STRATEGIES FOR OPTIMIZING PASSWORD MANAGEMENT AGAINST VERSATILE ATTACKS

KULE TITUS

BCI/38127/123/DU

&

BAKWANAMAHA ALLAN

BCI/38384/123/DU

AUGUST 2016

STRATEGIES FOR OPTIMIZING PASSWORD MANAGEMENT AGAINST VERSATILE ATTACKS

BY

KULE TITUS

BCI/38127/123/DU

&

BAKWANAMAHA ALLAN

BCI/38384/123/DU

A REPORT SUBMITTED TO KAMPALA INTERNATIONAL UNIVERSITY IN PARTIAL FULFILLMENT OF THE REQUIREMENT FOR THE AWARD OF THE DEGREE OF BACHELOR OF SCIENCE IN COMPUTER ENGINEERING

AUGUST 2016

DECLARATION

We hereby declare that this project titled Strategies for Optimizing Password Management against Versatile Attacks is our original, and no any other institution has ever presented it.

It contains neither materials previously published by another person nor material, which has been accepted for the award of any other degree of the university, except those, that due acknowledgment has been made in the text.

Signature……

Date……...

KULE TITUS

Signature……....

Date……

BAKAWANAMAHA ALLAN

APPROVAL

I have read and hereby recommend this project titled Strategies for Optimizing Password Management against Versatile Attacks for acceptance by Kampala International University in partial fulfillment of the requirements for the award of the degree of Bachelor of Science in Computer Engineer of Kampala International University.

_____

Mr. Adabara Ibrahim

Asst. Lecturer (SEAS)

Supervisor

DEDICATION

This project is dedicated to the Glory of God, and to our beloved families.

ACKNOWLEDGEMENT

Primarily we would like to express our thanks to the Almighty God whom without none of this would have been possible. He has provided us with everything we needed to accomplish what we were aiming for, and gave us the strength to go through it up to the end.

We would like to extend my acknowledgment to all the people who provided assistance during production of this report.

More thanks go to our Project Supervisors Mr. Ibrahim Adabara for their professional guidance and support, his valuable suggestions without which it would not have been possible to develop this project.

We are also grateful to our course mates for assisting us with the necessary resources for this project.

ABSTRACT

Managing passwords is a significant problem for most people in the modern world.

Passwords are a critical part of information and network security. Passwords serve as primary authentication method to protect user accounts but a poorly chosen password, if compromised, could put the entire network at risk. Many users do not understand why good passwords and password management are important for information systems. “We’re secure! We use passwords!” How many of us have heard this claim? Or even “We’re secure! We have a password policy!” Using a password or having a password policy in today’s world of computing is not enough. Understanding and practicing the policy is important to keep accounts secure.

In this project research, the author has conducted a survey to check password habits for user accounts on 200 academy staffs, non-academy and students within Kampala International University (Kampala campus). This survey allowed the author to understand password habits of users according to sensitive of their account, also reveals some critical issues associated with password choice. As a result, data on password strength, the types and lengths of passwords chosen, and how they vary by site or sensitivity of account has been considered.

Furthermore, recommendations are given based on different aspects of users` requirements. Hopefully, the result of this research project will be valuable to users who want to use password policy for securing user accounts.

TABLE OF CONTENT

LIST OF FIGURES

Chapter Two

Chapter Four

LIST OF TABLES

Chapter Four

CHAPTER ONE

INTRODUCTION

1.0 Introduction

The average user logs on to several systems each day by using passwords. Passwords are used to secure valuable data. Online services including banking, voting, mail, social networks, and commerce and enterprise resources depend on passwords in order to maintain secure transactions. The typical user has multiple password protected accounts and needs to manage each password. As the number of accounts increases, the management of passwords gets complicated. As a consequence, many users tend to adapt weak password management schemes which can significantly reduce the security of the system.

1.1 Background

In this age of IT revolution, Computer and Information security is the important issue, when whole world is connected to the internet. As users are dependent on computers and electronic media for connecting to the internet, it is important we rely on secure and confidential connection. Therefore, security has become major issue to consider for protecting data from indirect and direct attackers. Security areas like Firewalls, Intrusion detection system, Access control, cryptography, identification and authentication has been in wide use nowadays.

Authentication is the most ubiquitous form of identification method used as user access control to the system. Although other methods such as biometric identification and personal digital signature have been developed, user authentication is widespread. User authentication is the combination of username and password. Username is identity by which the user is identified. A password is information associated with username that confirms the user's identity (Bishop, M.), which may be used to grant, or deny access to user from secure system.

Passwords play a major role in the web user's life. They are universal means to gain access to all kind of user accounts that are protected. For example Email, bank accounts, social networking and portals. Passwords can be biometric image, design pattern or simple text.

Text passwords have dominated human-computer authentication since the 1960s (M. V. Wilkes). These passwords are created using alphanumeric characters.

Since passwords protect accounts with valuable assets, they have increasingly been subjected to attacks. Phishing attacks, where a user is lured into submitting information such as usernames, passwords and credit card details by masquerading as a trustworthy entity (Definition of phishing). Shoulder-Surfing, where access to user's password is known by looking over the shoulders of the user while typing password (Arash Habibi).

Passwords can be protected by using long passwords, non-dictionary words, using users own way of encrypting password. But sometime user tends to forget long passwords, so it is better to follow the password policy, which tells user how long the password should be, using different case letter to create a secure password, changing password in a period of time to escape from brute force attack. A password attack which continuously try different password combination, that are commonly used and all dictionary words (J. O. Pliam).

1.2 Problem Statement

The problem statements in this project are as follows:

- Does every user have different methods of choosing password?
- What specific aspects of password policy causes problems for users?
- Are there unexpected password issues not covered by existing policy?
- How to use this result to perform good password policy?

Password habits will be collected from different users of different age group. Then based on the results of the users, analysis will be done on the data. Everyone who has access to any password protected accounts, or access to password protected information, are expected to follow the guideline of the password policy. The purpose of password policy is to establish the rules for creation, safeguarding and termination of the user authentication.

1.3 Significance of the Project

With increasing reliance on computer systems worldwide for data processing and information storage, the need for legitimate security of information and data cannot be overemphasized. Unauthorized access, revelation or destruction of data can violate individual privacy and even threaten the existence of an organization. Since information is regarded as the live wire of an organization, it is, therefore, necessary to secure computer systems and the stored information.

Password is the key for authentication, which is unique for every user. But password policy is common for all the users. The weakest link for security is human, who chooses weak password and does not follow proper password policy.

This project research will help everyone who has access to any password protected accounts, or access to password protected information, are expected to follow the guideline of the password policy. Which will help them to establish the rules for creating password, safeguarding your data or information's and termination of the user authentication.

1.4 Objectives

1.4.1 General Objective

The objective of this project research to analyze the password usage methods and policy users follow to create passwords for their accounts. With the data collected from users, the analysis is done to see the password reuse and memory technique. Password parameters are considered to analyze the data.

The data was collected from 200 users and analysis is done with respect to that data. The main objective of this project research to make users aware of the password parameters, that is to be followed while creating the passwords and importance of following the password policy.

1.4.2 Specific Objectives

Specific objectives that this project research will achieve are the following.

- To highlight different methods and strategies for password usage and remembering.
- To carryout survey on the use of password among academic staffs, non-academic staffs and students in Kampala International University.
- To understand why individual find it difficult to follow password policies and recommend the use of password policies.
- To differentiate between high, moderate and low sensitive account.
- To understand the danger of password reuse and memory technique.

1.5 Scope of study

The scope of this project research will be limited to academic staffs, non-academic staffs and students in Kampala International University environment (Kampala Campus).

1.6 Outline of the Project Report

This project research is structured as follows:

Chapter 1 – Introduction - This chapter introduces the project by giving description of the problem and discusses about the background of the project, problem description, aims and objective.

Chapter 2 – Literature review – This chapter provides information relevant to password management and users‟ strategies to manage password.

Chapter 3 – Methodology – This chapter explains the methodology used in the project research, and provides information of the data collected.

Chapter 4 – Data Analysis and Discussion – This chapter presents the analysis of data and also discuss about the results achieved, and users` strategies in choosing passwords.

Chapter 5 – Conclusion and Recommendations – This chapter provides conclusion to the project research and some recommendations for users are also included.

CHAPTER TWO

LITERATURE REVIEW

2.0 Introduction

This chapter provides a general overview of security, outlining its goals, then its general techniques, followed by a more focused description of the techniques used for authenticating users, i.e., password. Finally, introduces to password policy which is the major requirement to create secure password.

2.1 Literature Review

Passwords are the key to security, it secure our account and personal data from others. Passwords are the cheapest way to secure our account. Password is the word which we hear many times in our day to day life. When considering the password authentication, user has to think about human and technical aspect of the system (John McCumber). Password authentication which is the easiest way to get access to the system, while new techniques like considering one time password additional to the regular password is used to secure the account. One time passwords are used in banks, governments and cooperate virtual networks to keep their users‟ account secure (Kenneth G. Paterson & Douglas Stebila).

One time passwords are used mostly in banks, but regular passwords are used everywhere in the user accounts, so user must be made aware of the importance of regular passwords. And policy should force them to use strong passwords. According to (Adam and Sasse), weak passwords are not created by carelessness of user but due to the weak password policy. Weak password policy, which does not force user to create strong password, when they are creating short length and dictionary passwords. Another problem next to weak password is reuse of password. Password reuse, which can become the gateway to another account of user, which has the same password. According to (Karen), password reuse cannot be prevented but it can be avoided by instructing the user.

Passwords are reused because it's easier to remember. But according to (Smith), password must be impossible to remember and never written down. Most users practice the habit of writing down there passwords somewhere in the table side or below keyboard or keeping sticky notes in purse.

There have been related works done before, like doing survey and finding the users habit of password management. Survey seems to be the best way to find the way users manage their passwords.

In 1979, survey was done by (Morris and Thompson) over 3289 passwords, in which they found 89% of the passwords where weak. Weak passwords are created due to the lack of knowledge about the policy.

In 1989, (Riddle and Miron), conducted the survey in the university. The survey was done by 6226 students and staff. They found that 72% of the passwords where short and dictionary words.

In 2004, (Brown and Bracken), conducted the survey on 218 students at Southern Methodist University, they found that 92.9% of the students reuse their passwords for multiple accounts.

In 2006, (Gaw and Felten), conducted the survey on 49 students from Princeton University, they found that students where reusing their passwords for multiple accounts. They even said that password reuse will become one of the bigger problems in the upcoming time.

The previous surveys where useful to conduct new survey, as that gave more idea to new surveyor to understand the habit most users follow to manage their passwords.

Conducting the survey also makes user more aware of password security and its importance. So when they are not aware of certain policies, and they come across that policy while doing survey, which makes them aware of it and they turn to secure their account by using that policy. There are many people, who have showed there interest on working with password policies and managing strategies, which gave more interest for me to work under password policy.

2.3 Security

With the rapid development in computer and network systems, it has become major issue to think about security. Security which means protecting secret information from illegal and unauthorized users. Security is the step which has to be followed in daily routine, for example using your website accounts give passwords, travelling by flight go through security check in, creating account in banks or government office show your identification card, and working in

office or studying in university have to swipe card to open the doors. So security has become source to be secure from any problem.

2.3.1 Computer and network security

Defining "computer and network security" is not trivial. The difficulty lies in developing a definition that is broad enough to be valid. Dieter Gollman defines computer security as: ”prevention and detection of unauthorized actions by users of computer systems” and ”measures we can take to deal with intentional actions by parties behaving in some unwelcome fashion” (Dieter Gollman). Computer security is frequently associated with three areas, which can be classified by the acronym "CIA", this is most commonly described as CIA model:

Confidentiality: Ensuring that information which users are providing from security is not accessed by any unauthorized persons.

Integrity: Ensuring that unauthorized person does not alter any information of authorized user, which is undetectable by the authorized person.

Authentication: Ensuring that person who is authorizing is the correct person, who has to be authorized.

Computer security is not just associated with these three areas, its future considered by Access control, Non-repudiation, Accountability, and privacy. While several techniques are used to protect computer from attackers, it is considered that most computer crimes are in fact committed by insiders, and most of the research in computer security since 1970 has been directed at the insider problem (Morrie Gasser).

2.3.2 Security threats

Security threats are mainly classified in two major categories, logic attacks and resource attack. Logic attacks are known to exploit existing software bugs and vulnerabilities with the intent of crashing a system. Some use this attack to purposely degrade network performance or grant an intruder access to a system. Resource attacks are intended to overwhelm critical system

resources such as CPU and RAM. This is usually done by sending multiple IP packets or forged requests (Definition of logic and resource attacks).

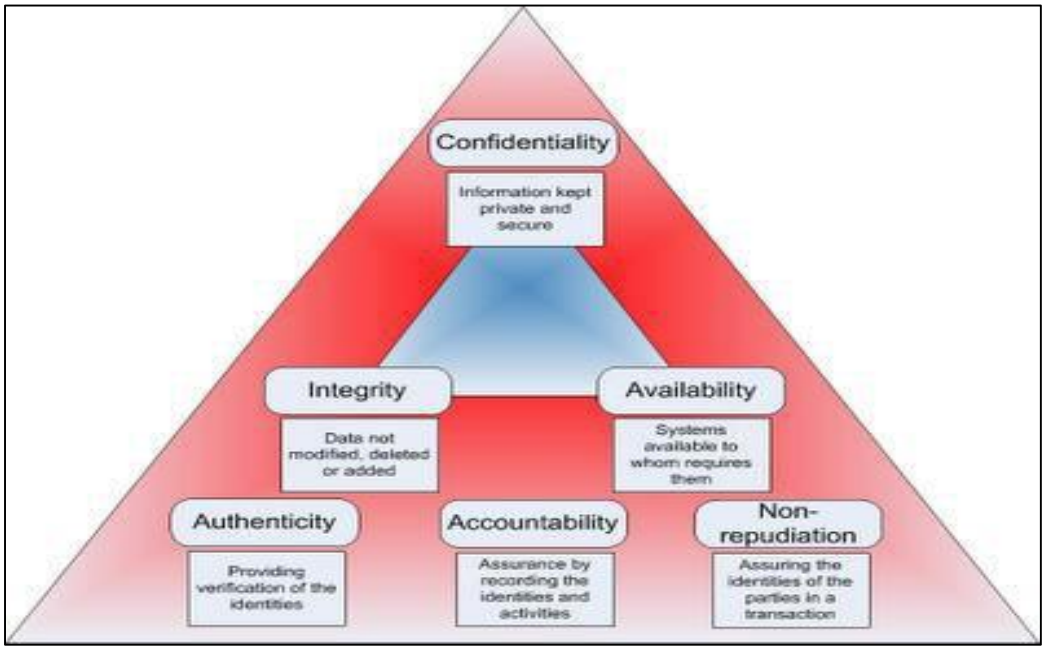

Figure 2.1 CIA model

Viruses

A software virus is a parasitic program written with the intention to modify data on the computer, without the knowledge of the user of the computer. Viruses are usually received or spread by email attachments, and infected files.

Adware

Adware (Advertising-supported software) displays advertising banners or pop-ups on computer while users are using application to run their programs or install software. Adware is not problem unless it install on the computer by itself without permission and starts running unwanted applications in the background with more banners or pop-up windows. Hijacks web browser to display more advertise banners.

Backdoor Trojans

Backdoor Trojans allows unauthorized user to take control over authorized user's computer via the internet without authorized user's permission. Once the Trojan start running, it adds itself to the startup process to monitor the user's computer until the user is connected to the internet.

2.4 Security Tools

2.4.1 Intrusion Detection System

Intrusion detection (ID) is a system that collects and analyzes information from different area within a network or within a computer to identify possible security attack from someone attempting to break into or compromise a computer. There are several ways to categorize Intrusion Detection System (IDS) (Seymour Bosworth and M.E.Kabay):

Misuse detection vs. Anomaly detection

In misuse detection, the IDS analyze the information it gathers and compares it to large databases of attack signatures. Essentially, the IDS look for a specific attack that has already been documented. In anomaly detection, the administrator defines the baseline, protocol, and typical packet size. The anomaly detector monitors network segments to compare their state to the normal baseline and look for anomalies.

Network based vs. Host based systems

In network based system [NIDS], the individual packets flowing through network are analyzed. This system is designed to detect malicious packets. It gains access to network traffic by connecting to a network hub. NIDS can be installed as software package in workstation that is connected to network. NIDS functions in the same way as high end antivirus. In the figure it represents the typical NIDS scenario, where an attempt has been made to increase the traffic through NIDS device on the network. Figure 2.2 shows NIDS network (Image of NIDS and HIDS).

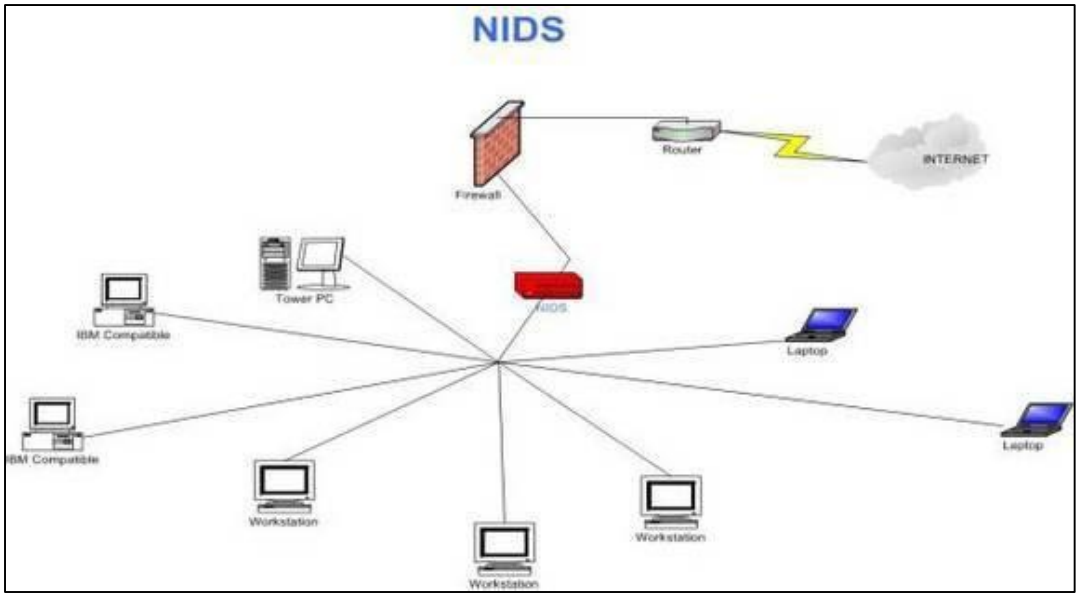

Figure 2.2 NIDS network

Host based system [HIDS], consists of an agent on a host that identifies intrusions by analyzing applications log files. It is installed locally on host machines making it easy to analyze. In host based system, the copy of log files is taken and checked frequently with new log file to see if there is any attack. Figure 2.3 shows HIDS network (Image of NIDS and HIDS).

Passive system vs. Reactive system

Passive intrusion detection systems simply detect threat and send alerts to the user. When any malicious traffic is detected, the system generates an alert and sends it to the user, for verification whether to block it or response to the alert.

Reactive intrusion detection system not only detect the threat and alert to the user, but also take pre-defined proactive actions to respond to the threat. Reactive system is also known as Intrusion prevention system (IPS), as it automatically response to the threat and block the traffic from that source IP address.

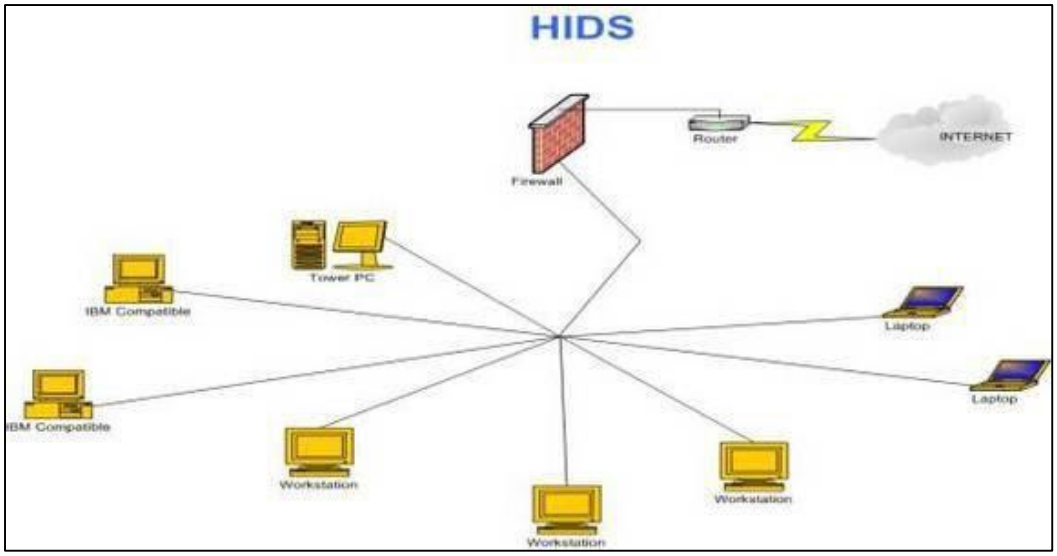

Figure 2.3 HIDS network

2.4.2 Firewalls

A firewall system can be composed of many different devices and components. The main component is traffic filtering, which is commonly called Firewall. A firewall allows or blocks traffic into and out of a private network or the user's computer. Firewalls can be either software-based or hardware-based.

Software Firewalls

Software firewalls is the firewall used on individual users computer. Firewall is installed on computer like any other software's, it can be customized as per users‟ requirement, for protecting their system from outsiders. Software firewall will only protect computer in which it is install not the network.

Hardware Firewalls

Hardware firewalls is the firewall that is built into a router or a stand-alone device to protect the network. It can be effective with no configuration, and will protect every system in the local network.

Types of Firewalls

There are three different types of firewalls used in the network, depending upon the communication in the network. Firewall runs in the layers of ISO/OSI model. The OSI model

describes how information is transmitted from an application on one computer to an application on another. Each layer performs a specific task on the information and passes it to the next layer.

Packet-filtering firewall

This firewall is typically a router used to filter packet content in the layer 3 and layer 4. Firewalls validate packets based on protocol, source and destination IP address, port number. Packet filtering is commonly used with Access Control List (ACL) on routers or switches. Since the filtering technique is performed at lower layer, there is problem with packet filtering as there is no means to verify source address. Figure 2.4 shows packet filtering firewall (Types of firewalls).

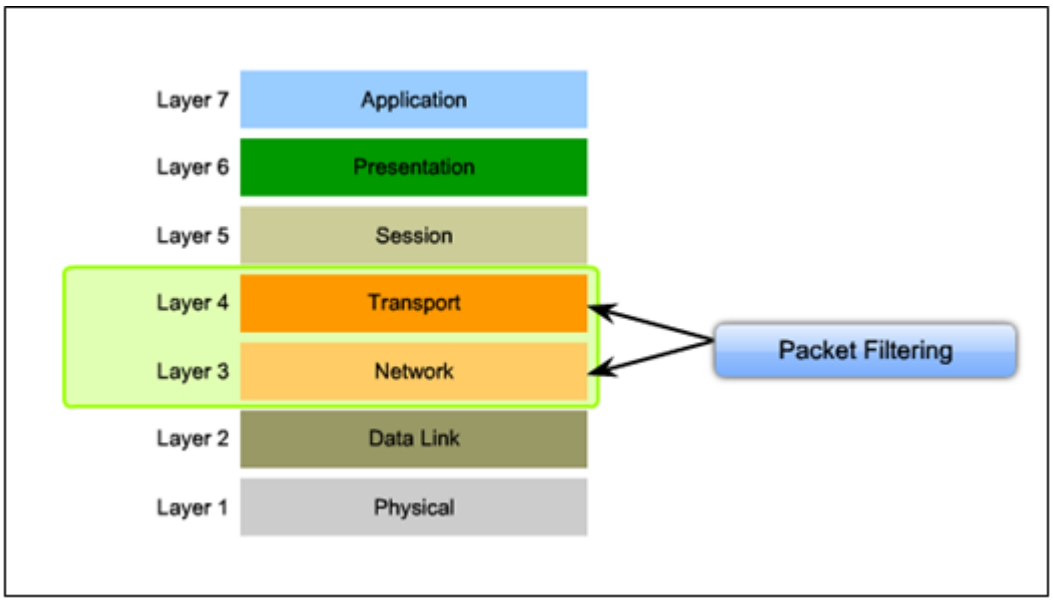

Figure 2.4 Packet filtering firewall

Application gateway firewall

Application firewalls, as indicated by the name, work at Layer 7 or the application layer of the OSI model. These firewalls intercept all packets travelling to and from application layer. When the client wants to make a connection to the internet, it first connects to the proxy server, from where the connection is established. And the proxy server act behalf of the client for hiding

and protecting the information. Figure 2.5 shows application gateway firewall (Types of firewalls).

Address translation firewall

A firewall that expands the number of IP addresses available and hides network addressing design. Figure 2.6 shows Address translation firewall (Types of firewalls), it is categorized into two types: network address translation (NAT) and port address translation (PAT)

Network address translation provides the capability to change source and destination IP address. This method is used when private address is used internally. NAT has one-to-one connection between inside and outside IP addresses.

Port address translation provides the space for using private address internally and using one public IP address. PAT has one-to-many connection, and can be used by client to access multiple resources using same IP address.

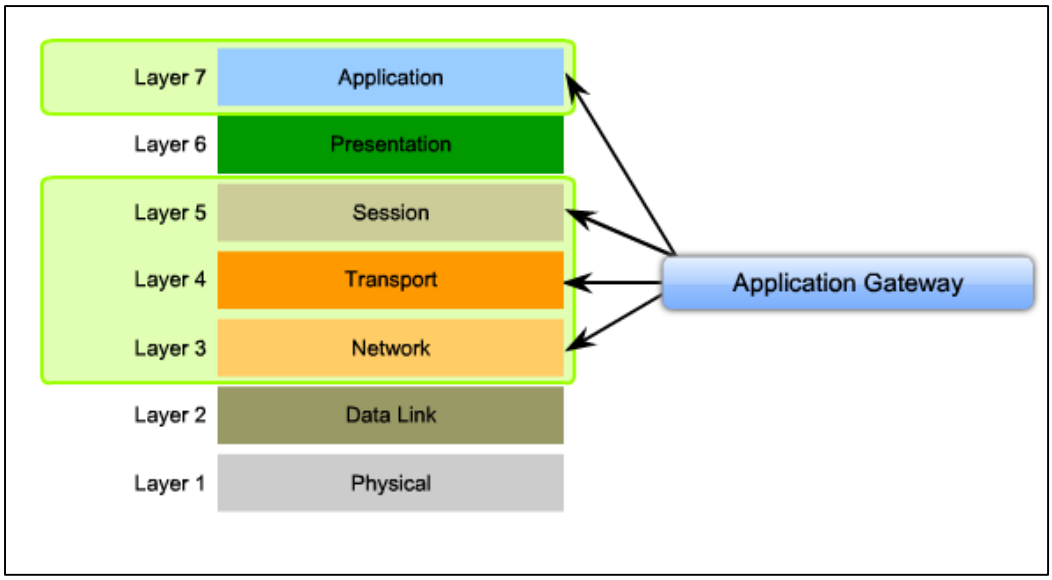

Figure 2.5 Application gateway

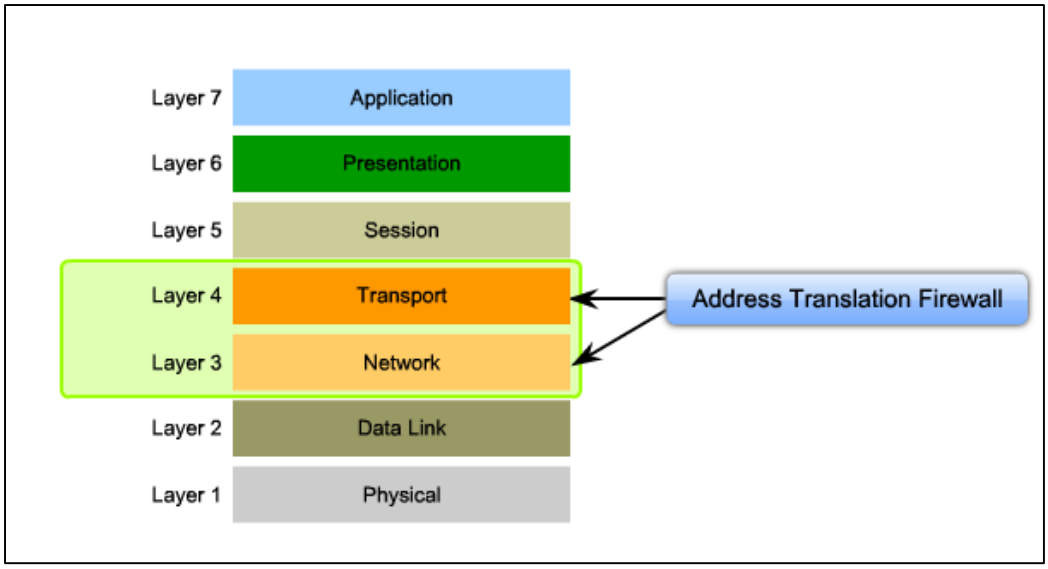

Figure 2.6 Address translation firewall

2.5 Authentication

Authentication is the process of verifying the identity of the user through special credentials, as a prerequisite for granting access to the system. Every time when users‟ want to access the secure system, they need to pass through authentication process to prove their identity and get access to the system. Some system requires several authentication steps to reduce the risk of attacker using the system (Seymour Bosworth and M.E.Kabay).

Authentication process is the key to unlock your system, to get access to information in the system. In some system, where there is high security to keep the information secure, they provide re-authentication (Sausan Yazji, Xi Chen). In this process, users` are required to give identity information for future security. Re-authentication process is commonly used for internet banking.

Dieter Gollman describes authentication as:

i. Something you know (passwords).
ii. Something you hold (token).
iii. Who you are (your body).
iv. What you do (your actions).
v. Where you are (space, time, context).

From the description of Dieter Gollman, authentication can be classified in three categories knowledge-based authentication, Token-based authentication and biometric authentication.

2.5.1 Token-based authentication

Token-based authentication, where the user presents some physical or digital object to the computer that is only with the user, for providing the security. Tokens are designed to be unique and difficult to forge. But tokens are so easy to pass on, take away or misuse. So token- based authentication is always used in combination with other authentication methods (Svigals, J.). Therefore, using token-based authentication increase the number of passwords, instead of decreasing them, this brings more difficulty for user's then simplicity. Examples of token-based authentication are smart cards, USB tokens or one- time passwords to mobile device or email.

2.5.2 Biometric authentication

Biometric authentication, where the user presents themselves to the computer for examination, so that it recognize there characteristic and give access to them to the system. These characteristics are unique and cannot be replicated. Biometrics are often used as an ultimate replacement of passwords (Murrer, E). There are two kinds of biometric authentication, physiological biometric authentication and behavioral biometric authentication (Dunn, Jeffrey S. and Fernando L. Podio). Figure 2.7 shows the methods of biometric authentication (Biometrics).

Physiological biometric authentication analyzes the physiological characteristics of an individual. Physiology is “a branch of biology that deals with the functions and activities of life or of living matter (as organs, tissues, or cells) and of the physical and chemical phenomena involved" (Physiology). This biometric authentication deals with fingerprints recognition, face recognition, hand and finger geometry, iris recognition and DNA analysis.

Behavioral biometric authentication analyze user based on the behavior, and the manner in which they conduct themselves through various activities. Behavioral authentication focus on signature recognition, voice recognition and keystroke recognition.

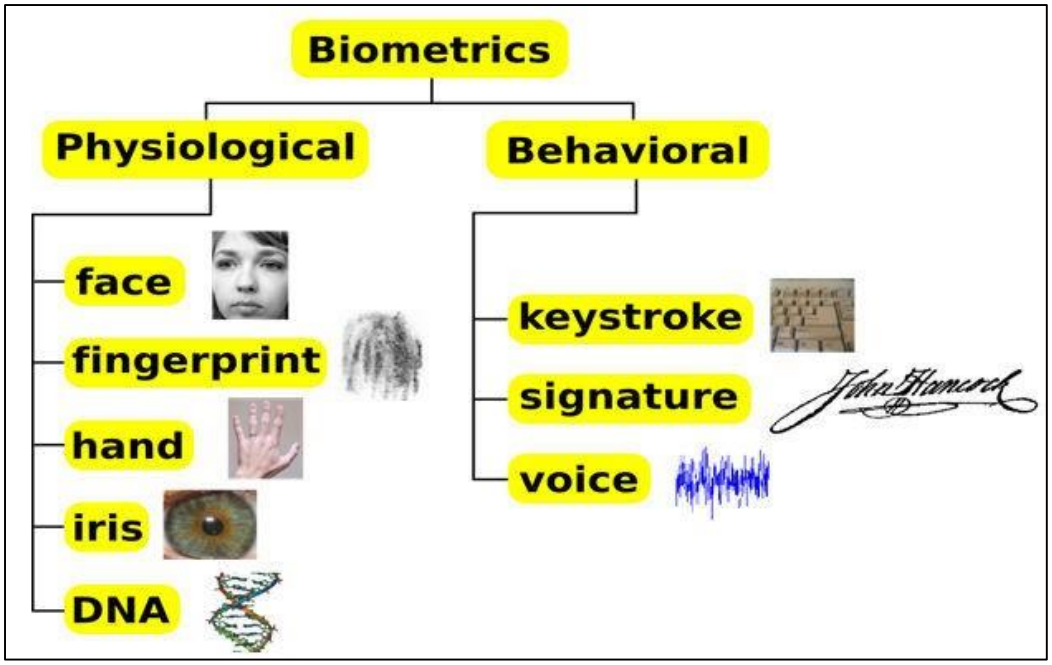

Figure 2.7 Types of biometric

2.5.3 Knowledge-based authentication

Knowledge-based authentication (KBA), where the user gives an secret information to the computer to recognize them, to get access to the system. Knowledge based authentication is mostly commonly referred to user password, which user creates with his own knowledge to access the system. Knowledge-based authentication can be classified in two types: static KBA and dynamic KBA.

Static KBA refers to a pre-defined questions, for which user has provided answers. When there is chance of forgetting password, then password can be retrieved by using these pre- defined questions.

Dynamic KBA is the more secure form of KBA, as the questions are not pre-defined. It does not rely on the information which is often publicly available about the user.

2.6 Passwords

The password is a string of characters that can either be automatically generated by the system (system generated password) or selected by the entity or user (user defined password). Passwords are used with username to get access to the secure system. Passwords can range from a single character to passphrases, which can be hundreds of characters in length and be

comprised of series of words and phrases. The goal of a password is to authenticate a user. It is a piece of information that the user knows.

2.6.1 Why do we need a password?

Passwords are used to secure a system or account, in which users‟ have their secret and personal information, in other words by using password user has secure their system or account from unauthorized user. A typical user has password for many purposes: logging in to web account, reading email, using social networks, using banking accounts, and many more the purposes go on. As the passwords keep on growing, the purpose to maintain secure account also keeps growing. The account is secure when it has secure password. User should never limit the password with personal information, as it is easy to guess and used by unauthorized user. User should create a strong password.

2.6.2 Password vulnerability

Passwords are the weakest link in the network. Strong passwords are difficult to crack or guess by unauthorized user, but easy to create and maintain. Knowing a password doesn't make someone an authorized user. The two general classifications of password vulnerabilities are organizational or end user and technical vulnerabilities (Kevin Beaver).

Organizational or end user vulnerabilities

This vulnerability is about lack of awareness on the part of end users and the lack of password policy that are enforced in the organizations. There are almost 3 trillion (eight- character) password combination possible using 26 letters of the alphabet and 0 to 9 numerals (Kevin Beaver). However, users like to create password that are easy to remember.

Technical vulnerabilities

This vulnerability is about weak encryption method and insecure storage of passwords on computer systems. When there is weak encryption method, it is easy to crack down password using password cracking software. Passwords should be encrypted in the way, as it is easy to remember by the user, but difficult to crack down.

2.6.3 Password cracking

Password cracking is the most used technique to hack the account of the user. Cracking can be done in two ways low-tech method which is using social engineering, shoulder surfing, and simply guessing password from user information and another is high tech method is using a password cracking software. High tech password cracking methods are dictionary attack and brute force attack.

Social engineering

Social engineering is the method of asking password, directly to the user. Hackers, make a telephone call to the user and are able to convince the people by means of emotions and trick them to give the information. To escape from social engineering, there is only one way, user awareness. Training user to understand that secret information should not to be shared in telephone to unknown users.

Dictionary attack

Dictionary attacks are performed using the words from dictionary, and most common used words. Another thing a hacker will to do is, run a program which will attempt to guess the correct password. In addition to dictionary words, it uses movie names, novels. To escape from dictionary attack, user should be trained not to use common words, dictionary words.

Brute force attack

Brute-force attacks can crack any password, in given sufficient time. Brute-force attacks try every combination of numbers, letters, and special characters until the password is discovered. It consists of systematically checking all possible keys until the correct key is found. In the worst case, this would involve traversing the entire search space. To get rid from brute force attack, the easiest way is to change password frequently.

Users should be made aware of the password cracking techniques, so that they can escape from there password getting hacked, and loosing there secure information. For this purpose user should follow and understand the password policy.

2.6.4 Password policy

Password policy, gives instruction to the users, how a password should be. So they can secure their account and system. Passwords are the key to get into users system to hack there information.

Strong Passwords

Strong password, which is the main and important policy to be followed while creating a password. Strong passwords should have length more than 8 characters. A good password has both upper and lower case letters, has digits and punctuation characters as well as letters, is easy to remember, so it does not have to be written down, is seven or eight characters long, and can be typed quickly so someone else cannot look over your shoulder (Garfinkel, S. & Spafford, G).

Passwords should not contain any words from the dictionary of any language. Many policies also inform user not to user previously used passwords. Instead of creating passwords with words, there is choice of creating a passphrase, which is the best way to secure your account and create the strong password.

Multiple Passwords

Multiple passwords, requiring users to create different password for different account. Many users felt it very hard, as it is complicated to memorize so many passwords and remember this password belong to this account. It also created more problems to user like forgetting password or forgetting to which account which password belongs. There are systems that frequently revoke a user's access to the account after a password has been entered incorrect for three times. Therefore there is compromise between user memory to remember many passwords and security of the system. User can create multiple passwords but with same pattern, so that it’s easier for them to remember.

Changing Password

Password changing is the procedure of changing password frequently, at least once in the six months. Many users never follow this policy, they never change their passwords. Some user, use same passwords for years. Website accounts do not have this policy of changing password on regular basics, they never mind if their users are using same passwords without changing.

Universities and banking websites have this policy as they mail users that their password has to be changed as it has not been changed in last 6 months. Changing password regularly secures user from high tech password cracking method.

Password Reuse

Password reuse is the problem of reusing same password for multiple accounts or using same password frequently while changing password. Users should be made aware of problems while reusing same passwords. Users should be made clear with the policy of not reusing password. They should be told that they can use same pattern for their passwords instead of using same password. When users are reusing their passwords, they are giving easy access to unauthorized users, as reused passwords are easy to crack.

Writing down Passwords

It is hard for human mind to remember multiple passwords for multiple accounts. The easiest way to remember is writing down it on paper or any device or having a copy in mail. Users should be informed while creating passwords, that they should never write their passwords anywhere or share with anyone. Password is the secret which has to be secret. Writing down passwords for easy access can give access to unauthorized person also, if he got our password. Sharing passwords over phone or mail should also be avoided, as there can be a man in the middle, who can get our password. Then it gives access to him to authorized users account.

Dictionary

Dictionary words are used by users to create their passwords. Some users try to use mixing of 2 or 3 dictionary words to create a single password. While some users try to use words from other countries language dictionary. Users should be given information regarding usage of dictionary words from local language dictionary or other foreign language dictionary, can be hacked and easily get access to authorized account. Dictionary attack is performed on the authorized account to find the password, if it has dictionary password, then hacker unauthorized user get complete access over authorized account.

Personal Information

Using personal information to create passwords like nickname, date of birth, telephone numbers, school or university name, parents, siblings or close friends name, street name, and

etc. There are many users who use personal information as their passwords, such users should be made aware of security of using unsecure password.

Securing passwords from outsider is the major issues to understand. To secure your accounts from outsider, best practice is to create strong passwords, change passwords frequently on regular basics, never sharing passwords with anyone, erasing the habit of writing down passwords, never using personal information and not using same password for multiple accounts.

CHAPTER THREE

METHODOLOGY

3.0 Introduction

This chapter describes the research method used in this project research. Password parameters like sensitivity of the account, password remembrance technique, pattern matching is considered for analysis.

In data collecting process, data are collected from multiple users and there way of using passwords for their accounts. Data graphs are created from the information taken from the users, so that it is easy to recognize the pattern in which users create passwords.

3.1 Objective

The objective of this project research to analyze the password usage methods and policy users follow to create passwords for their accounts. With the data collected from users, the analysis is done to see the password reuse and memory technique. Password parameters are considered to analyze the data.

The data was collected from 200 users and analysis is done with respect to that data. The main objective of this project research to make users aware of the password parameters, that is to be followed while creating the passwords and importance of following the password policy.

3.2 Environment

The data are collected using a survey method. A survey is one of the best tools to understand a present situation (Wakefield, R. L) The author of this project research developed the survey questions, and loaded onto the webpage (www.infotechinedu.com). The webpage link was given to users by email, and the survey was voluntary. The survey was accessible for one month, so that users can give their habit of using passwords. The survey was made in such a way that, user can takes the survey only once and cannot change the answers after finishing survey.

Once the survey was done, data was collected and plotted in graphs. So that it is easier to analyze the data and understand the habit of users, to manage their passwords. The data where

plotted according to the questionnaire. The main aspect that was considered while analyzing the data was, are users following the password policy correctly while creating passwords.

3.2.1 Parameters

The parameters that are considered for analysis are:

Writing down password

Writing down password, if they are writing down, are they doing it in secure way or using unsecure way. Like using encrypted or encoded method to write the password, or directly write it in clear text.

Voluntarily changing password

Voluntarily changing password are they changing password regularly, or changing only when system forces them to change password. If system is not forcing, are they using same passwords for years without changing.

Number of passwords currently

Number of passwords currently using how many accounts a single user has with passwords. This was considered to analyze, the number of passwords user has to remember.

Passwords ever been shared

Passwords ever been shared are users sharing their passwords with others. If they are sharing, what means of transmission are they using for sharing their passwords.

Using same password or pattern

Using same password or pattern are users using same password or same pattern for their multiple accounts. If they are using same password or same pattern, are they doing same things for both high and low sensitive accounts?

3.2.2 Limits of the data

The data may not include the true feelings and attitude of the responder. The technique was to use open-ended question to capture the feedback and the way of password habits. The data collected was analyzed using the password policy, to examine whether the user follows the policy or not to create secure password.

Many times user wants to create secure passwords, but forget to meet the password policy. Therefore, it leads outsider to get hack of your information. So it is always valuable to consider policy even if you create strong password.

From the data collected, the analysis is done on the password parameters. The analysis will also consider the sensitive of the account, and its password managing technique.

The sensitive of the account is categorized in three ways: High sensitive account, banking, and primary email

Moderate sensitive account are social networking site, secondary email, shopping website

Low sensitive account are news website, wiki

The analysis also considered about users usage on account, are they regularly using their accounts or rarely. It considered the parameters like:

Daily, Weekly, Monthly, and Yearly.

This was considered to check the frequency of usage. If they are rarely using their accounts, then there is a chance of forgetting password, so this increases the case of writing down their passwords, so they can remember when they are accessing their accounts.

The analysis also considered parameters like using mixed characters. Are users using mixed characters for creating passwords by their own pattern or they are doing so only when forced by the system to do so.

The analysis was done on the basis of the data collected and considering the policy that are supposed to be followed while creating the secure password.

CHAPTER FOUR
ANALYSIS AND DISCUSSION

4.0 Introduction

This chapter provides analysis of the data collected from the survey and discussion. The analysis is done by considering every parameters of the password policy. The analysis describes the users‟ way of following the password management to maintain their accounts and keep their passwords secure, other than the standard password policy that has to be followed.

And also covers the data comparison and discussion about some of the challenges found in the project. Since the main goal of this project research is to find the difficult of individual users to follow the password policies. It will also involve recommendation for improvement of password usage and remembering technique.

Responders are from different department in Kampala International University. Table 4.1 shows the number of responders from each country.

Table 4.1 Departments of Responders

Country	Number of responders
SEAS	113
SCIT	35
LAW	22
CEM	17
CHSS	13

4.1 Responders age and year of account creation

The analysis has been done considering five category of age group, from less than 20 years to greater than 60 years. Figure 4.1 shows the responder’s age group with respect to the number of responder’s in each age group. The graph shows that there are less than 10 users‟ in the age group less than 20 years and 40 to 50 years. The users below 20years, where not aware of the policy, they use same password and pattern for all their accounts. The younger users are not aware of the sensitive of the account also. Organization and systems should poke password

policy to younger users, when they are creating passwords. They should be advised to create passwords with both upper and lower case letters and using some special characters, so that their accounts will be secure. This will make them aware of the sensitive of using strong password.

Maximum users are in age group of 20-30years. These users‟ are aware of the sensitivity of the accounts, they use same pattern for their account to create passwords. They use same passwords for medium and low sensitive accounts but for high sensitive account they use same pattern but different password.

According to users‟ age password policy has to be shown to user, in the simplest way so that it’s easy for them to recognize the importance of passwords.

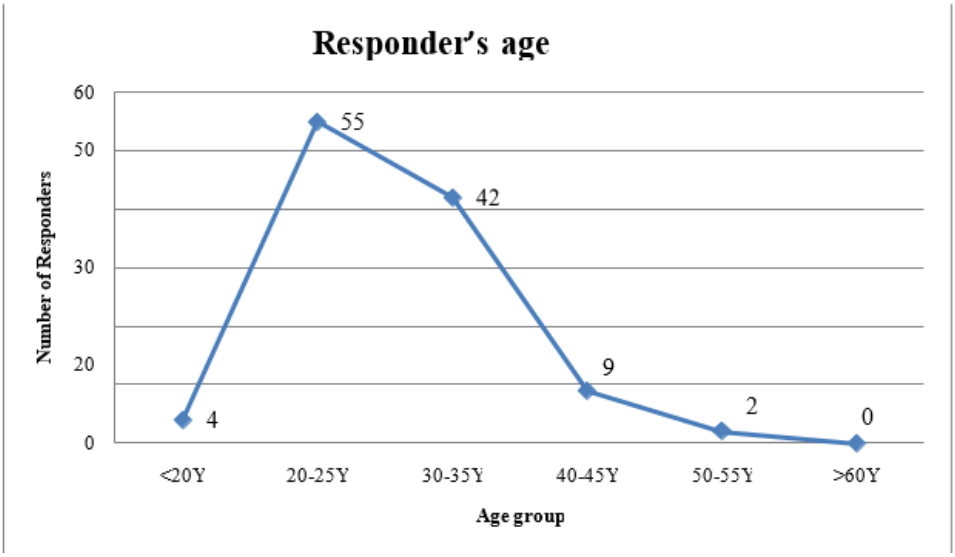

Figure 4.1 Age group

Figure 4.2 shows the year in which responder’s created their first web account with passwords. The graph shows the increasing in the number of accounts from year 2013 to 2015. It shows that many accounts are created between years 2011 to 2016, with respect to figure 4.1, it is understood that accounts created between this year’s maximum belong to the responders of age group 20-30 years. This is the year when there was increase in the creation of user account for social networking sites. There are many users who have first created social networking account

then they have created mail accounts. Users should be made aware of the social networking accounts, and keeping their password secure, as social networking sites can be misused.

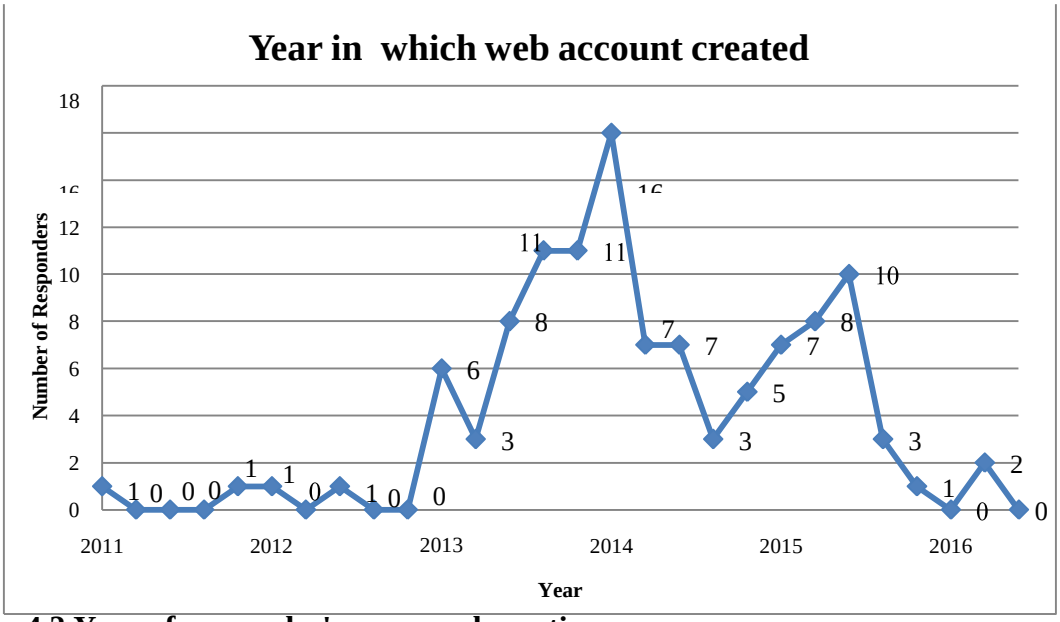

Figure 4.2 Year of responder's password creation

4.2Number of accounts

Figure 4.3 shows the number of computer accounts responder have, the account can be social networking, banking or email. A normal user has minimum 2-5 accounts, in his daily life to be accessed. As the number of accounts increase, the problems of remembering passwords for every account also increase. Maximum every user has at least one social networking account and banking account. So users‟ are aware of the high sensitive banking account and medium sensitive social networking account.

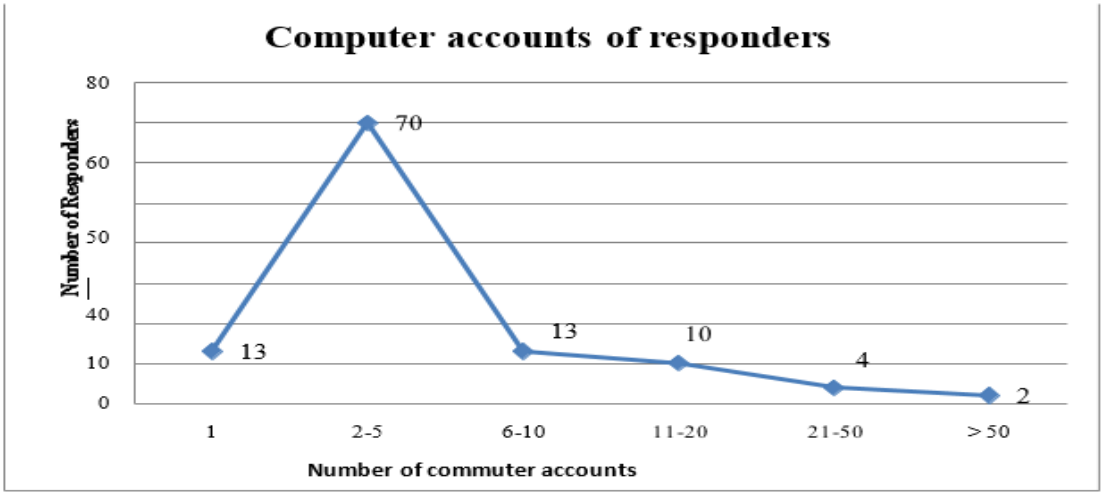

Figure 4.3 Number of responders account

4.3 Storage method

Password storing is the important aspect to be considered in password policy. When passwords are stored in insecure way, it can be easily known to outsider or hacker. If passwords are written down in paper and kept even under keyboards, thinking no one will know about it, is the biggest mistake. Because many users, use this method to write down and keep their password, which can be easily hacked. So it is necessary to not write down passwords, anywhere. They can be stored in encrypted form in offline device. In figure 4.4 it shows the result of responders, maximum responders store there password in memory. There are only 6 users, who store their passwords in paper. Among the 6 users, 5 users clearly write down their passwords on paper, as they are not aware of the passwords theft for hacking account. One user writes down his password in paper in encoded pattern, so that he can only understand what is written down in the paper. Many users have their own pattern to manage the password, so it's easy for them to remember their passwords.

There are three responders who follow the encryption technique in offline device. These users" are very much aware of the security of the password, as they encrypt their password even in the offline device, which is the best way to keep the password secure from others.

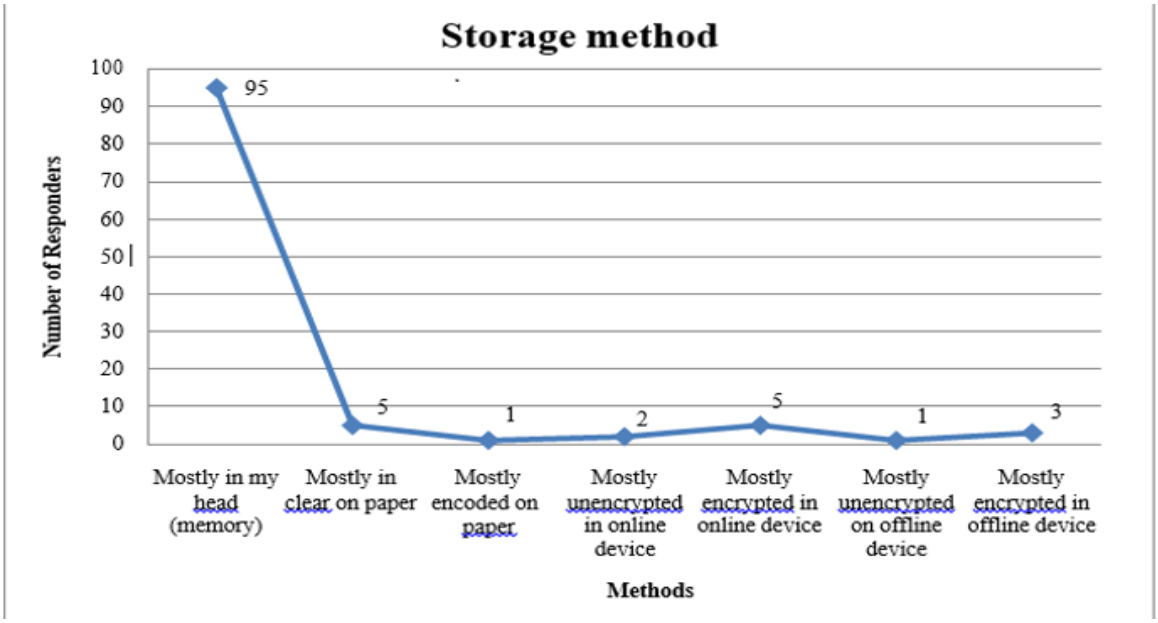

Figure 4.4 How passwords are stored

4.4 Number of characters

Passwords are basically string of characters. User prepares to use number of characters as per they can remember. The normal password policy is usage of more than 8 characters. There are three different types of account, based on which user creates the passwords. They are high sensitive, moderate sensitive and low sensitive accounts. User knows the difference between these three accounts.

4.4.1 High sensitive account

High sensitive account (banking, work and main email), users are aware of these accounts sensitivity. They create passwords with more than 8 characters long for these accounts. Figure 4.5 shows the number of characters users‟ use to create passwords for high sensitive account. There are ten users, who use more than 12 characters passwords for high sensitive accounts.

4.4.2 Moderate sensitive account

Moderate sensitive accounts are social networking account or secondary email (Hotmail, Gmail, or Yahoo etc.). Users know the sensitive of these accounts. The usage of secondary email is to send personal mail or contacting with family. Users use 6 to 8 characters passwords

for moderate sensitive account. Figure 4.6 shows there are 45 users, who use 6 to 8 character length passwords for their moderate account.

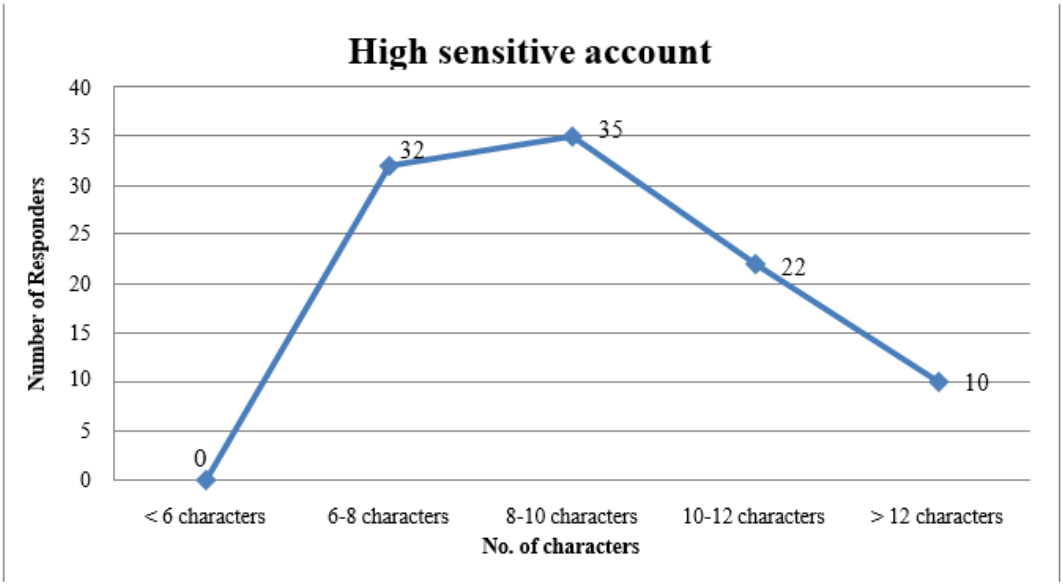

Figure 4.5 High Sensitive Account

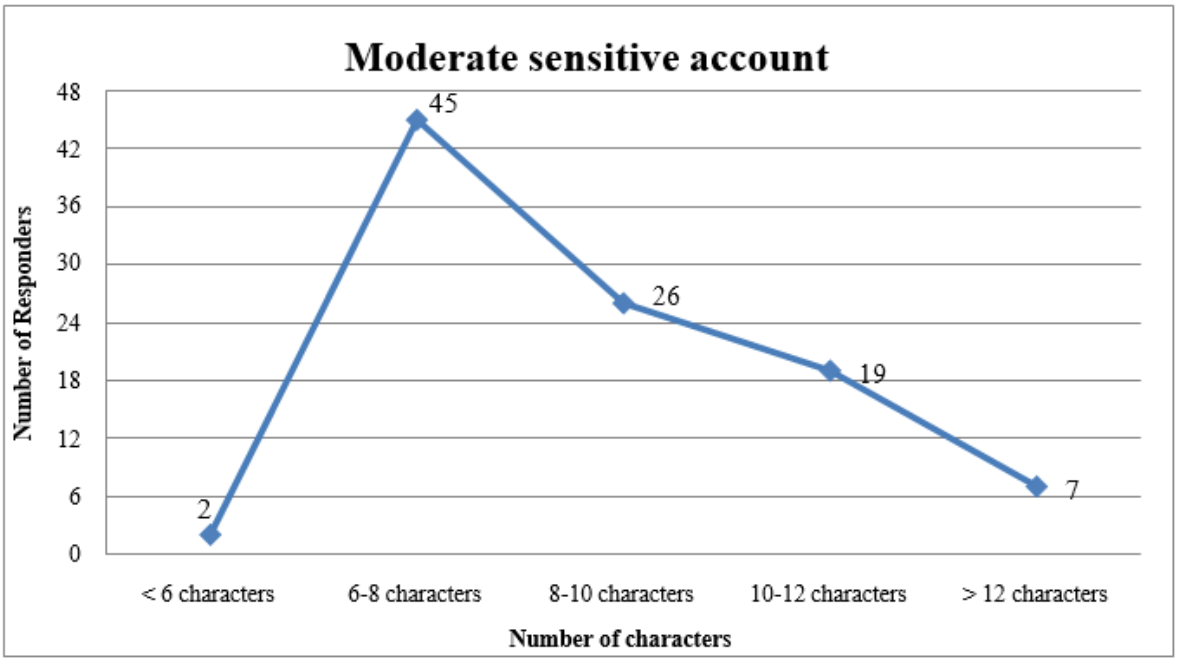

Figure 4.6 Moderate Sensitive Account

4.4.3 Low Sensitive Account

Low sensitive account (news website, wiki). These are the general accounts, for which users sometime share passwords with friends and family. Users create passwords using 6 to 8 characters length for low sensitive account. Some users prepare to use long password for these accounts also. The figure 4.7 shows 5 users who use strong password with greater than 12 characters length for low sensitive account.

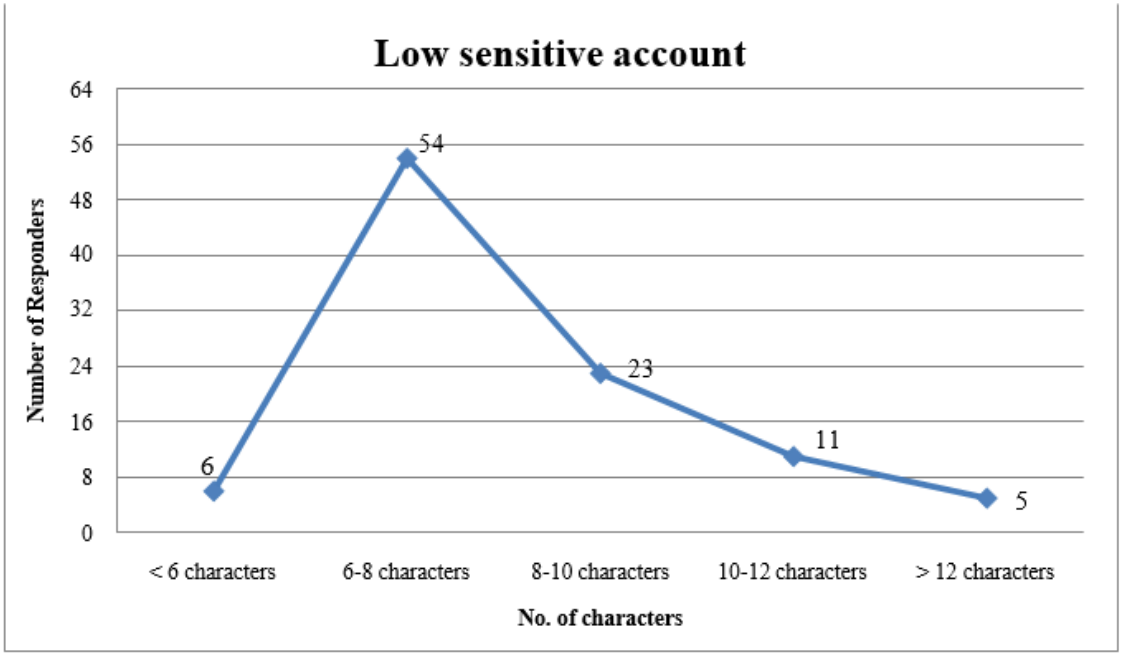

Figure 4.7 Low sensitive account

4.5 Password reuse

Figure 4.8 show that users reuse same password for their accounts. Users even use same password for high sensitive and low sensitive accounts. They should be made aware of using the different passwords for different account, or at least using different password for high and low sensitive accounts. There are 31 users, who reuse there passwords for high sensitive account. If passwords are reused it can be easily hacked using cracking tools. There are 34 users, who are aware of not using same password or reusing passwords for high sensitive account.

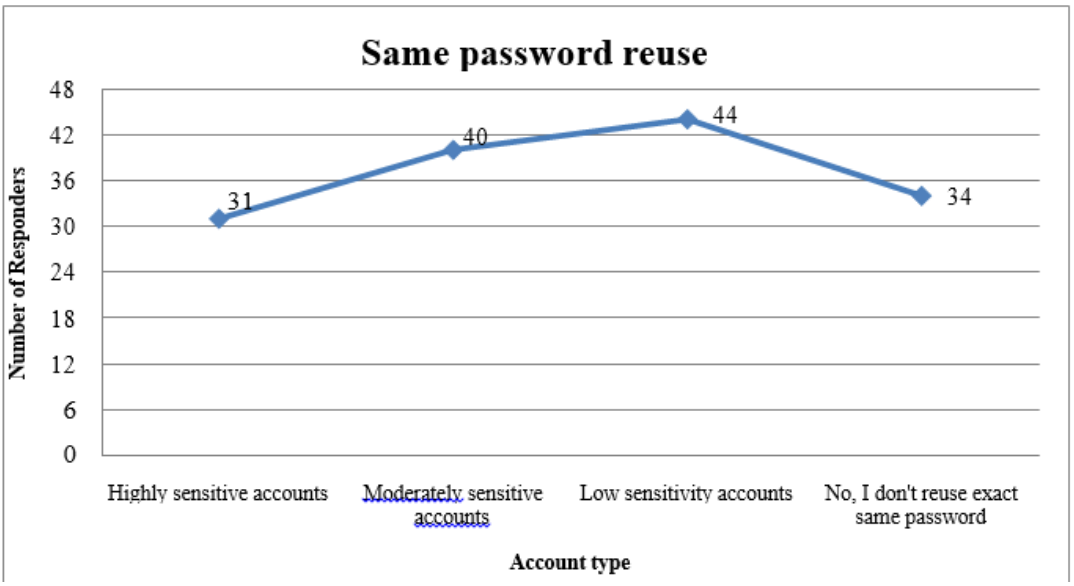

Figure 4.8 Password reuse

4.6Password pattern

Figure 4.9 shows the usage of password pattern. From the data, it shows that user use same pattern as same password for high and low sensitive accounts. Using same pattern for every account is not wrong, but there should be increase in number of characters of high sensitive account while compared to low sensitive account. Many users use same pattern for their accounts, so it's easy for them to remember their passwords to access their accounts. From the figure 4.8 and figure 4.9 it shows that there are 26 users, who don't use same pattern and passwords for their account.

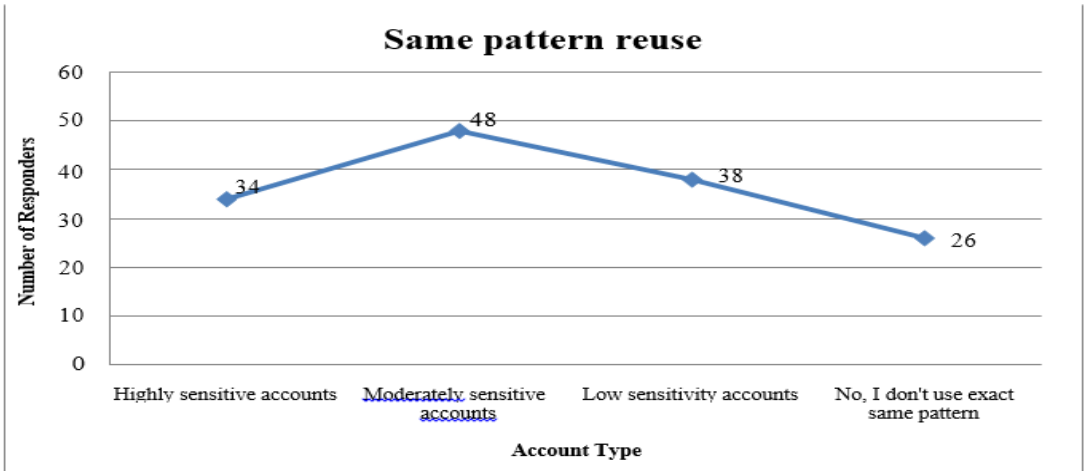

Figure 4.9 Password pattern

4.7 Reset of Password

Figure 4.10 shows the users password resetting data. Passwords resetting is the best method to keep users account secure. When hacker runs an tools like brute force method to hack the password, it takes at least minimum 6 months to hack 8 character length password, so if users reset the passwords frequently every 6months, then it's hard for password to be hacked using tools .From the data it is understood that, user reset passwords only when they are forced to reset the password. User should be made aware of password policy about resetting password, which secures their account. There are 11 users, who reset there password once every month.

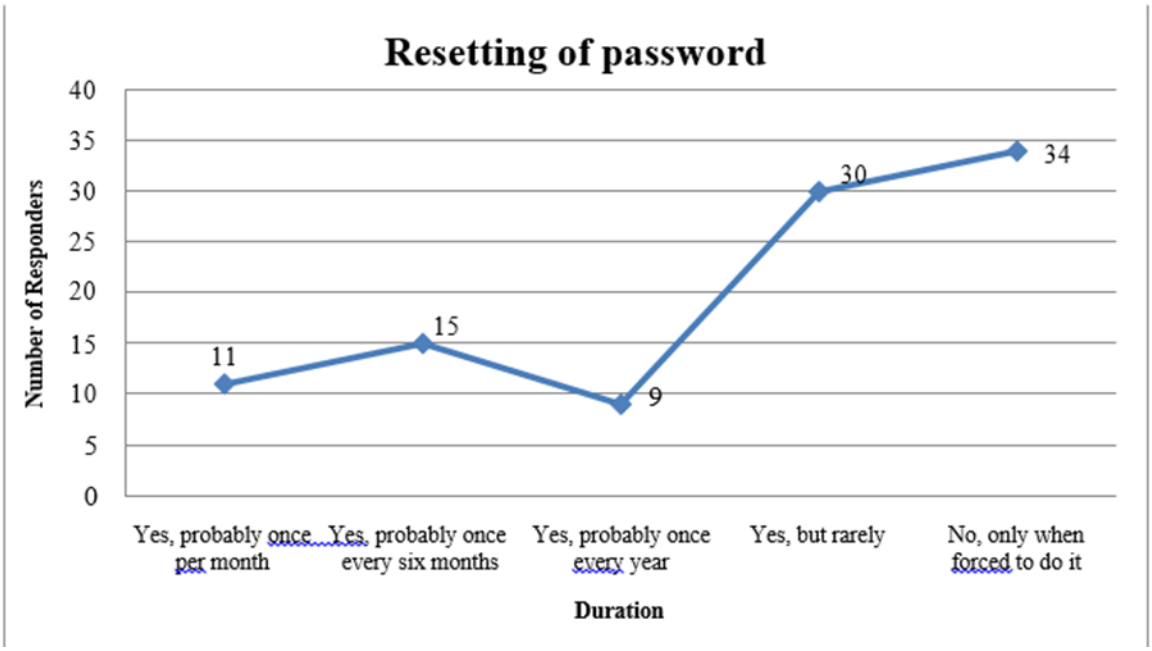

Figure 4.10 Password reset

4.8 Password sharing

Figure 4.11 shows the users bad habit of sharing passwords with others. In the figure 4.11, it is shown that maximum number of users share their password by different methods (direct oral communication, telephone, email, SMS, paper and any other physical medium). Mostly users share their passwords directly. Users should be made aware of not sharing their passwords

to others. Even if they are sharing to their friends or family, if third person hears password, then it can make secure information to be lost or hacked.

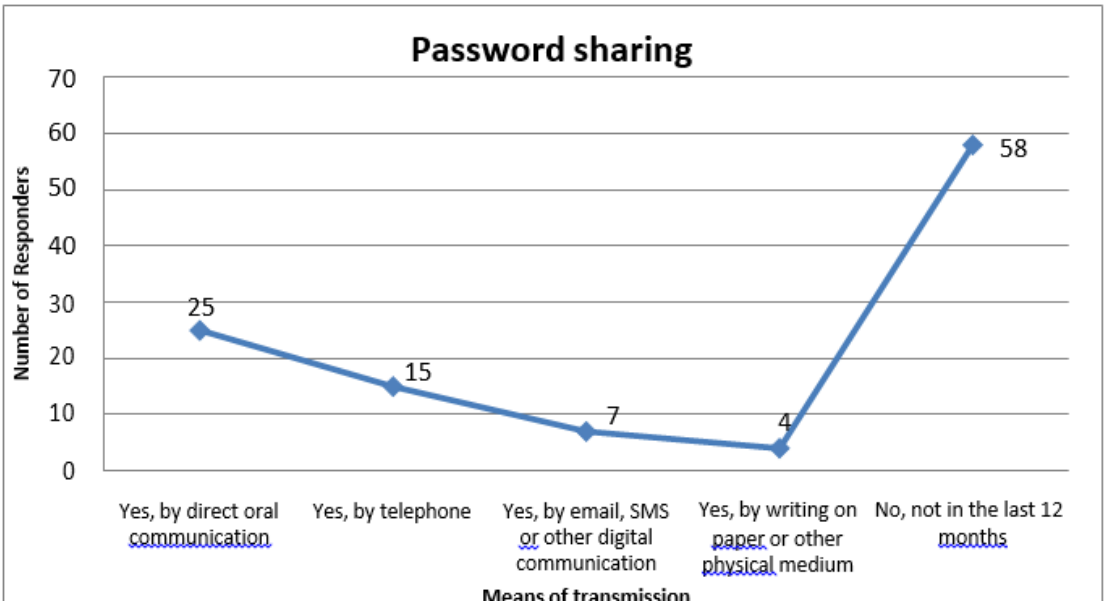

Figure 4.11 Password sharing

4.9 Usage on accounts

Figure 4.12 shows how many times the users access their accounts. There are 96 users, who uses their accounts daily. Users are regular in checking their accounts to see the updates in their account. When users are regular in checking their account, they tend to use smaller passwords and easy remembering passwords, so it's easy for them to access their accounts daily.

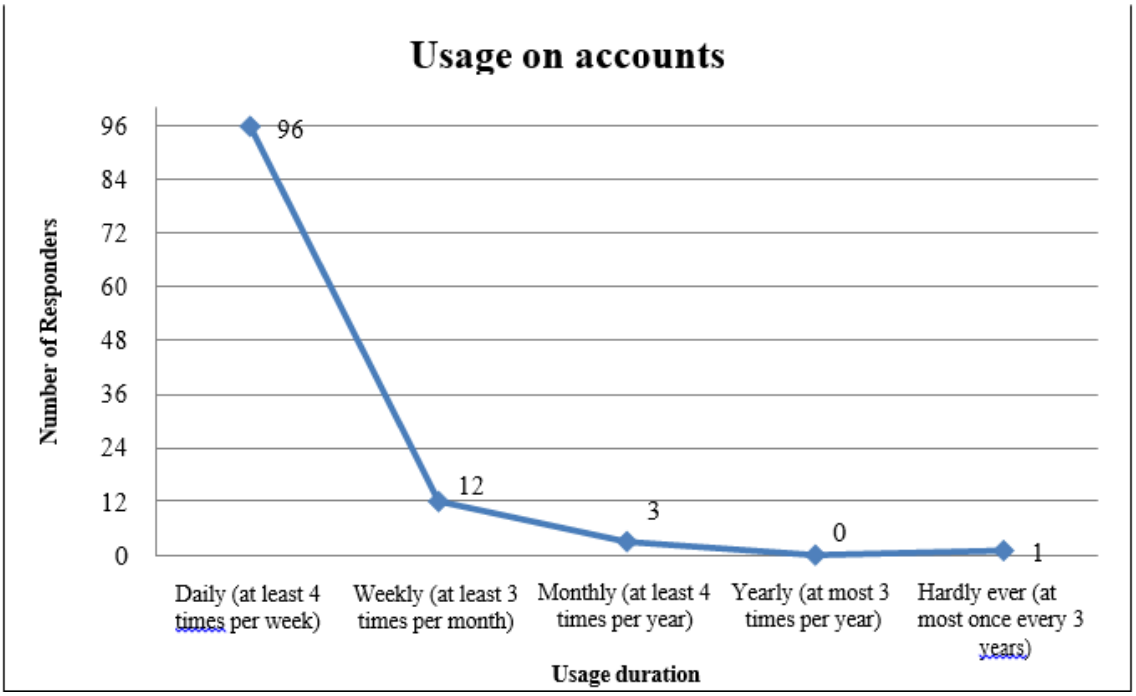

Figure 4.12 Account Usage

4.10 Passwords with mixed characters

Figure 4.13 shows the users habit of using mixed characters in their passwords. Users have to be made aware of using mixed characters passwords, having both small and upper case with special characters. From the figure, it is clear that users use mixed characters for creating their passwords. There are 56 users, who always use mixed character password. There are also 13 users, who use mixed character password only when system forces them to create password with mixed character.

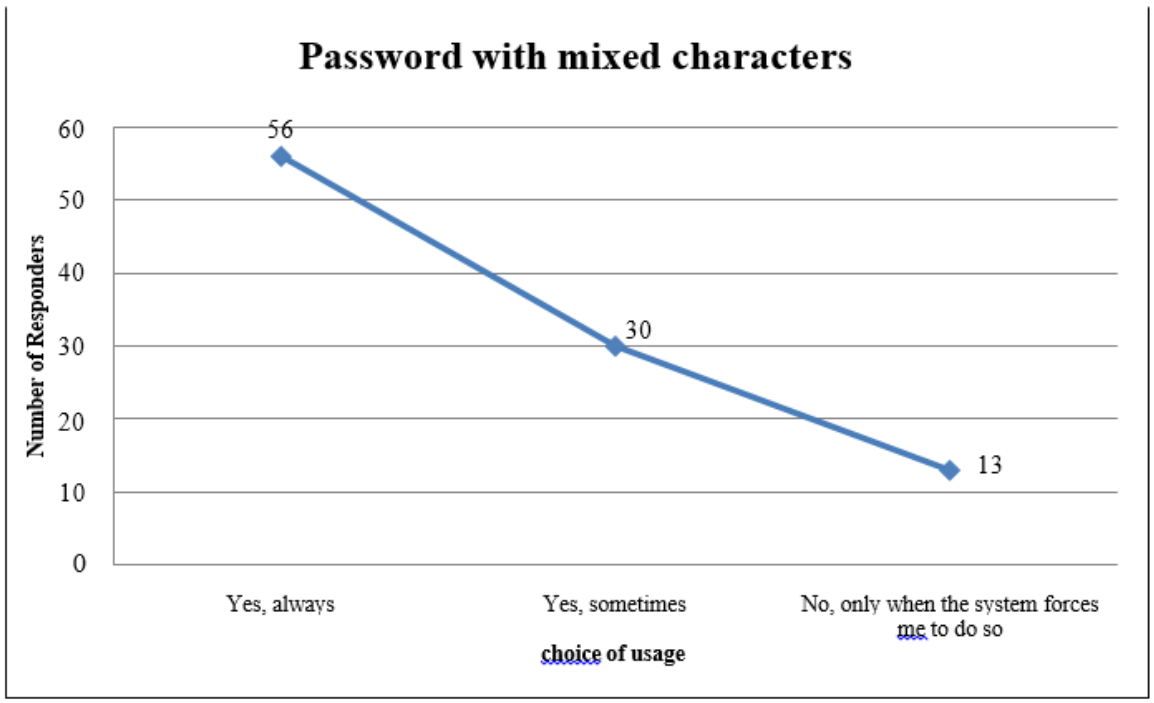

Figure 4.13 Mixed character passwords

The analysis shows that there are users, who are aware of the password policy but in the fear of forgetting passwords, they go for unsecure password or using weak passwords. Some users don't follow policy and create dictionary passwords. And some users use same password for high and low sensitive account.

There are also some users, who follow password policy and create strong password. They also have different pattern and different passwords for high and low sensitive account.

4.11 Data comparison

User should be made aware of the password security. Securing password is the most important thing. User should keep password secure as they keep their credit card or bank book. From the data collected, it shows clearly that user is not aware of the password policy, because they create same password pattern for high sensitive account and low sensitive account. User should be able to understand the difference between high and low sensitive accounts. While creating passwords they should follow the policy, so that their accounts are secure.

4.11.1Comparison of same password and same pattern

Figure 4.14 shows the comparison of reusing same password and same pattern. The blue line shows the reuse of same pattern and the red line shows the reuse same password. Maximum users, reuse same password and same pattern for moderate sensitive account.

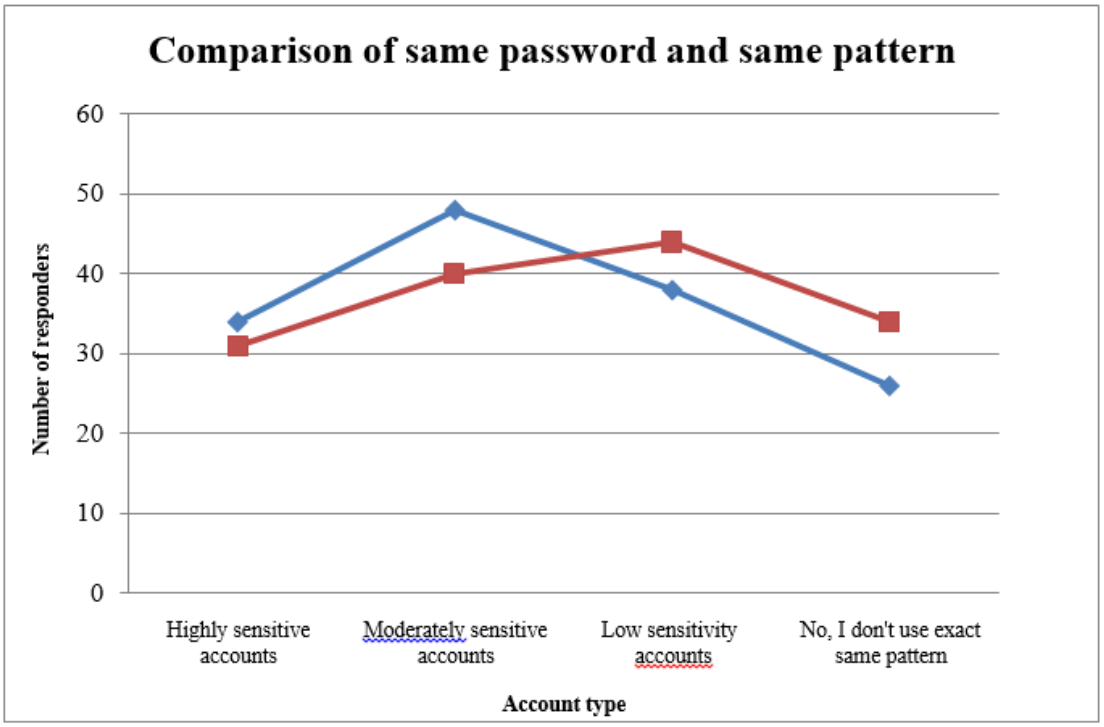

Figure 4.11 Comparison of same password and same pattern

4.11.2Comparison of high, moderate and low sensitive account

Figure 4.12 shows the comparison of high, moderate and low sensitive account. In the figure 4.12, blue line is high sensitive account, red line is moderate sensitive account and green line is low sensitive account. Users know the sensitive of the account and information stored in their account. Maximum users, use 8 to 10 characters for high sensitive account and 6 to 8 characters for low sensitive account.

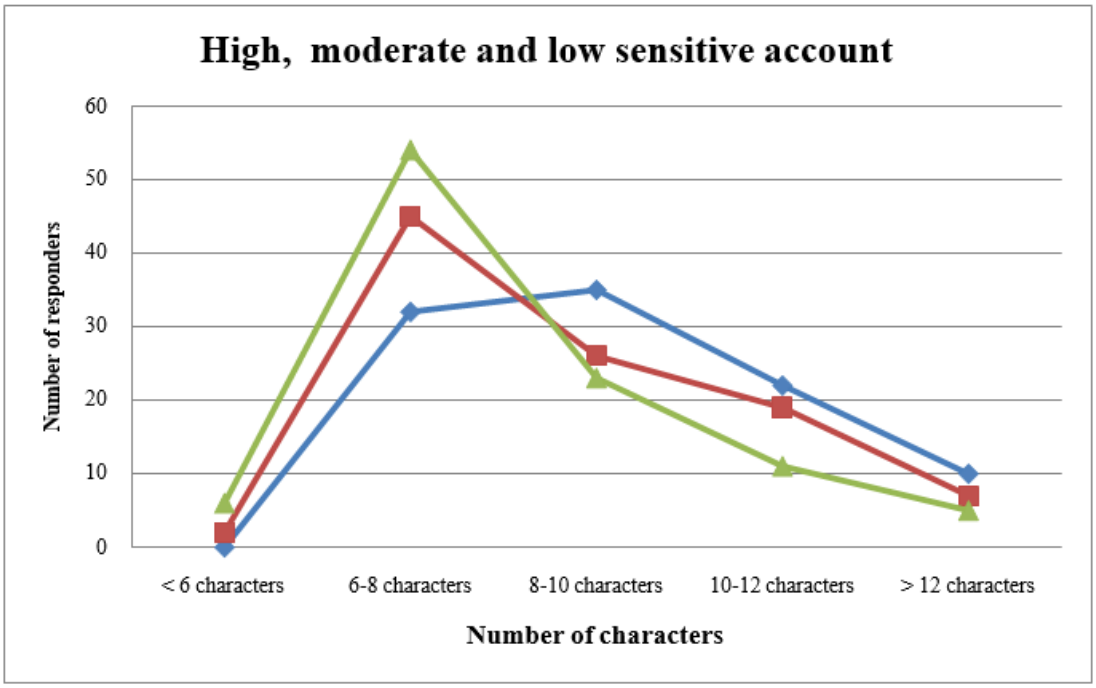

Figure 5.2 Comparison of high, moderate and low sensitive account

4.12 Method of choosing password

Every user has different method of choosing password. They choose passwords based on the easiest way to remember it. Some users use same pattern to create their passwords for every account, so that there is no need to write it down on paper, and they can recall it easily whenever they change their passwords. Some users reuse there passwords after few months of changing new passwords, so that it's easier for them to remember it. This shows that every user has their own method.

4.13 Problem causing password policy

There are specific password policies that causes problems to users while creating accounts. Some of these problems are most commonly faced by the users:

i. Forcing them to use both case letters, even though they have long length password with special characters.

ii. Not allowing them to create passwords with shorter length.

iii. Some websites have the option to check password strength, forcing to change password, when it does not meet the standard strength.

iv. Never indicating the sensitive of the account.

Some users they never follow the policy, they create password of their own idea, without considering the policy. There are few users, who never read the policy posted by the website for creating password. As policies are given in big paragraphs, which users don't have time to read, while creating password. It is necessary to mention and describes the policy in small sentences and highlight the important policy, so that users can find it easy to read and follow the policy, instead of avoiding it.

CHAPTER FIVE

CONCLUSION AND RECOMMENDATIONS

5.1 Conclusion

Passwords are an important component of securing our computer systems, but they are not the entire solution. Their purpose has been and should continue to be a mechanism for determining what a user knows. We need to include more than that. In addition to what we know, we should be including one or more of the following: “what you have”, “who you are”, and “what you produce”. What you have may include physical devices like smart cards and tokens. Who you are include physical features like fingerprints, hand geometry, retinal and iris scans, and facial scans. What you produce may include voice and signature patterns. Who you are and what you produce is the biometric method of authentication.

Passwords are never the only solution. User should be made aware of password policy. Password policy secure the user, as it recommends user to create strong passwords, avoid storing password, enforcing automatic system lock when not in use for certain time interval. User should be made to understand the importance between high sensitive and low sensitive account and use different passwords for different accounts.

Selecting strong password continues to be a problem, as user are forced to create passwords with mixing upper and lower case characters with symbols and numerals. Which makes user to write down their passwords in the fear of forgetting the characters used.

When users are creating passwords for their accounts, they should be made clear about the policies. So that they don’t create weak passwords or dictionary words or personal information as their passwords.

The analysis showed that users are creating strong passwords for high sensitive account with more than 8 character length password, but they are reusing same passwords for their low sensitive accounts also. Users should be aware of sensitive of the account and information in that account.

As the fight for creating strong password continues, the security of system and user accounts will continue to be a battle.

5.2 Recommendations

The emphasis placed on passwords will only increase, as security for securing system and information increases. Users remember many passwords, so they find ways that are easier, but forget about security and choose less secure way. Still majority of users write down there password or store password in unencrypted form. Organizations and networking sites should warn users about using weak passwords, storing passwords or sharing with others. So that users get aware about the security of passwords. Users should make best choice when it comes for password selection.

Enforce users to choose strong password. Strong passwords are creative passwords which should include criteria like using passphrase instead of passwords, change password every 6 months, don't reuse the same password within a year, and don't share password. This project research showed that users are using same passwords for their multiple accounts, so they must be made aware of using different passwords for different accounts.

Authentication is another important aspect to be considered. User should be aware of policies which says automate password reset, and lock account when wrong password is given three times. This eliminates hacker from trying brute force attack, where different passwords combination are tried to get access to user account.

5.2.1 Issues in exciting password policy

There are unexpected password issues, which has to be covered in exciting policy like:

i. Warning users when they create weak password with short length.
ii. Using encoding method to store users‟ previous 3 to 4 passwords, so that when users reuse passwords, they can be warned not to reuse it.
iii. Lock their account and send alert message to their mobile, if passwords is given three times wrong.
iv. If an account is inactive for more than 60 days, and then user logs in to that account, then user verification has to be done by asking security question.
v. When users are sharing passwords through mail accounts, there should be a tool to identify the keyword „password‟ and warn them, that they are sharing password.

Whatever the password policy is, it is imperative that all users be educated on the policy and that all users understand the importance of following the policy. Security is no longer an option, it is a requirement.

REFERENCES

Arash Habibi Lashkari; Samaneh Farmand; Dr. Omar Bin Zakaria; Dr. Rosli Saleh. Shoulder surfing attack in graphical password authentication. International Journal of Computer Science and Information Security,6(2):145–154, 2009.

Bishop, M. (2003). Computer Security. Art and Science. Addison Wesley.

Biometrics, Retrieved Mary 9, 2016, http://bio-metrica.com/biometric-theory

Brown A. S & E Bracken: Generating and remembering passwords, 2004.

Definition of phishing, Retrieved March 4, 2016 http://en.wikipedia.org/wiki/Phishing

Definition of KBA and types of KBA

http://searchsecurity.techtarget.com/definition/knowledge-based-authentication

Dunn, Jeffrey S. and Fernando L. Podio. "Biometric Authentication Technology: From the Movies to Your Desktop." National Institute of Standards and Technology. National Security Agency, 2008.

Dieter Gollman. Computer Security. John Wiley Sons, 2004.

Gaw S & E. W. Felten : Password management strategies for online accounts, 2006.

Garfinkel, S. & Spafford, G. (1991). Practical UNIX Security, Sebastopol, CA: O"Reilly & Associates, Inc., p. 35.

Ibrahim Adabara, Accessed: November, 21st, 2015, Information Technology in Education, www.infotechinedu.com.

Image of NIDS and HIDS

http://www.windowsecurity.com/articlestutorials/intrusion_detection/Hids_vs_Nids_Part1.html

J. O. Pliam, "On the Incomparability of Entropy and Marginal Guesswork in Brute-Force Attacks," in Progress in Cryptology-INDOCRYPT 2000, 2000.

John McCumber. Information Systems Security: A Comprehensive Model. In Proc. Ninth International Computer Security Symposium, 1993.

Kenneth G. Paterson & Douglas Stebila: One-time-password-authenticated key exchange, 2009

Kevin Beaver. Hacking for Dummies. John Wiley & Sons, 2014. 5th Edition

Karen Scarfone & Murugiah Souppaya. Guide to Enterprise Password Management (Draft) – NIST Special Publication 800-118. Technical report, National Institute of Standards and Technology, 2009.

Morris R & K Thompson: Password security: a case history, 1979.

M. V. Wilkes, Time-sharing computer systems. New York: Elsevier, 1968.

Morrie Gasser. Building a secure computer system, Van Nostrand Reinhold- 1988

Murrer, E. (1999). Fingerprint Authentication. Secure Computing (March), 26-30.

"Physiology." Medline Plus. Merriam-Webster Medical Dictionary. 2005: Merriam-Webster, Incorporated.

R.E. Smith. The Strong Password Dilemma. Addison-Wesley, 2002.

Riddle B. L & M. S. Miron : Passwords use in a university timesharing environment, 1989

Seth T. Ross, Unix system security tools, McGraw-Hill, 1999

Seymour Bosworth and M.E.Kabay. Computer Security Handbook, Fourth Edition. John Wiley Sons, Inc. New York, NY, USA, 2002.

Sausan Yazji, Xi Chen, Robert P. Dick, Peter Scheuermann. Implicit User Re- Authentication for Mobile Devices. Northwestern university, 2009

Svigals, J. (1994). Smartcards - A Security Assessment. Computers & Security, 13(2), 107-114.

Types of firewalls, Retrieved March 6, 2016 http://bi0os.blogspot.no/2010/11/types-of-firewalls.html

Wakefield, R. L. (2004). Network security and password policies. The CPA Journal,74(7), 6. Retrieved March 8, 2016, from the ABI/INFORM Research database.

APPENDIX

Questionnaire about password habits

This questionnaire is about password habits for a research project at Kampala International University - Uganda. Your answers are totally anonymous and will not be shared with anyone. All answers will be deleted after the end of the project research.

The project is conducted by undergraduate students Kule Titus and Bakawanamaha Allan under supervision of Mr. Ibrahim Adabara. Please contact Mr. Ibrahim <adabara360@gmail.com> if you have any questions.

1. Your age

<20Y

20-25Y

30-35Y

40-45Y

50-65Y

>60Y

2. Your Department

SEAS

SCIT

LAW

CEM

CHSS

3. In which year did you get your first email address?

2011

2012

2013

2014

2015

2016

4. How many computer accounts do you currently have?

1

2-5

6-10

11-20

21-50

> 50

5. How offend do you use at least one of your computer accounts?

Daily (at least 4 times per week)

Weekly (at least 3 times per month)

Monthly (at least 4 times per year)

Yearly (at most 3 times per year)

Hardly ever (at most once every 3 years)

6. How do you store passwords?

Mostly in my head (memory)

Mostly in clear on paper mostly encoded on paper

Mostly unencrypted in online device

Mostly encrypted in online device

Mostly unencrypted on offline device

Mostly encrypted in offline device

7. How many highly sensitive (e.g. bank, work, main email, etc.) accounts do you have?

1

2

3

4

8. How many moderately sensitive (e.g. social networks, secondary email, etc.) accounts do you have?

1

2

3

4

9. How many Low sensitivity (news, wikis, throwaway accounts, etc.) accounts do you have?

1

2

3

4

10. Do you sometimes reuse the exact same password for?

Highly sensitive accounts

Moderately sensitive accounts

Low sensitivity accounts

No, I don't reuse exact same password

11. Do you sometimes use the same pattern in passwords for?

Highly sensitive accounts

Moderately sensitive accounts

Low sensitivity accounts

No, I don't use exact same pattern

12. What is the typical length of password you use for Highly sensitive accounts?

< 6 characters

6-8 characters

8-10 characters

10-12 characters

> 12 characters

13. What is the typical length of password you use for moderately sensitive accounts?

< 6 characters

6-8 characters

8-10 characters

10-12 characters

> 12 characters

14. What is the typical length of password you use for Low sensitivity accounts?

< 6 characters

6-8 characters

8-10 characters

10-12 characters

> 12 characters

15. Do you ever change a password because you decide to do it?

Yes, probably once per month

Yes, probably once every six months

Yes, probably once every year

Yes, but rarely

No, only when forced to do it

16. Do you by your own choice use mixes of different character types?

Yes, always

Yes, sometimes

No, only when the system forces me to do so

17. Have you in the last 12 months shared any of your personal passwords with others (e.g. colleague, friend or partner)?

Yes, by direct oral communication

Yes, by telephone

Yes, by email, SMS or other digital communication

Yes, by writing on paper or other physical medium

No, not in the last 12 months