NIST Brief Comments
on
Recent Cryptanalytic Attacks on SHA-1

Cryptographic hash functions that compute a fixed size message digest from arbitrary size messages are widely used for many purposes in cryptography, including digital signatures. NIST was recently informed that researchers had discovered a way to "break" the current Federal Information Processing Standard SHA-1 algorithm, which has been in effect since 1994. The researchers have not yet published their complete results, so NIST has not confirmed these findings. However, the researchers are a reputable research team with expertise in this area. Previously, a brute force attack would expect to find a collision in 2^{80} hash operations. The researchers assert the "computational complexity" of their new attack would be less than 2^{69} hash operations to find a collision. This attack is of particular importance in digital signature applications, such as time stamping and notarization. However, many digital signature applications include contextual information that will make this attack difficult to carry out in practice. Other applications of hash functions, such as Hash-Based Message Authentication Codes (HMACs) and key derivation, are believed unaffected by this attack.

Due to advances in computing power, NIST already planned to phase out SHA-1 in favor of the larger and stronger hash functions (SHA-224, SHA-256, SHA-384 and SHA-512) by 2010. New developments should use the larger and stronger hash functions. In addition, agencies are encouraged to develop plans on a timely basis for an orderly transition to the larger hash functions, taking into account system sensitivity in prioritizing their efforts. As the full details of this attack become known, NIST will publish additional guidance.

To improve our understanding of the cryptographic strength of hash functions, NIST encourages further research in hash functions and their properties. NIST will continue to work collaboratively with the cryptographic community in this effort.

2/18/2005