We really *DO NOT* need SHA-256 for Message Authentication.

Open Letter to IPSec WG and SAAG

Russell Dietz, Doug Whiting, et. al…
rdietz@hifn.com, dwhiting@hifn.com

Open Security Area Directorate

54th IETF –

Yokohama, Kanagawa-Ken, Japan

Disclaimer…

I am NOT a cryptologist! I rely on some of the folks listed below for their abilities in the 'science'.

I DO implement/design 'security protocols', etc…

(Please don't shoot the messenger… TOO many times…)

- Doug Whiting, dwhiting@hifn.com
- David McGrew, mcgrew@cisco.com
- Dave Wagner, daw@cs.berkeley.edu
- Russ Housely, rhousley@rsdsecurity.com
- Niels Ferguson, niels@ferguson.net
- Thomas Hardjono, thardjono@verisign.com
- Scott Fluhrer, fluhrer@cisco.com
- Jesse Walker, jesse.walker@intel.com
- Mike Sabin, mike.sadin@worldnet.att.net
- John Kelsey, kelsey.j@ix.netcom.com

Basic issues in the letter

- HMAC-SHA1-96 (SHA-1) works as implemented and is ‘known’
- HMAC-SHA-256-128 (SHA-256) provides NO additional security over SHA-1
- SHA-256 has LIMITED time in service, ‘could’ find issues..
- Misleading statements in the draft (-00)

Misleading statements…

- SHA-256 has larger block size
  - Nope… Both are 512 bits
- SHA-256, less frequent re-keying
  - Nope… with neither 32 or 64 bit seq. #s
    - Are keys truly random? (more bits) [Uri]
- SHA-256, ‘stand up’ against attacks
  - Nope… not at 96 bits… if 128 then SHA-1!

Issues from FIPS 180-2

- SHA-1 (80 bits) vs. SHA-256 (128 bits)
  - Figure 1, page 3
  - Conclusion could be… AES-128 = SHA-256!
  - Nope… Hash collisions in a DS scheme
- SHA-256 helps in Key Exchange…
  - Match larger DH Security Strength
  - However… Message authentication… different attack model

Conclusions of the letter

- The inaccurate claims discussed above should be corrected or removed. (~-01)
- The document should be re-worked to clarify the fact that SHA1 is perfectly adequate, according to current knowledge. (-01)
- The resulting transform should be qualified as optional-to-implement, not mandatory (~-01)
- The draft should make clear under what circumstances the transform is an option worth pursuing (e.g. if SHA-1 is broken by advances in cryptanalysis, but SHA-256 is not) (pending)

Closing Requests…

- HMAC-SHA1-96 is a MUST in RFC2406
  - Legacy LIVES forever…
  - Works with AES…
  - No clear performance benefit in SHA-256
  - Implementation cost… DOWN
- Move to Experimental or Informational
  - Even –01 does not eliminate all confusion
  - Until it is required, SHA-256 not needed

We really *DO NOT* need SHA-256 for Message Authentication.

Open Letter to IPSec WG and SAAG

Russell Dietz, Doug Whiting, et. al…
rdietz@hifn.com, dwhiting@hifn.com

Open Security Area Directorate

54th IETF –

Yokohama, Kanagawa-Ken, Japan