SDP Security Descriptions is NOT RECOMMENDED and Historic

draft-mattsson-dispatch-sdes-dont-dont-dont

IETF 111, DISPATCH, John Preuß Mattsson, Magnus Westerlund

SDES has many known security weaknesses…

- Security Descriptions is vulnerable to SSRC collisions, which leads to so called "two-time pad" [RFC7201].
  - Worse than using a 32-bit MAC, as "two-time pad" may lead to loss of both confidentiality and integrity.
  - In addition to happening by itself with a non-negligible probability, the SSRC collision attack can also be triggered by an attacker in different ways. See e.g. [Replay-SDES].

- As Security Descriptions use plaintext keys [RFC7201], the keys often end up in logs and data retention systems. These systems are often accessible by many more user accounts than Lawful Interception (LI) systems.

- As explained in [Baiting-SDES] the model of slitting the security between two independent layers is flawed, is vulnerable to the Baiting attack [I-D.kaplan-sip-baiting-attack], and "This situation leads to security vulnerability and attacker could get master key by spoofing in unencrypted path."

- Security Descriptions [RFC4568] requires use of an encapsulating data-security protocol on each hop in the path giving at best hop-by-hop security. Several deployed systems are known to use Security Descriptions without any encapsulating data-security protocol to protect the SDP messages. A huge problem with SDP Security Descriptions is that the endpoints have no way of verifying if the path is protected or not.

SDES has many known security weaknesses…

- If the encapsulating data-security protocol without Diffie-Hellman is used, access to long-term keys enables attackers to compromise past and future sessions. Entities can get access to (and have gotten access to) long-term key material in many different ways: physical attacks, hacking, software bugs, social engineering attacks, espionage, weaknesses injected in hardware, software, or standards, buying access, or demanding access to keying material with or without a court order.

- The situation is maybe best summarized by [Hacking-SDES] that writes: **"the false sense of security might be more dangerous than simply leaving your voice calls unencrypted."**

- New systems and recommendations like WebRTC [RFC8827], PERC [RFC8871], and [RFC8862] do mandate support of DTLS-SRTP [RFC5764]. WebRTC forbids support of SDP Security Descriptions: "WebRTC implementations MUST NOT offer SDP security descriptions [RFC4568] or select it if offered."

- Using DTLS-SRTP with an ephemeral Diffie-Hellman key exchange (DHE or ECDHE) forces attackers to perform dynamic key exfiltration instead of static key exfiltration [RFC7624]. As required by [RFC7258], work on IETF protocols needs to consider the effects of pervasive monitoring and mitigate them when possible.

The question is not if SDES should be phased out but how

- The security level SDP Security Description provide is not on the level expected by an IETF in force proposed standard and there exist alternatives.

- Many implementations, devices, and libraries support DTLS-SRTP.

- Current draft suggestion:

> This document reclassifies [RFC4568] (SDP Security Descriptions) to Historic Status and also obsoletes RFC 4568.
>
> This document updates [RFC7201] (Options for Securing RTP Sessions) to note that SDP Security Descriptions SHOULD NOT be used.
>
> This document specifies that use of the SDP Security Descriptions [RFC4568] is NOT RECOMMENDED. Existing deployments SHOULD mandate support of DTLS-SRTP [RFC5764] and long-term phase out use of SDP Security Descriptions. If it is known by out-of-band means that the other party supports DTLS-SRTP, then SDP Security Descriptions MUST NOT be offered or accepted. If it is not known if the other party supports DTLS-SRTP, both DTLS-SRTP and SDP Security Descriptions SHOULD be offered during a transition period. New deployments SHOULD forbid support of Security Descriptions [RFC4568].

- **Should this be handled in MMUSIC WG or somewhere else?**