**Dictionary Attack**

**Description 1.**

In cryptanalysis and computer security, a dictionary attack is a technique for defeating a cipher or authentication mechanism by trying to determine its decryption key or passphrase by trying hundreds or sometimes millions of likely possibilities, such as words in a dictionary. A dictionary attack is based on trying all the strings in a pre-arranged listing, typically derived from a list of words such as in a dictionary. [1]

**Description 2.**

Dictionary Attacks are a method of using a program to try a list of words on the interface or program that is protecting the area that you want to gain access to. The most simple password crackers using dictionary attacks use a list of common single words, aka a "dictionary". More advanced programs often use a dictionary on top of mixing in numbers or common symbols at the beginning or end of the guessed words.

Some can even be given a set of personal information or a profile of the user and pick out important words to guess, even if they are not proper words, such as pronouns like last names and names of relatives.

A weakness of dictionary attacks is that it obviously relies on words supplied by a user, typically real words, to function. If the password is misspelled, is in another language, or very simply uses a word that is not in the dictionary or profile, it cannot succeed. Most of the time, even using two words in one password can thwart a dictionary attack. [2]

**Description 3.**

A dictionary attack is an attack that tries to guess at the key of a ciphertext by attempting many different common passwords and possible passwords that are likely to be used by humans. A dictionary attack makes use of what is called a dictionary, which stores common English words, phrases, and passwords ready to guess as the key. Dictionary attacks are more efficient than a Brute Force Attack as they don’t have to try nearly as many combinations – but with the downside that if the key is not contained in the dictionary, it will never successfully find it.

For example, let’s say that Bob encrypted his hard drive with the password “hunter2”. Alice then uses a dictionary attack to try every possible word in the dictionary. If “hunter2”, Bob’s password, is in the dictionary – then Alice will have the key and be able to get access to Bob’s hard drive. However, if Bob’s password was “ahiuhf23fg23tg8902g”, a phrase that is unlikely to be in Alice’s dictionary (which generally contain a variety of English words, variations, and common passwords) – Alice would never be able to gain access to his hard drive, and eventually would exhaust her dictionary without a positive match. [3]

References

[1] <https://en.wikipedia.org/wiki/Dictionary_attack>

[2] <http://web.cs.du.edu/~mitchell/forensics/information/pass_crack.html>

[3] <https://learncryptography.com/attack-vectors/dictionary-attack>