The Problem with Passwords

Sam Lubbe
Rembrandt Klopper

Abstract
The study that is reported here investigated password security and related issues at a South African tertiary institution. The main reason was to investigate why password security is such a problem for students. This was because students fell victim to people using their Internet identification to send nasty e-Mail, to visit pornographic websites, etc. The study used a questionnaire and IS&T students at the University of KwaZulu-Natal as respondents. The data shows that more than 60% of the students surveyed actively use passwords to protect their data and account security while 36% just used passwords when required by regulations. The researchers' primary recommendation is that tertiary institutions should rigorously enforce security regulations.

Keywords: Account, data protection, hacking, internet identification, log-in, password security, password sharing.

Literature Review
According to a minority staff statement during the 1996 USA Congressional Hearings on Intelligence and Security, a password is 'a protected word or string of characters that identifies or authenticates a user for access to a computer system, or a specific resource such as data set, file, or record.' Similarly, Wikipedia (2006) defines passwords as a form of authentication, which uses secret data to control access to a resource. In most cases, the key security mechanism is a password to verify to the operating system that the

associated account really belongs to the person who is using it to log on (Confirmed by Shinder, 2003). It is important that a user chooses a password that is hard to guess and that users keep this password a secret. A user password is a key to an account and anyone who knows it has access to files.

Shinder (2003) states that the basic concept of 'locking' an account with a password is simple. When a user account is created, a password is usually assigned to the user by the administrator. Depending on the type of user account (local account that can only log onto the computer or network account called a domain account), a database is stored either on the local hard disk or on an authentication server which Microsoft calls a domain server. The database contains a list of all the user accounts and their corresponding passwords. When a user logs on and enters the credentials, they are checked against this database, if the password matches, access is granted. Entering the user name and password every time a user wants to access a different resource on the computer or network would be cumbersome, so the authentication process is made transparent to the user after the initial logon.

On average, only about half of the users will actually use a password that satisfies the policy (Lemos, 2002). If 900 out of 1,000 employees use strong passwords, a password cracker can still guess the remaining 100 user/ID password pairs. When it comes to strong passwords, anything less than 100% compliance is weak (Lemos, 2001). With modern processing power, strong passwords are no match for current password crackers. While some user ID/ password pairs may take days or weeks to crack, approximately 150, or 15%, can be brute forced in a few hours.

Strong passwords are expensive. The second highest cost to help desks is related to resetting forgotten passwords. Many companies have full-time employees dedicated to nothing more than password resets. Bradley (2004) adds that, although alternatives for user authentication are available today, users log onto their computers and remote computers using a combination of their username and. The password 'jyg2&ti5' is harder to crack than 'bradley1'.

Description	Examples
1. English Upper Case Letters	A, B, C, … Z
2. English Lower Case Letters	a, b, c, … z
3. Westernized Arabic Numerals	0, 1, 2, … 9
4. Non-alphanumeric (‘special characters’)	For example, punctuation, symbols. ({}[],.<>;:''?/|\`~!@#$%^&*()_-+=)

Table 1: *Password characters*

Labmice.net (1998) adds that adopting password policies is one of the ways to ensure system security. It is up to each customer to determine how strong enough. A complex password that cannot be broken is useless if one cannot remember it. For security to function, one must choose a password one can remember and is complex. For example, Msi5!YO (My Son is 5 years old) OR IhliCf5#yN (WE have lived in California for 5 years now.

Bradley (2004) also states that sometimes less is more. System administrators force a password length of 8 characters and may even require a special character. In reality, a 7 character password is more secure than an 8, 10 or even 12 character password on Windows NT systems. When Windows NT stores a password in its local archive it breaks it down into 7-character chunks, pads the chunks to fill 2 complete chunks and encodes each chunk separately.

Hacking Passwords

As much as advanced passwords are designed and created, hacking will always be there. In the 1060’s computers were mainframes, locked away in temperature-controlled, glassed-in lairs. Smarter people created what they called ‘hacks’programming shortcutsto complete computing tasks more quickly (Granger, 2002). Security experts estimate that more than a million passwords have already been stolen on the Internet. A hacker will launch a dictionary attack by passing every word in a dictionary (which can contain

foreign languages as well as the entire English language) to a login program in the hope that it will eventually match the correct password. Users are too predictable in their choice of passwords (University of Michigan, 1997). Some companies are utilizing the expertise of convicted hackers to update their security features. These hackers come from a ready market for their expertise, and financial rewards.

Password Policies

Shinder (2003) states that some of the policies can be enforced through operating system or third party software. It is useful to enable security auditing and have the system write an event to the Security log when failed logon attempts are made one can determine when the attempts are occurring (Shinder, 2003). Over the past couple of years, the potential of information systems (IS) and its equally important support to organizational activities (to gain competitive advantage) has been recognized. Competencies in the area of IS are becoming important in business organizations (Quinn & Paquette, 1990). At one level of strategy, there are some organizational activities dedicated to looking at the vulnerability of data (i.e. data falling in the wrong hands, trying to maintain the availability, confidentiality and integrity of data at all times) (Quinn & Paquette, 1990).

Research Questions

A number of the problems mentioned have been solved. However, there are still some issues that need to be answered.

1. What efforts are institutions trying in order to improve security?
2. How will the institution benefit from password improvement measures?
3. What are other intended benefits of this research?

Research Options

The Researchers decided to apply quantitative research in the study. It is a numerical representation and manipulation of observations for the purpose of describing and explaining the phenomena that those observations reflect. The

aim was to gather valid, reliable, unbiased and discriminatory data from a representative sample of respondents (Technology Assessment, 2001). In this study, the characteristics of the subjects, and the independent and dependent variables defining the research question were measured.

It was decided to use a questionnaire to answer the research questions. The instrument was divided up as follows:

- Questions 1-3 deal with demography;
- Questions 4-5 deal with computer usage;
- Questions 6-11 deal with passwords;
- Questions 12-20 deal with physical security, software and system policies.

Results

This section is based on the analysis of results acquired from research questionnaire. This section addresses the treatment of data, the reliability of that treatment, the data analysis, and the results.

Demographics

The sample of one hundred and forty (140) students was evaluated for the ability to supply relevant data with regard to the research question. Of this sample, one hundred and seven (107) completed questionnaires were collected and collated. Gender in this research was mainly a criterion used to highlight the difference in interests between the two genders. The dominating age group was the 21-25 yea group. The final range of ages included in the analysis is from eighteen to twenty six and above years.

Online Log-in Accounts

As more people are resorting to technology and the internet, some are still sceptic. It is apparent that students indulge into online participation. Institutions and companies that conduct various sorts of activities on the Internet have become the target of fraudulent e-Mail and Web site scams. These scams are known as ‘phishes,’ (pronounced ‘fishes’) and they attempt to illegally obtain clients' personal and account information.

Using of the Same Password

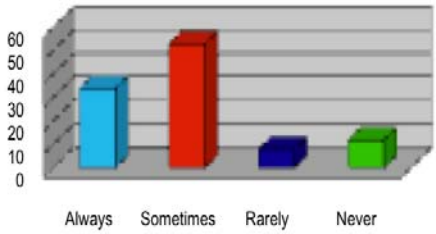

Figure 1: Using the same password to access multiple accounts

Users are still not aware of the implications of using the same password to access multiple accounts. This could be as a result of lack of awareness or just simple users being naive which could result in serious impacts. Since passwords were introduced in the 1960s, the notion of a 'good' password has evolved in response to attacks against them. First there was no rule about passwords except that they should be remembered and kept secret. As attacks increased in sophistication, so did the rules for choosing good passwords. Each new rule had its justification and, when seen in context, each one made sense. People rarely had trouble with any particular rule: the problem was with their combined effect (Shinder, 2003).

An early and important source of password rules was the Department of Defence Password Management Guideline codified the state of the practice for passwords. In addition to various technical recommendations for password implementation and management, the Guideline provided recommendations for how individuals should select and handle passwords. In particular, these recommendations yielded the following password rule: Passwords must be memorized. If a password is written down, it must be locked up (Shinder, 2003).

Password Sharing

Most of the respondents responded negatively when asked whether they share their passwords. This is an indication of an understanding of privacy, where accounts, data or even information is concerned. Shared accounts

confuse the lines of accountability and should be avoided. Each user on the system should have an individual account. The bad habit of sharing a password may be broken by selecting passwords that would create embarrassment if shared with anyone else. Change a password as soon as possible after it has been used in an emergency by someone other than the person with whom it usually is identified. When an account has been used illegally, it often turns out that someone gave away the password involved (Gates, 2004).

From a security standpoint non-technical steps should be taken to try to alleviate the 'users sharing passwords' problem, because it is a breach of security on a network. It's a step to figure out how to limit users to a single connection, but the problem is stopping users from sharing passwords. Depending on the current configuration of an account and password policies, a suggestion would be frequent password changes and account lockouts to drive home the point (Hunter, 2004).

Changing Passwords

The unfortunate part with the response for this question is that the majority responses were negative. According to the results, students take lightly to the concept of updating and changing of passwords. A password should be changed often. An account should always be created in a manner that forces the new user to change the password (Gates, 2004).

Response	Always	Sometimes	Rarely	Never
Number of Respondents	5	12	53	37

Table 2: *Frequency of changing passwords*

Forgetting Passwords

Figure 2 represents the respondents who forget their passwords. Forgetting a password can be dangerous since passwords are more or less used as keys for data and loosing a key can result in negative results. Some facts about people's use of passwords have emerged from a survey of over 3,000 IT

professionals and business executives. Just under a quarter have eight or more different names and passwords to access different parts of their computer system. Over half (55 %) of people have written their password down at least once, with most having written them down about three times. Nine percent of people always write their passwords down (McCarthy, 2003).

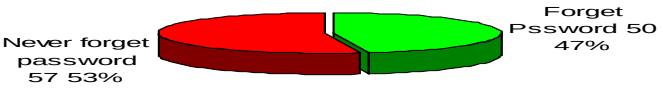

Figure 2: *Forgetting one's password*

Figure 2 represents the respondents who forget their passwords. Forgetting a password can be dangerous since passwords are more or less used as keys for data and loosing a key can result in negative results. Some facts about people's use of passwords have emerged from a survey of over 3,000 IT professionals and business executives. Just under a quarter have eight or more different names and passwords to access different parts of their computer system. Eighteen per cent are lucky enough to have just one, with most stuck with between three and four passwords. Over half (55 %) of people have written their password down at least once, with most having written them down about three times. Nine percent of people always write their passwords down (McCarthy, 2003).

Response	Always	Sometimes	Rarely	never
No of respondents	6	38	23	40
%	5.60%	35.50%	21.40%	37.30%

Table 3*: Logging on for visitors*

While just under half claim they have never forgotten their passwords, thirty-seven percent state just once or twice, and 10 % three or four times. Two percent of people admit to having forgotten their passwords eight or more times. Usernames and passwords are just a part of using computer systems (McCarthy, 2003). Forgotten or lost passwords can cost money. Technology Researchers Gartner estimates it costs US$ 14 -US $ 28 for companies to reset a password (Hunter, 2003).

Computer Security Problems

Respondents were asked if they experienced computer security problems. While security experts say the publicity has highlighted a serious problem, they are sceptical about the ability to do anything about it (Fester, 1998). He reports that computer security breaches were up 16% from 1996 to 1997, and computer-related crime including security breaches cost 241 surveyed organizations $136 million.

Response	Don't know	yes	no
No of respondents	70	32	5
% Respondents	65.40%	29.90%	4.60%

Table 4: *Intrusion detection system*

Intrusion detection is the art of detecting inappropriate, incorrect, or anomalous activity. Intrusion detection systems that operate on a host to detect malicious activity on that host are called host-based ID systems. The term intrusion is used to describe attacks from the outside; whereas, misuse is used to describe an attack that originates from the internal network.

Guidelines for Changing One's Password

Response	No	Yes
No of respondents	80	27
%	74.70%	25.20%

Table 5: *Guidelines for changing password*

A user password is the only means the computer system uses to verify identity. If an intruder gains access to an account, they can then compromise the security of the entire cluster. There are password requirements that have to be complied with:

1. A password should not be the same as a username, nor should it contain a username or simple permutations of it. (e.g., John should not use any of the following for passwords: bigboote, BigBoote, bootebig, etc.) A password should not contain any personal data or simple permutations thereof.
2. A password should not contain correctly spelled English words.
3. A password should not contain names of famous people, places, things, fictional characters, movies, TV shows, songs, etc. John should not use buckaroo, banzai, star trek, Kirk, etc, as passwords.
4. Do not use any example passwords given for a password.

Embed extra characters in the word. Symbols and control characters are especially good. Digits are good, too (e.g., abb@8d instead of abbaed, or buck@r0o, or ba%nz! Ai, Misspell words, e.g. buckarew or bonzaye). Use unusual capitalization. All lowercase, or all capitals, or capitalizing first letter of words (or all but 1st letters) are somewhat common; randomly capitalizing a letter or two is better. So John might want to use buckaroo or baNzaI. Embed one word in the middle of another, or interleave the letters of two words, e.g. stkirkar (Kirk in star) or sktiarrk (star and Kirk), combining two or three of the above is better.

If a user thinks that s/he has found a security problem on the University's data network or suspect a breach in security on any computer, whether it is an IS, a Departmental system or a personal system or computer systems there should be a method for reporting the findings. System policy refers to the management of the system (i.e. network and systems management; policy definition; policy objects; policy enforcement; policy monitoring). To prevent operators from drowning in detail, the level of abstraction needs to be raised in order to hide system and network specifics.

Correlations between Surveyed Factors

The Researchers used correlation to measure the relationship between the variables he used in the compilation of this study.

Always	many	44
	few	22
	one	8
Sometimes	few	18
	one	3
Rarely	few	4
	one	8

Table 6: *Comparison of regularity of computer usage and number of email accounts*

		OFTEN	ACCOUNTS
OFTEN	Pearson Correlation	1	.552(**)
	Sig. (2-tailed)	.	.000
	N	107	107
ACCOUNTS	Pearson Correlation	.552(**)	1
	Sig. (2-tailed)	.000	.
	N	107	107

** Correlation is significant at the 0.01 level (2-tailed).

Table 7: *Correlation table between gender and computer skills*

There was a strong relationship of .552. This proves that the more users use computers, they are very likely to have multiple user accounts, be it online or not. However this shows that as a result of more user accounts, the higher there is a chance of breach, due to the reason that number of accounts is dependant on regular usage of computers (University of Michigan, 2002).

Correlation between Year of Study and Computer Security Problems

First	always	5
	sometimes	2
	rarely	3
Second	sometimes	8
	rarely	4
Third	sometimes	16
	rarely	5
Fourth	always	3
	sometimes	29
	rarely	11
	never	5
Postgraduate	sometimes	8
	rarely	5
Masters	always	3

Table 8: *Year of study and computer security problems*

As the table shows, there is a weak relationship between the two. This means that regardless of which year of study a user is, they still experience security problems thus security problems is independent of the year of study.

		YEAR	COMPSEC
YEAR	Pearson Correlation	1	.068
	Sig. (2-tailed)	.	.485
	N	107	107
COMPSEC	Pearson Correlation	.068	1
	Sig. (2-tailed)	.485	.
	N	107	107

Table 9: *Correlation table between year of study and computer security problems*

Correlation between Forgetting Passwords and Computer Security Problems

Yes	always	2
	sometimes	34
	rarely	14
No	always	9
	sometimes	29
	rarely	14
	never	5

Table 10: *Passwords and computer security problems*

		FORGETP	COMPSEC
FORGETP	Pearson Correlation	1	.017
	Sig. (2-tailed)	.	.866
	N	107	107
COMPSEC	Pearson Correlation	.017	1
	Sig. (2-tailed)	.866	.
	N	107	107

Table 11: *Correlation between forgetting passwords and computer security problems*

Table 11 is an illustration of a correlation between the number of people who forget their passwords and people who experience computer security problems. As the table implies there is a 0.017 weak correlation. This means that if one forgets a password the chance of a user experiencing security problems is more likely the same as another user who does not. The reason for this is that as long one uses a password, accounts are kept secure at all times. Therefore using a password at the end of the day is for security Physical…, 2004).

Correlation between Gender and Sharing of Passwords

Male	always	2
	sometimes	16
	rarely	6
	never	38
Female	sometimes	3
	rarely	14
	never	28

Table 12: *Gender and password sharing*

		GENDER	SHAREP
GENDER	Pearson Correlation	1	.156
	Sig. (2-tailed)	.	.109
	N	107	107
SHAREP	Pearson Correlation	.156	1
	Sig. (2-tailed)	.109	.
	N	107	107

Table 13: *Correlation between gender and sharing of passwords*

Tables 12 and 13 above show the correlation between gender and sharing of passwords. The purpose of this correlation was to investigate how gender differs in terms of confidentiality. As shown by the graph, although there is a correlation, it is weak. This means that neither variable is dependent on the other. Whatever a user's gender is, it is likely that they share their passwords with other users and these pauses as a threat in terms of security.

Correlation between Number of User Accounts and Using the Same Password

Table 15 shows a correlation between number of user accounts and using the same passwords. The figure shows a negative and weak correlation. This means that the more accounts a user has does not necessarily mean that s/he is likely to use the same password for different accounts. Having different passwords for different accounts is advisable but at the same time might lead to users having to use easily guessable passwords that can be remembered and this is exactly how password security is weakened.

Many	always	5
	sometimes	32
	rarely	2
	never	5
Few	always	12
	sometimes	19
	rarely	5
	never	8
One	always	17
	sometimes	2

Table 14: *User accounts and using the same passwords*

		ACCOUNTS	SAMEP
ACCOUNTS	Pearson Correlation	1	-.332(**)
	Sig. (2-tailed)	.	.000
	N	107	107
SAMEP	Pearson Correlation	-.332(**)	1
	Sig. (2-tailed)	.000	.
	N	107	107

** Correlation is significant at the 0.01 level (2-tailed).

Table 15: *Correlation between number of user accounts and using the same password*

Recommendations and Conclusion

This section has been the analysis of the results acquired from the research questionnaire. This analysis included graphs and table as a method of presentation of data and results, which were then discussed as to what they mean. After this analysis, the author has realized that there is in fact importance of security (computer security) at the institution.

Password Security Challenges

User passwords are one of the security headaches, especially when users put their passwords on sticky notes that hang from their monitors; select easy-to-guess passwords like a child's name; use the same, weak password for all of their work and home accounts; and/or share their passwords with others when asked (Physical, 2004). The security measures that users should take to protect their passwords (e.g. using different passwords for different sites). The computer industry requires that passwords are of limited value, and means of augmenting those passwords are becoming mainstream. The best solution is two-factor authentication, combining a password with a piece of hardware that users have to carry around with them to get access to a secure system (Wagner, 2004).

Password Privacy

The point of password privacy cannot be stressed enough. Passwords should never be shared because it is only good if it is kept a secret. Ideally, passwords should never be written down, although, in reality, most like to document their passwords. Users should be sure they don't keep a password list in a computer or in any obvious place. If users want to keep a password a secret, remember a password can be stolen by observation. Be cautious of anyone looking over a shoulder when one types in a password (Berger, 2007)

If one loses a wallet, a person would probably know the sense of vulnerability that comes with it. Someone might be walking around with a false identification, pretending to be someone else. If someone stole passwords, they could do the same thing online. Each time user accesses personal account information a unique access code and password combination has to be entered. It is important that users remember never to share their password with any other person.

A Proposal for Constructing Strong Passwords by Using Mnemonically-based Passwords

One of the major problems that leads computer users to lax password protocols is that a single user often has to remember six or more passwords—one password to log on to a networked computer, a second password to log on to the institution's network, a third password to link on to her/ his bank account, a fourth password to log on to an online funds transfer facility like PayPal, a password for each of goodness knows many social networking websites where s/he is registered. To solve the problem of keeping track of multiple websites the authors propose a mnemonic device approach.

Wikipedia defines a mnemonic device as 'a memory aid' and then explains, 'Mnemonics rely not only on repetition to remember facts, but also on associations between easy-to-remember constructs and lists of data, based on the principle that the human mind much more easily remembers insignificant data attached to spatial, personal, or otherwise meaningful information than that occurring in meaningless sequences'.

The mnemonic device that the authors propose has three components, namely a prefix, a root and a suffix. Our proposal is that the root remains

constant across passwords, but that the prefix and suffix components change for each website password. Because the root is used constantly, and it therefore becomes easy to remember it, it could contain an unpredictable sequence of symbols like 1t0c3sp for which one devices a narrative mnemonic like 'one tea, no coffee, three sugars please'. The prefix and suffix elements of the password would depend on the website or network being accessed, for instance the prefix for one's online bank account could be lh (lolly house) and the suffix ae (almost empty). The computer user then constructs outer and inner narrative scenarios:

- Outer narrative: lolly house almost empty
- Inner narrative: one tea, no coffee, three sugars please

To access the university network one could use the prefix dh (varsity network) and the suffix bi (bloody irritating). This will render the passwords:

- Bank account: lh1t0c3spae—lolly house one tea no coffee three sugars please almost empty
- University network: dh1toc3spbi—damn hoops one tea no coffee three sugars please bloody irritating.

A related approach to formulate such a password could be to extract the root component from an easy to remember rhyme:

EoEhsasactfBAoAhdadabtr:
Eve oh Eve, how shiny and sweet and curved the fruit
But Adam oh Adam, how dark and deep and bitter the root

MTtlinft: Maggie Thatcher 'This lady is not for turning'

Being wary of using such a mnemonic approach to secure passwords is hardly a failure of memory, its a failure of imagination.

Password Guidelines

Passwords are a critical part of information and network security. Passwords serve to protect user accounts but a poorly chosen password, if compromised, could put the entire network at risk. Passwords are used to access any number of systems, including the network, e-Mail, the Web, and voicemail. Poor, weak passwords are easily cracked, and put the entire system at risk. Create a password that is easy to remember.

- Passwords should not be based on well-known or easily accessible personal information;
- Passwords should contain at least 8 characters;
- Passwords should contain at least 5 uppercase letters (e.g. N) or 5 lowercase letters (e.g. t) or a combination of both;
- Passwords should contain at least 2 numerical characters (e.g. 5) and should contain at least 1 special characters (e.g. $);
- A new password should contain at least 5 characters that are different than those found in the old password, which it is replacing;
- Passwords should not be based on users' personal information or that of his or her friends, family members, or pets. Personal information includes log-on ID, name, birthday, address, phone number, social security number, or any permutations thereof;
- Passwords should not be words that can be found in a standard dictionary (English or foreign) or are publicly known slang or jargon;
- Passwords should not be trivial, predictable or obvious;
- Passwords should not be based on publicly known fictional characters from books, films, and so on;
- Passwords should not be based on the company's name or geographic location.
- Generally Passwords should be changed every 60 days. Old passwords should not be re-used for a period of 6 months**.**
- Password Protection Guidelines
- Passwords should be treated as confidential information. No employee is to give, tell, or hint at their password to another person,

including IT staff, administrators, superiors, other co-workers, friends, or family members, under any circumstances;

- If someone demands a password, refer him or her to these guidelines or have him or her contact the IT Department;
- Passwords should not be transmitted electronically over the unprotected Internet, such as via e-mail;
- No employee is to keep an unsecured written record of his or her passwords, either on paper or in an electronic file;
- Do not use the 'Remember Password' feature of applications and do not create a 'hot key' for password use;
- Passwords used to gain access to company systems should not be used as passwords to access non-company accounts or information;
- If possible, don't use the same password to access multiple company systems;
- If an employee either knows or suspects that his/her password has been compromised, it must be reported to the IT Department and the password changed immediately;
- Do not use any of the password examples shown in this document;
- Finally, remember that there is no need to share IDs and passwords.

Password Limitations to be Taken into Account

Computer security is primarily concerned with ensuring the availability of information and protecting it against tampering, destruction or misuse. This is true when information is made easily available to a large community of potential users in multiple locations on networks.

However there are both use and time limitations:

- An account will be locked after three failed logon attempts.
- User passwords (online) will expire every 90 days
- After 90 days of inactivity, the user account will be locked.
- Passwords have a character limit and
- Passwords can be very easily lost and forgettable.

Answers to Research Questions

What Efforts are Institutions Trying in Order to Improve Security?

According to the findings of this study most institutions have some security measures implemented. However these measures are not enough since students do not just end by logging into the machines but also have other accounts, students can still get hold of other students registration numbers and access what is not theirs e.g. school assignments and e-mails, students still log on for other users, share their passwords, use the same password over and over again and there is no one to monitor such.

How will the Institution Benefit from Password Improvement Measures?

Students shall improve their education on security and acquire new knowledge. The information about child nutrition, agriculture and tertiary institutions application procedures will be provided by use of guidelines implemented by administrators at labs.

What are Other Intended Benefits of this Research?

The fewer complaints there are about security the more satisfied the students are. This will contribute to accurate and reliable work, thus providing a secure environment for studying and for promoting the use of computers for day-to-day activities by students; this will also give them a chance to improve their knowledge (where technology is concerned).

Conclusion

As intended to trust digital technology providers' users require protection from credentials, theft and unauthorized access to our personalized online resources, credit cards, accounts etc. Security is fundamental to virtually every organization today, yet not every company has achieved the fundamental goal of effectively securing itself.

One of the ways to protect information or physical property is to ensure that only authorized people have access to it. Verifying that someone is the person they claim to be is the next step, and this authentication process

is even more important, and more difficult, in the cyber world. Passwords are the most common means of authentication, but if you don't choose good passwords or keep them confidential, they're almost as ineffective as not having any password at all. Many systems and services have been successfully broken into due to the use of insecure and inadequate passwords, and some viruses and worms have exploited systems by guessing weak passwords.

References

Bradley, T 2004. Creating Stronger Passwords. Accessed May 3, 2008 at www.microsoft.com.

Berger, S 2007. Passwords. How to Choose. Accessed May 30, 2007, http://www.compukiss.com/articles/passwords-how-to-choose-2.html

Fester, P 1998. Computer Security. Accessed November 24, 2004 at www.about.com.

Gates, J 2004. Sharing Passwords. Accessed online November 24, 2004 at www.usmd.edu.

Granger, S 2002. The Simplest Security: A Guide to Better Password Practices. Accessed November 2, 2007 at http://www.Security focus.com/infocus/1537.

Hunter, L 2004. Windows Connectivity. Accessed online November 17, 2004 at www.isaserver.org.

How to bypass Bios Passwords. Accessed online August 25, 2004 at www.labmice.com.

Internet Security. Accessed online November 24, 2004 at www.microsoft.com.

Information Technology Solutions. Accessed online November 24, 2004 at www.winnetmag.com.

Labmice 1998. Password Security, Expensive. Accessed online 20 August, 2004 at http://labmice.techtarget.com/security/passwordsec.htm.

Lemos, R 2002. Passwords, the Weakest Link. Accessed online May 22, 2004 at www.tecrime.com/llartA03.htm.

Minority Staff Statement 1996. Security in Cyberspace, U.S. Senate Permanent Subcommittee on Investigations, June 5 1996. Accessed

online on 10 May 2008 at: http://ftp.fas.org/irp/congress/1996_hr/s960605a.htm.

McCarthy, K 2003. Passwords are evil and expensive Accessed online 20 August, 2004 at www.tecrime.com/llareA02.htm.

Physical access, Accessed 20 August, 2004 at www.about.com.

Quinn, JB & PC Paquette 1990. Technology in Services: Creating Organizational Revolutions. *Sloan Management Review* Winter: 67-78.

Shinder, D 2003. Passwords: The Weak Link in Network Security. Accessed online May 04 at www.tecrime.com.

University of Michigan 1997. ITCS: Frequently Asked Questions About Uniqnames and Passwords Accessed online 20 August 2004 at www.itd.umich.edu/help/faq/uniqnames/

Wikipedia 2006. Passwords Accessed online 20 August 2004 at http://en.wikipedia.org/wiki/Passwords accessed.(There has been instances where the credibility of Wikipedia has been questioned and this is why the authors correlated information from Wikipedia with information provided by other authors).

Sam Lubbe
School of Computing
University of South Africa
South Africa
Lubbesi@unisa.ac.za

Rembrandt Klopper
School of Information Systems & Technology
University of KwaZulu-Natal
South Africa
rklopper@gmail.com