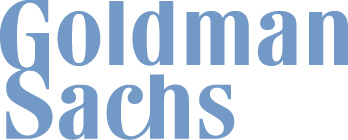
**MEMORANDUM**

To: Joanna Rycerz

24th August 2020

Warsaw, Masovian District, Poland

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

**MD5** algorithm was used for protecting passwords

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

Message Digest Algorithm 5 (MD5) is a **cryptographic hash algorithm that can be used to create a 128-bit string value from an arbitrary length string**. Although there have been insecurities identified with MD5, it is still widely used. MD5 is most commonly used to verify the integrity of files.

MD5 (Message-Digest algorithm 5) is a widely used cryptographic hash function that results in a 128-bit hash value. The 128-bit (16-byte) MD5 hashes (also termed message digests) typically are represented as 32-digit hexadecimal numbers (for example, ec55d3e698d289f2afd663725127bace). EAP-MD-5 typically is not recommended for wireless LAN implementations because it may expose the user’s password, and because several collision-based weaknesses have been demonstrated. It provides for only one-way authentication – there is no mutual authentication of wireless client and the network. And very importantly it does not provide a means to derive dynamic, per-session wired equivalent privacy (WEP) keys.

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

**Use salt**

Basically, a salt is a word you’ll add before and/or after each password

If your salt is “randomsaltformypassword” and the user choose “qwerty” as a password

You’ll use “randomsaltformypasswordqwerty” as the MD5 function parameter

**Long passwords**

Another solution is to force users to use longer password (maybe 15 characters or more)

You can also add passwords complexity to make sure they are using uppercase, lowercase and special characters

**Other hash functions**

Probably the best solution is to use another cryptographic algorithm

This is not the easiest because you probably have to change your database structure, but it could be the safest

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

* After cracking the passwords and examining them what I found is:
* Some password looks like they could be a dictionary word or a name. If it's a name with personal significance it might be easy to guess. If it's a dictionary word it could be cracked very quickly.
* Range of password limit that I found is in between 6-11. The longer a password is the more secure it will be
* Some password only contains letters. Or only numerals.
* Some password looks like it might just be a word and a few digits. This is a very common pattern and would be cracked very quickly.
* Although you have rule of not using space but there is no rule for making use of both symbols, numerals, capitals compulsory which could increase the strength of password

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

* Using at least eight characters long password.
* Making use of at least one upper case, number and symbol compulsory.
* Avoiding using username or previously used password as new password.
* Caution over use of verbs are nouns or adjectives.
* Using stronger Hashing algorithms such as SHA-256 and SHA-3 instead of MD5 which is insecure

**Jahnvi Srivastava**