Department of Information Technology

Academic Year: 2022-23 **Semester: V**
Class / Branch: TE IT
Subject: Security Lab (SL)
Subject Lab Incharge: Prof. Apeksha Mohite

EXPERIMENT NO. 10

Aim: To study and test message integrity by using MD5, SHA-1 for varying message sizes.

Theory:

Key differences between hash algorithms.

Keys For Comparison	MD5	SHA
Security	Less Secure than SHA	High Secure than MD5
Message Digest Length	128 Bits	160 Bits
Attacks required to find out original Message	2^{128} bit operations required to break	2^{160} bit operations required to break
Attacks to try and find two messages producing the same MD	2^{64} bit operations required to break	2^{80} bit operations required to break
Speed	Faster, only 64 iterations	Slower than MD5, Required 80 iterations
Successful attacks so far	Attacks reported to some extents	No such attach report yet

Verify Data Integrity :

The checksum is used to verify the correctness of a file. It can be described as a digital fingerprint of a file. By verifying the Checksum value we can determine the correctness of a file while it's been transferred from one location to another. The checksum is a long string of data containing various letters and numerals. All popular software downloading websites provides a checksum value for the downloaded file with which we can confirm our data by verifying the checksum value.

Generating Checksums:

A checksum is generated by a checksum algorithm. It generates a checksum value by taking the file as input. MD5 and SHA (Secure Hash Algorithms) are the most popular algorithms used for generating the checksums.

Command-line Checksum tools

Almost all Linux distribution provides the command line tools for various checksum algorithms. You can generate and verify checksum with them. Some of the standard command-line checksum tools used nowadays are the followings:

MD5 checksum tool is called: md5sum
SHA-1 checksum tool is called: sha1sum
SHA-256 checksum tool is called: sha256sum
SHA-384 checksum tool is called: sha384sum
SHA-224 checksum tool is called: sha224sum
SHA-512 checksum tool is called: sha512sum

md5sum: MD5 is an algorithm that is used to verify data integrity through the creation of a 128-bit message digest from a data input that is claimed to be as unique to that specific data as a fingerprint to a specific individual.

Sha1sum: SHA-1 (Secure Hash Algorithm 1) is a cryptographic hash function designed by the United States National Security Agency. SHA-1 produces a 160-bit (20-byte) hash value known as amessage digest. Please see the sha1 hash value for the same file.

sha256sum/sha512sum/sha224sum/sha384sum: SHA-2 is a family of two similar hash functions, with different block sizes, known as SHA-256 and SHA-512. They differ in the word size; SHA- 256 uses 32-bit words whereas SHA-512 uses 64-bit words. There are also truncated versions of each standard, known as SHA-224, SHA-384, SHA-512/224 and SHA-512/256.SHA-256 algorithm generates an almost-unique, fixed size 256-bit (32-byte) hash. Hash is a one-way function, which cannot be decrypted back.

Conclusion : We have seen how checksum are generated for MD5 and SHA. You can make use of this Checksum method as a redundancy check to detect errors in data. Hence. ensure the integrity of data portions for data transmission or storage.