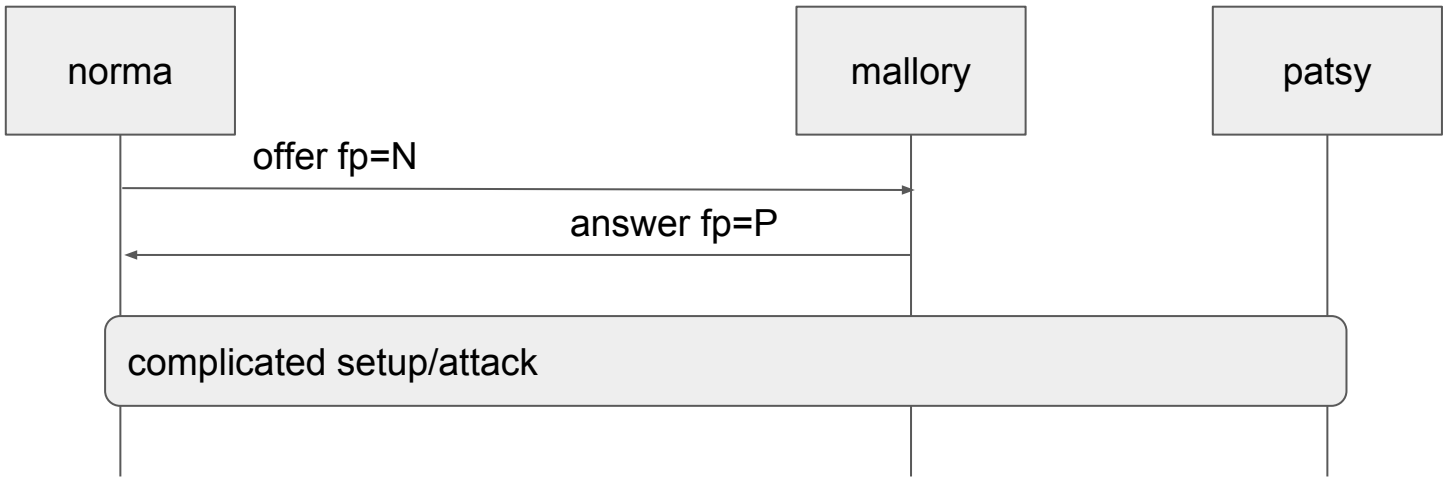
sdp uks

IETF 98

Synopsis

a=fingerprint isn't enough to guarantee that the participants in a call are correct

An attacker can switch their a=fingerprint attribute with another



norma is talking to patsy
but believes she is talking to mallory

Solution

Bind the connection establishment to the SDP

Obvious solution: add the a=dtls-id attribute to the handshake

- this is unique to the SDP, and acts as an identity

Problem: we have both TLS and DTLS connections

- a=dtls-id only applies to DTLS
- this potentially affects draft-ietf-mmusic-dtls-sdp

Choices

Option 1: define a=tls-id for TLS/TCP

+ unambiguous
- two things means that protocols need to switch (see PERC)

Option 2: rename a=dtls-id to a=tls-id

+ just one identifier
- Roman points out that a=dtls-id has a semantic that when applied to TLS would overlap with a=connection

Option 3: use sess-id from o= line as in -00

+ no dependency on dtls-sdp
- kinda kludgy, only 63 bits of entropy