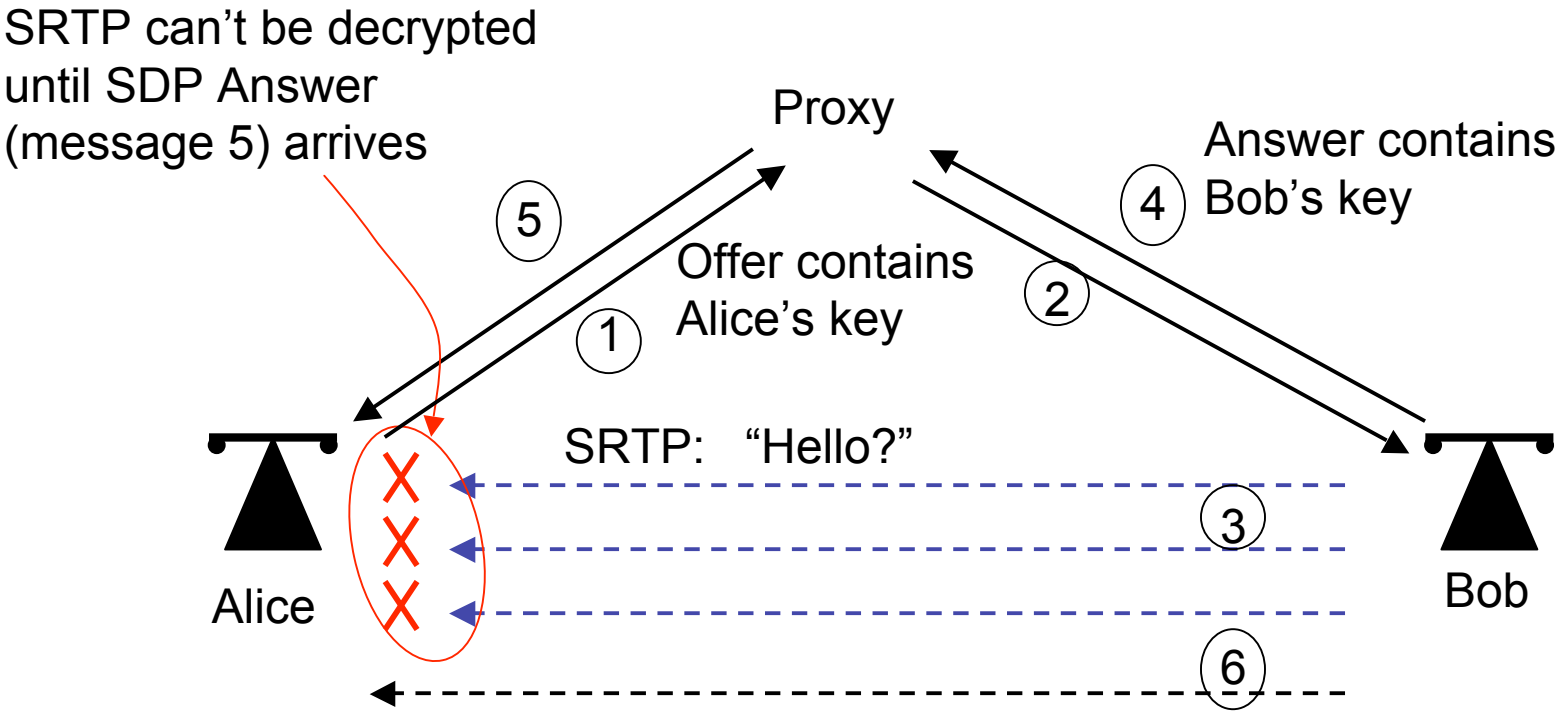
Early Media for Security Descriptions

sdes-early-media-00

Rob Raymond, rob@counterpath.com
Dan Wing, dwing@cisco.com
IETF MMUSIC, November 9, 2005

Early Media Difficulties with Security Descriptions



Media arrives before Answer

Media clipping causes poor user experience

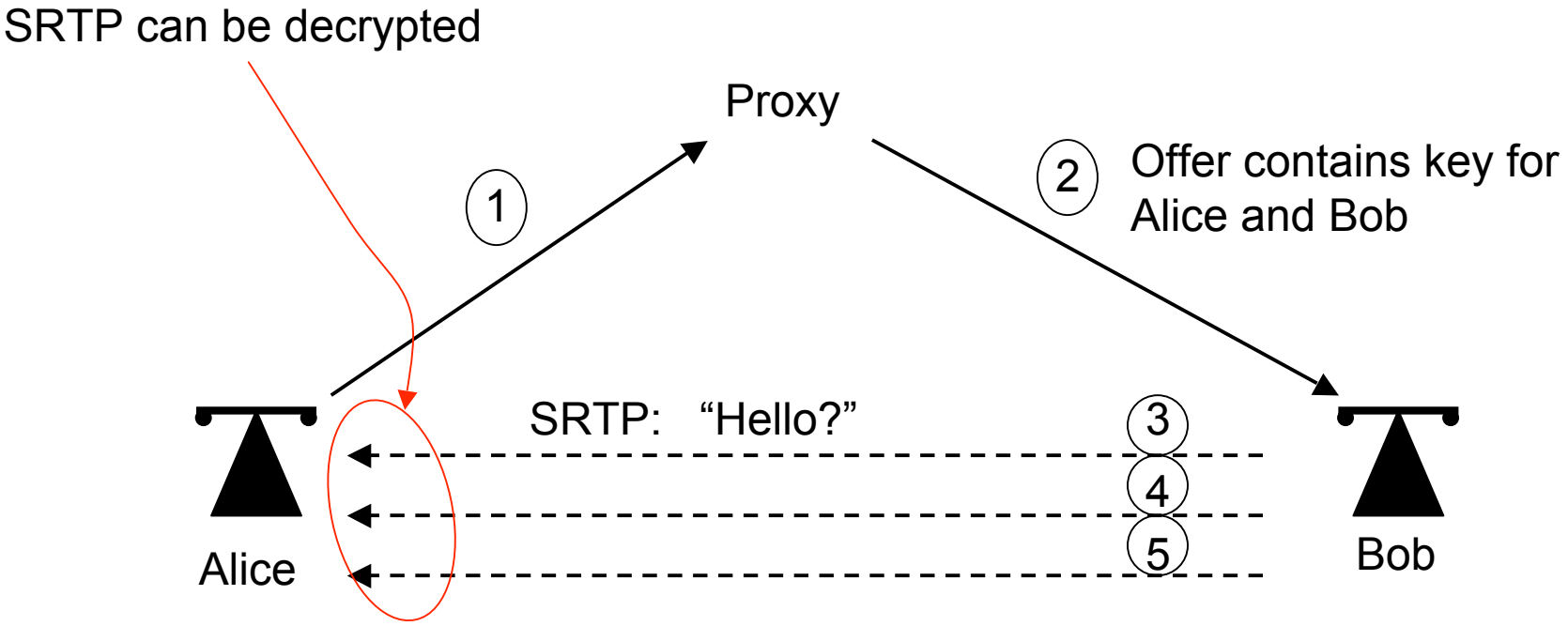
Why not use Security Preconditions?

- Additional call setup time in SIP ‘just for’ security
- Implementation feedback: too complex

Proposed Mechanism

- Calling party requests called party use a specific key initially
  - If called party understands and accepts, early media can be decrypted
- Doesn’t require PRACK or preconditions

Proposed Mechanism



"Hello" can be decrypted by Alice

Bob uses his own key when ….
(see next slide)

Proposed Additions to -01

- Called party changes to its own selected key after answer is received (see next slide)
- MKI indicates requested key is being used, and MKI isn’t used thereafter

Bob starts using his own key when:

- Bob receives SRTP from Alice
- Bob receives SRTCP from Alice
- Bob receives re-INVITE from Alice
- Bob receives SIP ACK
- Bob times out waiting for above
  - Timer H (ACK receipt) = 32 seconds
- ICE being received

Considerations

- Early media forking
  - Each branch uses same requested key
    - 2-time pad issues
    - Example:
      - “Welcome to FedEx” might be unsecured
      - Sending your PIN is secured, and answerer immediately rekeys on receipt of SRTP
  - Each branch knows keys in both directions
- Retargeting
  - Each target knows keys in both directions
- Requested key only used for early media
  - Thus maintains same properties as sdescriptions

Conclusion

- Provides SRTP early media with little additional complexity
- Accept as WG item?