NEW CRYPTOGRAPHIC HASH ALGORITHM FAMILY: NIST HOLDS A PUBLIC COMPETITION TO FIND NEW ALGORITHMS

Shirley Radack, Editor
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology

The National Institute of Standards and Technology (NIST), Information Technology Laboratory, is soliciting candidates for a new and robust cryptographic hash algorithm for use by federal government agencies in protecting their information systems and information. The invitation to submit candidate algorithms was issued by NIST last November, and all nominations must be received by NIST by October 31, 2008.

NIST is conducting an open, public process to identify suitable candidates for the new hash algorithm, which is needed because of recent advances in the cryptanalysis of hash functions. The new hash algorithm will be named SHA-3, and it will augment the hash algorithms currently specified in Federal Information Processing Standard (FIPS) 180-2, *Secure Hash Standard*. In a Federal Register Notice (Vol. 72, No. 212, pp. 62212-20) published on November 2, 2007, NIST invited interested parties to submit nominations, and provided the nomination requirements and the minimum acceptability requirements for the new algorithm. The notice also included the evaluation criteria that will be used to assess the nominations. The November Federal Register Notice is available on NIST's Web page: http://www.csrc.nist.gov/groups/ST/hash/documents/FR_Notice_Nov07.pdf.

Use of Hash Functions

Hash algorithms accept potentially large variable size input messages and produce a small (generally in the range of 160- to 512-bit) fixed-size output called a hash value or message digest, which is a condensed representation of the electronic data in the message. Hash functions are used as building blocks in many cryptographic algorithms and processes. In a digital signature application, the hash value of the message is signed instead of the message itself; the signature can later be used to verify the message signer as well as the integrity of the signed message.

A secure hash function is essentially a collision-resistant, one-way function. Collision resistance means that it is extremely difficult to find two different messages with the same hash value. One way means that it is easy to compute the hash value from the input, but the reverse operation is extremely difficult. As a result, hash functions are often used to determine whether or not data has changed. Many algorithms and processes that provide a security service use a hash function as a component of the algorithm or process, such as:

- Keyed hash message authentication code (HMAC)
- Digital signatures
- Key derivation functions

• Random number generators.

Secure Hash Standard

The federal government's first hash standard was issued by NIST in 1993 as Federal Information Processing Standard (FIPS) 180, *Secure Hash Standard*, which specified the hash algorithm SHA-0. This standard was revised and issued as FIPS 180-1 in 1995 and as FIPS 180-2 in 2002. These revisions replaced the original SHA-0 with more secure algorithms: the 160-bit SHA-1 and the SHA-2 family of hash functions, which includes SHA-224, SHA-256, SHA-384, and SHA-512 where the suffix indicates the size of the message digest.

Recently, cryptanalysts have found ways to attack several commonly used hash functions, and vulnerabilities have been published on SHA-1. Although no practical attacks have been successful to date against SHA-1, NIST decided that a new hash algorithm is needed to augment the hash algorithms that are currently available and to provide strengthened security for digital signature and other applications for future years.

The public competition for a new hash algorithm was modeled after the very successful Advanced Encryption Standard (AES) competition - a process that NIST had followed to develop the AES (FIPS 197). NIST launched the AES competition by first publishing the minimum requirements, submission requirements, and the evaluation criteria for public comment. An AES workshop was held to discuss these requirements and evaluation criteria before a call for new algorithms was issued. The review, analysis, and a variety of tests of the submitted algorithms were conducted in stages, by NIST and by the international cryptographic community. Public feedback was provided through an electronic forum and public conferences. After the winning algorithm was selected, NIST published a report that documented the AES development effort as well as the final selection.

Technical Considerations for SHA-3

NIST does not plan to withdraw the SHA-2 algorithms unless serious flaws are found, and is interested in SHA-3 candidates that can be substituted for SHA-2 in current applications and that can provide message digests of 224, 256, 384, and 512 bits. The 160-bit hash value produced by SHA-1 is becoming too small to use for digital signatures; therefore, a 160-bit replacement hash algorithm is not contemplated.

SHA-3 should preserve the following properties of SHA-2 hash functions:

- input parameters
- output sizes
- collision resistance, preimage resistance, and second-preimage resistance
- "one-pass" streaming mode of execution.

It is also desirable that SHA-3 offer features or properties that exceed, or improve upon, SHA-2.

The security strength of SHA-3 should be as close to the theoretical maxim as possible for the different required hash sizes, and for both the collision resistance and one-way properties. SHA-3 algorithms should be designed so that a potentially successful attack on SHA-2 would not be successful on SHA-3 functions. In addition, SHA-3 should be implementable on a variety of platforms, and should be more efficient than the hash algorithms currently specified in FIPS 180-2.

For interoperability, NIST strongly desires a single hash algorithm family that generates different message digest sizes in a similar manner. However, if more than one suitable candidate family is identified, and each provides significant advantages, NIST may consider recommending more than one family for inclusion in the revised *Secure Hash Standard*.

Minimum Acceptability Requirements

To be considered as a candidate, the hash algorithm must be publicly disclosed and available worldwide without royalties or any intellectual property restrictions. The algorithm also must be capable of being implemented on a wide range of hardware and software platforms. The candidate algorithm must support message digest sizes of 224, 256, 384, and 512 bits, and must support a maximum message length of at least 2^{64}-1 bits.

Evaluation Criteria

The security provided by an algorithm is the most important factor to be considered in the evaluation of candidate algorithms. Algorithms with the same hash length will be compared for the security that may be provided in applications such as digital signatures, key derivation, HMAC, and other applications. The candidate algorithm must support HMAC, pseudo random functions (PRFs), and randomized hashing. Each candidate algorithm must have at least one construction to support HMAC as a PRF; it may have additional constructions for other non-HMAC-based PRFs or for use in a randomized hashing scheme.

Hash algorithms will be evaluated against attacks or observations that may threaten existing or proposed applications, or demonstrate some fundamental flaw in the design, such as exhibiting nonrandom behavior and failing statistical tests. Attacks that violate the security of applications implementing an existing FIPS or a NIST Recommendation will be consider more serious than attacks on rare or obscure applications.

In addition to security considerations, candidate algorithms will be evaluated for the clarity of documentation of the algorithm, the quality of the analysis on the algorithm performed by the submitters, the simplicity of the algorithm, and the confidence of NIST and cryptographic community have in the long-term security of the algorithm. Other issues are the computational efficiency of the candidate algorithm for both hardware and software implementations. The memory required for both hardware and software

implementations of a candidate algorithm will be considered. NIST will test for memory requirements, and invites public evaluations as well.

Evaluation and Selection Process

After the close of the call for candidate algorithm submission packages, NIST will review the documentation received to determine if the submissions are complete and in proper form. After this preliminary review, NIST will post the candidate algorithms for the first round of public review on the Web page: http://www.nist.gov/hash-competition.

NIST will conduct a twelve-month public review period for the first round to evaluate the candidate algorithms. An open public conference will be held after the period for submission of candidate algorithms for SHA-3 ends on October 31, 2008. The submitters of each complete and proper candidate algorithm package will be invited to discuss and explain their candidate algorithms. The documentation for these candidate algorithms will be made available at the conference. Details of the conference will be posted on NIST's Web page referenced above.

NIST will form an internal selection panel composed of NIST employees to analyze the candidate algorithms, and will make the results of its analyses publicly available. NIST also invites public evaluation and publication of the results, including any complete or partial analysis of a candidate algorithm or component of an algorithm.

The technical committee that NIST appoints to review the submitted algorithms will also review the public comments received on the posted submissions, as well as all presentations, discussions, and technical papers presented at the first SHA-3 Candidate Conference, and other relevant cryptographic research. During this review period, NIST intends to perform correctness check, efficiency and other testing. The public is invited to conduct similar testing and to compare results on additional platforms.

A second SHA-3 Candidate Conference will be held near the end of the first period of review and public evaluation. The international cryptographic community will be invited to publicly discuss the candidate SHA-3 algorithms and to provide NIST with information to help narrow the candidate pool to approximately five candidate algorithms for more careful study and analysis during the second review period.

During the second round of review, NIST will conduct a variety of computational efficiency tests on the candidates on various platforms for the minimum message digest sizes specified. The rights to those candidates not selected for the second round of review will be returned to their owners. At the start of the second review period, submitters will have the option of providing updated optimized implementations for use during this phase of evaluation.

NIST will select approximately five candidates for intensive public scrutiny for a twelve- to fifteen-month period. At the end of this review period, NIST will hold a third SHA-3 Candidate Conference to discuss the finalist candidates. After this third conference, NIST

expects to select the winning algorithm, and to document the technical rationale for the selection in a final report. NIST then expects to propose a revised *Secure Hash Standard* that will include the newly selected SHA-3 for public review. To ensure standard compliance and interoperability among different implementations, NIST intends to develop a validation program for hash algorithm conformance testing by the time SHA-3 is incorporated into the revised *Secure Hash Standard*.

Information about the Cryptographic Hash Algorithm Competition

See NIST's Web page: http://www.nist.gov/hash-competition.

Contact Information for Submission of Candidate Algorithms

Email address for general information:
Hash-function@nist.gov

Candidate algorithm submission packages should be sent to:

Ms. Shu-jen Chang
Information Technology Laboratory
National Institute of Standards and Technology
Attention: Hash Algorithm Submissions
100 Bureau Drive, Stop 8930
Gaithersburg, MD 20899-8930

Questions related to specific submission packages may be directed to:
Shu-jen Chang
Information Technology Laboratory
National Institute of Standards and Technology
100 Bureau Drive, Stop 8930
Gaithersburg, MD 20899-8930
Telephone: 301-975-2940, Email: shu-jen.chang@nist.gov, Fax: 301-975-8670.

Questions concerning the technical requirements for SHA-3 may be directed to:

Mr. William Burr
Information Technology Laboratory
National Institute of Standards and Technology
100 Bureau Drive, Stop 8930
Gaithersburg, MD 20899-8930
Telephone: 301-975-2914, Email: william.burr@nist.gov, Fax: 301-975-8670.

Related Publications

The following FIPS and NIST Special Publications (SPs) require the use of a NIST-approved hash algorithm:

FIPS 186-2, *Digital Signature Standard*

FIPS 198, *The Keyed-Hash Message Authentication Code (HMAC)*

NIST SP 800-56A, *Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography*

NIST SP 800-90, *Recommendation for Random Number Generation Using Deterministic Random Bit Generators (DRBGs)*

For information about NIST standards and guidelines that are referenced in this bulletin, as well as other security-related publications, see NIST's Web page: http://csrc.nist.gov/publications/index.html.

Disclaimer
Any mention of commercial products or reference to commercial organizations is for information only; it does not imply recommendation or endorsement by NIST nor does it imply that the products mentioned are necessarily the best available for the purpose.