Crack leaked password database(Goldman Sachs)

Improved password Security Policies for Goldman Sachs

Project Overview

As a governance analyst it is part of your duties to assess the level of protection offered by implemented controls and minimize the probability of a successful breach. To be successful at your job you often need to know the techniques used by hackers to circumvent implemented controls and propose uplifts to increase the overall level of security in an organization. Gaining valid credentials gives the attackers access to the organization's IT system, thus circumventing most perimeter controls in place.

Project Objective

- ➢ What type of hashing algorithm was used to protect passwords?
- ➢ What level of protection does the mechanism offer for passwords?
- ➢ What controls could be implemented to make cracking much harder for the hacker in the event of a password database leaking again?
- ➢ What can you tell about the organization's password policy (e.g. password length, key space, etc.)?
- ➢ What would you change in the password policy to make breaking the passwords harder?

Project Report

Dear Ma'am/Sir

There are a total 19 hashcodes given out of that i am able to crack 13 hashcodes and get password. It proves that the MD5 algorithm is not secure for passwords. To make our password more secure we can use other algorithms like SHA-2, SHA-3, SHA-256 etc.

There are other factors are also more effective to make our password more reliable

1) Length of password should be more than 15 words.
2) Password must contain at least one Uppercase, one Lower case, one number, one symbol, one special character.
3) We can provide Two factor authentication to make passwords harder to crack.
4) Don't use user name as a password.

Thanking you,
Name: Suraj S. Mane

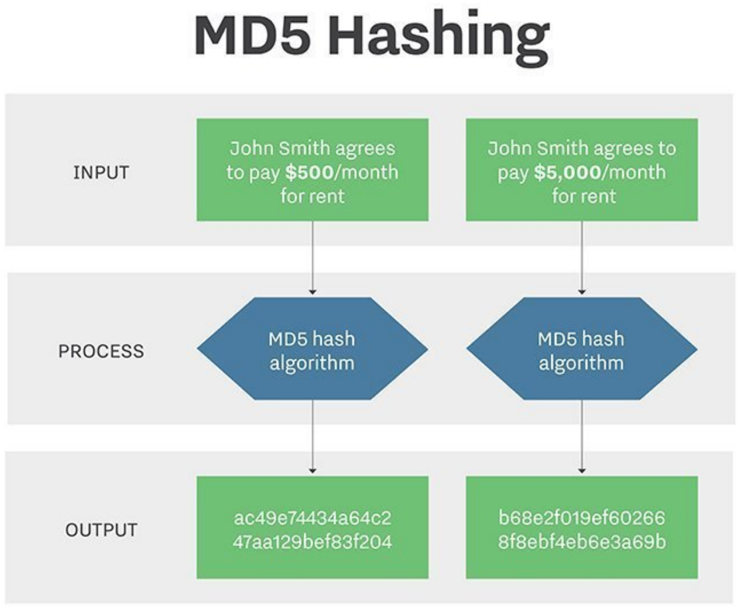
Observation

HashCodes	Security Algorithms	Cracked Passwords:
experthead:e10adc3949ba59abbe56e057f20f883e	MD5	123456
interestec:25f9e794323b453885f5181f1b624d0b	MD5	123456789
ortspoon:d8578edf8458ce06fbc5bb76a58c5ca4	MD5	qwerty
reallychel:5f4dcc3b5aa765d61d8327deb882cf99	MD5	password
simmson56:96e79218965eb72c92a549dd5a330112	MD5	111111
bookma:25d55ad283aa400af464c76d713c07ad	MD5	12345678
popularkiya7:e99a18c428cb38d5f260853678922e03	MD5	abc123
eatingcake1994:fcea920f7412b5da7be0cf42b8c93759	MD5	1234567
heroanhart:7c6a180b36896a0a8c02787eeafb0e4c	MD5	password1
edi_tesla89:6c569aabbf7775ef8fc570e228c16b98	MD5	password!
liveltekah:3f230640b78d7e71ac5514e57935eb69	MD5	qazxsw
blikimore:917eb5e9d6d6bca820922a0c6f7cc28b	MD5	Pa$$word1
johnwick007:f6a0cb102c62879d397b12b62c092c06	MD5	bluered

Conclusion

1. **What type of hashing algorithm was used to protect passwords?**

   It was a MD5. The MD5 (message-digest algorithm) hashing algorithm is a one-way cryptographic function that accepts a message of any length as input and returns as output a fixed-length digest value to be used for authenticating the original message.


MD5 Hashing
INPUT
John Smith agrees to pay $500/month for rent
John Smith agrees to pay $5,000/month for rent
PROCESS
MD5 hash algorithm
MD5 hash algorithm
OUTPUT
ac49e74434a64c2 47aa129bef83f204
b68e2f019ef60266 8f8ebf4eb6e3a69b

2. **What level of protection does the mechanism offer for passwords?**

   Using salted md5 for passwords is a bad idea. Not because of MD5's cryptographic weaknesses, but because it's fast. This means that an attacker can try billions of candidate passwords per second on a single GPU. It concludes that the MD5 provides very low security for password

3. **What controls could be implemented to make cracking much harder for the hacker in the event of a password database leaking again?**

   Make every password unique

   Make it long. This is the most critical factor. Choose nothing shorter than 15 characters, more if possible.
   Use a mix of characters. The more you mix up letters (upper-case and lower-case), numbers, and symbols, the more potent your password is, and the harder it is for a brute force attack to crack it.
   Avoid common substitutions. Password crackers are hip to the usual substitutions. Whether you use DOORBELL or D00R8377, the brute force attacker will crack it with equal ease. These days, random character placement is much more effective than common *leetspeak** substitutions. *(*leetspeak definition:*

an informal language or code used on the Internet, in which standard letters are often replaced by numerals or special characters.)

Don't use memorable keyboard paths. Much like the advice above not to use sequential letters and numbers, do not use sequential keyboard paths either (like *qwerty*). These are among the first to be guessed.

Use two-factor authentication. Even hackers that have stolen your passwords aren't going to easily access your accounts if you follow this tip. Two-factor authentication requires you to know something (your password), and to have something (a phone with a code, for instance).

Gmail's two-factor authentication is a good example of how this works: after entering your password, Gmail sends a code to your phone, which you then enter for access to your email. Unless hackers have both your password and have stolen your phone, this is a major roadblock.

4. **What can you tell about the organization's password policy (e.g. password length, key space, etc.)?**

minimum length of the password should be a 6 characters or more then that

There is no rule regarding use of special characters in the password.

5. **What would you change in the password policy to make breaking the passwords harder?**

i) The password must be of minimum 8 characters.

ii) Minimum 2 special characters (/,#,*,... etc) must be used in the password.

iii)An external Api based tool which checks for password strength should show that the used password is strong.

Reference

- https://www.techtarget.com/searchsecurity/definition/MD5#:~:text=The%20MD5%20(message%2Ddigest%20algorithm,for%20authenticating%20the%20original%20message.
- https://security.stackexchange.com/questions/19906/is-md5-considered-insecure
- https://blog.avast.com/strong-password-ideas
- https://arstechnica.com/information-technology/2013/05/how-crackers-make-minced-meat-out-of-your-passwords/
- https://en.wikipedia.org/wiki/Salt_(cryptography)
- https://en.wikipedia.org/wiki/Cryptographic_hash_function
- https://en.wikipedia.org/wiki/Password_cracking#Software

Complete report is available at