SRTP Security Issues

- Current profile has unusual design features
  - AES Counter Mode
  - Choice of MACs
    - HMAC-SHA
    - 32 bit HMAC-SHA
    - None!
- These don’t make sec guys comfortable

Why do things this way?

- Latency
  - Shorter packets mean less latency
    - For voice
  - MACs consume bandwidth
  - So do IVs
- Errors
  - Wireless channels are often noisy
  - With integrity bit errors mean total packet loss

What's the problem?

- Counter mode has no integrity protection
  - Easy to make predictable changes
  - Especially if you have known plaintext
  - Very desirable to have a MAC
- But the MAC is optional
  - And the standard MAC is weak
- The threat
  - Modified message streams
  - Forged traffic
  - Big problem for other kinds of media

Option 1: FEC

- FEC after encrypting/MACing
  - Then reconstruct before verifying
  - This isn’t perfect
    - Expands the packet somewhat
    - Won’t fix all bit errors
    - (There is a tradeoff here)
  - But we don’t have numbers for the impact

Option 2: Two Sets of Transforms

- Partial integrity--for wireless voice
  - Mandatory integrity protection over the control data only
  - Larger packet sizes
    - Same bandwidth and latency as full-packet integrity
  - But less sensitive to damage
    - How sensitive depends on message size
- Full integrity -- for everything else
  - An 80-bit MAC should be fine
    - The spec says 128
  - This should be the default

AD Bottom Line

- Spec revision
  - Current transform made optional
    - Tied to wireless voice (AMR/AMR-WB?)
  - New transform definitions (default)
- Timeframe?