Further Comments on Keyed MD5

by Bart Preneel and Paul C. van Oorschot.

This note follows on the excellent overview by Burt Kaliski and Matt Robshaw ("Message authentication with MD5," *CryptoBytes* vol.1 no.1) in which three schemes are recommended to the IPSEC working group. Citing forthcoming work, it was suggested the best attack (forgery) on these schemes required 2^{64} chosen message texts ("... except when the known messages are all the same length and end with the same suffix").

We have improved this attack in our recent paper[1] "MDx-MAC and building fast MACs from hash functions," *Proc. Crypto'95*. A generic attack is given requiring 2^{64} known text-MAC pairs and a single chosen text, independent of message lengths or suffixes – only for the second recommended scheme we need the messages to be of the same length. (Perhaps more significantly, the attack applied to CBC-MAC requires only 2^{32} known text-MAC pairs for MAC forgery.) The attack requires an additional 2^{64} *chosen* text-MAC pairs if only 64 bits of the hash result are retained; this suggests modifying the method to retain only 64 bits, which also saves bandwidth. The number of text-MAC pairs required can be further reduced if the known messages contain a common (not necessarily chosen) sequence of trailing blocks. The attack also applies if messages are fixed-length or prepended by length fields.

Adapting the same attack strategy allows a divide-and-conquer attack if the envelope method is used with distinct front and tail keys, effectively reducing security to the larger of the two. We also provide analysis of the secret prefix and secret suffix methods, and add here that the secret suffix method is subject to an off-line, memoryless, parallelizable attack requiring 2^{64} operations and a single chosen text (P. van Oorschot and M. Wiener, ACM-CCS'94, Fairfax).

Recent partial attacks on MD4, MD5, and the related RIPEMD, including in particular those of S. Vaudenay (Leuven Algorithms Workshop Dec.'94) and H. Dobbertin (Rump Session, Eurocrypt'95), suggest these functions are susceptible to manipulations of their internal structures. This raises concerns about hash-based MACs being susceptible to attacks exploiting properties of the underlying hash. We therefore advise caution in constructing such MACs, and recommend a design more conservative than the envelope method. We agree customized MACs may be preferable, but

[1] Available by FTP {ftp.esat.kuleuven.ac.be, directory pub/COSIC/preneel}.

are reluctant to discard the experience gained over time with MD4 and MD5.

With exquisite timing, our paper already (as submitted Feb. '95) makes a proposal in line with most of the suggestions of Kaliski and Robshaw: MD5-MAC, a customized MAC involving key processing at every compression function step, and built with only minor modifications from MD5 (to minimize the likelihood of introducing new flaws). The same construction yields MACs based on any of MD5, SHA, or RIPEMD.

In addition to being more conservative than the envelope method, only slightly slower (5-20%, depending on processor and implementation), and easily implemented from MD5, the theoretical underpinnings supporting the security of the envelope method, which assume the compression function of MD5 is pseudorandom, appear to similarly apply to MD5-MAC. We caution, however, that we are aware of no results regarding the pseudorandomness of MD5, and note this property may be independent of collision-resistance, the primary property studied to date.