NIST SP 800-106: Randomized Hashing for Digital Signatures

Quynh Dang

Computer Security Division

ITL, NIST

Motivation

- Message Modification attacks reduced collision strength of SHA1 to around 63 bits which did not meet NIST security strength requirement.
- NIST searched for a method which does not require any change to the hash function or the signing algorithm in digital signature algorithms, but can significantly improve security of many digital signature applications (a quick fix while NIST was looking for a long term solution).

Solution

- Based on work by Shai Halevi and Hugo Krawczyk (http://webee.technion.ac.il/~hugo/rhash/).
- Message is randomized with a random value before it gets hashed.
- The random value does not have to be signed.
- Signature Verifier uses the random value to randomize the received message before verifying the received signature.

Security

- The signature verifier does not get more security assurance from randomizing hashing.
- The technique helps only the signer against collision attacks by message preparer where part or all of the message is generated/prepared by the message preparer, not the signer.

Security Strength

- If random value generation function can be attacked by an attacker, then the security of the randomized method is the minimum of the two quantities below.
  1) The maximum of (collision resistance of the hash function, the security strength of random value generation function), and
  2) Second preimage resistance strength of the hash function.
- Otherwise, the security is the minimum of the two quantities below.
  1) Second preimage resistance of the hash function, and
  2) Security strength of the random value + collision resistance strength of the hash function.

Summary

- NIST is not aware of any damaging collision attacks on SHA2 and SHA3.
- Attacks can get better.
- Randomizing hashing is an additional layer protection for a signer who does not have control over the whole content of each message she/he signs.

Comments

NIST's Crypto Toolkit: http://csrc.nist.gov/groups/ST/toolkit/index.html.

Any comments/questions?

Quynh.dang@nist.gov.