Version as of 11:51 AM, June 13, 2002

The purpose of this letter is to comment on an existing Internet Draft, draft-ietf-ipsec-ciph-sha-256-00.txt, dated Nov 2001, co-authored by S. Frankel and S. Kelley. This draft, hereafter referred to as DRAFT-SHA-256 for brevity, defines how to use the new SHA-256 algorithm from NIST (FIPS 180-2) for packet authentication within the ESP and AH mechanisms of IPSec.

Our basic argument here is that, while the new SHA-256 algorithm is definitely useful in other contexts, in fact there is no evidence that DRAFT-SHA-256 provides any meaningful additional cryptographic security over the HMAC-SHA-1-96 algorithm defined in RFC2406 and already in widespread use for packet authentication in IPSec. For all we know, quite the contrary may be true, as SHA-256 is a new transform and thus has seen considerably less public review so far than SHA1 has already received. In any case, it is extremely unlikely that HMAC-SHA1 will be the weak point in any system using IPSec. Hence, it is not clear that trying to improve its security makes any sense, given the costs and instability associated with such a change.

Unfortunately, the current draft is misleading in this regard:

> "Using the SHA-256 block cipher, with its increased block size (512 bits) and increased hash length (256 bits), provides the new algorithm with the ability to withstand continuing advances in crypto-analytic techniques and computational capability. It also allows less frequent re-keying, which is useful for high-speed networks and high-volume applications."

It is our belief that, as currently defined in DRAFT-SHA-256, the use of SHA-256 does not achieve any of these stated goals.

First of all, the block size of SHA-256 (512 bits) is identical to that of SHA-1, so the first assertion in the quote above is simply false, although frankly it would have no relevance if true. Second, there is no known reason why DRAFT-SHA-256 would in fact allow less frequent rekeying, using either 32-bit or 64-bit sequence numbers. Finally, and most importantly, while it is true that SHA-256 can output 256 bits, in the current draft the HMAC-SHA-256 output is in fact truncated to 96 bits, as is HMAC-SHA-1 in RFC2406. For the HMAC-SHA-1-96 and DRAFT-SHA-256 algorithms, there is every reason to believe that the limiting factor in security is the number of bits of hash included in the packet, not the length before truncation. The best attacks known on HMAC-SHA-1-96 and DRAFT-SHA-256 depend only on the length after truncation, not the length before truncation. Hence, the HMAC-SHA-1-96 and DRAFT-SHA-256 have equivalent security against known attacks, and there seems to be little reason to prefer either one over the other, from a cryptographic perspective. For any given number of output bits, up to the SHA-1 limit of 160 bits, this would continue to be the case. If it was desired to have a MAC value longer than 160 bits, then the use of SHA-256 would likely be appropriate, but there is no apparent need for such a MAC tag length, according to current knowledge.

It is possible that the draft was initiated from a fundamental misunderstanding of Figure 1 (page 3) of the NIST draft FIPS 180-2. This figure states that the "security" of SHA-1 is 80 bits, while the "security" of SHA-256 is 128 bits. A naive reading of this figure would thus lead one to conclude that only SHA-256 is appropriate for use with AES-128. However, the figure in question deals with the strength of the hash functions against collisions as part of a digital signature scheme. It is likely that the use of SHA-256 is very appropriate for the digital signatures used in the certificates of the IKE exchange used to generate AES-128 and HMAC-SHA-1-96 keys for ESP and AH. This is in fact the application for which SHA-256 was designed.

However, while Figure 1 in FIPS 180-2 is correct for digital signatures, it has no direct relevance to the issue of packet authentication in ESP and AH as addressed in DRAFT-SHA-256. Packet authentication has a completely different attack model. In particular, there is no known feasible "birthday attack" problem in the packet authentication context, as has been shown by Krawczyk and others (e.g., "Keying Hash Functions for Message Authentication" by Bellare, Canetti, and Krawczyk, Crypto '96).

Since HMAC-SHA1-96 (RFC2406) is already a "MUST" for IPSec compliance, all IPSec implementations, hardware or software, already have it and must continue to support it for many years to come. Any possible argument that somehow SHA-256 can replace SHA-1 to save hardware cost is thus extremely ill-founded. In fact, quite the opposite is true: adding DRAFT-SHA-256 as an IPSec option will only increase hardware cost, with no accompanying security benefit.

We expect that if the WG approved DRAFT-SHA-256, it would be optional rather than mandatory. However, there would be a strong risk that vendors and their customers might feel compelled to use it out of a misunderstanding of the cryptographic issues. Already we have heard potential customers asking for support for DRAFT-SHA-256, with the rationale being, "if IETF approves it, it must be good".

Our purpose in submitting this letter is to make sure that the IPSec working group has a reasonable understanding of the issues involved in DRAFT-SHA-256. If the WG decides to approve the draft, we strongly suggest that, at a bare minimum,

a) the inaccurate claims discussed above should be corrected or removed,
b) the document should be re-worked to clarify the fact that SHA1 is perfectly adequate, according to current knowledge,
c) the resulting transform should be qualified as optional-to-implement, not mandatory, and
d) 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)

However, given that there is no known cryptographic benefit to implementing this proposed standard, we respectfully submit that the IPSec WG should not approve this draft.

Doug Whiting, Hifn
David McGrew, Cisco
Dave Wagner, UC Berkeley
Russ Housely, RSA Labs
Niels Ferguson, MacFergus BV
Thomas Hardjono, Verisign
Scott Fluhrer, Cisco
Jesse Walker, Intel
Mike Sabin, Independent Consultant