An Investigation of Approaches Used When Creating Passwords and their Relative Security

Niall Dowdall

A dissertation submitted in partial fulfilment of the requirements of Dublin Institute of Technology for the degree of
M.Sc. in Computing (Advanced Software Development)

March 2013

I certify that this dissertation which I now submit for examination for the award of MSc in Computing (Advanced Software Development), is entirely my own work and has not been taken from the work of others save and to the extent that such work has been cited and acknowledged within the test of my work.

This dissertation was prepared according to the regulations for postgraduate study of the Dublin Institute of Technology and has not been submitted in whole or part for an award in any other Institute or University.

The work reported on in this dissertation conforms to the principles and requirements of the Institute's guidelines for ethics in research.

Signed: _____

Date: ***25 March 2013***

Abstract

When securing a computer system there are many areas to be tackled these include the protecting of the information held on the system and insuring that authorise users can trust that the information is right and that they will have access when needed. To achieve this a number of different elements must work together to fulfil these needs. This project will focus on how passwords are used to insure only authorise users can get access to the system. To achieve this it will look at how users use passwords and how this behaviour affects the security of the system as a whole including what affects other parts of a security policy have on limiting the effects of user behaviour.

Passwords have being used to secure computer systems for years. They have remained largely unchanged in that time with only the length and complexity changing. The basic idea remaining the same, you supply a code to the system which you must then supply every time you want to access that system. The security of the password is made up of two main parts the users actions and the methods used to store them on the system

First this project will look into how passwords are used in computer systems focusing on whether they provide the protection they are believed to by the users. It will also examine the different security standards in use today and how they use passwords to help secure the system. The way these standards affect the use of passwords will be looked at including limits that they place on the user's chose of password.

Next user behaviour will be looked at to try and identify the behaviour which leads users to pick less secure passwords. The behaviour of attackers will be looked at examining the different forms of attack focusing on password cracking. Combining the results of these two areas of study an algorithm will be developed which it is hoped can be used to insure that a user does not select a password which an attacker can easily guess.

Lastly a look at the current alternatives to passwords will be looked at to see if they are as vulnerable to user behaviour as passwords and if current user behaviour would allow them to improve the security of systems if they replaced passwords

ACKNOWLEDGEMENTS

I would like to express my sincere thanks to the following people for their help, support and encouragement throughout this project

First my heartfelt thanks to my dissertation supervisor Damian Gordon for his advice and guidance during this research project

I would also like to thank the staff of the DIT who have helped including Deirdre Lawless and Brendan Tierney for their help in preparing me to undertake this project

I would also like to thank all those who took part in the survey which formed part of this project.

Finally I would like to thank my family for their support during the course of this project

Table of Contents

Table of Figures

Table of Tables

1. Introduction

1.1 Project Background

Computer security is an area of growing concern. As more and more information is stored and transmitted using computers. The need to insure that that information is secure becomes greater, with the amount of people now using online methods to pay bills and shop. In the US "Forrester expects that online sales will grow from 7% of overall retail sales to close to 9% by 2016"[S. Mulpuru 2012].While "The U.K. Internet economy is likely to grow by 10 percent per year, reaching 10 percent of GDP by 2015"[C. Kalapesi et al. 2010] . This creates a greater incentive for criminals to try and gain access to information stored in online systems. This puts greater focus on the mechanisms used to keep this information secure. With the increasing potential gain to a hacker from accessing this information, they are willing to put more time and money into their attempts, which requires a greater effort to stop them.

As more and more systems are connected through the internet the risks increase. If one system is compromised, then all system which trusts it will be compromised as well. This makes the idea that you can be too small or of no interest to hackers untrue, as if they hack you they might get access to a bigger system through you.

Another new security issue in more recent years is the growth of mobile smart devices including smart phones and tablet devices. These devices are computer systems which people now carry around with them all the time, they are used to store personal and in some cases financial details. This makes them a perfect target for both hackers and other criminals. They are easy to steal from the person, being light weight and normally carried on the person, while if they are hacked the information which could be gained by just monitoring their uses and location could be of value to others. The number of theft from person offences in Ireland in 2011 rose by 28% to 3683 over 2010 [Central Statistics Office 2012]. This means that these devices need to be protected from both local and remote hacking while retaining their usability.

Another issue with the increase in the number of different systems a user interacts with. A study by Forrester Research found that a normal user has 15 passwords to keep track of just for web sites [R. Kanaley 2001] add to that logons for a home and work computer, a phone, and pins used for debit and credit cards the number increases. This causes users to reuse the same passwords, add to this that users when asked to make passwords will likely pick something which has some meaning to them [A Adams & M. A Sasse 1999] this makes it more likely that an attacker will crack the password. With the fact that a user could have reused that password elseware the one success by the attacker could allow access to different systems and all systems which the user users the same password are dependent on the security of the weakest system.

1.2 Project Description

This project aims to investigate the effectiveness of passwords as a security mechanism. It will investigate the various password standards currently in use, their role within wider security policies and standards, as well as user behaviour in password generation and protection. It will also examine common attack mechanisms and the effectiveness of various standards in response to these attacks. Using the results of this, a new algorithm will be developed to incorporate more effective mechanisms to assist both system administrators and users in selecting passwords less vulnerable to attack.

The project will start by first examining what password police standards are in use today across different industries and their role within wider security policies and standards. User behaviour in password generation also has an impact and will therefore also be investigated. In addition research will be conducted into the most common forms of password hacking attacks currently in use and how these are addressed by the various standards. The password standards will then be assessed in terms of their vulnerability to the various attacks.
The research will inform the development of a design for an application which will aid a system to insure that a user does not select a password which would be easy to guess based on their personal information.

1.3 Research Objectives

This project aims to investigate the effectiveness of passwords as a security mechanism. It will investigate the various password standards currently in use, their role within wider security policies and standards, user behaviour in password generation and protection.

Common attack mechanisms and the effectiveness of various standards in response to these attacks will also be investigated. Using the results of this, a new algorithm will be developed to incorporate more effective mechanisms to assist both system administrators and users in selecting passwords less vulnerable to attack

- Conduct a literature review
- To identify common password standards and the degree to which they are used and their role within wider security policies and standards to identify the role of user behaviour in password security protection
- To identify common password hacking attacks
- Assess the effectiveness of password standards against common hacking attacks
- Conduct a series of experiments to assess the effectiveness of common password standards against common hacking attacks using a test data set including passwords derived according to common password standards

1.4 Thesis Roadmap

In chapter 2 this paper will look at the wider area of computer security. Looking at the different types of security concerns, as well and the different type of attacks they are exposed to..

Then in chapter 3 we look at passwords and the different types in use as well as the standards employed today

In chapter 4 we examine the results of a survey conducted as part of this research and develop a system to gather further data about the password habits of normal users.

Finally in chapter 5 we look at one possible use for the gathered data in the creation of a design for an application which will help an organisation insure that users pick better passwords.

2. Computer Security

2.1 Introduction

Computer security focus on four main points they are;

- Secrecy, who has access to the system and the information on that system
- Integrity, insuring that the information is stories as it was entered and that changes ore controlled.
- Accountability, being able to track who has done what with the system.
- Availability, the system and information must be accessible to authorized users at all times.

The security polices of different organizations will include elements from the four points with the focus changing between them. A telecoms company might require that availability be the most important while a government might see secrecy as on top concern. [B. Lampson 2004]

Integrity can be dealt with in a number of ways from a simple hashing routine to more robust systems which track all changes made to the data and allows those changes to be undone at a later date. This is important from a number of different reasons the first being to insure that a hardware fault does not damage the data in any way, the second is to insure that any attempt by an unauthorised person to change the data either fails or is detected and can hopefully be undone

Accountability is normally handled by keeping a log of what every user of the system does and from where. This means that every action performed by a user from they logon till they logoff is logged so that any breach of the security of the system can be traced to a single user.

Availability is normally dealt by hardware. The simplest way is to have a complete copy of the system running at another location. In this way if anything happens to the main system the copy can be used with very little downtime. This system can also be used to allow upgrades to happen with no interference to the users, it is however expensive other options include having systems which allow failed parts to be swapped out while the rest of the

system is still running. This offers some relief from some hardware issues but is still exposed to larger problems.

Secrecy is managed by the use of some form of authentication system to gain access to the system. There are many different ways that a computer system is secured falling into four groups; something you know, something you have, something you are, something you do. These different types can be used together such as using a credit card, something you have and a pin, something you know.[W. Stallings & L. Brown 2011]

2.2 Computer Systems Security Controls

Von Solms (2000) states that computer system security can be split into three waves.

In the first wave the technical controls are considered. When computer were first introduced to business this was all that was needed to protect a system from attack. At this time fire alarms, surge protectors and identity cards were enough (Russell & Gangemi 1991). As computing power increased the need to protect the data held on them increased to insure both the integrity and confidentiality of that information (Von Solms 2000)

In the second wave the management takes a role in the security of the computer systems. This was necessitated by an increase in the amount of information held on computer systems and the need to reassure customers that this information was secure and that the company could be trusted with it. This is where computer security polices originate from. They set a standard for employees to follow to insure that the computer system stays secure and also allows companies to hold employees responsible for their activates (Herold 2005)

In the third and last wave the focus moved to international standards as the use of the internet expanded the risk of attacks from outside increased no longer did an attacker need to tap into the corporate network they could attack the company's internet presence be that remote access for employees or the company's web site and email systems. This has lead to the creation of internal standards some of which are backed by state law one example of this is the European data protection Directive which is found in Irish law under the data protection act 1988??. This has moved the focus from just worrying about company data to compliance with the increasing number of regulations and laws (Herold 2005)

2.3 Security Awareness

Security awareness as stated by Desman (2002) puts the focus on making the users of a system aware of why security is needed and what is needed for good security as well as the effect of a failure in the security.

Security awareness is important among users, if a user has no understanding of why they must follow certain rules about security then they will be less likely to follow them. Take crossing the road as an example people do not complain about having to look both ways when crossing a road even a one way street because they understand the consequences of not doing so, Yet these same people complain about having to use a password to logon to a computer system which could have just a dire consequences for the company if an attacks gains entry. It is there for important to make users aware of the reasons for the different security systems in place within the organisation to help them better accept the need for them

2.4 Attacks

Attacks on passwords fall into four main groups they are

- Brute force attacks
- Dictionary attacks
- Rainbow tables
- Social engineering

2.4.1 Brute force attacks

In brute force attacks an attacker will try every possible combination of the used alphabet. This is often the weakest of the attack types which gets harder with an increase in possible length possible symbols used in the password. For example the table 1 below shows the different possible passwords for different alphabets. This type of attack is guaranteed to work unless limits are put in place as to the number of failed guess a user can have.

Upper case letters(26)	Lower case letters(26)	Numbers (10)	Total possible alphabet	Number of guesses needed	Time to crack at 1 billion guess per hour[1]
Yes	No	No	26	2.0882X10^11	104.4
Yes	Yes	No	52	5.3459X10^13	26729.8
Yes	Yes	Yes	62	2.1834X10^14	109170.0

Table 1: Number of possible passwords of 8 charters in length

2.4.2 Dictionary attacks

In a dictionary attack, a list of words is tried, this list can be an actual dictionary or a list made up of words assisted with the user. These attacks are faster to run then a brute force one. It does however not guarantee success like the brute force attack.

2.4.3 Rainbow tables

In this attack, the attacker first creates a dictionary to work with just like the dictionary attack. Then creates the hash value for each entry in the dictionary including all the possible salt values. This results in a large table of hashed values which can be tried against a user's password. This attack type is faster than a dictionary attack but the hash table can be very large running into the 10s of GB of data

2.4.4 Social engineering

This type of attack is one which tries to get the user to revel their password. It can take many forms including the attacker impersonating an IT support worker and just asking for the password to fix a problem.

There is no one defence which will prevent all these types of attack. The easiest type to defend against is the dictionary attack. To prevent this type of attack from working all that is needed is that the user not use a word found in any dictionary as there password. They must also not user any combination of words. A common mistake made by people is that using a

[1] Assuming only 50% of possible passwords need to be tried

foreign language word will defeat these types of attack, however most dictionary attacks will use dictionaries form many different languages even adding some common slang terms or terms commonly used in the industry if they are focusing on one company to attack. It is also common that the attacker will try reversing the words in this type of attack. The HSE even state in there password policy that passwords must not have and word from any language dictionary, must not use slang words, must not use a reversed word and must not be one of the above with number added to it. [HSE 2013]

A rainbow table attack is defeated in the same way as a dictionary attack the only new concretisation is the speed that the attacker can run through the possibilities. This allows the attacker to use more possibilities in the same time.

The only way to prevent a brute force attack is to use a large alphabet and limit the number of possible tries before locking out the account. This can be hard to implement given the growing use of mobile devices which are used away from the office where the IT staff are located and might be needed to reset an account. Another method which could prevent the attacker is to limit the number of tries to one per some timeframe such as one a minute or three per day. This will allow the user to make an error while entering their password but will not need the intervention of IT staff to allow them to use their account again. If the tries are limited enough then an attacker would not have time to try all possibilities before the password is changed.

Social engineering attacks can only be prevented with education, insuring that all users know not to reveal there passwords to anyone for any reason. This can be helped by the IT staff resetting the users password if they do need to logon as that user then getting the user to change it when they have finished. This type of attack is also used against people in their personal lives the phishing attacks are a type of social engineering attack. Once again the only way to spot these attacks is to educate the users not to follow links sent to them. Companies can help this by not including links in official emails that way a link will look out of place to the user as they will not be expecting it and will not just click it out of habit.

With all types of attack limiting the number of tries will reduce the risk while it is always possible that the attacker could get lucky and gain access with on early try.

Given that there is a possibility that an attacker can gain access to an account it can be useful to track the times that the user logs on at this can be useful in a workplace where logons outside normal working hours could be checked or flagged to the user the next time they logon. Another idea which works more for little use systems is to display the user the date and time they last logged on at. This would work on all systems and allow the user to see if the last logon was them. However a user would get used to clicking through this message and would soon not even look at it this can be seen with other confirmation dialog boxes such as those at application close the 'are you sure' message users get so used to clicking yes that they click it without noticing it.

2.5 Remote systems

In the paper Basic Principles for Increasing Security in a Mobile Computing Program the authors state that there are 7 important points when dealing with mobile security they are; data encryption, password enforcement, device management, compliance and configuration management, data access, trust and confidence and enablement and ease of use [Will Ro 2012]

Data encryption. This must not impact one the usability of the device but should insure that data stored on it or sent from it is protected from unauthorized access. This is a balancing act the more encryption used on the system the longer the encryption and decryption will take but the more protected the data will be. Another consideration for mobile devices is power use given that they are likely to be used on battery and encryption involves a large number of calculations which can reduce battery run time.

Password enforcement. This is especially important on mobile devices, while a company can control access to the computers on it premises with doors and locks they can't protect mobile devices in the same way as such they can be exposed to an attacker who has physical access to the device

Device management. Given the relative ease of the device being lost or stolen it would be beneficial to have some system in place which could wipe data from the device remotely.

This system would depend on the device being connected to the internet at some point after it is lost. There is a danger whit this type of system that the wrong device could be wiped

Compliance and configuration management. Given the number of different mobile devices that a company could make use of and the number of different applications which can be used on those systems some form of application test and certification should be put in place this should be used to insure that a user only installs approved applications on any device which holds company data. This is especially important in the area of smart phones where there is easy installing of third party applications built into most of those operating systems such as the Google Play store for android devices

Data access. When deciding what data to allow a remote or mobile user to access and store on the mobile device consideration should be given to what use the user has for that data and if they need access to it while mobile

Trust and confidence. It is important that the user understands the trust that is being placed with them and that the company trusts that the user will only use company information for valid purposes.

Enablement and ease of use. The users must be shown the benefits of all the security methods that they must endure and that they see them as a help to their work and not a hindrance to it

2.6 Conclusions

In this chapter we looked at the different concerns relating to computer security. We also looked at the different systems used to help insure a system stays secure.
Then we looked at the different types of attack which a system could suffer. Finishing up with a look at remote systems and the requirements for such a system

3. Passwords

3.1 Introduction

Passwords are stored in a password file. This file stores the user ID and their password. The password can be stored in plain text or can be hashed. Hashing is a mathematical function which can take variable length inputs and produce a fixed length output. Most current password systems use a salt value, which is added to the password the user picks before it is hashed. This salt value must be stored in the password file so that it can be added to the password a user enters when accessing the system. The salt value is used to increases the amount of possible passwords as well as hide the fact that a user is reusing the same password in more than one location

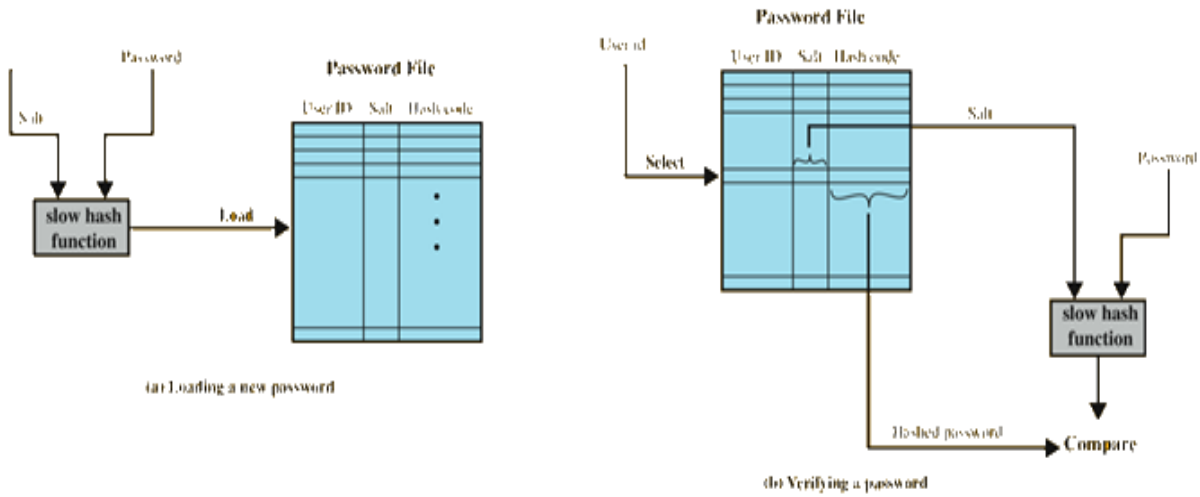

Figure 1: Password hashing [W Stallings & L Brown 2011]

3.2 Alternates

There are many different approaches to replacing passwords. As seen in the paper Secure Alternatives to Password-based Authentication Mechanisms [Patrick Elftmann 2006] he states that alternatives to password-based authentication mechanisms already exit, but, however, are not widely adopted in systems. This is in part due to costs and mistrust of what is new

He states the following requirements are believed to be important for an authentication mechanism in order to be considered as an alternative to a password-based authentication system.

- No additional hardware required
- Higher security
- Better memorability
- Simple and easy to use
- Large area of application[Patrick Elftmann 2006]

These range from using some other memory based activate such as a graphical password where the users must remember a pattern to draw on a grid this screen is used on some smart phones. One example is on Samsung devices where the user is shown a three by three grid of dots as shown in figure 2 and must join them in the right way to unlock the device shown in figure 3

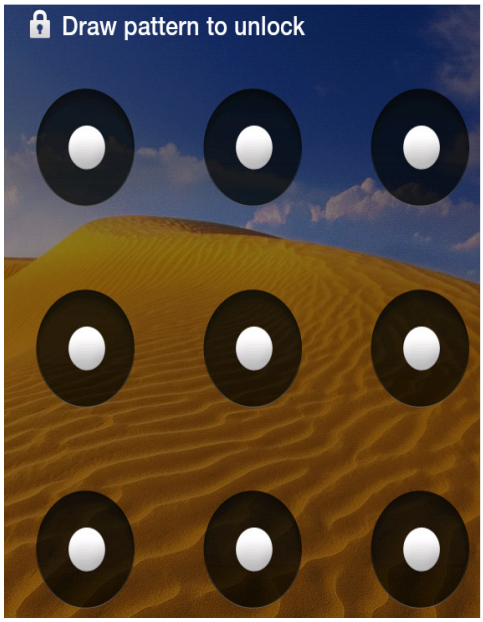

Figure 2 Screen from Samsung graphical lock

Figure 3 Screen from Samsung graphical lock

Another alternative which is growing in use is Biometric based systems. These include systems which use something unique to the user to identify them this can be a finger print, an iris scan, face recognition or even voice pattern recognition. This type of system is growing

in use among mobile systems with newer models of laptops now being equipped with fingerprint scanners.

The danger of this type of system is that if a security breach takes place then the biometric data could be compromised and given that the user cannot change this information it could render them unable to use this type of system, for example if using an iris scanner then if that data is compromised then the user could use their other eye but this would be there last option unlike passwords where there is a near unlimited amount for a user to select from. It could also be an issue if it is used widely, given that it is advised not to use the same password across different systems using biometrics you have little choice in that matter and one weak system could lead to all systems being open to the attacker.

Token based systems relay on the user having a physical device which is used in some way to identify them to the system. One common type of this is a smart card this is an item which generates a code for the user to enter to the system, this code changes at a predetermined time the system can also generates a code using the same algorithms and compares the one entered by the user with the one it generates if they match the user is allowed onto the system. This type of system prevents an attacker from retrieving the password as it passes across the network as the password changes. The problem with this type of system is the cost of the devices and the risk that the whole system is dependent on the algorithm staying secret.

Another version of this system has been used for many decades by the banking industry. The pass machines which use a card that the user must enter and then the user must supply a pin so this type of system is mixing the token based system with a password

3.3 Password standards

Password policy's used in different companies very to some extent. They all set out the minimum requirements of the password including requirements such as length and charter types used. This can vary within a company with different requirements for different access levels as can be seen below in the extract from a password policy. The administrator level passwords must be changed quarterly while user level passwords must only be changed biannually.

- “All system-level passwords (e.g., root, enable, Windows Administrator, application administration accounts, etc.) must be changed on at least a quarterly basis.
- All production system-level passwords must be part of the InfoSec administered global password management database.
- All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every six months.
- Where SNMP is used, the community strings must be defined as something other than the standard defaults of "public," "private" and "system" and must be different from the passwords used to log in interactively. A keyed hash must be used where available (e.g., SNMPv2).
- All user-level and system-level passwords must conform to the guidelines described below.”[SANS 2013]

The guidelines given are requiring that a password must have a lower and upper case letters, a numbers, punctuation and special characters as well as setting the length to 15 characters. It then goes on to give examples of week passwords and includes a hint as to how to make secure passwords

“Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase” [SANS 2013]

Another example of a password policy is that issued by the HSE it is largely similar to the one above. It lists the following areas as part of the password standard.

Password Length

Password Complexity

Password History

Password Aging

Password security

[HSE 2013]

This policy requires administration level passwords to be changed every quarter while user level passwords are every 4 months. There is also a requirement that a password not be reused for 12 months this focuses a user to create at least 3 strong passwords.

These two different policies have the same frequency of change required of administrator level passwords while the seconded one requires the user to change their passwords more often three times a year instead of twice. The need to change a password is often seen as an annoyance by users this can lead to the user using one password and simply amending a number or letter to it every time they are required to change it.

3.4 Conclusions

In this chapter we looked at passwords and some of the alternatives to them. We then went on to look at some common password policies in use in industry today.

4. Experiment

4.1 Introduction

The purpose of this experiment is to identify the common types of passwords that users use across different systems and to try and identify if there is any way that an application could try and prevent the user picking an easy to guess password. To achieve this first data is to gather data from a group of users. Then using this information create the requirements for an application to limit the users use of easy to guess passwords

4.2 Experimentation

The first part of the experiment was to conduct a survey to gage the types of passwords in use. This survey had 19 questions. The results from this survey was largely in line with what was expected based on the research involving other similar areas of study.

4.2.1 Survey Design

The Survey was deigned to be something that a person could complete quickly, this was to encourage more people to respond to it. To achieve this, the questions were limited in number and length to allow the complete survey to fit on a single page.

The questions were mostly multiply choose to allow people to answer the survey in a shorter time.

The survey was divided into three sections the first was questions relating to general information about the respondent. The second relates to the users password habits this is the main part of the survey, while the third section gather more information about the respondents habits about general security in their life outside computers as well as allowing them to give feed back

4.2.2 Survey Results

The first set of results which needs to be looked at is the age range of the different respondents. This is shown in figure 4 below. This shows that the majority of respondents were in the 18 -25 age range. This age range is the most active on social media online. Given

this the number of different systems that this group will be higher on average than the other age ranges.

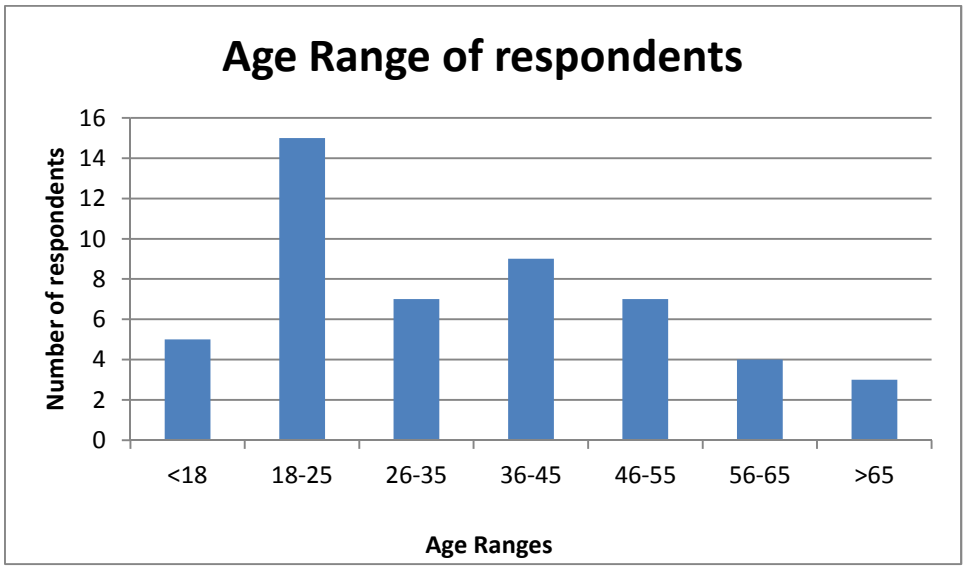

Figure 4 Age range of respondents

It also should be noted that the majority of respondents where male at 64% male to 36% female.

Another thing of note from this survey is the number of respondents who think that their personal passwords are more important than the ones they use in their work. This is shown in figure 5 below as can be seen the split is about 2 thirds favour passwords used for home.

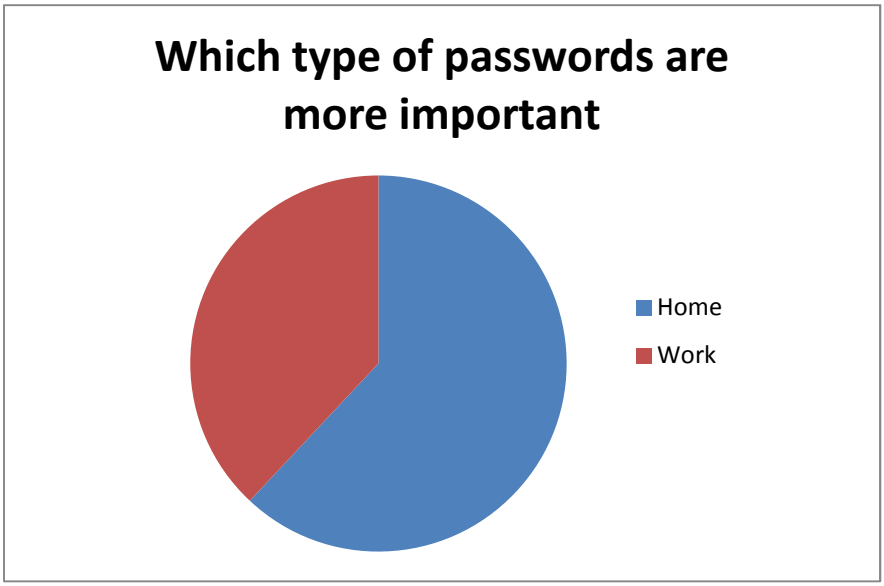

Figure 5 Which type of password are more important

The next area of interest is the types of passwords used.

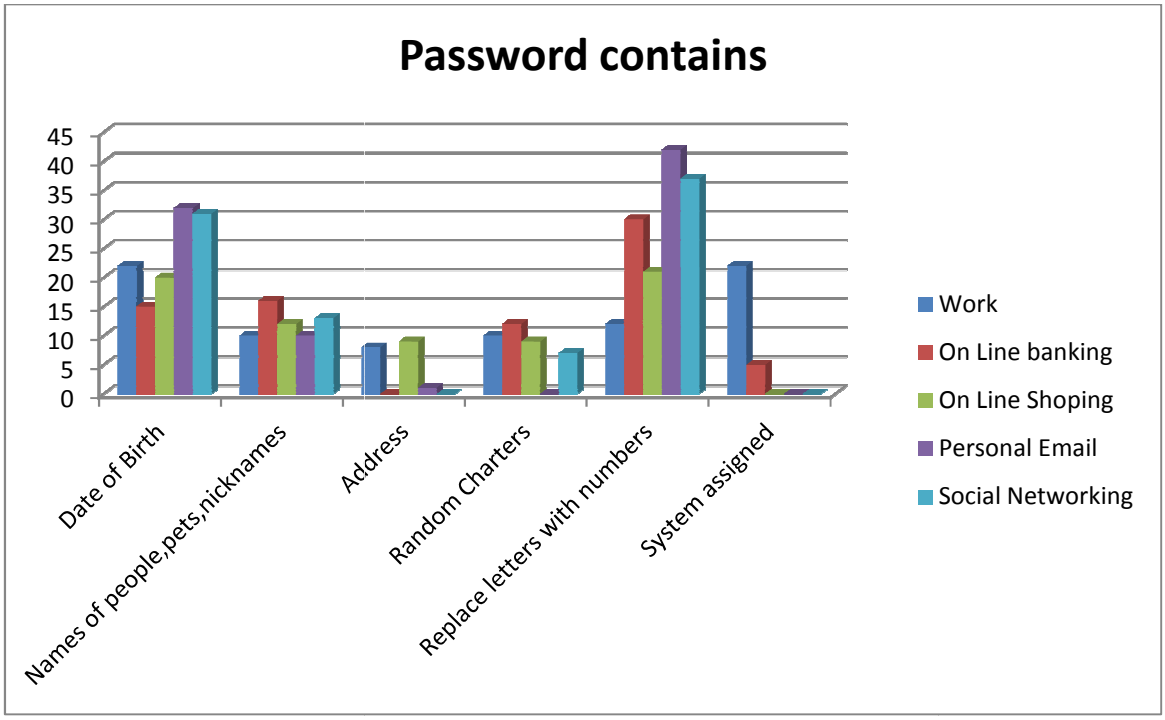

Figure 6 Contents of passwords used in different systems

As shown in Figure 6 above people use different types of password for different things. It is of note that 22 respondents state that there work assigns them a password while 5 respondents state then there online banking issues them with a password. This taken with figures 7 to 10 shown below which stats that 5 respondents are unable to change their work passwords while 10 are unable to change there on line banking passwords. While some of this might be due to user education or poor interface design it is notable. Also to be noted is that despite the high percent of people who believe that personal passwords are of higher importance most of the respondents to this survey state that they never change their social networking of personal email passwords. The sometimes group stays around the same number across all system types.

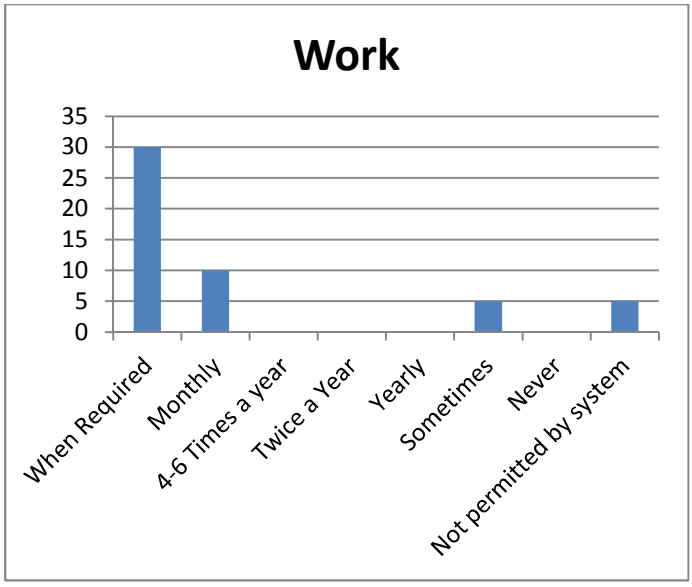

Figure 7 Frequency of password change, Work.

The majority of respondents only change their passwords when required. This could show that users will only change their passwords when made to do so by the system. Some users might normally change their passwords but are made to do so by the system more often than they normal would.

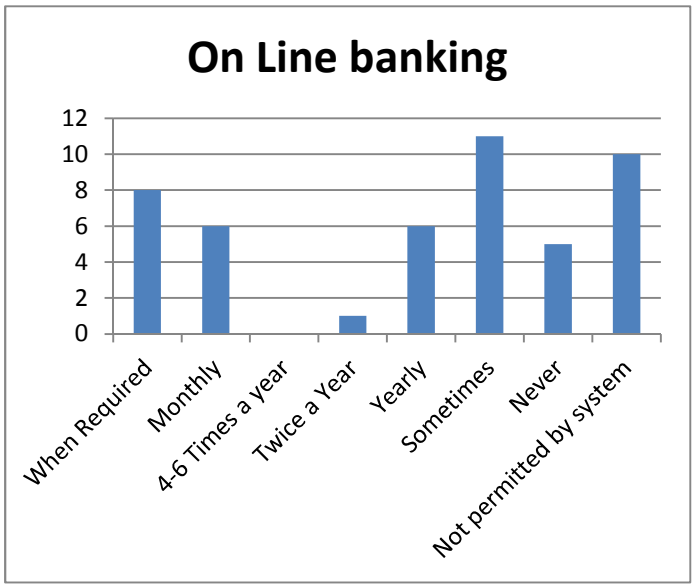

Figure 8 Frequency of password change, Banking.

Of note about the results of the changing of online banking passwords it the high number who are unable to change it. This could leave the system more open to brute force attacks which can be carried out over a long time to avoid detection by the system given that the attacker knows that the password will never change.

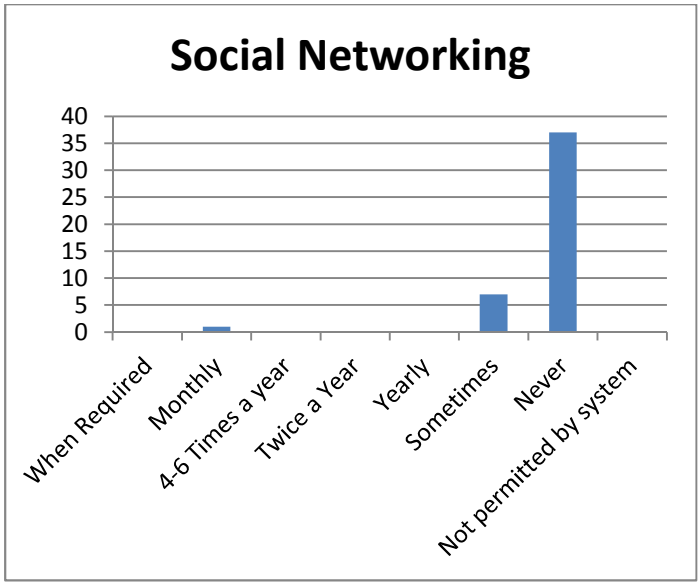

Figure 9 Frequency of password change, Social Networking

By far most respondents do not change their social networking passwords. This is quite worrying as a lot of users of social networking sites store personal information about themselves and their friends, family which could be of value to an attacker. The information could be used to gather data for marketing or scam emails. This type of personal information could also be used in an attack on other systems.

Figure 10 Frequency of password change, Shopping

Many respondents never change the password they use of online shopping. While most do change their password at least yearly, with most of those that do change their password doing so monthly. It should be noted that more people change their password used of on line shopping then for on line banking, this could come from the base trust people have had in banks for many years while online shopping is still relative new.

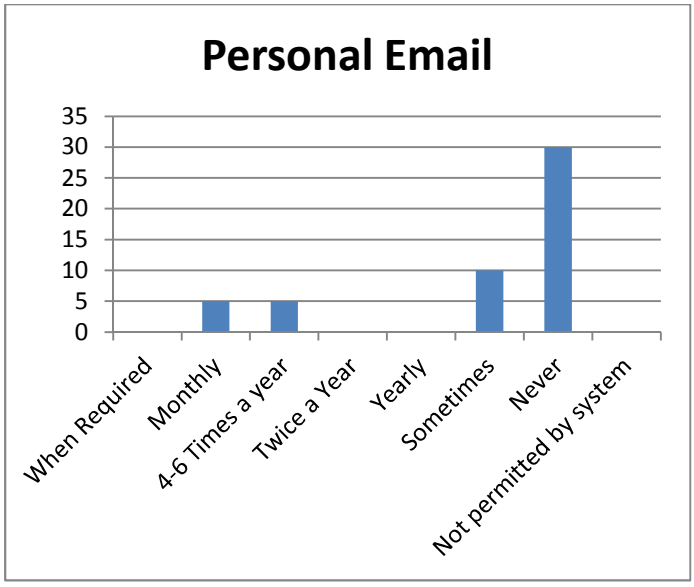

Figure 11 Frequency of password change, Email

The number of people who never change there email password is second only to the number who never change their password of social networking websites. This could be an issue for mush the same reason given that people use their email to communicate with friends and family and also potently with work and commercial companies, so the amount of information stored could be of interest to an attacker and the emails address stored by the system could be used to lunch scams against

4.3. Using the results

4.3.1 The Application

The next part of the experimentation was to gather more detailed information for a smaller group of users. To achieve this a small application was developed. This application was used to gather more details about the passwords people pick under different situations.

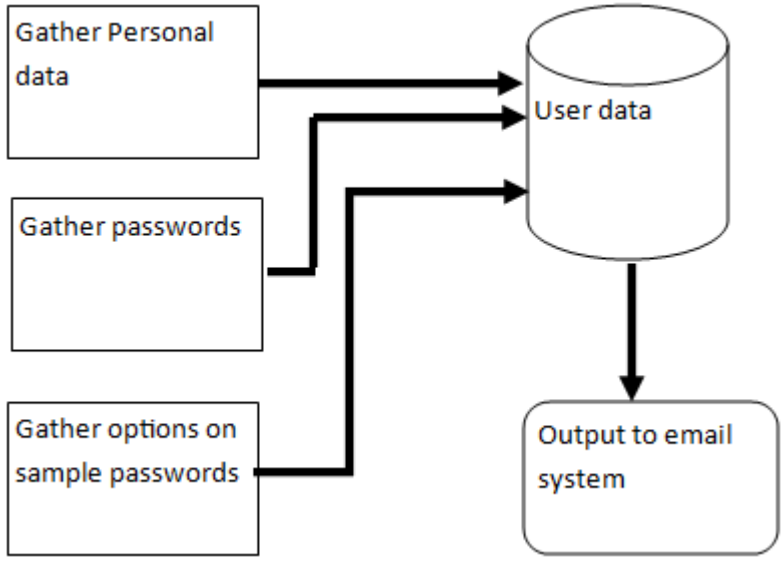

Figure 12: Application Design

The main focus of this application was to gather data from users to this end a simple design as shown in figure 12. This consisted of a single data class file to hold the information entered by the user. This class was also responsible for outputting this data to both the user at the end and for the email which was sent back. The rest of the classes in the application were to gather data from the user and were user interface classes using windows forms as was the final screen which presented the data to the user.

The application was split into three parts the first asked the user to enter some personal details including the items most commonly used by respondents to the survey to generate their passwords. This information was presented on a single screen to the user shown in figure 13

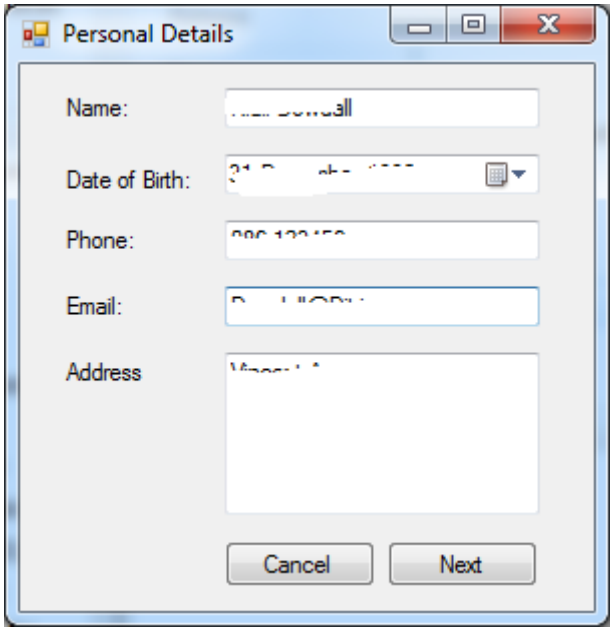

Figure 13 Application part 1 screen

The second part presented the user with a series of six questions each one stating different minimum requirements for the password. This part was to try and gage how a user works with the requirements the system places on them when generating a password. The six requirements were as follows;

1. Any length.
2. At least 6 charters long. Containing at least one letter and number
3. Between 6 and 10 charters in length. Containing at least one number, small and large letter
4. At least 10 charters long. Containing at least one number, symbol ,small and capital letter
5. At least 15 charters long. Containing at least three numbers, symbols, small and capital letters
6. At least 8 charters long. Containing at least one number, symbol ,small and capital letter

In the third part the user is presented with a list of passwords and asked which one they believe to me the most secure. This was left till the end to avoid influencing the user's option when they were completion the second part. There were four groups of passwords presented to the user these are shown below in table 2

List 1	List 2	List 3	List 4
password	TeethHandle	Dundalk150987	r:Y!1243vK
password1234	HorizontalLine	Kids109315	N.xAyt><4n
PassWord	CatsAreCool	11N0vemBer1918	ml)mRqci$u
PassW0rd	Themyouwillneveruse		C=UH7>=5;
PassW0ed!	pasfhocal		WerthoultyQwertpQ

Table 2: Password lists used in application

At the end the user was asked to enter one of the passwords they had entered in the second part, this was used as a way check if the user had entered random strings for the passwords or if they picked passwords they could remember. The application then allowed the user to select what information they wanted to allow be used as part of the research.

4.3.2 Results

There were 12 participants in this section of the research. They were from a wide area of knowledge as follows;

Respondent	Age Range	Gender	Technology skill
1	18-25	Male	Beginner
2	18-25	Female	Intermediate
3	26-35	Male	Intermediate
4	36-45	Male	Advanced
5	26-35	Male	Intermediate
6	36-45	Male	Beginner
7	26-35	Male	Intermediate
8	18-25	Male	Advanced
9	36-45	Male	Intermediate
10	18-25	Female	Intermediate
11	26-35	Male	Advanced
12	26-35	Female	Intermediate

Table 3: Application respondents list

One notable fact about the responses is that the passwords entered by users did not differ much between the different requirements. One respondent selected the following responses for the six different requirements was “J3006*88dG” this was the same one selected for all but the fifth choose which needs to be at least 15 charters long, for this the following was entered “QQQJ3006*88dG!!!aaa” this contains the same password as the others only with added charters to fulfil the requirements. The thing of note about this is that the first requirements place no restrictions on the passwords entered yet the one picked was as the same on the later ones this could mean that this is a password user by this person. It is also noteworthy that the numbers could be at date 30 June 88 form the data given to the application this is the this persons date of birth but could be another date of note to them. They know the password they were asked at the end.

Of the 12 responses 7 picked a password which meant the basic requirement of most systems in having a letter, number and capital letter for the first response which placed no requirements on the user while only 5 of them pick such a password for the second which placed no requirement on the use of a capital letter as shown in table 4 and table 5 below.

1	Poul”3
2	J3006*88dG
3	L23$op
4	Well
5	1s’an
6	K3v!n11
7	gHam01
8	1
9	p0pp)tS
10	F”t7&oIPQ1
11	kyti
12	120991

Table 4: Responses to passwords any length

1	Poul23
2	J3006*88dG
3	L07yuot
4	Myself
5	1234L!w
6	11K3v!n
7	gHam01
8	1Q23456
9	Da1ryM!lk
10	f£T8*Oipq2
11	kvti
12	12099i

Table 5: Responses to password 6 long. number and letter

This result implies that when a user is given a list of requirements to follow that more people are inclined to follow them compeered to those who will go over the minimum requirements while if no requirements are listed a user will pick a password which meats the most common requirements by default.

The fifth question which wanted a password of at least 15 charters and three of each symbol, number small and capital letter produced instruction results of the 12 respondents only 1 appeared to pick a unique password while the other pick simpler passwords with extra bits added at the beginning or end this is shown in table 6

1	Poul”3Poul”3Poul”3
2	QQQJ3006*88dG!!!aaa
3	WERtyu123$%^L23
4	K3yB0raD-12-15-
5	QWErty123$%^789
6	WhyS0L0ng”8-15”
7	HFR568hrey%*(ryu
8	weiuSDFKJ&^&*9784
9	IreLand4Ever123!”£
10	WayT00L0ng-it-is-
11	euiowtOUIY87*&^3
12	UIkjh876&*^Wkjh

Table 6: Responses to password question 5

It should be noted that only one person was asked to enter this password as the test at the end and they did get it right it was the tenth respondent. Some of the entry’s look like random presses of the keyboard which could invalidate them as possible passwords for those people because they might not be able to remember them, it also implies that the respondents felt that this was too long of a password to be expected to user some even say that in there passwords namely respondents 6 and 10.

In the third part of the application the users where shown sample passwords each respondent was shown the same list so that their responses could be compared with greater accuracy. Figure 14 below shows the results of each of the different questions in this section and the number of respondents who picked each one.

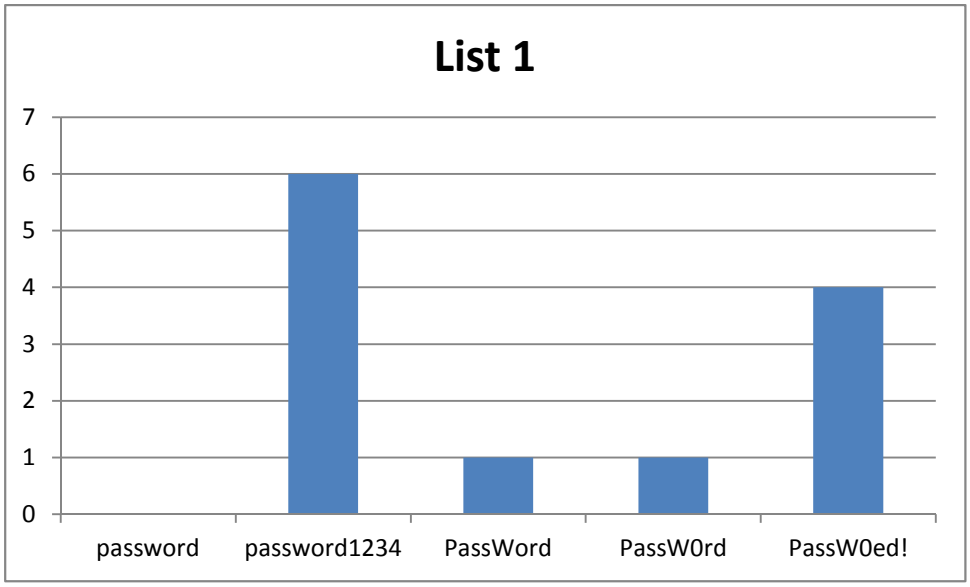

Figure 14: Responses to part three of application, List 1

It can be seen that in the first list the most users picked the longest password while the last option was the best as it uses both capital letters and symbols which increases the number of tries a brute force attack needs.

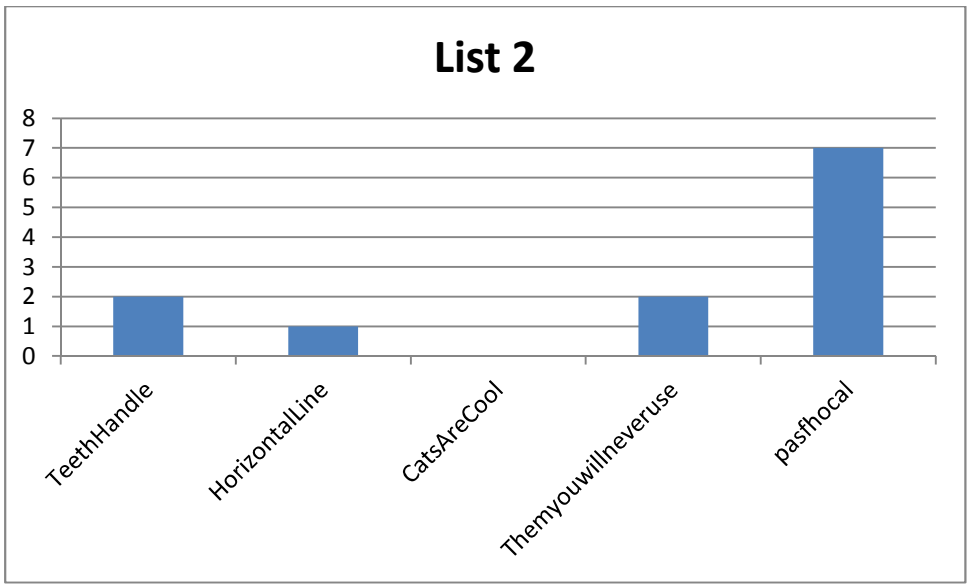

Figure 15: Responses to part three of application, List 2

On list 2 the most users picked the last option which is a Irish word this would be the easiest for both a brute force attack and a dictionary attack to break given the small length and its inclusion in a dictionary even if it is not an English.

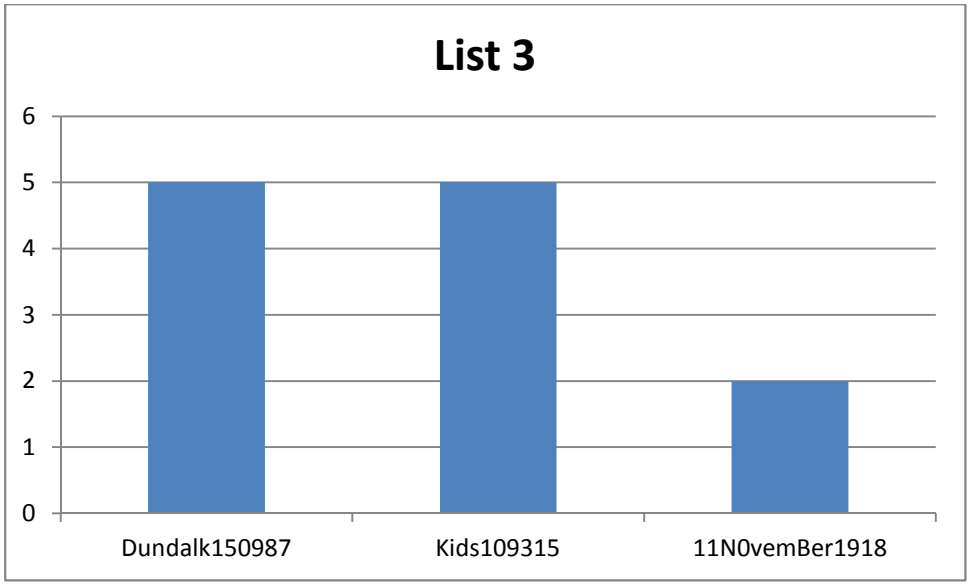

Figure 16: Responses to part three of application, List 3

On list 3 equal numbers of users selected the last 2 options while both similar in strength against a brute force attack the last option is the date of the Armistice Day in world war one which is a date a lot of people know.

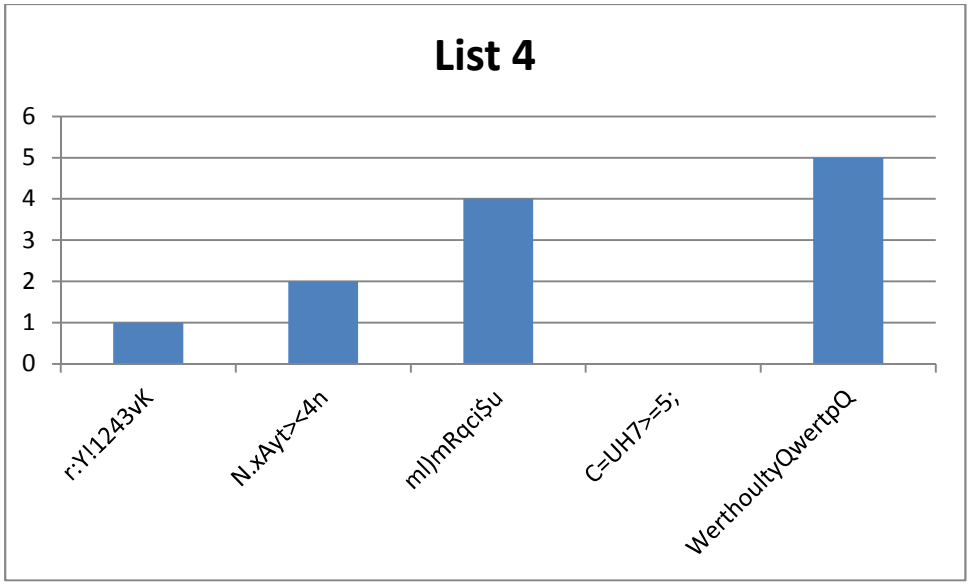

Figure 17: Responses to part three of application, List 4

On list 4 once again the longest option was picked which also happens to be the weakest because it does not use and numbers or symbols.

Based on these results it can be seen that a lot of users think that length is the most important factor in password security where in fact that is only one part of it, The larger the possible alphabet is the greater the number of possible values and therefor the longer a brute force attack will take.

4.4 Conclusions

In this chapter we first created a survey to gather data form a large group of people we then examined this data to see what it meant to how passwords are used by people. Then we developed an application to further refine the data gathered by getting a smaller group of users to give more detailed information which we examined to identify any trends in how people perceive passwords.

5. Conclusions and Future Work

5.1 Conclusions

As is evident in the research for this project users have a tendency to pick easily guessed passwords. With this in mind further research into replacements for passwords. There is also some evidence that users pick less secure passwords due to the requirements placed on them by the systems. When asked for a password a user will enter one that they can remember, if they are then told that that does not conform with the requirements some tend to just pick one which matches the requirements which might be less secure then there first chose.

The survey carried out for this project showed that users tend to reuse the same passwords across different systems; this might be a cause for concern depending on what systems this relates to. If a user is using the same password for their bank account as a random forum on the internet that would be a reason for concern as the forum might not have their password file held securely unlike a bank, if however the passwords are shared on two unimportant internet forum then the risks are lower even if the password is compromised. This is one area of farther study to identify any patterns or trends as to which systems users reuse passwords and see if any steps could be put in place to reduce the risks of this activity. One are to look at is the use of a third party to allow logging onto different using a single username and password. This type of system is in place within some companies notability colleges where a student's college system logon is used al allow that student at access third party resources such as email or on line journal repositories.

The system outline given in this document could form the base of research into the creation of a system to fill that function. This would require greater research into the types of data the different systems could have access to and gather the views of industry members as to the merits of investing time in developing such a system instead of creating a different authentication system which relays less on a remembered password

5.2 Future Work

5.2.1 Design

In order to implement a system which can prevent a user from selecting a password easy to hack you must use information about the user. This information should include name, address and date of birth at a minimum. This information would not be known to many systems that a user interacts with. The systems they use as part of their employment could have access to this level of information as it is already used in the workplace it would only be a matter of linking the employee data to this system. Some users do provide this information to websites normal social media sites this would allow these sites to use this type of password system however not everyone supplies this information and some will give false information to hide their real identity.

Given the limited amount of systems which could reliability have access to this information and the need for it to be at the base level of the system to reduce the change of it its self being comprised the most likely places to have a use for this type of system would be work places. The system could be used to test a user's password every time the user changed it. It could filter out any passwords using personal information about that user and possible any user on the system to prevent a user from using the name of a colleague as their password to the system.

5.2.2 Software Design

With this in mind this system must be able to perform the following

- Read user information from personal data store. This could be a database or other storage system
- Compare the password a user enters with the personal data
- Evaluate if the entered password is derived from the personal data
- Interface with the system at a low level either adding to or replacing the root systems password manager. This could be the operating systems or a custom application.

- Prevent users from accessing any personal data. If the password is filtered out the reason should not show what personal information it was a match to protect the personal data of users from being seen by another user

First this system needs a generic data system. This can be achieved by using in memory data structures offered by programming languages such as datasets offered by the .net framework. This will allow a custom function to be used to import from the different storage systems in the different environments. The first step is to create the work flow of the system which is shown in figure 18 below.

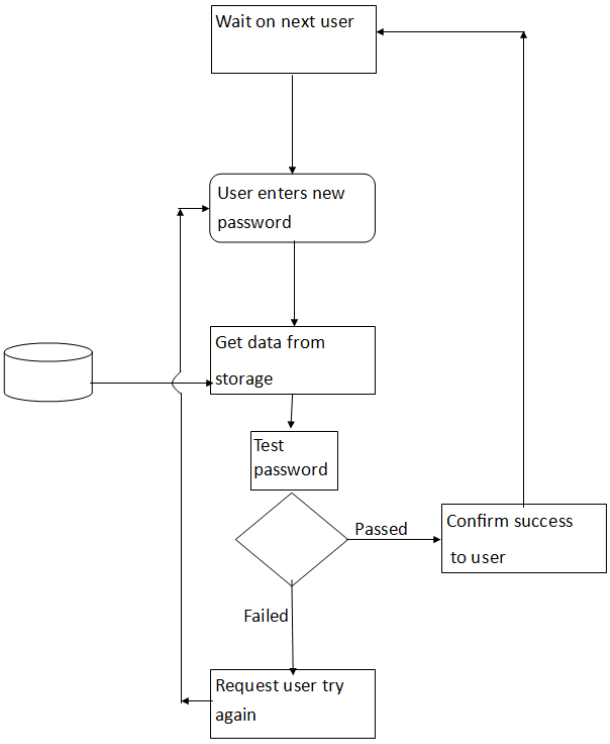

Figure 18 Suggested workflow

The data design of this system would be simple only containing two elements, a collection of user elements as shown in figure 19 below

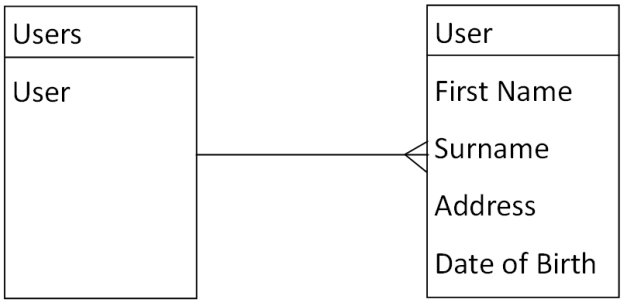

Figure 19 Data design

The user element could be expanded to include other pieces of data if the host system could provide them but the ones listed are the main ones which would be known to anyone who know the user. This data setup could be created by using class files one class called user which have private members to hold the data while allowing access to them through public methods which could be used to insure only valued data and access requests would make it to the data. Another element ‘users’ would simply be a collection of user elements and could be within the main application class of as its own class depending on the language used and performance requirements.

Bibliography

Central Statistics Office (2012) Available http://www.cso.ie/Quicktables/GetQuickTables.aspx?FileName=cja01c16.asp&TableName=Theft+and+related+offences&StatisticalProduct=DB_CJ [accessed 01 May 2012]

C. Kalapeso and S. Willersdorf and P. Zwillenberg. (2010) *The Connected Kingdom* The Boston Consulting Group

S. Mulpuru (2012) US Online Retail Forecast, 2011 to 2016 Forrester

W. Stallings & L. Brown (2011) *Computer Security. Principles and Practice* 2nd ed Prentice hall

B. Lampson (2004) Computer security in the real world IEEE

R. Kanaley (2001) Login error trouble keeping track of all your sign-ons? Here's a place to keep your electronic keys, but you'd better remember the password. San Jose Mercury News (2001)

A Adams & M. A Sasse (1999) *Users Are Not The Enemy* Communications of the ACM Vol 42 No 12

SANS (2013) *Password Policy* Accessed via http://www.sans.org/security-resources/policies/Password_Policy.pdf on 4 January 2013

HSE (2013) *Password standards policy* accessed via http://www.hse.ie/eng/services/Publications/pp/ict/Password_Standards_Policy.pdf

Will Ro (2012) *Basic Principles for Increasing Security in a Mobile Computing Program* HTC Pro

Patrick Elftmann (2006) *Secure Alternatives to Password-based Authentication Mechanisms* Laboratory for Dependable Distributed Systems RWTH Aachen University

von Solms, B 2000, *Information Security—The Third Wave?* Computers & Security,

Russell, D & Gangemi, G.T 1991, *Computer Security Basics*, O'Reilly Media, Inc.

Desman, M.B 2002, *Building an Information Security Awareness Program*, Auerbach Publications.

Herold, R 2005, *Managing an Information Security and Privacy Awareness and Training*, Auerbach Publications.

Appendix A

Computer password security survey

Please answer the questions below all questions are optional your help in greatly appreciated.

Please note if you fill in this questionnaire, your answers will be treated in a highly confidential way. Neither I, the Dublin Institute of Technology nor any other third part will identify your name, email address or any other personal details, nor will it be possible to identify you in any way in the report I will publish as part of my MSc dissertation. I would like to personally thank you for your time in taking part in this survey.

Please DO NOT include any passwords which you use or have used in any response

Section A

1) Please indicate your age — Under ☐ 18-25 ☐ 26-35 ☐ 36-45 ☐ 46-55 ☐ 56-65 ☐ Over 65 ☐

2) Please indicate your gender? — Female ☐ Male ☐

3) Hours spent on computer per week at Home? — <5 ☐ 6-10 ☐ 11-15 ☐ 16-20 ☐ 20-25 ☐ 25-30 ☐ 30> ☐

4) Hours spent on computer per week at Work? — <5 ☐ 6-10 ☐ 11-15 ☐ 16-20 ☐ 20> ☐

5) Are computers the main part of your work? — Yes ☐ No ☐

6) How long have you being using computers in years? — <5 ☐ 6-10 ☐ 11-15 ☐ 16-20 ☐ 20> ☐

Section B

7) In your opinion are passwords used for work more important then the ones you use for yourself? Home ☐ Work ☐

8) Which of the following would you use any of the following as either a part of a password of all of the password?

	Date of birth	Names of people, pets or nicknames	Address	Random	Replace vowels with numbers Eg (0 for o 1 for i)
Work	☐	☐	☐	☐	☐
On Line banking	☐	☐	☐	☐	☐
On Line Shopping (EG EBay, amazon)	☐	☐	☐	☐	☐
Personal Email	☐	☐	☐	☐	☐
Social networking (EG Twitter, Facebook)	☐	☐	☐	☐	☐

9) Would you ever write down your passwords? — Yes ☐ No ☐ Sometimes ☐

10) Do you use the same password for more then one system? — Yes ☐ No ☐

11a) Have you ever used a password manager? — Yes ☐ No ☐

11b) Would you consider using one? — Yes ☐ No ☐ Don't know ☐

12a) Does your workplace have a Computer use poli- — Yes ☐ No ☐ Don't know ☐

12b) Have you read it? — Yes ☐ No ☐

13) How often do you change your passwords?

	When required	Monthly	4-6 times a year	Twice a year	Yearly	Never
Work	☐	☐	☐	☐	☐	☐
On Line banking	☐	☐	☐	☐	☐	☐
On Line Shopping (EG EBay, amazon)	☐	☐	☐	☐	☐	☐
Personal Email	☐	☐	☐	☐	☐	☐
Social networking (EG Twitter, Facebook)	☐	☐	☐	☐	☐	☐

Section C

14) Would you describe yourself as cautious in general? Yes ☐ No ☐

15a) Do you have a house alarm? Yes ☐ No ☐

15b) Do you set the alarm every time you leave the house? Yes ☐ No ☐

16) Do you shred old bank statements pay slips and bills? Yes ☐ No ☐ Sometimes ☐

17) Do you have a key lock code set on your phone? Yes ☐ No ☐

18) How do you pick passwords in general?

19) Any further Comments

If it would be ok to contact you for an interview in the future please supply your preferred contact information _____

Thank you for taking the time to complete this survey.

If you have a question or concern about this survey please email me at d11123915@mydit.ie