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

draft-johnston-dispatch-osrtp-01

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 from UTA WG

History of this Topic

- ZRTP introduced “Best Effort SRTP” in RFC 6189
- Requirements resonated with industry looking for transition path from all RTP to all SRTP
- draft-kaplan-mmusic-best-effort-srtp was first attempt to formalized it
- Many implementations today

Acknowledgement

- This work is dedicated to our friend and colleague Francois Audet who is greatly missed in our community. His work on improving security in SIP and RTP provided the foundation for this work.

Why Now?

- SIP Forum SIPconnect SIP trunking recommendation would like to add it
- IMTC "Best Practices for SIP Security” uses it
- Many vendors implement it
- Opportunistic Security now has respectibility
- The more Internet traffic is encrypted, the better
- It works

Why Not Just Publish draft-kaplan-mmusic-best-effort-srtp ?

- Draft has lots of motivation and arguments for “Best Effort Security” that is not needed today
- “Best Effort Security” approach is slightly different from Opportunistic Security as defined in RFC 7435.
  - OS relaxes authentication requirement
  - OS has specific UI recommendations
- The draft does not discuss more recent keying such as DTLS-SRTP
- The -01 version has a mechanism for a unique payload type for SRTP that no one likes or uses
- However, we could publish it as informational/historic

Approach

- A new draft that is short and concise and fully aligned with OS
- No new attributes or elements defined
- Simply a different way to use existing, applying principles of OS
- Specifically:
  - 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

Approach Continued

- Not specific to any SRTP keying method
  - 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:F
    9:8D:52:10:62:89:C0:19:55:2C:48:3F:8
    4: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:F
    9:8D:52:10:62:89:C0:19:55:2C:48:3F:8
    4: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!

Charter Text 1/4

Charter for Opportunistic Security for RTP Working Group (OSRTP)

Real-time voice and video communication using RTP is widely used over the Internet today, and much of it is negotiated using SIP and SDP offer/answer. Secure media transport negotiated using SIP and SDP with the secure profile of RTP, SRTP, is unfortunately not widely deployed today for voice and video communication. One reason for this is the difficulty in negotiating the use of SRTP. SDP offer/answer was not originally designed to negotiate profiles of RTP, and extensions such as SDP Capability Negotiation, RFC 5939, have not achieved enough deployment to be useful for negotiating secure media. Without extensions, a caller needs to decide in advance that secure media is used, but if chosen in advance and the called party does not support it, the session will fail. This presents a serious barrier to incremental deployment of secure media

Charter Text 2/4

Opportunistic Security (OS), defined in RFC 7435, is an approach to security that defines a third mode for security between "cleartext" and "comprehensive protection" that allows encryption and authentication to be used if supported but will not result in failures if it is not supported. An opportunistic approach for secure media would allow SRTP to be used if the called party support the opportunistic approach, but will fall back to RTP if the called party does not. This will allow SRTP to be incrementally introduced in voice and video communication networks during the transition from no encryption to always-on encryption.

Charter Text 3/4

WG Objectives

This WG will work on a solution for Opportunistic SRTP (OSRTP) that does not require SDP Capability Negotiation, but instead will be based on currently deployed techniques in many voice and video systems that use SDP offers that do not specify a secure profile, but instead use AVP and the presence of SRTP keying SDP attributes in the SDP offer and answer to negotiate secure media. The approach will be general enough to work with a variety of SRTP key agreement protocols including, but not limited to SDP Security Descriptions, DTLS-SRTP, and ZRTP.

It is important to note that OSRTP makes no changes, and has no effect on media sessions in which the offer contains a secure profile of RTP, such as SAVP. Also, approaches that always require secure media, such as RTCWEB, will never utilize OSRTP.

As allowed by Opportunistic Security, some authentication requirements of SRTP key agreement approaches will be relaxed. However, confidentiality requirements will not be relaxed.

Charter Text 4/4

The working group will perform the following work:

1. Define the goals and requirements of an Opportunistic Security approach for RTP
2. Define a specification for OSRTP.

Non Goals

This work will not define any new extensions to SIP or SDP, but it may make changes in some offer/answer procedures or authentication requirements of key agreement protocols. No changes to SRTP or RTP will be made.

Collaboration

The working group may coordinate with SIPCORE, MMUSIC and AVTCORE as needed.

Input to the WG

draft-johnston-dispatch-osrtp (a starting point for the goals and requirements and protocol)

draft-kaplan-mmusic-best-effort-srtp-00 (for historical reasons and background)

Needed Next Steps

- Don’t need to do requirements, design, etc
- But, could use some thorough security reviews

Path Forward

- Who is interested in the topic?
- Who would like to work on/review?
- Hopefully we don’t need to actually form a WG...