Datagram TLS Secure RTP (DTLS-SRTP) Key Transport

draft-wing-avt-dtls-srtp-key-transport-00

Dan Wing, dwing@cisco.com

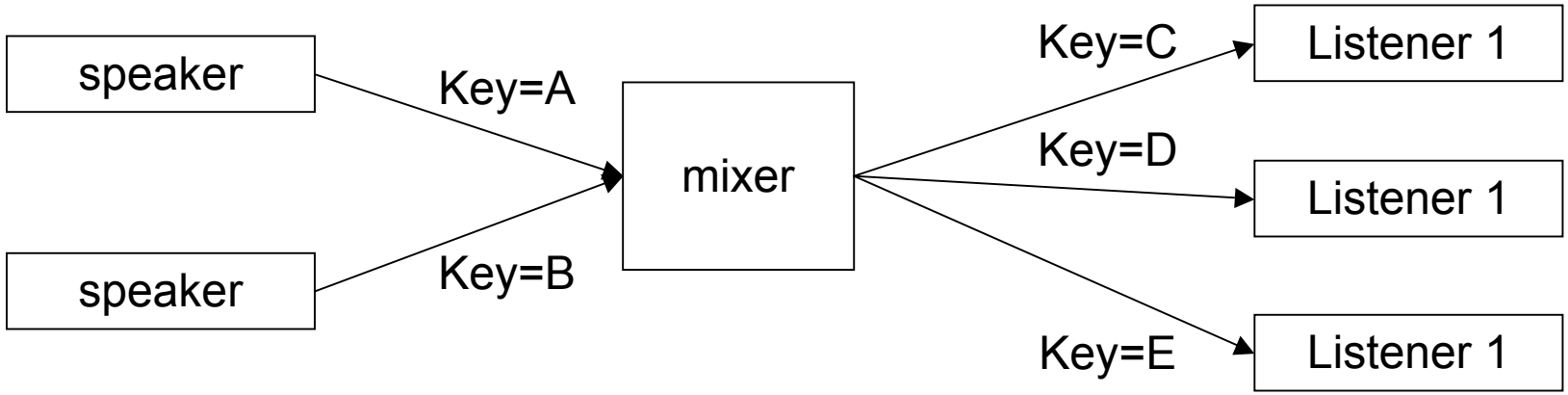
Overview

- In Prague, IETF selected DTLS-SRTP as the preferred SRTP keying mechanism
- Unicast, point-to-point was in scope

- This proposal extends DTLS-SRTP to work efficiently with unicast, point-to-multipoint

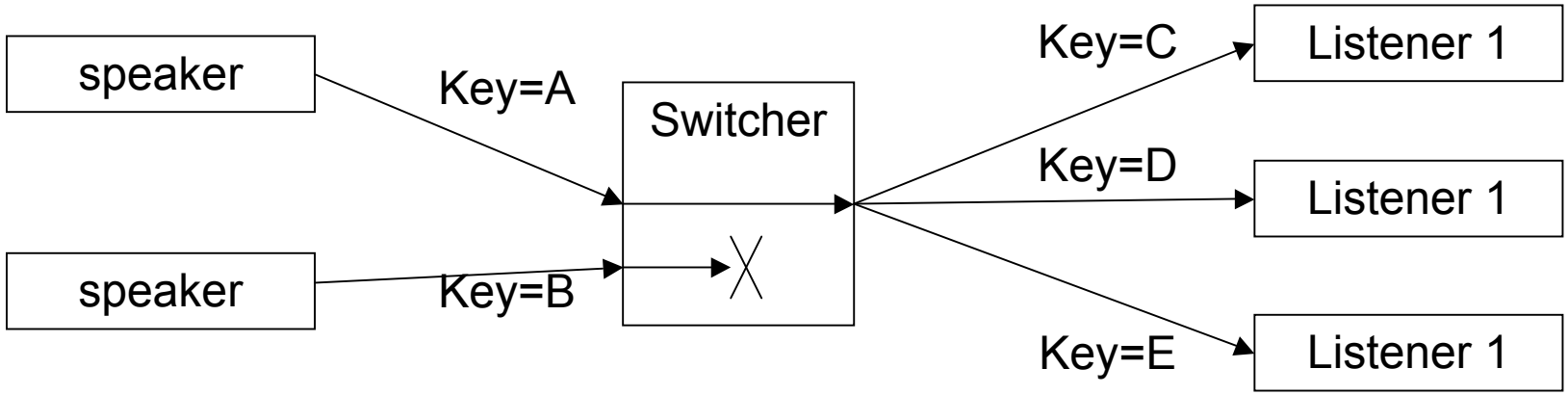
Problem 1: Mixers

- DTLS-SRTP requires unique, per-listener encryption



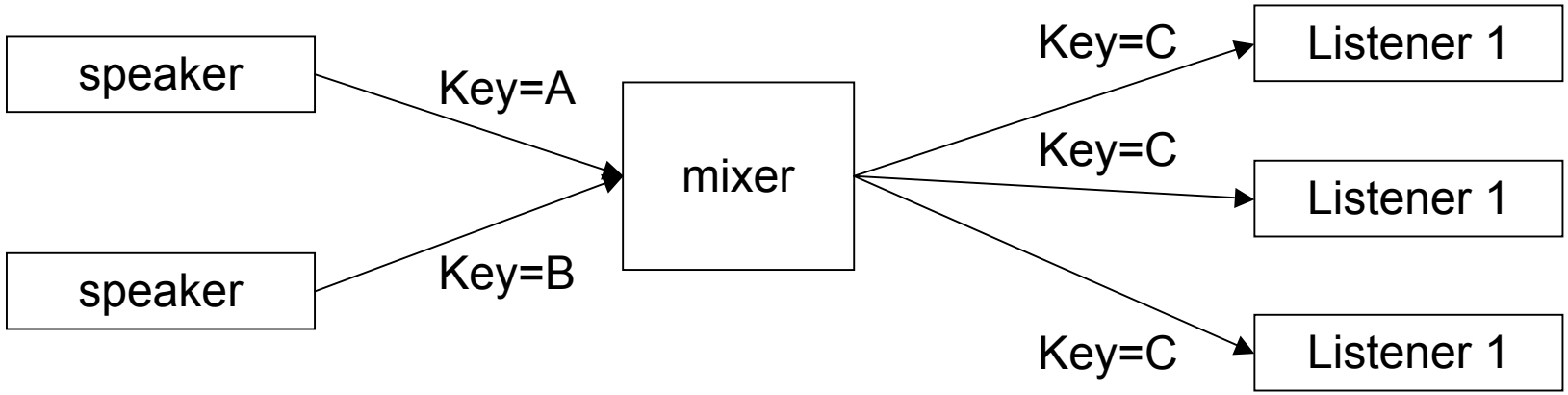
Problem 2: Video Switchers

- DTLS-SRTP requires unique, per-listener encryption



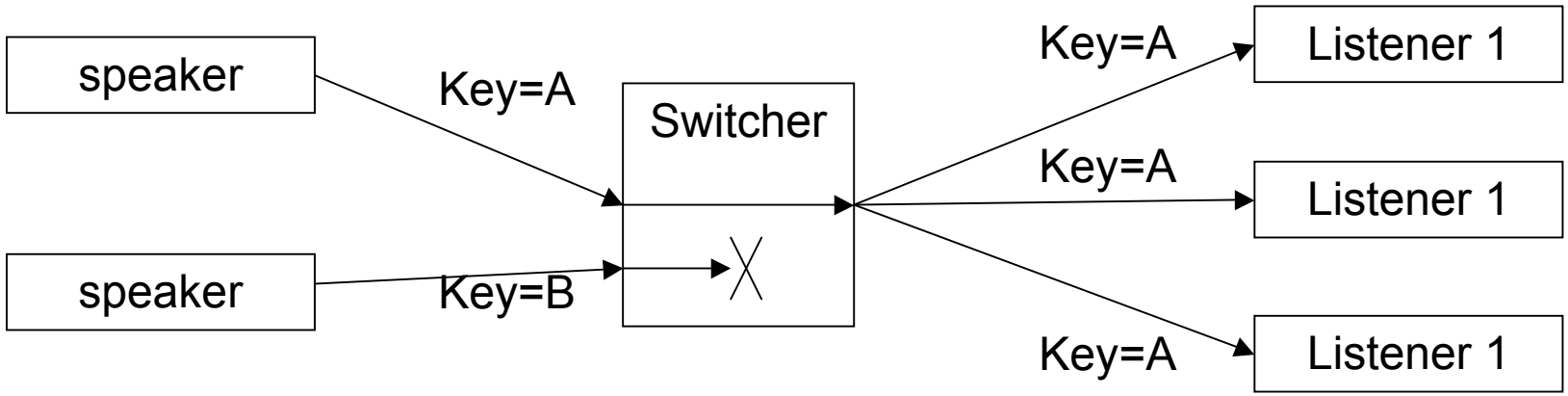
Proposed Solution for Mixers

- Transport one SRTP key, inside of the per-listener DTLS session, to legitimate listeners



Proposed Solution for Video Switchers

- Transport speaker's key to listeners



Requirements

- When listeners change (add/join), SRTP key MUST change
  - For mixers, mixer knows how to do this
  - For video switchers, sender needs to be instructed to rekey
- This is supported in the current draft

Going Forward

- Is there interest in efficiently doing DTLS-SRTP keying with media mixers? With video switchers?

- Eric Rescorla suggested this may be useful for TLS (not just DTLS-SRTP)

Questions

draft-wing-avt-dtls-srtp-key-transport-00

Dan Wing, dwing@cisco.com