Survey on Awareness and Security Issues in Password Management Strategies

D.Santhi Jeslet[1], G.Sivaraman[2], M. Uma[3], Dr.K.Thangadurai[4], Dr. M.Punithavalli [5]
[1&2] Department of Computer Science, M.G.R.College,Hosur,TN, India

[3] Research scholar, Dravidian University, Kuppam, AP, India
[4]Department of Computer Science, Government Arts College(Men) , Krishnagiri- 635 001, India
[5]Director, Sri Ramakrishna College of Arts & Science for Women, Coimbatore - 641 044. India.

Abstract
Any communication via Internet travels across unsecured channels. This gives raise to security breaches. So user identification and authentication is needed to overcome these security breaches. Password-based systems remain the predominant method of user authentication despite the many sophisticated and viable security alternatives that have emerged. However, this survey shows that passwords are often compromised through the poor security and management practices of users. This paper also concentrates on user password composition and security practices for email accounts. The results of a survey that examines user practice in creating and using passwords are reported. Toward the end of this paper, we give some recommendation for the education of user in creating and maintaining their passwords.
Keywords: Password management, security, user authentication, password composition and management.

1. Introduction

Computers and information system are dominating our modern world. Internet is the technology that helps to access the widespread computing and communication networks. Any communication via internet travels across unsecured channels. This gives raise to security breaches. User identification and authentication along with encryption key distribution is one of the important function provided by communication network services. The use of specialized software and hardware such as firewalls is used to implement basic access control. The means by which users make themselves known to the system is through a unique identifier such as name or an account number. Once the access control mechanism establishes that the user is a valid user, authentication of that user is undertaken.

The first step in minimizing loss of information is to establish security on the boundary of a system. Access controls are the usual type of security control implemented on the boundary of a system [5]. The main functions of these controls are to restrict the use of system and resources to authorized user. Apart from this, it limits the type of actions that authorized users can perform. Users can be authenticated by following any one of the approach [6]:

- Smart card or other token
- Fingerprint, Retinal image, Voice or Facial pattern
- Password or PIN.

Each approach has its own advantages and flaws. Regardless of the approach selected by the organization, there is a trade-off between the value of resources and the effectiveness and cost of implementing and maintaining it. Even though significant advances have been made in graphics-based approaches, password remains the most common approach for authenticating a user.

In spite of their weaknesses, passwords-based system prevails because they can prove effective protection if they are used correctly. However, they are simple for both system designers and end users. End users often compromise password security by forgetting them, writing them somewhere, sharing them with other people and selecting easily guessed words. Research has shown that users are one of the main risks to the effectiveness of security measures designed to counter information system threats. [4].
Users are helpless to security threats. This is because many do not have adequate knowledge to recognize the risks nor to implement appropriate protection mechanism. This study focuses on password issues by examining the behaviors of the user when creating and managing passwords. This paper also gives the outlines of the major problems associated with password-based authentication system.

Manuscript received April 5, 2010
Manuscript revised April 20, 2010

2. a. Security Issues Associated with Passwords

The password-based approach to user authentication has a number of shortcomings. There are many methods used to compromise password security. Some of which needs little or no technical knowledge while others require a high level of technical expertise. Guessing, observing, viewing some written records, tricks and being told, requires less technical knowledge. Keyboard monitoring, packet interceptions, keystroke interception and host emulation requires high level of technical knowledge.

Several studies have proved that password can be determined or 'cracked'. A modern program designed to crack passwords, can determine the password with 5 characters within two seconds and 8-characters within ten hours [2]. Longer passwords needs more time to discover. If the password used is a common word or a word from the dictionary, the time taken to discover it by brute force attack is reduced significantly[2]. Many researchers have suggested various strategies to overcome the threat of software to break passwords.

Researchers have also been recommending strategies to overcome inherent limitations in password system, most focused on the user [1]. The following are the major strategies for overcoming the inherent weakness in password usage:

- **Password length of at least 8 characters:** Longer passwords increase the time taken by software cracking program to determine it.
- **Password with mixed case/symbols:** Including both upper/lower case and some special symbols increase the number of character permutations that must be tried.
- **Non-Dictionary words:** Selecting non-dictionary words as password prevents the use of dictionary based attacks. Such attack can identify password in less than 20 minutes.
- **Password ageing:** Systems allow intruder who got a valid password, until it is noticed. Users need to change their passwords regularly.

These strategies may help to improve password security. But these restrictions make memorizing of passwords a complex and unintuitive exercise. Public access system requires users to manage a large number of passwords on a day-to-day basis. Consequently, users may be tempted to reuse passwords to access multiple systems for ease of memorizing.

b. Survey of Email Password Security

Password reuse can compromise the security of all of the password systems that a user might access. Users choose passwords that are easy to remember. Typically these passwords are based on some meaningful combination of names and/or numbers [1]. If the security of one system is breached, then all other password-based system and other computing assets might become vulnerable to unauthorized access and malicious damage.

Electronic mail (email) is universally the most widely adopted password protected application. It affects the daily life of almost every working person [4]. Employees from a manufacturing of garments organization were chosen to be the research participants. Among 884 employees, there were marginally more females than males in the sample. The majority of the participants were under 28 years of age; 213 participants were under 28 and 584 between 28 and 32 years. The remaining 87 participants were mature aged (>36 years of age). Most of the participants were full time workers (811) and 59 were part-time workers. 13 did not respond to this question and one participant was a trainee. The majority of the participants had used computers for more than 5 years. 480 had used computers between 6-10 years and 252 for longer than 10 years. Only 25 participants had used computers for less than 2 years, while 126 had used computers between 3 and 5 years. Table 1 shows these details.

Participants were asked for what purpose they used computers. More than 83% of participants indicated their main use was Internet (92.9%), email (90%) and home use (83.4%).

Variable	Category	Total	%
Gender	Male	378	42.8
	Female	505	57.1
	No Response	1	0.1
Age	<28 Years	213	24.1
	28-32 Years	584	66.1
	33-35 Years	55	6.2
	>36 Years	32	3.6
Working Status	Full Time	811	91.7
	Part Time	59	6.7
	Trainee	1	0.1
	No Response	13	1.5
Computing Experience	0-2 Years	25	2.8
	3-5 Years	126	14.3
	6-10 Years	480	54.3
	>10 Years	252	28.5
	No Response	1	0.1
Total Participants		884	100

Table 1: Demographic Details of Participants

Banking (50.2%) and work use (47.7%) formed a second grouping and other areas of use (study and research, entertainment including games and online purchasing and selling) accounted for 15%

Participants were also asked to indicate what their email usage was. Personal email use was 95.5% followed by organization use (84.7%) and work related use (24.9%). The majority of participants had either two or three email accounts. 49.4% had two and 27.9% had three, 11.7% has one account and 11% has four or more email accounts.

Since 95% of the participants were using email for personal communication, serious implications for organization security are raise; especially when they reuse password across email. This is because password reuse and poor security practices increases the likelihood that a password might be deduced thereby increasing the vulnerability of other system where this password had been used.

Participants were then asked about the composition and choice of password. The table 2a shows it.

Since the survey data is categorical, nonparametric statistics were employed in analyzing the data across three variables: gender, age and employment status. The table 2b specifies it.

Variable & Category	Total	%
Password Length		
1-5 characters	31	3.5
6 characters	126	14.3
7 characters	93	10.5
8 characters	258	29.2
9 characters	104	11.8
10 characters	68	7.7
11 characters	34	3.8
>11 and <26 characters	65	7.4
No response	105	11.9
Password Composition		
1. Alphabetic only	348	39.4
2. Numeric only	57	6.4
3. Alphanumeric	374	42.3
4. Includes symbols	36	4.1
5. Other	3	0.3
No Response	66	7.5
Choice of Password		
1. Meaningful data	381	43.1
2. Combo meaningful data	210	23.8
3. Pronounceable word	46	5.2
4. Random characters	95	10.7
5. Not self-chosen	14	1.6
6. Other	71	8.0
No response	67	7.6
Frequency of Changing Password	547	61.9
1. Never	119	13.5
2. Less than once a year	56	6.3
3. 1-3 times a year	79	8.9
4. 4-6 times a year	10	1.1
5. Once a month	6	0.7
6. Several times a month	67	13.5
No response		

Table.2a:Participant Practice Relating to Password Composition and Management

From the analysis we can say that females are more likely to choose alphabetic or numeric characters only, while males choose a combination of characters including symbols. With respect to age group, participants aged 25 years and under are more likely to choose alphabetic or numeric characters only; while the older participants choose alphanumeric combinations that may include symbols. Full time employees and those who were under training tend towards combination of characters while those who were employed in part-time basis were more likely to choose alphabetic or numeric characters only. There is a significant difference in the method of choosing passwords for gender only. Females are more likely to choose more meaningful detail or some combination thereof, while males tend towards pronounceable passwords or a random combination of characters.

The frequency of changing passwords was only significant for age groups. Older participants were likely to change their passwords more often than those who were younger. There was only a significant difference in whether the participant had forgotten their passwords for age group. It appears that the other participants, the more likely they are to forget their password.

Password Compostion				
Gender	**Groups**	**Count**	**Mean Rank**	**P-value**
	Male	346	430.54	0.014
	Female	470	393.10	NS
Age Groups	<28 Years	202	347.91	0.000
	28-32 Years	541	418.05	
	33-35 Years	48	515.03	
	>36 Years	26	524.91	
Employment	Full Time	63	413.23	0.004
	Part Time	499	378.03	
	Trainee	230	432.00	
Choice of Password				
Gender	**Groups**	**Count**	**Mean Rank**	**P-value**
	Male	346	438.36	0.014
	Female	470	386.52	
Age Groups	<28 Years	202	393.46	0.290 NS
	28-32 Years	541	412.32	
	33-35 Years	48	389.48	
	>36 Years	26	530.12	
Employment	Full Time	62	388.98	0.761 NS
	Part Time	497	399.82	
	Trainee	231	387.96	

Frequency of Changing Password				
Gender	**Groups**	**Count**	**Mean Rank**	**P-value**
	Male	347	412.77	0.593
	Female	469	405.34	NS
Age Groups	<28 Years	201	383.33	0.042
	28-32 Years	541	410.73	NS
	33-35 Years	49	470.46	
	>36 Years	26	402.91	
Employment	Full Time	62	433.20	0.204
	Part Time	497	388.80	NS
	Trainee	231	399.79	

Forgotten Password				
Gender	**Groups**	**Count**	**Mean Rank**	**P-value**
	Male	339	319.45	0.125
	Female	467	412.25	NS
Age Groups	<28 Years	200	374.41	0.002
	28-32 Years	534	404.00	
	33-35 Years	48	471.25	
	>36 Years	25	488.92	
Employment	Full Time	61	383.29	0.383
	Part Time	492	386.07	NS
	Trainee	229	405.63	

NS = Not Significant p>0.01

Table 2b: Results of Non-parametric Analyses of Number of Password

3. Discussion

From the above analysis it is very clear that email account are heavily used with approximately 30% of participants checks their mail several times a week and 50% who check one or more times a day. Many of the users used the exact same password or had passwords with slight variations. Another fact is that many users used the password of eight or more characters in length which makes the software a very long time to identify the password. But three quarter of the users use meaningful words or pronounceable words reduces its impact. This implies the passwords are easier guess, especially by those who are very close and knows the user personally (eg. Using name of a person, date-of-birth etc). A serious lack of concern with password security is that over three quarter of the participants, never changed their password or changed it no more than three times a year.

The participants were prepared to go to secure their passwords by selecting password length of 8 or more characters. The issue is that reuse of passwords. We can say that the participants (users) are either not sufficiently informed of the risks they are facing through poor password practices or they do not believe that they are at risk even though most are aware of one or more of the techniques used to break passwords.

It is also clear that age is a contributing factor to poor password practices. Younger participants are more likely to have simple passwords and they do not change their passwords as frequently as older participants. But they are also less likely to forget their password. Both males and females have poor practices. Females are more likely to have simple password that are meaningful, but they also are less likely to reuse them. On the other hand males have pronounceable words using combination of symbols and characters but are more likely to reuse them. From this we can conclude that both females and males have equally poor practices when it comes to password management.

Overall, participants appear to be unconcerned about the risks associated with poor password composition and management practices. Over 82% of the participants can be considered as experienced computer users since they had been using computers for six or more years. So we can say that there is a need for a better education process on password composition and management for users. The education or training should focus on the risks of not having appropriate password practices and the consequences for the failure to such practices.

4. Recommendations

Education or training should provide information regarding the password through online. But this will not achieve the purpose if the users do not use Internet frequently. Information can also be sent through circular but its success depends on the understanding capacity of the user. Information session or orientation program can be conducted, but again not all users would be able to or even willing to attend. A tutorial available on CD, DVD or online is another strategy that could be used to educate users. It can also be given as a screen saver. While user awareness increased, it is necessary to change the screen saver regularly, otherwise users become bored with the message. Vendors who supply relevant software such as operating system, firewalls and other security software's and email system could also build in tutorials or rule sets for constructing and maintenance of passwords. These components should be integral part of the software suite, should be active in the application and it should not be considered as an add-on. If a user creates a password by following the rule sets given by the software, some reward or appreciation should be given. If password is rejected, project the security risks in accepting that password, so that the user can change the password themselves.

5. Conclusion

The aim of this survey is to judge the attitudes and awareness of users to password security issues and to gain some insight into password composition reuse and management practice. This study has taken email because it is the universally used password-protected application. The results from this study provide important insight into ongoing issues relating to the creation and management of user-based password management system. Participants typically operate two or more email accounts as well as a host of other computer-based applications that require the use of passwords. As anticipated, this created password management difficulties for users and encouraged password reuse across different email accounts, and/or other computer based application. Moreover, users do not appear to fully realize the risks of their poor password practices, not are they aware of many of the consequences associated with breaches in security.

Our results show that the vast majority of users are choosing passwords that are based on meaningful personal details that can be easily guessed by others. Younger participants appear to have the worst practices in terms of password management and so are the most at risk. Any educational/training programs should highlight the risks of such poor practices in terms of younger people can relate to. Several options for providing education have been suggested including training program, online messages and through software vendors. Some combination of all would provide the broadest possible coverage in practicing and maintaining the password.

Further research can be built on this study's findings to determine the underlying reasons why younger people tend to have poorest password practices. Research can also be targeted towards full-time and part-time employees in order to examine whether it is organizational requirements that is driving their password practices. Knowledge gained from such research can then be used as a basis for sound educational programs that focus on improving personal password practices.

References

[1] Bishop. M & Kelin.D.V (1995) "Improving System Security via Proactive Password Checking" Computer Security, Vol 14 No.3, pp 233-249.

[2] Keith. M, Shao. B & Steinhardt. P.J(2006)."The Usability of Passphrases for Authentication: An Empirical Study", International Journal of Human-Computer Studies, forthcoming.

[3] Rhodes. K (2004) "Operating Security Awareness: The Mind Has No Firewall", Computer Society Journal, Vol 16 No 2, pp27-36.

[4] Rudy. I.A (1996) "A Critical Review on Research on Electronic Mail", European Journal of Information Systems, Vol 4, pp 198-213.

[5] Weber. R (1999) *Information Systems Control and Audit*, Prentice-Hall, Upper Saddle River, NJ.

[6] Furnell. S.M, Download, P.S. Illingworth, H.M & Reynolds. P.L(2000) "Authentication and Supervision: A Survey of User Attitudes", Computers & Security, Vol.19 No.6, pp 529-539.

D. Santhi Jeslet is a Faculty member in the Department of Computer Science at M.G.R. College , Hosur. She received her Master's Degrees from University of Madras, India in 1996. She received her M.Phil in Computer Science from Manonmaniam Sundaranar University, Tirunelveli in 2003.

G. Sivaraman is a Faculty member in the Department of Computer Science at M.G.R. College , Hosur. He received his Master's Degrees from Madurai Kamaraj University, India in 2000. He received his M.Phil in Computer Science from Bharathidasan, Tiruchi in 2004.

Dr. K. Thangadurai is a Faculty member in the Department of Computer Science at Government Arts College (Men), Krishnagiri. He received his dual Master's Degrees from the Bharathidasan University, India in 1996 and 1999 respectively. He received his M.Phil in Computer Science from M.S University, Tirunelveli in 2002 and received Ph.D in Computer Science in Vinayaka Mission's University, Salem, India in 2009. His research interests include Software Engineering, OOAD and cloud computing.

Dr. M. Punithavalli is a Faculty member and Director in the Department of Computer Applications in SRCW, Coimbatore, India. She received her Master's Degree from the Avinashilingam University, India in 1994. She received her M.Phil in Computer Science from Bharathiar University ,in 2000 and received Ph.D in Computer Science in Alagappa University, India in 2007. She has published papers in the following: International Journal of Computer Science, International Journal of Computer Science and Knowledge Engineering, International Journal of Data Mining and Knowledge Engineering, International Journal of Computer Science and System Analysis, Journal of Computer Science, Journal on Software Engineering etc.