



SECURE HASHING ALGORITHM (SHA-1)

1. A hashing algorithm is a cryptographic algorithm that can be used to provide data integrity and authentication. They are also typically used in password based systems to avoid the need to store plaintext passwords.
2. In previous revisions of the Information Security Manual (ISM) DSD recommended that agencies use the SHA-2 family of hashing algorithms in preference to the SHA-1 hashing algorithm. DSD has removed SHA-1 from the list of DSD Approved Cryptographic Algorithms (DACA) in the 2012 release of the ISM.

ATTACKS ON SHA-1

3. There are a number of attacks on SHA-1, all relating to what is known as collision resistance.
4. Although the majority of uses for hashes do not solely rely on collision resistance, these kinds of attacks have the potential to lead to further developments that are far more serious.
5. The risk of these attacks has reached a level that is higher than acceptable for SHA-1 to continue to be a DACA.

WHAT DOES THIS MEAN?

6. For the majority of uses, these attacks do not yet present a practical vulnerability.
7. However, you should consider using DACAs for new systems and assess the implications of using SHA-1 in existing systems.
8. For example, if you are using SHA-1 for the storage of passwords, there are no password-recovery attacks as at December 2011 that make use of the collision attacks on SHA-1.
9. As always, the best mitigation to password recovery attacks is to ensure the use of strong passwords.

WHAT IS A HASHING ALGORITHM?

10. A hashing algorithm is a deterministic function that takes in an arbitrary length block of data, and returns a fixed-size string, which is called the hash value.
11. A secure hashing algorithm has three main properties:

- **Preimage resistance.**

Given a hash value, it should be difficult to find any message that hashes to that value.

- **Second-preimage resistance.**

Given an input, it should be difficult to find another input, which is different to the first, where they both hash to the same value.

- **Collision resistance.**

It should be difficult to find two different inputs such that have the same hash values.

WHERE ARE HASHING ALGORITHMS USED?

12. There are three common uses of cryptographic hashes:

- **Digital signature algorithms.** A message is transmitted with its hash, allowing the recipient to hash the message and compare outputs. By signing the hash before sending, the sender can prove that the message has not been tampered with.
- **Storage of passwords.** Rather than storing a user’s password, a system will typically store the hash of the password instead. When a user enters their password, the hash is then computed and compared with the stored hash. If the hash matches, due to the collision resistance property of hashing algorithms, it implies that the passwords match.
- **Integrity checking.** The sender can hash a file before sending to the recipient. The recipient will then hash the file received and check the hashes match. This can also be used for the storage of files, to ensure files have not been corrupted or modified.

CONTACT

13. Australian government agencies seeking further information can contact DSD via: OnSecure (www.onsecure.gov.au) forums, email to: assist@dsd.gov.au or call 1300 CYBER1 (1300 292 371).