

Cain and Abel research paper example

[Sociology](#), [Violence](#)



Cain and Abel

A brute force attack attempts every code and combinations until the required password are achieved. Several factors affect the difficulty of a brute force attack. These factors include the length of the key, the possible values that each component can have, the period it takes to attempt each key and the possibility of a mechanism, which locks the attacker after some failed attempts.

A dictionary attack, on the other hand, uses a targeted technique whereby all words are successively tried in a list called the dictionary. The list is prearranged. Unlike in brute force attack where there is a large portion of key space is looked into in a systematic way, a dictionary attack will try options, which are likely to come out successfully. This list is derived from text databases like dictionary or bible and so on. In general, dictionary attacks tend to succeed because people tend to choose passwords, which are short (for example 7 characters and below), simple words that are found in dictionaries, and words, which can easily be, predicted.

Dictionary attack is faster when compared to Brute force attack although there is no possibility that the password will be cracked in the end. This is because the combinations that are tried depend on the wordlist that is found in the dictionary. On the other hand, Brute force attack will take time but the password will always be recovered if given time to finish its operations. This is because it tries to permute all the available keys to try a password. The problem is that if the key length is long, that means the time it will take to

recover the password will also be long. The good thing is that the password will be recovered in the end.

References

Cross, M., & Shinder, L. D. (2008). Scene of the cybercrime. New Jersey: Syngress.

Kim, D., & Solomon, M. (2010). Fundamentals of information systems security. Texas: Jones & Bartlett Learning.

Moore, R. (2010). Cybercrime: Investigating high-technology computer crime. New York: Elsevier.