Computer Password Practices and its Awareness among students - A Case Study at the Jigme Namgyel Engineering College(JNEC)

Jamyang Tashi[*], Tashi Wangchuk[**]

[*] Department of Information Technology, Jigme Namgyel Engineering College, Royal University of Bhutan

Abstract- This paper examines the current password practices and its awareness among the students in Jigme Namgyel Engineering College (JNEC), Royal University of Bhutan. Password is the most common methods or an approaches for users to validate themselves when login into any computing devices and social networking sites. The study was aimed at learning the student's best password practices in real life scenario with the theoretical background and principles in one's mind.

The study was conducted in the college distributing the survey questionnaires to 280 students and at the same time total of 120 password hashes were collected from the students' personal computers. The study has found that 78% of the respondents were aware of the best password practices and policies in setting up the strong password in protecting the one's data in the personal computers or any of the websites but when it comes to the usage, respondents choose the passwords which are easy to remember that contradicts the fact that they were aware of the password policies.

Index Terms- Best password practices; password cracking; password policy awareness

I. INTRODUCTION

Password is a string of characters used to authenticate when the user attempts to log on to the computer system or any computing devices such and laptop, palmtop, smart phone etc. The passwords are being used in order to prevent unauthorized access to any resource available with the user's computers or devices. As long as there are resources and devices of interest, there are unauthorized users making attempts to gain access to those resources and devices. Such important resources and devices have to be protected with strong passwords to avoid unauthorized access. published research work also provides a big weight-age to get admissions in reputed varsity. Now, here we enlist the proven steps to publish the research paper in a journal.

Similarly, the many of the computer user possess lots of information that should maintain the confidentiality, integrity and availability of their data at all times of their needs. In order to do so, the user must be aware of the best password practices and password policies.

A strong password is defined as a password that is difficult to guess in a short period of time either through human guessing or the use of specialized software (Rao, Jha, & Kini, 2013).

The passwords can be guessed and cracked in several ways. Using all the possible combination of characters, symbols, numbers ensures the strong password for the system but then it is still possible for users' to crack the password. The users' passwords can be cracked using cracking techniques which will yield character string that can have the same encrypted hash like the target password would have (Scarfone & Souppaya, 2016).

The user uses the passwords for protecting their data and information in the personal computers. The user also uses passwords for emails, social networking sites, and mobile devices in order to protect the identity and the information the one possess in the computer system or in the network. However the study has found that 61% of users reuse the same password on multiple accounts and also 44% of users change their password only once a year or less (CSID, 2012).

The changing of passwords on a regular basis is recommended in general to avoid the passwords being compromised. The users' passwords being known to others or getting compromised is the risk if the same password is being used for longer period of time. The users are found changing the passwords only when they are being forced to do so. Mandated password changes are a long-standing security practice designed to periodically lock out unauthorized people who have learned someone else's passwords (Ingelsant & Sasse, 2010).

The main purpose of the study was to meet the following objectives:

i. To study the awareness of the best password practices of JNEC students.
ii. To study the implementation of the best password practices in the users' personal computers while creating or choosing the passwords.

II. LITERATURE REVIEW

According to the study conducted by Helkala and Bakas (2013) in "National Password Security Survey", users own multiple user accounts where the user provides the usernames and passwords to authenticate and authorize to the systems but it is found that the same username and password is being used in multiple accounts in which it breaches the security policy and the best password practice. It is easy for an attacker or unauthorized user to guess the password of account if same

passwords are being used in multiple user accounts and systems.

Many similar studies had been carried out to protect the confidential data and secure the information being compromised. The study has found that more secure forms of authentication to be built such as special key cards, fingerprint identity, facial detection and retinal scanners are being introduced which provide simple and direct means of protecting a system or user account. However, using the passwords for accessing the system remains to be simpler and cheaper means of authentication. (COISPP, 2009).

Having strong passwords helps to lower the probability of guessing and cracking. The strength of the password is determined by the number of characters used and its complexity in which the user need to create a password using the combination of upper-case and lower-case, numeric and special characters. If the password is complex and having minimum of eight characters long, it will be difficult to guess and crack by the hackers. Even if the password gets compromised, the time taken to crack will be prolonged (Scarfone & Souppaya, 2016).

The study found that 18 to 24 year-old users used the complex passwords to protect their user accounts, however this group agreed to having reused the same password in multiple user accounts as they felt it was easy for them to remember (CSID, 2012).

Helkala, K., & Bakas, T., H., 59% of the respondents mentioned that they got awareness and guidance on selecting a good password in which 28% of these respondents got awareness from the newspapers or websites, 22% from work place, 9% from academic learning and remaining from friends and colleagues. From all respondents, 6% did not remember whether they got awareness or not and rest 35% did not get any awareness and guidance on the password best practices and password policies.

Hitachi ID Systems, (2015), the duration of the same password being in use without changing increases in which the passwords will be known by friends, coworkers in an organization, or even be guessed leading to compromise of passwords. In order to avoid the passwords being compromised in long run, organizations enforce users to change their passwords on regular basis not exceeding 90 days.

In order to protect the data of the users, security of password policies is being designed, developed, implemented and at the same time, it is also found that the password policies are breached by the people only. It seems that currently hackers pay more attention to human factors than security designers do. The passwords are mainly compromised through social engineering technique which exploits users' lack of security awareness (Adams & Sasse, 1999).

The study also found that with the ever increasing of the use of information technology, there are also ever increasing number of user who uses the technologies for the daily activities. When too many user accounts are created on the computing system and websites, the user either tries to use the same password to the multiple accounts or they use different password but those are easy to remember which can be easily compromised to the hackers. Similarly, when user uses different password for the different account, then user tend to write down on the piece of paper, books or any sort of bits as it is hard to remember which also leads to the compromising the password to unauthorized users. (HKSAR, 2008)

Brute-force attack and dictionary attacks are most common types of attack besides using the key loggers. No matter how strong the password the user has set, the hackers uses computer program or a script login with possible password combination of symbols, numbers and characters. The more complex password, the intensity of the time spent for the cracking is longer. Dictionary attack is the most common attack where the password easily gets compromised since user uses the plain dictionary works. It is found easy for hackers and unauthorized people to guess within the short span of time. (Dinei, 2010)

III. METHODOLOGIES

The study was carried out in Jigme Namgyel Engineering College (JNEC), Royal University of Bhutan in the year 2017 as it is the tertiary education where students have knowledge of the use of information technology and every students do have one or other user account with any of the computing device or webites. The study was carried out broadly using the two different methods. Paper-based survey questionnaires were distributed to 280 students randomly irrespective of the courses, gender and department that the students are studying and the data were collected accordingly. The questionnaire was adapted from the National Password Security Survey: Results, 2013. The data collected through the questionnaires were analyzed using Microsoft excel and the results were brought down in the form of percentages.

Other method used in this study was a total of 120 encrypted Windows Operating System password hashes were also collected randomly from student's personal computers of the students that too was irrespective of the gender, the course that they study and department etc. And those hash files were taken to the system where Kali Linux Operating System was is installed. There the hashes are tried brute force for at least eight hours using John the Ripper tool that is inbuilt with the Kali Linux OS.

IV. RESULT AND DISCUSSION

The total of 280 questionnaires distributed to the students responded the survey questionnaires and interestingly the study have found that 78% of the respondents were aware of the best password practices. Respondents were aware that weak password may lead to the breached the security of the

computer and user account. At the same time, study has found that although the respondents were aware of the password policies and best practices they still prefer to keep password simple. About 40% of the respondents uses the same password for multiple accounts because they find it is easier to remember single password. The study also found that 36% of the respondents never change the passwords while 31% of the respondents changes passwords on the monthly basis.

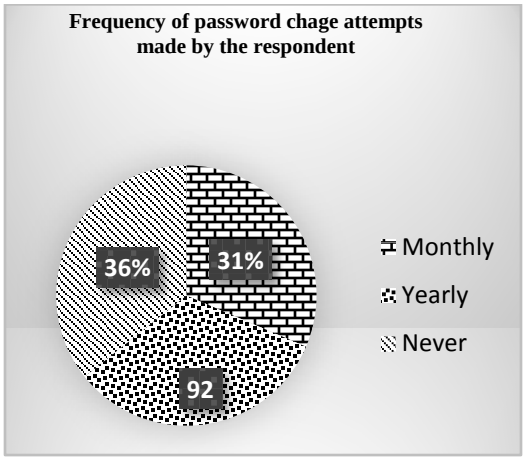

Fig 1. The frequency of password change attempts made by the respondents.

While coming to the habit of sharing password within the families and friends, 32.86% of the responded that they have at least shared their passwords with to either family members, friends among which family members was highest. The study also found that other 67.14% responded that they keep password up to themselves not sharing to anybody.

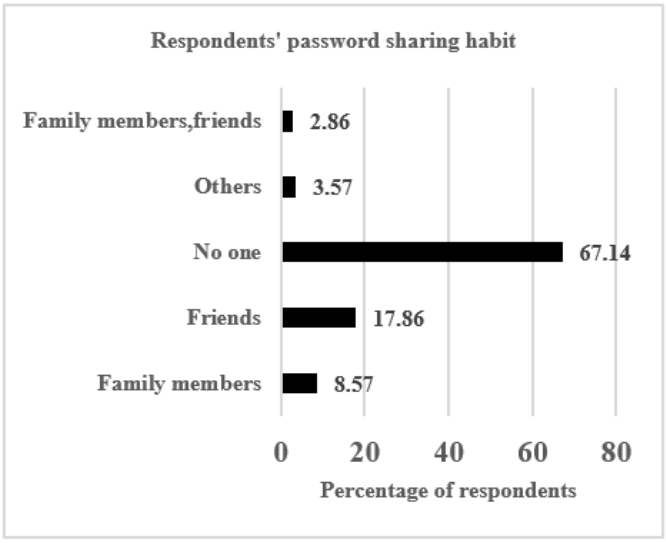

Fig 2. Percentage of respondents sharing passwords

The total of 120 encrypted password hashes collected from the students' personal computers, about 56.66% of the hashes were cracked within 8 hours of time which indicates that the users have not used strong password to protect their personal computer system which is otherwise called weak passwords as per the password guiding policy. From the number of cracked password hashes, the study has found that 41.18% of the passwords were either person's names or non-dictionary word (in lowercase), followed by either personal phone numbers or only numbers less than 8 digits (29.41%), dictionary word (14.71%) and alpha-numeric (14.71%). While coming to the phone number being used as the password for the personal computers or any of the user accounts on the websites, it is easy for hacker or disgruntle user get hold of the system.

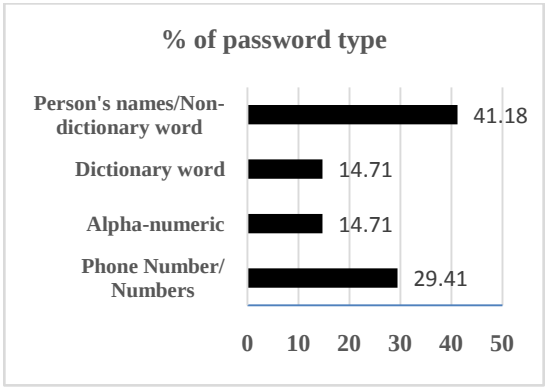

Fig 3. Percentage of the types of passwords used

V. CONCLUSION AND RECOMMENDATION

The study was conducted in Jigme Namgyel Engineering College (JNEC) and all respondents were aware of the best password practices and they are also aware that weak password on their system or any account may lead their data and information prone to an attacker. In real life situation and practicality, respondents preferred to use the simple passwords because it was easy for them to remember. The respondents feel that they like to choose the password which are not complicated but those are prone to an attack. The study clearly states that the theoretical knowledge on the best password practices is not being implemented practically and this kind of study reminds the users and the respondents about security measures to be taken up in protecting the confidentiality of the information, integrity of the information and availability of information at all times of their needs. The similar kind of studies can be conducted in colleges and tertiary educational institution where the usage of the information technology is intense and accordingly, users of the information technology will have an opportunity to reflect upon their knowledge and actions to protect their information and data in the personal computers, social networking sites and so on.