Hritika Kucheriya
Student at University at Mumbai

Question1:

What type of hashing algorithm was used to protect passwords?

Answer:

MD5 was mostly used as a hashing algorithm used while some of them remained unidentified.

Question2 :

What level of protection does the mechanism offer for passwords?

Answer:

MD5 provides a very low level of security to passwords.

MD5 is an “**iterative**” hash function.

MD5 is generally a **considerable mechanism** for storing passwords in production.

MD5 produces a **128-bit hash.**

MD5 is born out of **RSA’s algorithm** (defined in Internet RFC).

MD5 is a utility that can **generate a digital signature of a file**. MD5 belongs to a family of one-way hash functions called **message digest algorithms**. The MD5 system is **defined in RFC 1321**.

The algorithm takes as input a message of **arbitrary length** and produces as output a **128-bit "fingerprint" or "message digest"** of the input. It is conjectured that it is **computationally infeasible** to produce two messages having the same message digest or to produce any message having a given prespecified target message digest. The MD5 algorithm is **intended for digital signature applications**, where a large file must be **"compressed"** in a secure manner before being encrypted with a private (secret) key under a public-key cryptosystem such as **RSA**.

Question 3:

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

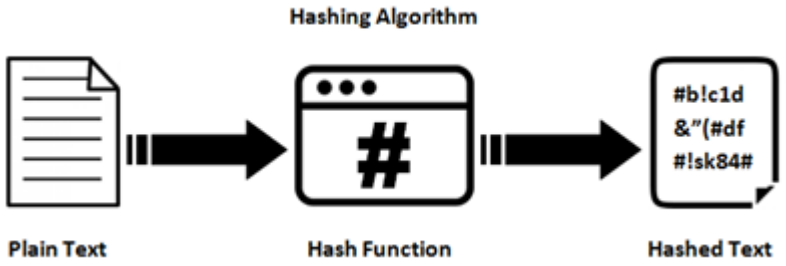
Answer:

One way of making the password hard to crack is by **maintaining credentials from a multitude of services in a manager** like dashlane because they tend to use **varied hashing** algorithms & even hashing over hashed passwords [e.g. md5(md5($plaintext))] to store and keep the **strength high**, meeting to the rigidity of a strong case for an algorithm to process.

Reduce redundancy across services such that in case of a leak out of one service doesn't make the **other passwords vulnerable**.

Use an alphanumeric characters with **special characters**.

Reducing the occurrence of an **adjective on noun or verb** which is an obvious prey to brute force attacks.



Question 4 :

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

Answer:

It can be very well determined that the organization's **password policy is not up to the mark** as:

The key length is at an **average of 11**.

Although they do not allow spaces, the use of **special characters is probably resisted** by a set of common delimiters like '_'.

The use of **numbers increases the resistance** of passwords by a factor of **10 times the digit appears**.

The **lack of capital characters** splits the password strength by half.

Not avoiding the occurrence of English verbs like book, popular, eating, hero, life, John Wick, interest, expert in turn making the password vulnerable to brute force attacks.

Question 5 :

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

Answer :

Keeping a **threshold on length**.

Caution overuse of **verbs is nouns or adjectives**.

Mandating minimum of **3 special characters and a minimum of one capital letter**.

Applying a **hashing algorithm over another**, recursively to have a strong hashing function e.g. md5(strtoupper(md5($plaintext)))

Not allowing sibling credentials to assist the password naming, like name/surname/date of birth/sex.

Refer to the following table for more details:

username	**hash**	**Hash type**	**Original password**
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
flamesbria2001	9b3b269ad0a208090309f091b3aba9db	Unknown	-
oranolio	16ced47d3fc931483e24933665cded6d	Unknown	-
spuffyffet	1f5c5683982d7c3814d4d9e6d749b21e	Unknown	-
moodie	8d763385e0476ae208f21bc63956f748	Unknown	-
nabox	defebde7b6ab6f24d5824682a16c3ae4	Unknown	-
bandalls	bdda5f03128bcbdfa78d8934529048cf	Unknown	-