X-Sieve: CMU Sieve 2.2
Subject: Comments on Hash Function Criteria
Date: Fri, 27 Apr 2007 14:28:26 -0700
X-MS-Has-Attach: yes
X-MS-TNEF-Correlator:
Thread-Topic: Comments on Hash Function Criteria
Thread-Index: AceJEvxD8GPN7n1HQ9+KIW27YQQGFw==
From: "Miles Smid" <msmid@orionsec.com>
To: <hash-function@nist.gov>
Cc: <djohnson@cygnacom.com>
X-Proofpoint-Virus-Version: vendor=fsecure engine=4.65.5502:2.3.11,1.2.37,4.0.164 definitions=2007-04-27_06:2007-04-27,2007-04-27,2007-04-27 signatures=0
X-PP-SpamDetails: rule=spampolicy2_notspam policy=spampolicy2 score=0 spamscore=0 ipscore=0 phishscore=0 adultscore=0 classifier=spam adjust=0 reason=mlx engine=3.1.0-0703060001 definitions=main-0704270146
X-PP-SpamScore: 0
X-NIST-MailScanner: Found to be clean
X-NIST-MailScanner-From: msmid@orionsec.com

Please see our attached comments on the NIST proposed Secure Hash Function Criteria.

Miles E. Smid
CygnaCom Solutions
http://cygnacom.com
15216 Centergate Drive
Silver Spring, MD 20905

Comments follow below.

Dear NIST,

Entrust supports the Secure Hash Function Criteria proposed by NIST in the January 23, 2007 Federal Register with the two additional recommendations stated below. To discuss either of these comments further, please contact Don Johnson or Miles Smid.

1. On C.1 second bullet: As hash functions are being used as components in the design of pseudo-random functions, Entrust agrees that a pseudo-randomness property should be made explicit as a criterion. One aspect of this is that the input may contain both secret and non-secret bits and the output should still appear to be random and not allow backtracking to the secret bits that is easier that the hash security level. We think that this point should be specifically stated in the criteria.

2. On C.3.1 iii: Historically, hash functions have been designed as either (A) built upon an existing cryptographic primitive, such as MDC-4 based on the DES symmetric block cipher algorithm or (B) independent of any existing cryptographic primitive. When viewed from a constrained environment perspective, it seems clear that sometimes method A will be preferred over method B, for example, when the constrained cryptosystem already needs to include a block cipher to achieve other security properties. Entrust suggests that there be 2 competitions, one for independent hash functions and one for hash functions built on a block cipher algorithm. This will also provide for some future resiliency, if one hash function should break in the future, there is still the other.