(Not All) Active Internet-Drafts

- draft-ietf-ipsec-doc-roadmap-01.txt
- draft-ietf-ipsec-arch-sec-01.txt
- draft-ietf-ipsec-auth-header-01.txt
- draft-ietf-ipsec-esp-v2-00.txt
- draft-ietf-ipsec-ipsec-doi-03.txt
- draft-ietf-ipsec-isakmp-08.txt
- draft-ietf-ipsec-isakmp-oakley-04.txt
- draft-ietf-ipsec-oakley-02.txt
- draft-ietf-ipsec-revised-enc-mode-01.txt
- draft-ietf-ipsec-inline-isakmp-01.txt
- draft-ietf-ipsec-vpn-00.txt
- draft-ietf-ipsec-cbc-00.txt
- draft-ietf-ipsec-ciph-3des-expiv-00.txt
- draft-ietf-ipsec-ciph-arcfour-00.txt
- draft-ietf-ipsec-ciph-blowfish-cbc-00.txt
- draft-ietf-ipsec-ciph-cast-div-00.txt
- draft-ietf-ipsec-ciph-cast128-cbc-00.txt
- draft-ietf-ipsec-ciph-des-derived-00.txt
- draft-ietf-ipsec-ciph-des-expiv-00.txt
- draft-ietf-ipsec-ciph-des3-00.txt
- draft-ietf-ipsec-ciph-desx-00.txt
- draft-ietf-ipsec-ciph-idea-cbc-00.txt
- draft-ietf-ipsec-ciph-rc5-cbc-00.txt

(We have a lot of them)

Active Internet-Drafts

- draft-ietf-ipsec-doc-roadmap-01.txt
  - IP Security Document Roadmap
  - R. Thayer, R. Glenn, July 1997
- draft-ietf-ipsec-arch-sec-01.txt
  - Security Architecture for the Internet Protocol
  - S. Kent, July 30, 1997 (Not yet in I-D)

Active I-D's, II

- draft-ietf-ipsec-auth-header-01.txt
  - IP Authentication Header
  - S. Kent, R. Atkinson, July 21, 1997
- draft-ietf-ipsec-esp-v2-00.txt
  - IP Encapsulating Security Payload (ESP)
  - S. Kent, R. Atkinson, July 21, 1997

Active I-D's, III

- draft-ietf-ipsec-isakmp-08.txt
  - D. Maughan, M. Schertler, M. Schneider, J. Turner, July 26, 1997
  - Internet Security Association and Key Management Protocol (ISAKMP)
- draft-ietf-ipsec-ipsec-doi-03.txt
  - The Internet IP Security Domain of Interpretation for ISAKMP
  - D. Piper, July 30, 1997 (not yet in I-D)

Active I-D's, IV

- draft-ietf-ipsec-oakley-02.txt
  - The OAKLEY Key Determination Protocol
  - H. K. Orman
- draft-ietf-ipsec-isakmp-oakley-04.txt
  - The resolution of ISAKMP with Oakley
  - D. Harkins, D. Carrel, July 1997

Active I-D's, V

- draft-ietf-ipsec-revised-enc-mode-01.txt
  – A revised encryption mode for ISAKMP/Oakley
  – R. Canetti, P. Cheng, H. Krawczyk, July 1997
- draft-ietf-ipsec-inline-isakmp-01.txt
  – Inline Keying within the ISAKMP Framework
  – B. Sommerfeld, March 1997

Active I-D’s, VI

- draft-ietf-ipsec-vpn-00.txt (WILL BE REPLACED)
  - Implementation of Virtual Private Network (VPNs) with IP Secrity
  - N. Doraswamy, March 12, 1997

Encryption Algorithms

- draft-ietf-ipsec-ciph-des-expiv-00.txt
  - The ESP DES-CBC Cipher Algorithm With Explicit IV
  - C. Madson, N. Doraswamy, July 1997
- draft-ietf-ipsec-ciph-des-derived-00.txt
  - The ESP DES-CBC Transform
  - P. Metzger, W. Simpson, July 1997

Encryption Algorithms, II

- draft-ietf-ipsec-ciph-3des-expiv-00.txt
  - The ESP 3DES-CBC Algorithm Using an Explicit IV
  - R. Pereira, R. Thayer, July 17, 1997
- draft-ietf-ipsec-ciph-des3-00.txt
  - The ESP Triple DES Transform
  - N. Doraswamy, P. Metzger, W. Simpson, July 1997

Encryption Algorithms, III

- draft-ietf-ipsec-ciph-cast-div-00.txt
  - The ESP CAST5-128-CBC Transform
  - W. Simpson, July 1997
- draft-ietf-ipsec-ciph-cast128-cbc-00.txt
  - The ESP CAST128-CBC Algorithm
  - R. Pereira, G. Carter, July 2, 1997

Encryption Algorithms, IV

- draft-ietf-ipsec-ciph-arcfour-00.txt
  - The ESP ARCFOUR Algorithm
  - R. Thayer
- draft-ietf-ipsec-ciph-rc5-cbc-00.txt
  - The ESP RC5-CBC Algorithm
  - Roy Pereira, R. Baldwin, July 2, 1997

Encryption Algorithms, V

- draft-ietf-ipsec-ciph-blowfish-cbc-00.txt
  - The ESP Blowfish-CBC Algorithm Using an Explicit IV
  - R. Adams, June 23, 1997
- draft-ietf-ipsec-ciph-desx-00.txt
  - The ESP DES-XEX3-CBC Transform
  - W. Simpson, R. Baldwin, July 1997

Encryption Algorithms, VI

- draft-ietf-ipsec-ciph-idea-cbc-00.txt
  - The ESP IDEA-CBC Algorithm Using Explicit IV
  - R. Adams, June 23, 1997
- draft-ietf-ipsec-cbc-00.txt
  - ESP with Cipher Block Chaining (CBC)
  - W. Simpson, July 1997

Message Authentication Code Specs

- draft-ietf-ipsec-auth-hmac-sha196-00.txt
  - The Use of HMAC-SHA-1-96 within ESP and AH
  - C. Madson, R. Glenn, July 1997
- draft-ietf-ipsec-hmac-md5-96-00.txt
  - The Use of HMAC-MD5-96 within ESP and AH
  - C. Madson, R. Glenn, July 1997

MAC Specs, II

- draft-bitan-auth-des-mac-00.txt
  - The Use of DES-MAC within ESP and AH
  - S. Bitan, D. Frommer, July 1997

Obsolete Drafts

- draft-ietf-ipsec-ah-hmac-md5-96-00.txt
- draft-ietf-ipsec-ah-hmac-sha-04.txt
- draft-ietf-ipsec-ah-hmac-sha-1-96-00.txt

Observations

- We have too many documents
- For the top-level documents
  - To rework them would require too much work
  - We want to get these documents out!
  - Current editors have done a lot of work already

Observations, II

- Do we need all the encryption algorithm and MAC documents?
  - What do we do with them? Options are:
    - Drop some. (Eliminate all with predictable IV)
    - Publish as experimental
    - Publish as proposed
      - with expectation that w/o implementations, we drop them at the next stage and move them to historic

Requests to the wg

- Please read the I-D's
  - Especially the top-level documents
- Concentrate on the big picture
  - Don't sweat the small stuff.
  - Make sure we have a conherent, implemental set of specs.
  - Publish them ASAP!