Cryptographic Algorithm Implementation Requirements and Usage Guidance for ESP and AH

draft-ietf-ipsecme-esp-ah-reqts-00

Presented by Brian Weis
Overview

• Based on future draft-mcgrew-ipsecme-esp-ah-reqts-00

• Incorporates feedback from WG
  – Triple-DES now a MAY (instead of SHOULD NOT)
  – HMAC-MD5 now ignored (instead of a SHOULD NOT)
  – MAY algorithms only listed if they were previously SHOULD, SHOULD+, or MUST
What’s new in the draft

• Adds a section discussing algorithm diversity
  – Cites new work on the selection of future cryptographic standards

• More secure rationale
  – Cites publication showing insecurity of 64-bit block ciphers (e.g. Triple-DES) used to encrypt more than a gigabyte of data
Next Steps

• Please review and send feedback to WG and authors