SDP Format for BFCP

draft-ietf-mmusic-sdp-bfcp-00.txt

Gonzalo.Camarillo@ericsson.com

Key Distribution and Crypto Algorithm Selection

- Shared secret between client and server needed for digest authentication
- BFCP allows servers to challenge clients to provide a nonce
- BFCP may support more hashing algorithms than HMAC-SHA1 in the future
  - We will build support for algorithm selection in BFCP

Security Descriptions

- Optimization
  - Avoid an initial challenge from the server
  - SDP offer/answer can provide the client with
    - Initial nonce
    - Supported crypto algorithms
  - Include nonce and crypto algorithms in SDP
    - SDP Security Descriptions
    - Use the SDP crypto attribute

Server Selection

- Peer-to-peer scenarios
  - Who is the server?
- Clarify that the server is the one providing the conference ID and the user ID
- What about having two servers?
  - Two ‘m’ lines
- Server authentication?
  - Peers will not typically have server certificates