This that are generated using cryptographic hash

Business, Decision Making

Thispaper reviews an exercise carried out to determine file(s) that will be neededto ensure minimal system integrity by running MD5 algorithm, a hash functionwhich is widely used to produce 128-bit hash value. Initially MD5 was developedto be used as a cryptographic hash function but due to its higher possibilitiesof being vulnerable it is often only used as a checksum to verify dataintegrity.

Data integrity isthe validity of data which needs to be maintained consistently in order toavoid any compromises, either while replicating the data or transferring it. Tocheck the integrity of data or files the MD5 checksum is used to compare the checksums, since there is a very small possibility of getting two identical checksums fortwo different files. Integrity checksnot only detect data corruption, but they also help in tracking anyalternations made to file, or any malicious attacks. According to a technicalreport from Stony Brook University, the author says " Checksums that are generatedusing cryptographic hash functions prevents unauthorized users from generatingcustom checksums to match the malicious data modifications that they have made1. Following are ways the integrity of data can be compromised: · Damage to hardware– disk crash· Damage to software– bugs, malware, viruses, etc.· Compromise of datafrom transfers· Data Alternations· User Error (HumanError)There have beenmultiple ways to validate the authenticity of a file. It was very crucial tocheck the authenticity for many different purposes.

One factor could be just toensure that the file was downloaded properly. Other ways also includesimultaneously comparing the file contents within the archive, the dates whenthe file was created, and the size of the file

which has been downloaded. Allthese contents can be compared to the targeted file/program which was supposedto be downloaded. Checksums areusually calculated using a hash function, which is normally given along withthe download. To verify the integrity of the file, the user can calculate thechecksum using a checksum software program or through the command line. Acommon method widely used by the developers of software and Linux distributionsto provide an ISO which they send through an encryption method called MD5 whichprovides a unique checksum. Below I'll show a similar example of this exercise.

The motive for this exercise is that a user will download any file from thewebsite and then run a tool which creates an MD5 checksum against that file. The checksum hashing algorithm returned from the tool should match the onelocated on the website from which the file was downloaded, possibly thesoftware developer's website. To run MD5 in ensureminimal system integrity, I downloaded the ' Microsoft File Checksum IntegrityVerifier' as shown below. Like I mentioned earlier, the checksum can be checkedeither from the terminal or from an application (MD5 software), which is eitherincluded in the operating system or can be downloaded.

Moving on, afterdownloading the checksum identifier on windows, I used the command prompt tocompare the algorithm. To do so, I used the following command " fciv. exe –sha1″along with the file I had downloaded. This command quickly processed to revealthe hashing algorithm for the file.

I later checked the website to compare ifboth the source destination and the downloaded file match their checksumsOften, an attackermanages to hack

into or take control of one’s system by penetrating thesecurity layers. Their first step is usually to tamper with the system is sucha way that the intrusion detection system is unable to perform its functions. Therefore, to avoid being set up in trap the intruder might have set its better to checkthe integrity of our system before starting it. “ Physical security is the firstmost important thing you should do.

In fact, if we fail on this line it willnot help us to have intrusion detection systems, firewalls, or the bestsoftware” says Adrian Stolarski. 2MD5 hash functionsare not meant for encryption since they can be easily cracked by brute-forceattack. The security of MD5 is very weak. According to CMU Software EngineeringInstitute MD5 is “ cryptographically broken and unsuitable for further use. Thiscontext related to its purpose in security and not as a checksum verifier, which we intended to perform this exercise for.

This feature can be useful bothfor comparing the files and their integrity control. Nate Lord, editor fromData Insider mentions “ For modern enterprises, data integrity is essential forthe accuracy and efficiency of business processes as well as decision making. It’s also a central focus of many data security programs.” 3