NIST requests public comment on proposed SHA-3 cryptographic standard

30 May 2014

The National Institute of Standards and Technology (NIST) has requested public comments on its newly proposed "Secure Hash Algorithm-3" (SHA-3) Standard, which is designed to protect the integrity of electronic messages.

The draft Federal Information Processing Standard Publication 202, SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions, specifies six permutation-based "sponge" functions based on Keccak, the winning algorithm selected from NIST's SHA-3 Cryptographic Hash Algorithm Competition. The functions include four fixed-length cryptographic hash functions, and two closely related "extendable-output" functions (XOFs). The four fixed-length hash functions provide alternatives to the SHA-2 family of hash functions specified in FIPS 180, Secure Hash Standard, which FIPS 202 will supplement. The XOFs can be specialized to hash functions, subject to additional security considerations, or used in a variety of other applications.

Cryptographic hash algorithms are a cornerstone of modern information security. They transform a digital message into a short "message digest" for use in digital signatures. Even a small change in the original message text creates a change in the digest, making it easier to detect accidental or intentional changes to the original message. Hash algorithms are used by many security applications, including random bit generation.

More information: Comments from the public on the draft of FIPS 202 are welcome for the next 90 days until August 26, 2014, after which NIST will incorporate them into the final version of the specification. The draft is available at csrc.nist.gov/publications/dra … 2/fips_202_draft.pdf. Comments may be sent to NIST either electronically or by mail. Full details appear in the Federal Register at federalregister.gov/a/2014-12336.

Provided by National Institute of Standards and Technology