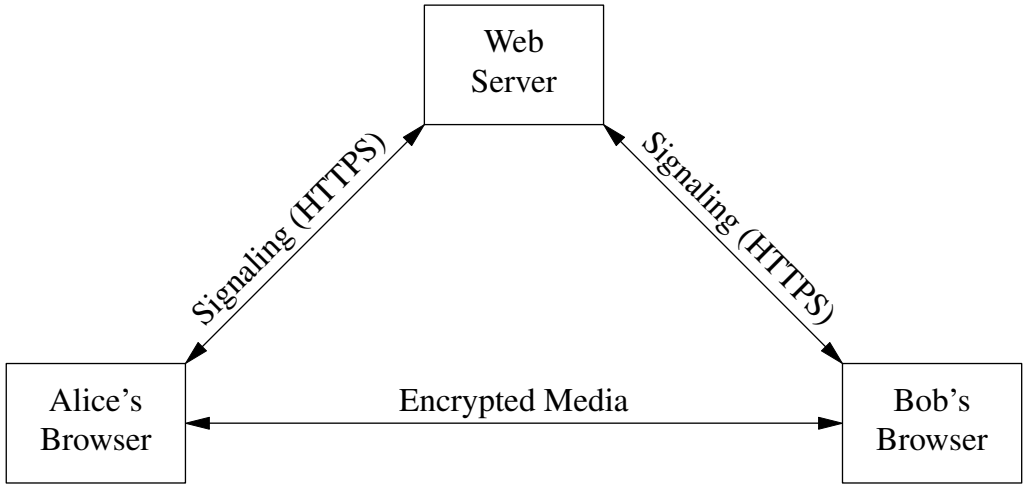
Key Management Options

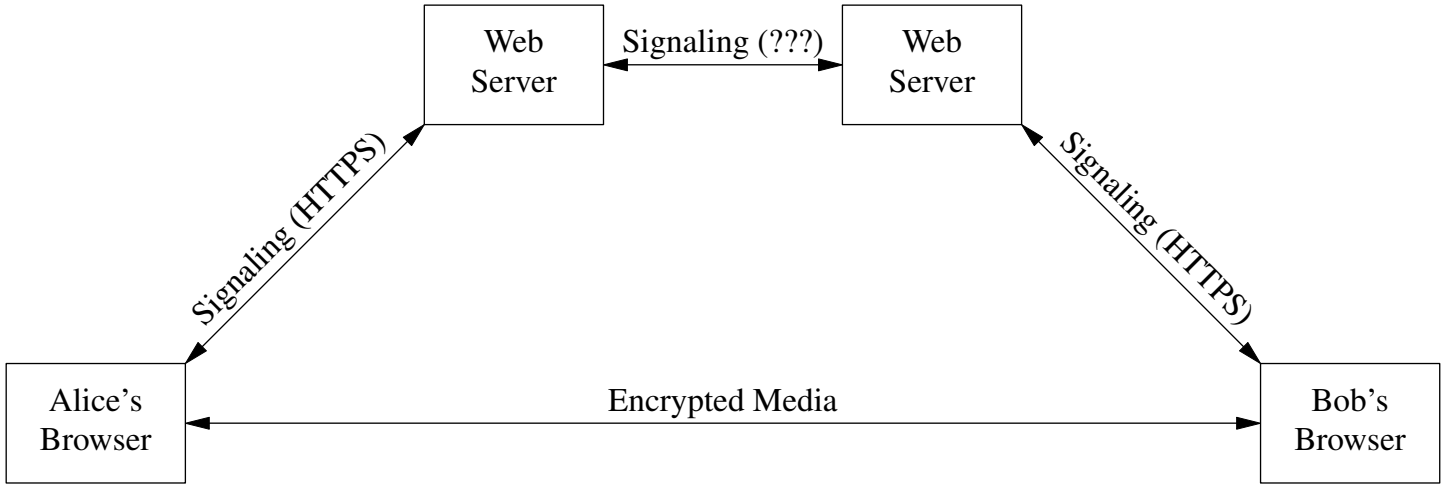
RTW Workshop

ekr@skype.net

Setting (same site)



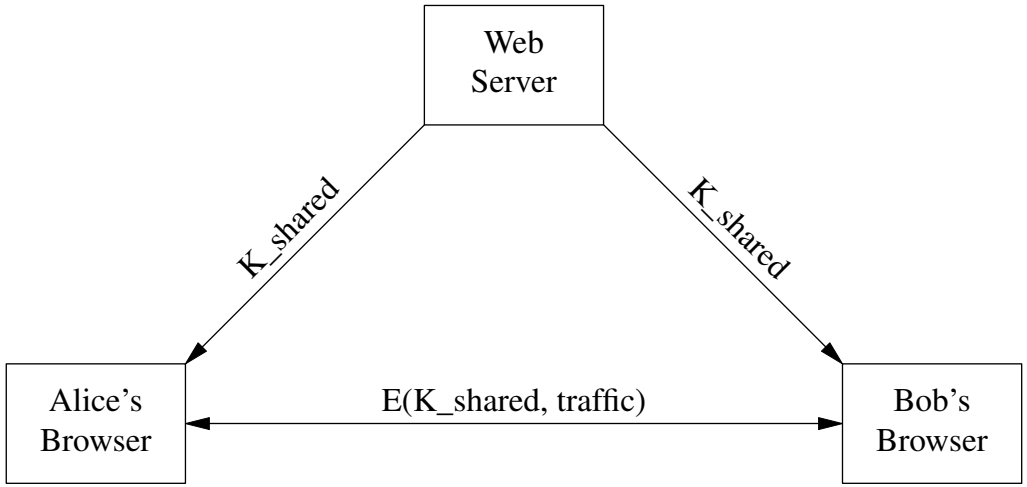
Setting (different sites)



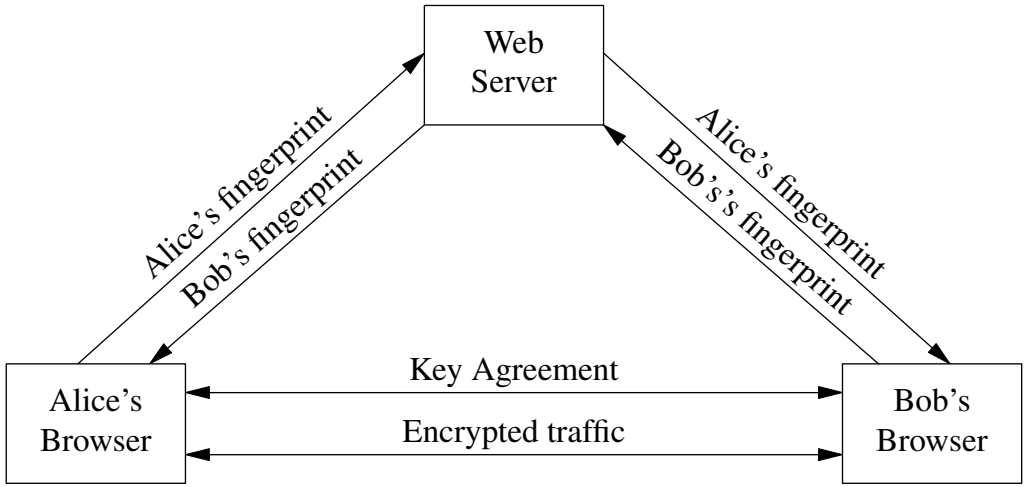
Basic Options

- Server generates keys ("SDES")
  - If more than one server, servers somehow agree upon keys
  - Clients just use distributed keys directly to encrypt traffic
- End-to-end key establishment ("DTLS-SRTP")
  - Clients do a public-key based key exchange
  - Endpoints authenticated via the signaling protocol

Server-Generated Keys



End-to-End Key Establishment



Merits of Server Key Distribution

- Advantages
  - Simplicity/ease of implementation
  - Compatibility with legacy endpoints which do SDES (not clear how many)
  - Easy monitoring
- Disadvantages
  - Far less secure (server logs, traffic sniffing, ...)
  - No support for non-multimedia traffic

Merits of End-to-End Key Establishment

- Advantages
  - Security (isn't that the point of the exercise?)
    - Perfect forward secrecy
    - Harder to accidentally reveal keying material
  - Flexibility
    - Support for non-RTP traffic
  - Natural interlock with traffic permissions "intentionality" checks
- Disadvantages
  - Modestly more complexity
    - But browsers already have TLS stacks
  - More effort required for monitoring

What about multicast/conference bridges?

- Same traffic is sent to multiple receivers (not clear how often that happens)
  - Annoying to reencrypt for each recipient
  - Solution is use the same key for everyone
- Easy to do with server key distribution
- Straightforward solutions with end-to-end key establishment
  - First establish pairwise keys
  - Focus pushes the shared key to everyone over the pairwise channels