
# Use of VBR audio with SRTP

draft-perkins-avt-srtp-vbr-audio-02.txt

Colin Perkins

# Use of VBR audio with SRTP

- Research has shown that spoken phrases can be identified in encrypted VBR audio SRTP sessions by observing packet lengths
  - For *some* VBR audio codecs, and *some* phrases

Wright *et al*, “Spot me if you can: Uncovering spoken phrases in encrypted VoIP conversations”, IEEE Security & Privacy Symposium, May 2008. http://tinyurl.com/yjs9ox3

- This is *potentially* a security risk
  - As a result, draft-zimmermann-avt-zrtp-15 says it “is RECOMMENDED that VBR codecs be avoided” in the context of ZRTP calls
  - A similar recommendation is in draft-perkins-avt-srtp-vbr-audio-02.txt for regular SRTP, since the problem is not ZRTP specific
- Should AVT be making such a recommendation?
  - If so, is draft-perkins-avt-srtp-vbr-audio-02.txt an appropriate starting point?