Passwords:

Password	MD5 Hashed	Time Taken To Crack
Z	21c2e59531c8710156d34a3c30ac81d5	Less than a second / 0.0004699230194091797s
AD	e182ebbc166d73366e7986813a7fc5f1	Less than a second / 0.03285813331604004s
God	aeb9573c09919d210512b643907e56b8	Around a second / 0.9671869277954102s
1234	81dc9bdb52d04dc20036dbd8313ed055	47.67334985733032s
AbCdE	37e464916dcb6dfc3994ca4549e97272	1 hour 51 minutes/ 6701.898176193237s
Trojan	a5312fd5717d3e2fd419132e3c3ac51b	18 hours 24 minutes
F1ghtOn	57b46b0a1ac529ef1a3d6fa016b6995e	Estimated to take weeks to a month as there would be 62^7 possible combinations.

Earlgrey	46216a0b09453799f35d04e7343ba0e6	Estimated to take more than a month as there would be 62^8 possible combinations

Analysis:

By seeing the time taken to crack the passwords above using brute-force techniques, we can see that the time taken increases exponentially as password length increases. This is because the number of possible password combinations increases exponentially when the size of the password increases. The difference between the time taken to crack the passwords between 1 and 2-character words or 2 and 3-character words is not that big. However, as the length becomes longer, the difference in time taken increases by a lot. For instance, cracking a 6-character password takes more than 10 times longer than cracking a 5-character password.

The possible characters in these passwords are lowercase letters, uppercase letters, and numbers which means that there are 62 possible choices for each character of the password. This would mean that a 1-character password would have 62^1 or 62 possible combinations, a 2-character password can contain 62^2 or 3844 possible combinations, a 3-character password can contain 62^3 or 238328 possible combinations, a 4-character password can contain 62^4 or 14776336 possible combinations, a 5-character password can contain 62^5 or 916132832 possible combinations, a 6-character password can contain 62^6 or 56800235584 possible combinations, a 7-character password can contain 62^7 or 3,521,614,606,208 possible combinations, and an

8-character password can contain 62^8 or 218,340,105,584,896 possible combinations. With these differences, it can be seen that the number of possible combinations drastically increases for even a small change in password length. Additionally, the percentage increase in possible combinations also increases drastically as the password length is longer and longer. As most computers can only generate around 10,000 to 200,000 passwords a second, it will take a lot of time to crack longer passwords. Thus, password length strongly influences the time that takes to crack a password.

There are some methods that can make password cracking faster. For example, Parallel Processing can be done. Here, multiple computers or processors will simultaneously do the password-cracking algorithms in order to make the overall task and process faster and more efficient. Basically, the task of cracking passwords is divided into smaller pieces and is sent to other processors and computers for concurrent processing. For example, for an 8-character password, one system could check the first 4 characters and the other system could check the last 4 characters, making the process faster.

Another way of making the password-cracking process faster is to utilize the GPU. GPUs are generally faster than regular CPUs when running or processing computer algorithms, which can make them useful for password cracking. Due to its parallel architecture, it can run multiple algorithms or calculations simultaneously. Overall, with a GPU the brute-force cracking algorithm can generate more passwords in a shorter period of time.

The password-cracking algorithm can also be broken down into smaller pieces and distributed to other computers or processors. This is useful for larger passwords that require a lot of combinations to crack. Additionally, rather than simply generating random passwords, another approach like a hybrid attack can be implemented where dictionary and brute-force approaches can be utilized to make the process more efficient. For instance, a dictionary attack can be used to generate a proper password and with a brute-force attack, variations of the password can be generated and compared. This approach can be useful depending on the context but can take a lot of time if the password is something that is not there in a pre-defined list.

Overall, it can be seen that it takes a lot of time to crack passwords with long lengths and this time also increases exponentially. However, there are definitely ways to speed up the process to make it more efficient.

Citations:

Specialist, B., Rudisail, B., Specialist, I., 17, N., Brad Rudisail IT Specialist opens a new window opens a new window Brad Rudisail i, Brad Rudisail IT Specialist opens a new window, . . . Opens a new window Brad Rudisail is a technical writer and a former IT manager specializing in delivering today's complex technical subjects in a palatable format to tech-savvy business leaders. Brad has spent 20 years in the IT fi. (n.d.). Password-cracking with high-performance gpus: Is there a way to prevent it? Retrieved April 27, 2023, from https://www.spiceworks.com/it-security/identity-access-management/articles/tackling-gpu-enabled-password-cracking/

Writer, A., & Arthur BelloreCybersec WriterI'm a tech content creator. I enjoy breaking up seemingly complicated topics into easy-to-understand pieces for people to read. When I'm not in front of a computer. (2021, March 30). How parallel computing will affect the

security industry. Retrieved April 27, 2023, from https://auth0.com/blog/how-parallel-computing-will-affect-the-security-industry/

How long does it take a hacker to brute force a password? " IronTech Security. (2022, November 11). Retrieved April 27, 2023, from https://irontechsecurity.com/how-long-does-it-take-a-hacker-to-brute-force-a-password/

Hashlib - secure hashes and message digests. (n.d.). Retrieved April 27, 2023, from https://docs.python.org/3/library/hashlib.html