oath
initiative for open authentication

SHA-1 & HMAC OTP Frequently Asked Questions

Recently, there has been considerable coverage in the press about an upcoming paper from Academics in China that describes an attack on SHA-1. OATH is providing this overview and companion paper to explain the nature of the results and why the result is not a security issue for the HMAC OTP algorithm currently being promoted by OATH within IETF organization.

Q: What is SHA-1?
A: Secure Hash Algorithm, a hash function developed by the NSA for use with NIST's Digital Signature Standard (DSS). NSA almost immediately developed a minor change known as SHA-1. Both SHA and SHA-1 produce a 160-bit digest. SHA-1 is used in SSL.

Q: Why has there been so much news about SHA-1 lately? Some reports say that it is 'broken', what does that mean?
A: A research team of Xiaoyun Wang, Yiqun Lisa Yin, and Hongbo Yu (from Shandong University in China) have been circulating a draft paper describing an attack on SHA-1 that 'breaks' SHA-1. Cryptographers' use the term broken whenever they can demonstrate the vulnerability is more successful than a simple 'brute force' attack. In this case the vulnerability is related to collisions and the exploit would still require significant computing power.

While the news should not be ignored, these results have important implications for the use of SHA-1 as a hash for digital signatures but, not for HMAC.

Q: What is the connection between digital signatures and hash functions?
A: All major digital signature signing techniques (including DSA and RSA) involve first hashing the data then signing the hash. Raw message data is not signed because of both performance and security reasons.

Q: What is a collision and how does it affect the security of a hash function?
A: Collision vulnerability finds two messages with the same hash, but the attacker can't pick what the hash will be. To exploit the collision vulnerability an attacker would have to find two messages that produce the same hash where one message is benign and the other message malicious.

Q: What are the implications for HMAC SHA-1 and HMAC OTP algorithm? Does the use of SHA-1 make HMAC OTP flawed in anyway?
A: HMAC (Hashed Message Authentication Code) uses SHA-1 internally. The difference is that a MAC uses a secret key. The use of the secret makes collision attacks of the type identified by Wang, et. al. irrelevant. Security of the HMAC OTP algorithm is not affected because HMAC was designed so that collisions in the hash function would not produce forgeries in HMAC.

No flaws have been identified in HMAC-OTP. As described above, the use of SHA-1 introduces no known vulnerabilities into HMAC-OTP.

SHA-1 & HMAC OTP Frequently Asked Questions

Q: Will OATH participants propose other hash functions to use with HMAC OTP?
A: The current OATH-generated IETF draft references HMAC SHA-1 as defined in RFC 2104. The authors of the draft will continue to reference this RFC. Currently, there is no security need to change the hash function used in HOTP. Extensions to HMAC OTP (including additional hash functions) algorithm may be possible in the future.