Security Question’s Security

Project Report

By

Mohammad Areeb Ahmad

[E-mail-m.areeb.ahmad@gmail.com](mailto:E-mail-m.areeb.ahmad@gmail.com)

Date : 23 April, 2020

Certificate Of Declaration

This is to certify that I, Mohammad Areeb Ahmad have worked on the “*Security Question’s Security*” on 23rd of the month of April, 2020. This project has been undertaken to my interest and it doesn’t include influence of any other organization.

Name : Mohammad Areeb Ahmad

E-mail id : m.areeb.ahmad@gmail.com

* *Passwords*
* Password refers to a specific combination of alphabets, numbers and special symbols used to authenticate oneself to the website server.
* *Cracking of Passwords*
* Cracking of password refers to revealing of password from the local drive or during the transmission process. Sniffing and then targeting FTP data packets could be done because it is this protocol where the data transmitted is in ‘text-form’.
* *What passwords do people generally choose?*
* The passwords that most of us choose are stuffs related to our day to day lives. However, this is not the right way to create and use the passwords but people claim doing so makes it easy for them to remember.

Some of them include :

* Names of family members, pet animals, sports, superhero, etc
* Locations, Swears, religious stuffs
* Adding numbers to the end or the beginning
* Using high school names, name of your loved ones, etc.The motivation behind setting up the password authentication is to protect the data from the unwanted access by any other person. This process is obeyed to in order to avoid the damage to the three pillars of cyber security, that is Confidentiality, Integrity and Availability, also called as CIA. Setting up such passwords, increases the chance of happening of any of the CIA threat to the data.

# However the issue remains the same, generation of difficult password but the one that could be remembered.

* *Proper Password Policies :*  
  The proper password policies include setting up of a password that is related to any one the under mentioned criteria.

1. *Your Identity* : This is probably what most of us know as biometrics. This uses your unique body attributes as your passwords. It could be either your fingerprints, face or retina. With the development in information technology and security, Microsoft introduced the world to 3D face recognition system in Windows 10. The 3D face recognition system allowed the user to claim is identity based on his facial attribute. Use of 2D item such as photographs, now could not be used in front of the devices to unlock them. The software would detect the absence of depth and can easily differentiate between a 3D and a 2D figure.
2. *Your Resources* : Often used in the banks as ATM cards, this include use of a resource that one posses to claim his/her identity. This is however not the safest way to be used as a password but it is anyway still better than being without password.
3. *Your Knowledge* : This comprises of what most of us use, a specific combination of alphabets, numbers and special symbols used to authenticate oneself to a website server/ login us to some account, the passwords and PINs. This probably has the highest level of security amongst the three. However, passwords could still be hacked, one can avoid any such situation by focussing on complexity of password.

* *Complexity of Password :*

Complexity of password refers to as a way of making the cracking of passwords more difficult by increasing the number of characters and length.

Reports and researches have shown that the complexity of the password is majorly governed by the length of passwords.

Hackers may use dictionary to find words to break into someone’s system or account. Setting up some common word as a password but with increase in the length would definitely take a very long time to get cracked if done by Brute force attack.

Microsoft policies of password complexity include following a minimum of any of the three conditions, which are mentioned below.

1. Upper Case Characters (ABCD)
2. Lower Case Characters (abcd)
3. Numbers (1234)
4. Special Symbols (\_$&\*#@%)

Amongst all the special characters, space remains so far the best one to go with.

* Some common password trends used that must be avoided are mentioned below.
* Use of ‘@’ as a : b@tm@n
* Use of ‘3’ as e : Openm3
* Use of ‘$’ as s : $ril@nk@
* Use of ‘#’ as H : #ouse
* Use of ‘0’ as O : 0p3nm3
* Use of ‘!’ as I : l3tm3!n
* The ‘@’ ‘3’ ‘$’ ‘0’ ‘!’ are known as fab-five.
* *Security Questions :*

When someone forgets the password to their account and are unable to go through the authentication process, ‘Click here if you forgot your password’ option comes into the picture. After one clicks on this, a new page is opened where in one has to answer certain questions which he had opted for during the creation of the account. It may include questions like :

* What is your mother’s middle name?
* What is your primary school name?
* Which is your favourite soccer team?
* What is your favourite dish?
* And many more of such stuffs.
* *The Problem and Challenge*

Answering these questions is very easy for someone who has sincerely forgot his password because the answers to the questions are directly linked to the life of that person.

But is it possible that someone else could answer these personal questions on behalf of the actual user?

Yes. All thanks to social media. People out there on the social media have made clear signs of their likes and dislike, be it there favourite movie, name of primary school they went to, etc. As a matter of fact more than 80% of answers could just be found out in the ‘bio’ of the user on that particular social media handle.

So the question now arises on the existence of passwords, are we secure yet? Even after answering the ‘security questions’? Are security questions really secure?

This is a real big issue and must be addressed soon as cyber security is not just the need but is the right of each individual.