is mandated by policy. Some legacy systems support encryption, but implement only outdated algorithms or protocol versions. Compatibility with these systems avoids the need to resort to cleartext fallback.”